STMicroelectronics

Cryptographic library NESLIB 6.11.3 on ST31R480 B01 Security Target for composition

Common Criteria for IT security evaluation

SMD_NL-ST31R480_ST_23_004 Rev 01.2

January 2025

life.augmented

BLANK

NesLib 6.11.3 on ST31R480 B01 Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: NesLib 6.11.3 on ST31R480 B01 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev 01.2, issued in January 2025.

3 Registration: registered at STMicroelectronics under number SMD_NL-ST31R480_ST_23_004.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the cryptographic library **NesLib 6.11.3 on ST31R480 B01.**

5 This TOE is a composite TOE, built up with the combination of:

- The Security IC **ST31R480 B01**, designed by STMicroelectronics, and used as certified platform,
- The cryptographic library **NesLib 6.11.3**, developed by STMicroelectronics, and built to operate with this Security IC platform.

6 Therefore, this Security Target is built on the Security IC Security Target Eurosmart - Security IC Platform Protection Profile with Augmentation Packages, referenced BSI-CC-PP-0084-2014.
The Security IC Security Target is called "Platform Security Target" in the following.

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

8 A glossary of terms and abbreviations used in this document is given in *Appendix A*.

Contents

List of tables

List of figures

1.3 Context

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

10 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL5 augmented by ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2.

11 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE, and to summarise its chosen TSF services and assurance measures.
Since the TOE is a composite TOE, this Security Target is built on the Security IC Security Target *ST31R480 B01 Security Target for composition*, referenced *SMD_ST31R480_ST_23_004*.

12 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 the Platform Security Target, some in compliance with *[JILSR]* and *ANSSI-PP0084.03*.

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

13 Extensions introduced in this ST to the SFRs of the Protection Profile (PP) are detailed in *Section 5*.

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

1.4 TOE identification

15 The Target of Evaluation (TOE) is the NesLib 6.11.3 on ST31R480 B01.

16 "NesLib 6.11.3 on ST31R480 B01" completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 17: Guidance documentation*, and its development and production sites indicated in *Table 18: Sites list*.
Refer also to the corresponding tables in the *ST31R480 B01 Security Target for composition*.

Table 1. TOE components

Platform identification					Library identification
IC Maskset name	**Master identification number**	**IC version**	**Firmware version**	**RngLib version**	**NesLib cryptographic library version**
K4H0A	0x0299	B	3.0.6	2.0.2	6.11.3

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 Datasheet, referenced in the *ST31R480 B01 Security Target for composition*.

18 The NesLib User Manual, referenced in *Table 17: Guidance documentation,* details how to check the library integrity and version.

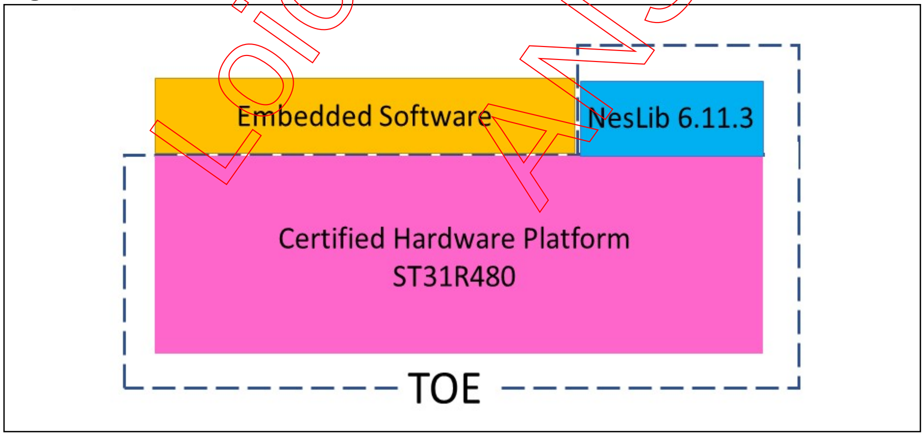
1.5 TOE overview

19 This TOE consists of a certified hardware platform and a secure cryptographic library, built on this platform.

20 The hardware platform is the ST31R480 with its firmware. It is identified as ST31R480 B01 which means it includes the components listed in the “Platform identification” columns in*Table 1: TOE components*, and detailed in the Security IC Security Target *ST31R480 B01 Security Target for composition*, referenced *SMD_ST31R480_ST_23_004*. This Platform Security Target also references the guidance documentation directly related to the hardware platform.

21 *Figure 1* provides an overview of the TOE.

Figure 1. TOE overview



22 The hardware platform is not fully described in the present Security Target, all useful information can be found in its dedicated Platform Security Target *[PF-ST]*. Nevertheless, the related assets, assumptions, threats, objectives and SFRs are reproduced in this document.

23 The secure cryptographic library NesLib 6.11.3 is a software library, with its own guidance documentation, listed in *Table 17: Guidance documentation*. It provides additional cryptographic functions that can be operated on the hardware platform.

24 This library is part of the Embedded Software (ES).
The rest of the ES is not part of the TOE.

25 The TOE doesn't need non-TOE hardware, software or firmware, but the developer of the Embedded Software will have to link the secure cryptographic library NesLib 6.11.3 into his applicative code, in order to exercise its functionality.

26 Note that the notion of various different roles and privileges does not exist inside NesLib. Only one role (the ES) is defined at the level of NesLib and there are no privileges, the ES having access to all the functions of the NesLib API.

1.6 TOE description

1.6.1 TOE hardware description

27 The ST31R480 B01 is described in the Platform Security Target *ST31R480 B01 Security Target for composition*.

28 Note that the usage of the hardware platform and associated firmware is not limited or constrained when the cryptographic library is embedded. The functions provided by the Security IC platform remain normally accessible to the ES.

1.6.2 TOE software description

29 The ST31R480 B01 firmware, included in the platform evaluation is described in the *ST31R480 B01 Security Target for composition*.

30 The cryptographic library NesLib is an applicative Embedded Software comprised in the ST31R480 User NVM.
NesLib is a cutting edge cryptographic library in terms of security and performance.

31 NesLib is embedded by the ES developer in his applicative code.

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

- a symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard cryptographic algorithm[a] (DES) and Triple DES *[3]*,
- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES) *[7]*,
- a cryptographic support module that provides hash functions (SHA-1[b], SHA-2 *[5]*), SHA-3, Keccak and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3 *[25]*,
- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[16]*), and Diffie-Hellman *[23]*,
- 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)

[a] Note that DES and triple DES with two keys are no longer recommended as encryption functions. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength.

with elliptic curves in short Weierstrass form *[14]*, and provides support for ECDH key agreement *[20]* and ECDSA generation and verification *[6]*,

- a module for supporting elliptic curve cryptography on Curve edwards25519, in particular Ed25519 signature generation, verification and point decompression *[26]*,
- a module for supporting elliptic curve cryptography on Curve edwards448, in particular Ed448 signature generation, verification and point decompression *[26]* *[6]*,
- a module for supporting elliptic curve cryptography on curve Curve25519, in particular X25519 for key agreement *[27]*,
- a module for supporting elliptic curve cryptography on curve Curve448, in particular X448 for key agreement *[27]*,
- a module for supporting the (post-quantum) stateful hash-based LMS signature scheme *[21]*,
- support for Deterministic Random Bit Generators (DRBG) *[18]*,
- prime number generation and RSA key pairs generation *[4]*.

33 NesLib also provides a set of basic functions to securely manipulate data:

- Copy,
- Compare,
- Swap,
- Shift,
- XOR.

1.6.3 TOE documentation

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

- the platform user guidance documentation listed in the *ST31R480 B01 Security Target for composition*,
- the NesLib User manual,
- the NesLib Security Recommendations,
- the NesLib release note.

35 The complete list and details of guidance documents is provided in *Table 17*, except those of the platform, listed in the *ST31R480 B01 Security Target for composition*.

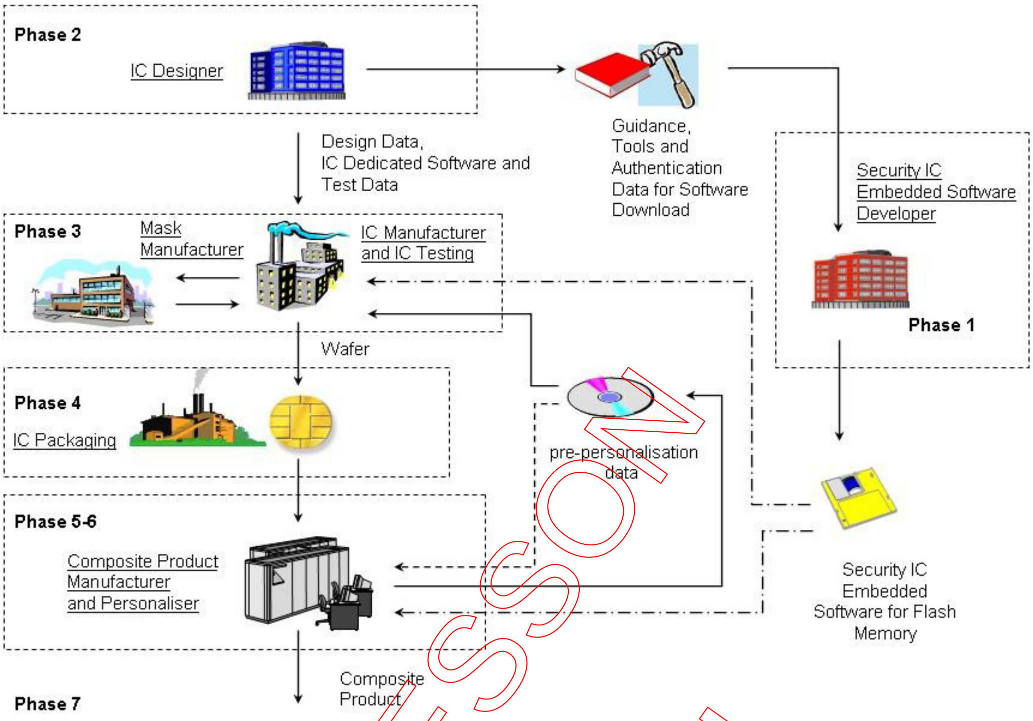
1.7 TOE life cycle

36 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.

37 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.

[b] Note that SHA-1 is no longer recommended as a cryptographic function. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

Figure 2. Security IC Life-Cycle



38 The life cycle phases are summarized in *Table 2*.

39 The security IC platform life cycle is described in the Platform Security Target, as well as its delivery format.

40 The development centres possibly involved in the development of the NesLib are denoted by the activity “ES-DEV” in *Table 18*.

41 The IT support centers potentially involved in the development of the NesLib are denoted by the activity "IT" in table “Sites list” in *Table 18*.

42 NesLib is delivered as part of Phase 1, as a software package, downloaded by ST entitled employees, from a controlled centralized system, then sent encrypted to the customer.

43 The sites potentially involved in the complete TOE life cycle are listed in *Table 18*, except those dedicated to the Security IC platform, already detailed in the Platform Security Target.

Table 2. 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

Table 2. Composite product life cycle phases (continued)

Phase	Name	Description
3	IC manufacturing and testing	integration and photomask fabrication IC manufacturing IC testing IC pre-personalisation
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary
5	Security IC product finishing process	composite product finishing process composite product testing
6	Security IC personalisation	composite product personalisation composite product testing
7	Security IC end usage	composite product usage by its issuers and consumers

1.7.1 TOE intended usage

44 The cryptographic library is intended to be used in support to the development of secure embedded software in phase 1, then embedded on the ST31R480.

45 In Phase 7, the TOE is in the end-user environments. Depending on the application, the 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.

46 The end-user environment therefore covers a wide range of very different functions. The TOE is designed to be used in unsecured and unprotected environments.

1.7.2 Delivery format and method

47 The Security IC platform can be delivered in form of wafers, micromodules or packages, as described in the *ST31R480 B01 Security Target for composition*.
All the possible forms of delivery are equivalent from a security point of view.

48 The cryptographic library is specifically delivered in form of a ciphered and signed binary file, so that the ES developer embeds it and links it to his applicative code.

49 All the guidance documents are delivered as ciphered pdf files.

2 Conformance claims (ASE_CCL, ASE_ECD)

2.1 Common Criteria conformance claims

50 The NesLib 6.11.3 on ST31R480 B01 Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

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

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

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

The reader can find their certified definitions in the text of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*".

53 This Security Target defines an additional extended Security Functional Requirement, FDP_SBO.1 “Secure basic operation on data”, described in *Section 5*.

54 The assurance level for the NesLib 6.11.3 on ST31R480 B01 Security Target is EAL5 augmented by ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2.

55 The ST31R480 B01 platform has been evaluated according to the evaluation level EAL6 augmented by ALC_FLR.2 and ASE_TSS.2, thus ensuring compatibility between the assurance levels chosen for the platform and the composite evaluations.

2.2 PP Claims

2.2.1 PP Reference

56 The NesLib 6.11.3 on ST31R480 B01 Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), as required by this Protection Profile.

57 The following packages have been selected from the *BSI-CC-PP-0084-2014*, and addressed by the Security IC platform:

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

2.2.2 PP Additions

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

- Those described in the *ST31R480 B01 Security Target for composition*,
- Addition #1: “Support of Cipher Schemes” from *[AUG]*.

59 This addition is used to address additional functionality provided by the TOE, and not covered by the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*, nor by the Platform Security Target *ST31R480 B01 Security Target for composition*. It addresses the additional functionality provided by the NesLib.

60 All refinements are indicated with type setting text ***as indicated here***, original text from the *BSI-CC-PP-0084-2014* being typeset as indicated here and ~~here~~. Text originating in *[AUG]* is typeset as indicated here. Text originating in *[JILSR]* is typeset as indicated here.

61 The security environment additions relative to the PP are summarized in *Table 3*.

62 The additional security objectives relative to the PP are summarized in *Table 4*.

63 The additional SFRs for the TOE relative to the PP are summarized in *Table 6*.

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

2.2.3 PP Claims rationale

65 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 6*. They have been introduced in the previous section.

66 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*.

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

68 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*.

69 Similarly, the security requirements rationale presented in *Section 6.4* has been updated with respect to the protection profile.

70 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)

71 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.

72 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security aspects defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security aspects have been introduced in the Platform Security Target and in this one.

73 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.

74 A summary of all these security aspects with their respective origin and status of inclusion in the *ST31R480 B01 Security Target for composition* is provided in *Table 3*.
All the security aspects defined in the *ST31R480 B01 Security Target for composition* are valid for the present Security Target.

75 Only the ones introduced in this Security Target, are detailed in the following sections (column "In *[PF-ST]* " = No).

Table 3. Summary of security aspects

	Label	Title	Origin	In *[PF-ST]*
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage	*[PP0084]*	Yes
	BSI.T.Phys-Probing	Physical Probing	*[PP0084]*	Yes
	BSI.T.Malfunction	Malfunction due to Environmental Stress	*[PP0084]*	Yes
	BSI.T.Phys-Manipulation	Physical Manipulation	*[PP0084]*	Yes
	BSI.T.Leak-Forced	Forced Information Leakage	*[PP0084]*	Yes
	BSI.T.Abuse-Func	Abuse of Functionality	*[PP0084]*	Yes
	BSI.T.RND	Deficiency of Random Numbers	*[PP0084]*	Yes
	BSI.T.Masquerade-TOE	Masquerade the TOE	*[PP0084]*	Yes
	AUG4.T.Mem-Access	Memory Access Violation	*[AUG]*	Yes
	JIL.T.Open-Samples-Diffusion	Diffusion of open samples	*[JILSR]*	Yes
	T.Confid-Applic-Code	Specific application code confidentiality	*[PF-ST]*	Yes
	T.Confid-Applic-Data	Specific application data confidentiality	*[PF-ST]*	Yes
	T.Integ-Applic-Code	Specific application code integrity	*[PF-ST]*	Yes
	T.Integ-Applic-Data	Specific application data integrity	*[PF-ST]*	Yes
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production	*[PP0084]*	Yes
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality	*[PP0084]*	Yes

Table 3. Summary of security aspects (continued)

	Label	Title	Origin	In *[PF-ST]*
	BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality	*[PP0084]*	Yes
	AUG1.P.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	AUG1.P.Add-Functions-Lib	Additional Specific Security Functionality	*[AUG]*	No
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation	*[PP0084]*	Yes
	BSI.A.Resp-Appl	Treatment of User Data	*[PP0084]*	Yes

3.1 Description of assets

76 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 the *ST31R480 B01 Security Target for composition*.

77 NesLib computes user data as well as TSF data, which are part of the assets addressed by the Platform Security Target and the Protection Profile.

3.2 Threats

78 The threats are all described in the Platform Security Target *[PF-ST]*, and just recalled here.

BSI.T.Leak-Inherent	Inherent Information Leakage
BSI.T.Phys-Probing	Physical Probing
BSI.T.Malfunction	Malfunction due to Environmental Stress
BSI.T.Phys-Manipulation	Physical Manipulation
BSI.T.Leak-Forced	Forced Information Leakage
BSI.T.Abuse-Func	Abuse of Functionality
BSI.T.RND	Deficiency of Random Numbers
BSI.T.Masquerade-TOE	Masquerade the TOE
AUG4.T.Mem-Access	Memory Access Violation
JIL.T.Open-Samples-Diffusion	Diffusion of open samples
T.Confid-Applic-Code	Specific application code confidentiality
T.Confid-Applic-Data	Specific application data confidentiality
T.Integ-Applic-Code	Specific application code integrity
T.Integ-Applic-Data	Specific application data integrity

3.3 Organisational security policies

79 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.

80 ***ST*** applies the Additional Specific Security Functionality policy (*AUG1.P.Add-Functions-Lib*) as specified below.
Complementary to the additional specific security functionality provided to the ES by the platform, NesLib provides the cryptographic functionality listed in *AUG1.P.Add-Functions-Lib*.
NesLib uses the platform hardware AES accelerator to provide AES security functionality, and the platform hardware triple DES accelerator to provide DES security functionality. NesLib also uses the platform Cryptography Accelerator (Nescrypt) to provide RSA, ECC and Diffie-Hellman functionalities.

BSI.P.Process-TOE	Identification during TOE Development and Production
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
BSI.P.Ctrl-Loader	Controlled usage to Loader Functionality
AUG1.P.Add-Functions	Additional Specific Security Functionality

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

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

- Triple Data Encryption Standard (DES),
- Advanced Encryption Standard (AES),
- ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),***
- ***Keccak,***
- ***Keccak-p,***
- ***Deterministic Random Bit Generator (DRBG),***
- Rivest-Shamir-Adleman (RSA)***,***
- ***Diffie-Hellman,***
- ***Elliptic Curves Cryptography on Weierstrass Curves, including ECDSA and ECDH,***
- ***Elliptic Curves Cryptography on Edwards Curves, consisting of Ed25519 and Ed448,***
- ***Elliptic Curves Cryptography on Montgomery Curves with X25519 and X448,***
- ***Stateful hash-based LMS signature,***
- ***Prime Number Generation,***
- ***Secure data copy,***
- ***Secure data compare,***
- ***Secure data swap,***
- ***Secure data shift,***
- ***Secure data XOR.***

Note that DES and triple DES with two keys are no longer recommended as encryption functions. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength.

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

3.4 Assumptions

81 The assumptions are all described in the Platform Security Target *[PF-ST]* and 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)

82 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 access control functionality,
- provide cryptographic support.

83 Since this Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), all the security objectives defined in the Protection Profile apply to the TOE.
In order to address complementary TOE security functionality not defined in the Protection Profile, some security objectives have been introduced in the Platform Security Target and in this one.

84 Note that the origin of each security objective 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.

85 A summary of all the TOE security objectives with their respective origin and status of inclusion in the *ST31R480 B01 Security Target for composition* is provided in *Table 4*.
All the security objectives defined in the *ST31R480 B01 Security Target for composition* are valid for the present Security Target.

86 Only the ones introduced in this Security Target, are detailed in the following sections.

Table 4. Summary of security objectives

	Label	Title	Origin	In *[PF-ST]*
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage	*[PP0084]*	Yes
	BSI.O.Phys-Probing	Protection against Physical Probing	*[PP0084]*	Yes
	BSI.O.Malfunction	Protection against Malfunctions	*[PP0084]*	Yes
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation	*[PP0084]*	Yes
	BSI.O.Leak-Forced	Protection against Forced Information Leakage	*[PP0084]*	Yes
	BSI.O.Abuse-Func	Protection against Abuse of Functionality	*[PP0084]*	Yes
	BSI.O.Identification	TOE Identification	*[PP0084]*	Yes
	BSI.O.RND	Random Numbers	*[PP0084]*	Yes
	BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader	*[PP0084]*	Yes
	BSI.O.Ctrl-Auth-Loader	Access control and authenticity for the Loader	*[PP0084]*	Yes

Table 4. Summary of security objectives (continued)

	Label	Title	Origin	In *[PF-ST]*
TOE	JIL.O.Prot-TSF-Confidentiality	Protection of the confidentiality of the TSF	*[JILSR]*	Yes
	JIL.O.Secure-Load-ACode	Secure loading of the Additional Code	*[JILSR]*	Yes
	JIL.O.Secure-AC-Activation	Secure activation of the Additional Code	*[JILSR]*	Yes
	JIL.O.TOE-Identification	Secure identification of the TOE	*[JILSR]*	Yes
	O.Secure-Load-AMemImage	Secure loading of the Additional Memory Image	*[PF-ST]*	Yes
	O.MemImage-Identification	Secure identification of the Memory Image	*[PF-ST]*	Yes
	BSI.O.Authentication	Authentication to external entities	*[PP0084]*	Yes
	AUG4.O.Mem-Access	Area based Memory Access Control	*[AUG]*	Yes
	O.Firewall	Specific application firewall	*[PF-ST]*	Yes
	AUG1.O.Add-Functions	Additional Specific Security Functionality	*[AUG]*	Yes
	AUG1.O.Add-Functions-Lib	Additional Specific Security Functionality	*[AUG]*	No
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE	*[PP0084]*	Yes
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	*[PP0084]*	Yes
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	*[PP0084]*	Yes
	BSI.OE.Loader-Usage	Secure communication and usage of the Loader	*[PP0084]*	Yes
	BSI.OE.TOE-Auth	External entities authenticating of the TOE	*[PP0084]*	Yes
	OE.Composite-TOE-Id	Composite TOE identification	*[PF-ST]*	Yes
	OE.TOE-Id	TOE identification	*[PF-ST]*	Yes
	OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	*[PF-ST]*	Yes
	OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	*[PF-ST]*	Yes

4.1 Security objectives for the TOE

BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
BSI.O.Phys-Probing	Protection against Physical Probing
BSI.O.Malfunction	Protection against Malfunctions

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

AUG1.O.Add-Functions-Lib Additional Specific Security Functionality:

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

– Triple Data Encryption Standard (DES),

– Advanced Encryption Standard (AES),

– Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),

– Keccak,

– Keccak-p,

– Deterministic Random Bit Generator (DRBG),

– Rivest-Shamir-Adleman (RSA)***,***

– Diffie-Hellman,

– Elliptic Curves Cryptography on Weierstrass Curves, including ECDSA and ECDH,

– Elliptic Curves Cryptography on Edwards Curves, consisting of Ed25519 and Ed448,

– Elliptic Curves Cryptography on Montgomery Curves with X25519 and X448,

– Stateful hash-based LMS signature,

– Prime Number Generation,

– Secure data copy,

– Secure data compare,

– Secure data swap,

– Secure data shift,

– Secure data XOR.

Note that DES and triple DES with two keys are no longer recommended as encryption functions. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength.

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

4.2 Security objectives for the environment

87 All security objectives for the environment are detailed in the *ST31R480 B01 Security Target for composition* and still valid in the same terms for this Security Target. The clarifications made there also apply.

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

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

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

BSI.OE.Process-Sec-IC	Protection during composite product manufacturing	Up to phase 6
BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader	Up to phase 6
BSI.OE.Loader-Usage	Secure communication and usage of the Loader	Up to phase 7
BSI.OE.TOE-Auth	External entities authenticating of the TOE	Up to phase 7
OE.Composite-TOE-Id	Composite TOE identification	Up to phase 7
OE.TOE-Id	TOE identification	Up to phase 7
OE.Enable-Disable-Secure-Diag	Enabling or disabling the Secure Diagnostic	Up to phase 7
OE.Secure-Diag-Usage	Secure communication and usage of the Secure Diagnostic	Up to phase 7

4.3 Security objectives rationale

90 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]*, those already introduced in the *ST31R480 B01 Security Target for composition* 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.

91 All security objectives are already justified in the Platform Security Target *[PF-ST]*, except the one denoted by “New” in *Table 5*.

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

- organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions-Lib*)"

93 Only this security policy and its associated objective will be detailed in the following.
No threat nor assumption have been added versus the Platform Security Target *[PF-ST]*.

94 The justification of this additional policy provided in the next subsection shows that it does not contradict to the rationale already given in the protection profile *BSI-CC-PP-0084-2014* and in the *ST31R480 B01 Security Target for composition* for the assumptions, policy and threats defined there.

Table 5. 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

Table 5. 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
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	
BSI.P.Ctrl-Loader	*BSI.O.Ctrl-Auth-Loader* *JIL.O.Secure-Load-ACode* *JIL.O.Secure-AC-Activation* *JIL.O.TOE-Identification* *O.Secure-Load-AMemImage* *O.MemImage-Identification* *BSI.OE.Loader-Usage* *OE.TOE-Id* *OE.Composite-TOE-Id*	
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
AUG1.P.Add-Functions-Lib	*AUG1.O.Add-Functions-Lib*	New
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* *OE.Enable-Disable-Secure-Diag* *OE.Secure-Diag-Usage*	
BSI.T.RND	*BSI.O.RND*	
BSI.T.Masquerade-TOE	*BSI.O.Authentication* *BSI.OE.TOE-Auth*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
JIL.T.Open-Samples-Diffusion	*JIL.O.Prot-TSF-Confidentiality* *BSI.O.Leak-Inherent* *BSI.O.Leak-Forced*	
T.Confid-Applic-Code	*O.Firewall*	
T.Confid-Applic-Data	*O.Firewall*	
T.Integ-Applic-Code	*O.Firewall*	
T.Integ-Applic-Data	*O.Firewall*	

4.3.1 Organisational security policy "Additional Specific Security Functionality"

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

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

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

5 Extended Components Definition (ASE_ECD)

98 The extended components included in this Security Target are mainly taken from the *BSI-CC-PP-0084-2014* Protection Profile, and defined there.

99 There is only one extended component specific to this Security Target.
The additional family FDP_SBO of the class FDP: User data protection, is defined in *Section 5.1*. This family describes the security functional requirements for secure basic operation on data.

100 The FDP class, defined in CC Part 2 (*CCMB-2017-04-002 R5*), specifies requirements related to protecting user data within a TOE. The additional family “Secure basic operation on data” (FDP_SBO) of the class FDP addresses protection of user data when it is manipulated thanks to basic functions.

5.1 Secure basic operation on data (FDP_SBO)

Family behaviour

101 This family defines requirements for the TOE to provide secure basic operations on data.

Component levelling

FDP_SBO Secure basic operation on data	----------------------------	1

FDP_SBO.1 Requires the TOE to provide secure basic operations on data.

Management: FDP_SBO.1
There are no management activities foreseen.

Audit: FDP_SBO.1
There are no actions defined to be auditable.

FDP_SBO.1 Secure basic operation on data

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SBO.1.1 The TSF shall provide a [selection: *Copy, Compare, [assignment: other operation]*] function on data [selection: *from [assignment: memory area] to [assignment: memory area]*, *stored in [assignment: memory area]*].

6 Security requirements (ASE_REQ)

102 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE (*Section 6.1*), a section on security assurance requirements (SARs) for the TOE (*Section 6.2*), a section on the refinements of these SARs (*Section 6.3*) as required by the "*BSI-CC-PP-0084-2014*" Protection Profile. This chapter includes a section with the security requirements rationale (*Section 6.4*).

6.1 Security functional requirements for the TOE

103 The selected security functional requirements (SFRs) for this TOE (NesLib 6.11.3 on ST31R480 B01) are summarized in *Table 6*.
This table also specifies:

- Their type i.e. drawn from *CCMB-2017-04-002 R5* or extended,
- Their origin i.e. defined in the *BSI-CC-PP-0084-2014* Protection Profile, in *[AUG]*, or in the Platform Security Target *[PF-ST]*. All SFRs are inherited from *[PF-ST]*, except those identified by “This ST”.

104 Most of the extended SFRs are defined in the "*BSI-CC-PP-0084-2014*" Protection Profile. The new extended SFR FDP_SBO.1, defined in this Security Target is detailed in *Section 5.1*.

105 Except FDP_SBO.1, all extensions to the SFRs of the "*BSI-CC-PP-0084-2014*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2017-04-002 R5*.

106 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.

Table 6. 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 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality	*BSI-CC-PP-0084-2014*	Extended
FMT_LIM.2 / Test	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-CC-PP-0084-2014* Operated	
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing		*CCMB-2017-04-002 R5*
FDP_SDI.2	Stored data integrity monitoring and action			
FPT_PHP.3	Resistance to physical attack		*BSI-CC-PP-0084-2014*	
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1 /PTG.2	Random number generation - PTG.2	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	Extended
FCS_RNG.1 / PG	Random number generation			
FCS_RNG.1 / RngLib	Random number generation			
FDP_SBO.1 / Copy	Secure basic operation on data - Copy	Data manipulation support	This ST	
FDP_SBO.1 / Compare	Secure basic operation on data - Compare			
FDP_SBO.1 / Swap	Secure basic operation on data - Swap			
FDP_SBO.1 / Shift	Secure basic operation on data - Shift			
FDP_SBO.1 / XOR	Secure basic operation on data - XOR			

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FCS_COP.1 / TDES	Cryptographic operation - TDES	Cipher scheme support	[AUG] #1 Operated / [PF-ST]	CCMB-2017-04-002 R5
FCS_COP.1 / AES	Cryptographic operation - AES			
FCS_COP.1 / SW-DES	Cryptographic operation - DES & Triple DES		[AUG] #1 Operated / This ST	
FCS_COP.1 / SW-AES	Cryptographic operation - AES			
FCS_COP.1 / RSA	Cryptographic operation - RSA			

Table 6. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FCS_COP.1 / ECC-WC	Cryptographic operation - ECC-WC	Cipher scheme support	[AUG] #1 Operated / This ST	CCMB-2017-04-002 R5
FCS_COP.1 / ECC-EC	Cryptographic operation - ECC-EC			
FCS_COP.1 / ECC-MC	Cryptographic operation - ECC-MC			
FCS_COP.1 / SHA	Cryptographic operation - SHA			
FCS_COP.1 / Keccak	Cryptographic operation - Keccak			
FCS_COP.1 / Keccak-p	Cryptographic operation - Keccak-p			
FCS_COP.1 / Diffie-Hellman	Cryptographic operation - Diffie-Hellman			
FCS_COP.1 / SFH-DSA	Cryptographic operation - SFH-DSA			
FCS_COP.1 / DRBG	Cryptographic operation - DRBG			
FCS_CKM.1 / Prime-generation	Cryptographic key generation - Prime generation		This ST	
FCS_CKM.1 / RSA-key-generation	Cryptographic key generation - RSA key generation			
FDP_ACC.2 / Memories	Complete access control	Memory access violation	[PF-ST]	
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		[PF-ST]	
FIA_API.1	Authentication Proof of Identity	Masquerade	BSI-CC-PP-0084-2014 Operated	Extended
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality		
FMT_LIM.2 / Loader	Limited availability			

Table 6. Summary of functional security requirements for the TOE (continued)

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

Table 6. Summary of functional security requirements for the TOE (continued)

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

107 All these SFRs have already been stated in the *ST31R480 B01 Security Target for composition*, and are satisfied by the *ST31R480* platform, except the following ones, dedicated to the NesLib:

- *FDP_SBO.1 / Copy*, *FDP_SBO.1 / Compare*, *FDP_SBO.1 / Swap*, *FDP_SBO.1 / Shift*, *FDP_SBO.1 / XOR*
- *FCS_COP.1 / SW-DES*, *FCS_COP.1 / SW-AES*, *FCS_COP.1 / RSA*, *FCS_COP.1 / ECC-WC*, *FCS_COP.1 / ECC-EC*, *FCS_COP.1 / ECC-MC*, *FCS_COP.1 / SHA*, *FCS_COP.1 / Keccak*, *FCS_COP.1 / Keccak-p*, *FCS_COP.1 / Diffie-Hellman*, *FCS_COP.1 / SFH-DSA*, *FCS_COP.1 / DRBG*,
- *FCS_CKM.1 / Prime-generation*, *FCS_CKM.1 / RSA-key-generation*.

108 The SFRs from the Platform Security Target are detailed in the *ST31R480 B01 Security Target for composition [PF-ST]*.

6.1.1 Security Functional Requirements for the secure data manipulation services

Secure basic operation on data (FDP_SBO.1) / Copy

109 The TSF shall provide a ***Copy*** function on data ***from ROM, RAM or NVM to RAM***.

Secure basic operation on data (FDP_SBO.1) / Compare

110 The TSF shall provide a ***Compare*** function on data ***stored in ROM, RAM or NVM***.

Secure basic operation on data (FDP_SBO.1) / Swap

111 The TSF shall provide a ***Swap*** function on data ***stored in RAM***.

Secure basic operation on data (FDP_SBO.1) / Shift

112 The TSF shall provide a ***Shift*** function on data ***stored in RAM***.

Secure basic operation on data (FDP_SBO.1) / XOR

113 The TSF shall provide a ***XOR*** function on data ***from ROM, RAM or NVM to RAM***.

6.1.2 Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

114 The TSF shall perform ***the operations in*** *Table 7* in accordance with a specified cryptographic algorithm ***in*** *Table 7* and cryptographic key sizes ***of*** *Table 7* that meet the ***standards in*** *Table 7****.***

Table 7. FCS_COP.1 iterations (cryptographic operations)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
SW-DES	* encryption and decryption with single-key DES, 2-key or 3-key Triple DES in Cipher Block Chaining (CBC) mode, * single-key DES, 2-key and 3-key Triple DES block ciphers and their inverses as a toolbox to implement other modes: - encryption modes (ECB, CFB, OFB, CTR), - authentication modes, - authenticated encryption, - key derivation modes	Data Encryption Standard (DES) and Triple DES[(1)]	56 bits (DES), 112 (Triple DES 2 keys), 168 (Triple DES 3 keys)	*NIST SP 800-67* *NIST SP 800-38A*
SW-AES	* AES encryption (cipher) and decryption (inverse cipher) in Cipher Block Chaining (CBC) mode * Message authentication Code computation (CMAC) * Authenticated encryption/decryption in Galois Counter Mode (GCM) * Authenticated encryption/decryption in Counter with CBC-MAC (CCM) * AES block ciphers and their inverses as a toolbox to implement other modes: - encryption modes (ECB, CFB, OFB, CTR), - authentication modes, - authenticated encryption, - key derivation modes	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS 197* *NIST SP 800-38B* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38C*

Table 7. FCS_COP.1 iterations (cryptographic operations) (continued)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
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*
ECC-WC	* private scalar multiplication * prepare Jacobian * public scalar multiplication * joint 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 186-5* *ANSI X9.62, section 7*
ECC-EC	* Ed25519 generation * Ed25519 verification * Ed25519 point decompression * Ed25519 scalar multiplication * Ed448 generation * Ed448 verification * Ed448 point decompression * Ed448 scalar multiplication	Elliptic Curves Cryptography on GF(p) on Curves in Edwards form, with Curves Ed25519 and Ed448	256 bits 448 bits	*RFC 8032*
ECC-MC	* X25519 for key agreement * X448 for key agreement	Elliptic Curves Cryptography on GF(p) on Curves in Montgomery form, with Curves Curve25519 and Curve448	256 bits 448 bits	*RFC 7748*

Table 7. FCS_COP.1 iterations (cryptographic operations) (continued)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
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 180-4*
	* HMAC using any of the above protected hash functions		up to 1024 bits	*FIPS 198-1*
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 (SHA-3)	no key for plain functions, variable key length up to security level for protected functions (security level is last number in function names and c/2=(1600-r)/2 for Keccak)	*FIPS 202*
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 202*
Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	up to 4096 bits	*ANSI X9.42*

Table 7. FCS_COP.1 iterations (cryptographic operations) (continued)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
SFH-DSA	LMS signature verification	Leighton-Micali stateful hash-based digital signature algorithm	the security strength is set with the LMS parameters: LMOTS_SHA256_N32_W4 and LMS_SHA256_M32_H10	*NIST SP 800-208*
DRBG	* SHA-1[2] * SHA-224 * SHA-256 * SHA-384 * SHA-512	Hash-DRBG	None	*NIST SP 800-90A* *FIPS 180-4*
	*AES	CTR-DRBG	128, 192 and 256 bits	*NIST SP 800-90A* *FIPS 197*

1. Note that DES and triple DES with two keys are no longer recommended as encryption functions. 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. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.

Cryptographic key generation (FCS_CKM.1)

115 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm***, in*** *Table 8***,*** and specified cryptographic key sizes ***of*** *Table 8* that meet the following ***standards in*** *Table 8****.***

Table 8. 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 140-3* *FIPS 186-5*
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 140-3* *ISO/IEC 9796-2* *PKCS #1 V2.1*

6.2 TOE security assurance requirements

116 Security Assurance Requirements for the TOE for the evaluation of the TOE are those taken from the Evaluation Assurance Level ***5*** (EAL5) and augmented by taking the following components:

- ALC_DVS.2,
- AVA_VAN.5,
- ***ALC_FLR.2.***

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

118 As stated at section 6.3.3 of *BSI-CC-PP-0084-2014*, the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE since it is intended to defend against sophisticated attacks.

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

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

Table 9. **TOE security assurance requirements**

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
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.4	Production support, acceptance procedures and automation	EAL5/*BSI-CC-PP-0084-2014*
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.2	Flaw reporting procedures	Security Target
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	EAL5/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL5/*BSI-CC-PP-0084-2014*

Table 9. TOE security assurance requirements (continued)

Label	Title	Origin
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.1	TOE summary specification	EAL5/*BSI-CC-PP-0084-2014*
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*

6.3 Refinement of the security assurance requirements

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

122 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.

123 An impact summary is provided in *Table 10*.

Table 10. Impact of EAL5 selection on ***BSI-CC-PP-0084-2014*** refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	4	None
ADV_ARC	1	1	None
ADV_FSP	4	5	None, presentation style changes
ADV_IMP	1	1	None
ATE_COV	2	2	None
AGD_OPE	1	1	None
AVA_VAN	5	5	None

6.4 Security Requirements rationale

6.4.1 Rationale for the Security Functional Requirements

124 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 introduced in the Platform Security Target *[PF-ST]*, and 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 11. Security Requirements versus Security Objectives

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

Table 11. Security Requirements versus Security Objectives

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

Table 11. Security Requirements versus Security Objectives

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

Table 11. Security Requirements versus Security Objectives

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

Table 11. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
AUG1.O.ADD-FUNCTIONS-LIB	"*Cryptographic operation - DES & Triple DES*" *FCS_COP.1 / SW-DES* "*Cryptographic operation -AES*" *FCS_COP.1 / SW-AES* "*Cryptographic operation - RSA*" *FCS_COP.1 / RSA* "*Cryptographic operation - ECC-WC*" *FCS_COP.1 / ECC-WC* "*Cryptographic operation - ECC-EC*" *FCS_COP.1 / ECC-EC* "*Cryptographic operation - ECC-MC*" *FCS_COP.1 / ECC-MC* "*Cryptographic operation - SHA*" *FCS_COP.1 / SHA* "*Cryptographic operation - Keccak*" *FCS_COP.1 / Keccak* "*Cryptographic operation - Keccak-p*" *FCS_COP.1 / Keccak-p* "*Cryptographic operation - Diffie-Hellman*" *FCS_COP.1 / Diffie-Hellman* "*Cryptographic operation - SFH-DSA*" *FCS_COP.1 / SFH-DSA* "*Cryptographic operation - DRBG*" *FCS_COP.1 / DRBG* "*Cryptographic key generation - Prime generation*" *FCS_CKM.1 / Prime-generation* "*Cryptographic key generation - RSA key generation*" *FCS_CKM.1 / RSA-key-generation* "*Secure basic operation on data - Copy*" *FDP_SBO.1 / Copy* "*Secure basic operation on data - Compare*" *FDP_SBO.1 / Compare* "*Secure basic operation on data - Swap*" *FDP_SBO.1 / Swap* "*Secure basic operation on data - Shift*" *FDP_SBO.1 / Shift* "*Secure basic operation on data - XOR*" *FDP_SBO.1 / XOR*
AUG4.O.MEM-ACCESS	"*Complete access control*" *FDP_ACC.2 / Memories* "*Security attribute based access control*" *FDP_ACF.1 / Memories* "*Static attribute initialisation*" *FMT_MSA.3 / Memories* "*Management of security attribute*" *FMT_MSA.1 / Memories* "*Specification of management functions*" *FMT_SMF.1 / Memories*
O.Firewall	"*Complete access control*" *FDP_ACC.2 / Memories* "*Security attribute based access control*" *FDP_ACF.1 / Memories* "*Static attribute initialisation*" *FMT_MSA.3 / Memories* "*Management of security attribute*" *FMT_MSA.1 / Memories* "*Specification of management functions*" *FMT_SMF.1 / Memories*

125 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 6* and *Table 11*, 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.

126 All justifications for Security Objectives and SFRs have been already provided in the Platform Security Target *[PF-ST]*, except for *AUG1.O.Add-Functions-Lib* and its associated SFRs.

127 This rationale must show that security requirements suitably address this objective.

128 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* and in *[PF-ST]*, they form an internally consistent whole, is provided in the next subsections.

6.4.2 Additional security objectives are suitably addressed

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

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

130 The security functional requirements “Cryptographic operation (FCS_COP.1)” (*FCS_COP.1 / SW-DES*, *FCS_COP.1 / SW-AES*, *FCS_COP.1 / RSA*, *FCS_COP.1 / ECC-WC*, *FCS_COP.1 / ECC-EC*, *FCS_COP.1 / ECC-MC*, *FCS_COP.1 / SHA*, *FCS_COP.1 / Keccak*, *FCS_COP.1 / Keccak-p*, *FCS_COP.1 / Diffie-Hellman*, *FCS_COP.1 / SFH-DSA*, *FCS_COP.1 / DRBG*), "Cryptographic key generation (FCS_CKM.1)" (*FCS_CKM.1 / Prime-generation*, *FCS_CKM.1 / RSA-key-generation*) ***and*** "Secure basic operation on data (FDP_SBO.1)" (*FDP_SBO.1 / Copy*, *FDP_SBO.1 / Compare*, *FDP_SBO.1 / Swap*, *FDP_SBO.1 / Shift*, *FDP_SBO.1 / XOR*) exactly require those functions to be implemented that are demanded by *AUG1.O.Add-Functions-Lib*. Therefore, all these SFRs ***are*** suitable to meet the security objective.

6.4.3 Additional security requirements are consistent

"Cryptographic operation (FCS_COP.1)” (*FCS_COP.1 / SW-DES*, *FCS_COP.1 / SW-AES*, *FCS_COP.1 / RSA*, *FCS_COP.1 / ECC-WC*, *FCS_COP.1 / ECC-EC*, *FCS_COP.1 / ECC-MC*, *FCS_COP.1 / SHA*, *FCS_COP.1 / Keccak*, *FCS_COP.1 / Keccak-p*, *FCS_COP.1 / Diffie-Hellman*, *FCS_COP.1 / SFH-DSA*, *FCS_COP.1 / DRBG*)

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

"Cryptographic key generation (FCS_CKM.1)” (*FCS_CKM.1 / Prime-generation*, *FCS_CKM.1 / RSA-key-generation*)

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

"Secure basic operation on data (FDP_SBO.1)” (*FDP_SBO.1 / Copy*, *FDP_SBO.1 / Compare*, *FDP_SBO.1 / Swap*, *FDP_SBO.1 / Shift*, *FDP_SBO.1 / XOR*)

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

6.4.4 Dependencies of Security Functional Requirements

134 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 justified in the *ST31R480 B01 Security Target for composition [PF-ST]* security requirements rationale,
- those justified in *[AUG]* security requirements rationale,
- the dependency of FCS_COP.1 and FCS_CKM.1 on FCS_CKM.4 (see discussion below).

135 Details are provided in *Table 12* below.

136 Note that in order to avoid repetitions of the SFRs iterated in this Security Target, and improve readability, some are mentioned in a generic form in this table.

Table 12. Dependencies of security functional requirements

Label	**Dependencies**	**Fulfilled by security requirements in this Security Target**	**Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]***
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-CC-PP-0084-2014*
FPT_FLS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Test	FMT_LIM.2 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Test	FMT_LIM.1 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Loader	FMT_LIM.2 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Loader	FMT_LIM.1 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Sdiag	FMT_LIM.2 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Sdiag	FMT_LIM.1 / Sdiag	Yes	Yes, *BSI-CC-PP-0084-2014*
FAU_SAS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDC.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDI.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FPT_PHP.3	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes, by FDP_ACC.2 / Memories and FDP_IFC.1	Yes, *BSI-CC-PP-0084-2014*
FPT_ITT.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-CC-PP-0084-2014*	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PTG.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1 / PG	None	No dependency	Yes, *BSI-CC-PP-0084-2014*

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FCS_RNG.1 / RngLib	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SBO.1	None	No dependency	No
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by 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.1 / Memories	FDP_ACF.1 / Memories	Yes	Yes, *[PF-ST]*
FDP_ACF.1 / Memories	FDP_ACC.1 / Memories	Yes, by FDP_ACC.1 / Memories	Yes, *[PF-ST]*
	FMT_MSA.3 / Memories	Yes	
FMT_MSA.3 / Memories	FMT_MSA.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No, see *[AUG]* ***#4***	
FMT_MSA.1 / Memories	[FDP_ACC.1 / Memories or FDP_IFC.1]	Yes, by FDP_ACC.1 / Memories and FDP_IFC.1	Yes, *[PF-ST]*
	FMT_SMF.1 / Memories	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Memories	No	Yes, *[PF-ST]*
FMT_SMF.1 / Memories	None	No dependency	Yes, *[PF-ST]*
FIA_API.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FTP_ITC.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_UCT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014*, in *[PF-ST]* or in *[AUG]*
FDP_UIT.1 / Loader	[FTP_ITC.1 / Loader or FTP_TRP.1 / Loader]	Yes, by FTP_ITC.1 / Loader	Yes, *BSI-CC-PP-0084-2014*
	[FDP_ACC.1 / Loader or FDP_IFC.1 / Loader]	Yes, by FDP_ACC.1 / Loader	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	Yes, *[PF-ST]*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	Yes, *[PF-ST]*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FIA_UID.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FIA_UAU.1 / Loader	FIA_UID.1 / Loader	Yes	Yes, *[PF-ST]*
FDP_SMF.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FPT_FLS.1 / Loader	None	No dependency	Yes, *[PF-ST]*
FAU_SAS.1 / Loader	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FAU_SAR.1 / Loader	FAU_GEN.1	No, by FAU_SAS.1 / Loader instead, see discussion below	Yes, *[PF-ST]*
FTP_ITC.1 / Sdiag	None	No dependency	Yes, *[PF-ST]*
FAU_SAR.1 / Sdiag	FAU_GEN.1	No, see discussion below	Yes, *[PF-ST]*

137 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, "Cryptographic key generation (FCS_CKM.1)" 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.

138 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.

6.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5

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

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

141 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. The requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

142 Note that detailed and updated refinements for assurance requirements are given in *Section 6.3*.

Dependencies of assurance requirements

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

144 The augmentation to this package identified in *Section 6.2* does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_FLR.2 has no dependency.

7 TOE summary specification (ASE_TSS)

145 This section demonstrates how the TOE meets each Security Functional Requirement, and includes a statement of compatibility vs. the Platform Security Target *[PF-ST]*.

7.1 TOE Security Functional Requirements realisation

146 This section argues how the TOE meets each SFR.

147 The TOE is evaluated as a composite TOE, made of the underlying hardware platform and the NesLib cryptographic library on top of it.

148 Consequently, the *ST31R480 B01 Security Target for composition* details how all the platform SFRs are met, and in the following only the SFRs related to NesLib are addressed.

7.1.1 Secure basic operation on data: Copy (FDP_SBO.1) / Copy

149 The NesLib library provides to the ES developer secure copy functions from ROM, RAM or NVM memories to the RAM:

- copy from a source memory buffer to a target buffer, protected against faults,
- copy from a source memory buffer to a target buffer, protected against faults and side channel attacks.

7.1.2 Secure basic operation on data: Compare (FDP_SBO.1) / Compare

150 The NesLib library provides to the ES developer secure compare functions, protected against faults and side channel attacks, in ROM, RAM or NVM memories:

- compare a memory buffer to a constant,
- compare two memory buffers.

7.1.3 Secure basic operation on data: Swap (FDP_SBO.1) / Swap

151 The NesLib library provides to the ES developer a secure swap function, protected against faults and side channel attacks:

- swap content of 2 buffers in RAM.

7.1.4 Secure basic operation on data: Shift (FDP_SBO.1) / Shift

152 The NesLib library provides to the ES developer a secure shift function from ROM, RAM or NVM memories to the RAM, protected against faults and side channel attacks:

- shift right or left content of a memory buffer.

7.1.5 Secure basic operation on data: XOR (FDP_SBO.1) / XOR

153 The NesLib library provides to the ES developer a secure XOR function from ROM, RAM or NVM memories to the RAM, protected against faults and side channel attacks:

- make a XOR from a source memory buffer to a target buffer.

7.1.6 Cryptographic operation: DES and Triple DES operation (FCS_COP.1) / SW-DES

154 The cryptographic library NesLib provides to the ES developer the following DES functions, conformant to *NIST SP 800-67* and *NIST SP 800-38A* with intrinsic counter-measures against attacks:

- encryption and decryption with single-key DES, 2-key or 3-key Triple DES encryption in Cipher Block Chaining (CBC) mode,
- the single-key DES, 2-key or 3-key Triple DES block ciphers and their inverses as a toolbox suitable for the ES to implement other modes such as encryption modes (e.g. ECB, CFB, OFB, CTR), authentication modes, authenticated encryption and key derivation modes.

155 For all these functions, NesLib uses the EDES+ accelerator certified in the Hardware Platform.

156 Note that DES and triple DES with two keys are no longer recommended as encryption functions. Hence, Security IC Embedded Software may need to use triple DES with three keys to achieve a suitable strength.

7.1.7 Cryptographic operation: AES operation (FCS_COP.1) / SW-AES

The cryptographic library NesLib provides to the ES developer the following AES functions for key sizes of 128, 192 and 256 bits, conformant to *FIPS 197, NIST SP 800-38A*, *NIST SP 800-38B*, *NIST SP 800-38C,* and *NIST SP 800-38D* with intrinsic counter-measures against attacks:

- encryption and decryption with AES in Cipher Block Chaining (CBC) mode,
- authentication with AES in CMAC mode,
- authenticated encryption with AES in Galois Counter Mode (GCM) and its associated verification and decryption mechanism,
- authenticated encryption with AES in Counter with CBC-MAC Mode (CCM) and its associated verification and decryption mechanism,
- the AES-128, AES-192, AES-256 block ciphers and their inverses as a toolbox suitable for the ES to implement other modes such as encryption modes (e.g. ECB, CFB, OFB, CTR), authentication modes, authenticated encryption and key derivation modes.

157 For all these functions, NesLib uses the AES accelerator certified in the Hardware Platform.

7.1.8 Cryptographic operation: RSA operation (FCS_COP.1) / RSA

158 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.

159 For these functions, NesLib uses the Cryptography Accelerator (Nescrypt) of the Hardware Platform.

7.1.9 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC-WC

160 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,
- joint public scalar multiplication,
- point validity check,
- Jacobian conversion to affine coordinates,
- general point addition,
- point expansion and compression.

161 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 186-5* and specified in *ANSI X9.62*, section 7.

162 For these functions, NesLib uses the Cryptography Accelerator (Nescrypt) of the Hardware Platform.

7.1.10 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC-EC

163 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 Ed25519 and Ed448, all conformant to *RFC 8032*, including:

- generation (with ephemeral key in vanilla, context or prehash flavour),
- verification,
- point decompression,
- scalar multiplication.

164 For these functions, NesLib uses the Cryptography Accelerator (Nescrypt) of the Hardware Platform.

7.1.11 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC-MC

165 The cryptographic library NesLib provides to the ES developer functions implementing:

- the X25519 primitive as specified by *RFC 7748*, for key agreement using curve Curve25519,
- the X448 primitive as specified by *RFC 7748*, for key agreement using curve Curve448.

166 For these functions, NesLib uses the Cryptography Accelerator (Nescrypt) of the Hardware Platform.

7.1.12 Cryptographic operation: SHA-1 & SHA-2 operation (FCS_COP.1) / SHA

167 The cryptographic library NesLib provides the SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS 180-4*.

168 The cryptographic library NesLib provides the SHA-1, SHA-256, SHA-384, SHA-512 secure hash functions conformant to *FIPS 180-4*, and offering resistance against side channel and fault attacks.

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

7.1.13 Cryptographic operation: Keccak & SHA-3 operation (FCS_COP.1) / Keccak

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

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

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

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

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

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

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

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

7.1.14 Cryptographic operation: Keccak-p operation (FCS_COP.1) / Keccak-p

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

7.1.15 Cryptographic operation: Diffie-Hellman operation (FCS_COP.1) / Diffie-Hellman

175 The cryptographic library NesLib provides the Diffie-Hellman key establishment operation over GF(p) for size of modulus p up to 4096 bits, conformant to *ANSI X9.42*.

176 For these functions, NesLib uses the Cryptography Accelerator (Nescrypt) of the Hardware Platform.

7.1.16 Cryptographic operation: LMS signature verification (FCS_COP.1) / SFH-DSA

177 The cryptographic library NesLib provides the verification of LMS signatures based on SHA-256, conformant to *NIST SP 800-208*, with parameters:

- LMOTS_SHA256_N32_W4 and,
- LMS_SHA256_M32_H10.

7.1.17 Cryptographic operation: DRBG operation (FCS_COP.1) / DRBG

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

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

- Hash-DRBG,
- CTR-DRBG.

7.1.18 Cryptographic key generation: Prime generation (FCS_CKM.1) / Prime-generation

180 The cryptographic library NesLib provides prime numbers generation for prime sizes up to 2048 bits conformant to *FIPS 140-3* and *FIPS 186-5*, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

7.1.19 Cryptographic key generation: RSA key generation (FCS_CKM.1) / RSA-key-generation

181 The cryptographic library NesLib provides standard RSA public and private key computation for key sizes from 829 bits to 4096 bits conformant to *FIPS 140-3, ISO/IEC 9796-2* and

PKCS #1 V2.1, optionally with conditions and/or optionally offering resistance against side channel and fault attacks.

7.1.20 Limited fault tolerance (FRU_FLT.2)

182 The TSF provides limited fault tolerance, by managing faults or errors related to cryptographic operations, thus preventing risk of malfunction.

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

183 The TSF provides preservation of secure state by generating a software reset, managed by the Platform, in case of detected fault attack on the crypto library.

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

184 The TSF prevents the disclosure of internal and user data thanks to leakage protection.

7.2 Statement of compatibility

185 This section details the statement of compatibility between this Security Target and the Platform Security Target *[PF-ST]*.

186 The following mappings regarding SFRs, objectives and assurance requirements demonstrate that there is no inconsistency between this composite Security Target and the *ST31R480 B01 Security Target for composition*.

7.2.1 Compatibility of security objectives

187 There is no conflict between the security objectives of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 13. Platform Security Objectives vs. TOE Security Objectives

Platform Security Objectives	TOE Security Objectives
BSI.O.Leak-Inherent	*BSI.O.Leak-Inherent*
BSI.O.Phys-Probing	*BSI.O.Phys-Probing*
BSI.O.Malfunction	*BSI.O.Malfunction*
BSI.O.Phys-Manipulation	*BSI.O.Phys-Manipulation*
BSI.O.Leak-Forced	*BSI.O.Leak-Forced*
BSI.O.Abuse-Func	*BSI.O.Abuse-Func*
BSI.O.Identification	*BSI.O.Identification*
BSI.O.RND	*BSI.O.RND*
BSI.O.Authentication	*BSI.O.Authentication*
BSI.O.Cap-Avail-Loader	*BSI.O.Cap-Avail-Loader*

Table 13. Platform Security Objectives vs. TOE Security Objectives

Platform Security Objectives	TOE Security Objectives
BSI.O.Ctrl-Auth-Loader	*BSI.O.Ctrl-Auth-Loader*
JIL.O.Prot-TSF-Confidentiality	*JIL.O.Prot-TSF-Confidentiality*
JIL.O.Secure-Load-ACode	*JIL.O.Secure-Load-ACode*
JIL.O.Secure-AC-Activation	*JIL.O.Secure-AC-Activation*
JIL.O.TOE-Identification	*JIL.O.TOE-Identification*
O.Secure-Load-AMemImage	*O.Secure-Load-AMemImage*
O.MemImage-Identification	*O.MemImage-Identification*
AUG1.O.Add-Functions	*AUG1.O.Add-Functions* *AUG1.O.Add-Functions-Lib*
AUG4.O.Mem-Access	*AUG4.O.Mem-Access*
O.Firewall	*O.Firewall*

188 There is no conflict between the security objectives for the environment of this Security Target and those of the Platform Security Target *[PF-ST]*:

Table 14. Platform Security Objectives for the Environment vs. TOE Security Objectives for the Environment

Platform Security Objectives for the Environment	TOE Security Objectives for the Environment
BSI.OE.Resp-Appl	*BSI.OE.Resp-Appl*
BSI.OE.Process-Sec-IC	*BSI.OE.Process-Sec-IC*
BSI.OE.Lim-Block-Loader	*BSI.OE.Lim-Block-Loader*
BSI.OE.Loader-Usage	*BSI.OE.Loader-Usage*
BSI.OE.TOE-Auth	*BSI.OE.TOE-Auth*
OE.Enable-Disable-Secure-Diag	*OE.Enable-Disable-Secure-Diag*
OE.Secure-Diag-Usage	*OE.Secure-Diag-Usage*
OE.Composite-TOE-Id	*OE.Composite-TOE-Id*
OE.TOE-Id	*OE.TOE-Id*

7.2.2 Compatibility of Security Functional Requirements

189 All platform SFRs are relevant for this Composite ST.

190 The Composite ST SFRs do not show any conflict with the platform SFRs.

191 The following platform SFRs are used by this Composite ST because of their security properties providing protection against attacks to the TOE as a whole:

- FRU_FLT.2,
- FDP_SDC.1,
- FDP_SDI.2,
- FPT_PHP.3,
- FDP_ITT.1,
- FPT_ITT.1,
- FDP_IFC.1.

192 Complementary, the *Table 15* below shows the mapping between the Platform SFRs specifically used to implement a security service and security mechanisms by SFRs of this Composite ST.

Table 15. Platform Security Functional Requirements vs. TOE Security Functional Requirements

Platform SFR	Composite ST SFRs
FRU_FLT.2	FRU_FLT.2
FPT_FLS.1	FPT_FLS.1 FDP_SBO.1 / Copy FDP_SBO.1 / Compare FDP_SBO.1 / Swap FDP_SBO.1 / Shift FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES FCS_COP.1 / RSA FCS_COP.1 / ECC-WC FCS_COP.1 / ECC-EC FCS_COP.1 / ECC-MC FCS_COP.1 / SHA FCS_COP.1 / Keccak FCS_COP.1 / Keccak-p FCS_COP.1 / Diffie-Hellman FCS_COP.1 / DRBG FCS_COP.1 / SFH-DSA FCS_CKM.1 / Prime-generation FCS_CKM.1 / RSA-key-generation
FMT_LIM.1 / Test	FMT_LIM.1 / Test
FMT_LIM.2 / Test	FMT_LIM.2 / Test
FAU_SAS.1	FAU_SAS.1
FDP_SDC.1	FDP_SDC.1
FDP_SDI.2	FDP_SDI.2
FPT_PHP.3	FPT_PHP.3

Table 15. Platform Security Functional Requirements vs. TOE Security Functional Requirements (continued)

Platform SFR	Composite ST SFRs
FDP_ITT.1	FDP_ITT.1 FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES
FPT_ITT.1	FPT_ITT.1 FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES
FDP_IFC.1	FDP_IFC.1 FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES
FCS_RNG.1 / PTG.2	FCS_RNG.1 / PTG.2 FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES FCS_COP.1 / RSA FCS_COP.1 / ECC-WC FCS_COP.1 / ECC-EC FCS_COP.1 / ECC-MC FCS_COP.1 / SHA FCS_COP.1 / Keccak FCS_COP.1 / Keccak-p FCS_COP.1 / Diffie-Hellman FCS_COP.1 / SFH-DSA FCS_COP.1 / DRBG FCS_CKM.1 / Prime-generation FCS_CKM.1 / RSA-key-generation
FCS_RNG.1 / PG	FCS_RNG.1 / PG FCS_COP.1 / SW-DES FCS_COP.1 / SW-AES FCS_COP.1 / RSA FCS_COP.1 / ECC-WC FCS_COP.1 / ECC-EC FCS_COP.1 / ECC-MC FCS_COP.1 / SHA FCS_COP.1 / Keccak FCS_COP.1 / Keccak-p FCS_COP.1 / Diffie-Hellman FCS_COP.1 / SFH-DSA FCS_COP.1 / DRBG FCS_CKM.1 / Prime-generation FCS_CKM.1 / RSA-key-generation
FCS_RNG.1 / RngLib	FCS_RNG.1 / RngLib

Table 15. Platform Security Functional Requirements vs. TOE Security Functional Requirements (continued)

Platform SFR	Composite ST SFRs
FCS_COP.1 / TDES	FCS_COP.1 / TDES FCS_COP.1 / SW-DES
FCS_COP.1 / AES	FCS_COP.1 / AES FCS_COP.1 / SW-AES FCS_COP.1 / DRBG
FDP_ACC.2 / Memories	FDP_ACC.2 / Memories
FDP_ACF.1 / Memories	FDP_ACF.1 / Memories
FMT_MSA.3 / Memories	FMT_MSA.3 / Memories
FMT_MSA.1 / Memories	FMT_MSA.1 / Memories
FMT_SMF.1 / Memories	FMT_SMF.1 / Memories
FIA_API.1	FIA_API.1
FMT_LIM.1 / Loader	FMT_LIM.1 / Loader
FMT_LIM.2 / Loader	FMT_LIM.2 / Loader
FTP_ITC.1 / Loader	FTP_ITC.1 / Loader
FDP_UCT.1 / Loader	FDP_UCT.1 / Loader
FDP_UIT.1 / Loader	FDP_UIT.1 / Loader
FDP_ACC.1 / Loader	FDP_ACC.1 / Loader
FDP_ACF.1 / Loader	FDP_ACF.1 / Loader
FMT_MSA.3 / Loader	FMT_MSA.3 / Loader
FMT_MSA.1 / Loader	FMT_MSA.1 / Loader
FMT_SMR.1 / Loader	FMT_SMR.1 / Loader
FIA_UID.1 / Loader	FIA_UID.1 / Loader
FIA_UAU.1 / Loader	FIA_UAU.1 / Loader
FMT_SMF.1 / Loader	FMT_SMF.1 / Loader
FPT_FLS.1 / Loader	FPT_FLS.1 / Loader
FAU_SAR.1 / Loader	FAU_SAR.1 / Loader
FAU_SAS.1 / Loader	FAU_SAS.1 / Loader
FTP_ITC.1 / Sdiag	FTP_ITC.1 / Sdiag
FAU_SAR.1 / Sdiag	FAU_SAR.1 / Sdiag
FMT_LIM.1 / Sdiag	FMT_LIM.1 / Sdiag
FMT_LIM.2 / Sdiag	FMT_LIM.2 / Sdiag

7.2.3 Compatibility of Security Assurance Requirements

193 The level of assurance of the TOE is EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2, while the level of assurance of the Platform is EAL6 augmented with ALC_FLR.2 and ASE_TSS.2.

194 Therefore, the set of Security Assurance Requirements of this composite evaluation represents a strict subset of the Security Assurance Requirements of the underlying platform.

195 There is no conflict regarding the Security Assurance Requirements.

8 Identification

Table 16. TOE components

Platform identification					Library identification
IC Maskset name	Master identification number	IC version	Firmware version	RngLib version	NesLib cryptographic library version
K4H0A	0x0299	B	3.0.6	2.0.2	6.11.3

Table 17. Guidance documentation

Component description	Reference	Version
Cryptographic library NesLib 6.11 - User manual	UM_NesLib_6.11	1
ST31R secure MCU platforms - NesLib 6.11 security recommendations - Application note	AN_SECU_ST31R_NESLIB_6.11	1
NesLib 6.11.3 for ST31R platforms - Release note	RN_ST31R_NESLIB_6.11.3	1

Table 18. Sites list

Site	Address	Activities[1]
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217 38019 Grenoble Cedex France	ES-DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq ZI de Rousset-Peynier 13106 Rousset Cedex France	ES-DEV
ST Tunis	STMicroelectronics Elgazala Technopark, Raoued, Gouvernorat de l'Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B 3d floor 1831 Diegem/Machelen Belgium	ES-DEV

[1] ES-DEV = development, IT = Network infrastructure

9 References

Table 19. 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 20. Platform Security Target

Ref	Component description	Reference	Version
[PF-ST]	ST31R480 B01 Security Target for composition	SMD_ST31R480_ST_23_004	B01.4

Table 21. Protection Profile and other related standards

Ref	Component description	Reference	Version
[PP0084]	Eurosmart - Security IC Platform Protection Profile with Augmentation Packages	BSI-CC-PP-0084-2014	1.0
[AUG]	Smartcard Integrated Circuit Platform Augmentations, March 2002.		1.0
[JILSR]	Security requirements for post-delivery code loading, Joint Interpretation Library, February 2016		1.0

Table 22. 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 800-90B	NIST special publication 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation, National Institute of Standards and Technology (NIST), January 2018
[3]	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
[4]	FIPS 140-3	FIPS 140-3, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), March 2019
[5]	FIPS 180-4	FIPS 180-4 Secure Hash Standard, National Institute of Standards and Technology (NIST), August 2015

Table 22. Other standards

Ref	Identifier	Description
[6]	FIPS 186-5	FIPS 186-5, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), February2023
[7]	FIPS 197	FIPS 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 2001
[8]	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
[9]	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
[10]	NIST SP 800-38B	NIST special publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), June 2016
[11]	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), July 2007
[12]	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
[13]	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
[14]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, January 2000
[15]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[16]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[17]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[18]	NIST SP 800-90A	NIST Special Publication 800-90A rev. 1: Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), June 2015
[19]	FIPS 198-1	FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[20]	NIST SP 800-56A	NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), April 2018

Table 22. Other standards

Ref	Identifier	Description
[6]	FIPS 186-5	FIPS 186-5, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), February2023
[7]	FIPS 197	FIPS 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 2001
[8]	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
[9]	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
[10]	NIST SP 800-38B	NIST special publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), June 2016
[11]	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), July 2007
[12]	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
[13]	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
[14]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, January 2000
[15]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[16]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[17]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[18]	NIST SP 800-90A	NIST Special Publication 800-90A rev. 1: Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), June 2015
[19]	FIPS 198-1	FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[20]	NIST SP 800-56A	NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), April 2018

Table 22. Other standards

Ref	Identifier	Description
[6]	FIPS 186-5	FIPS 186-5, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), February2023
[7]	FIPS 197	FIPS 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), November 2001
[8]	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
[9]	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
[10]	NIST SP 800-38B	NIST special publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), June 2016
[11]	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), July 2007
[12]	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
[13]	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
[14]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, January 2000
[15]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[16]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[17]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[18]	NIST SP 800-90A	NIST Special Publication 800-90A rev. 1: Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), June 2015
[19]	FIPS 198-1	FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[20]	NIST SP 800-56A	NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), April 2018

Table 22. Other standards

Ref	Identifier	Description
[21]	NIST SP 800-208	NIST SP 800-208 Recommendation for Stateful Hash-Based Signature Schemes (NIST), October 2020
[22]	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
[23]	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)
[24]	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
[25]	FIPS 202	FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, National Institute of Standards and Technology (NIST), August 2015
[26]	RFC 8032	S. Josefsson and I. Liusvaara, Edwards-Curve Digital Signature Algorithm (EdDSA), Internet Research Task Force (IRTF) RFC 8032, January 2017
[27]	RFC 7748	A. Langley, M. Hamburg, S. Turner, Elliptic Curves for Security, Internet Research Task Force (IRTF) RFC 7748, January 2016
[28]	ANSSI-PP0084.03	PP0084: Interpretations, ANSSI, April 2016

Appendix A Glossary

A.1 Terms

Authorised user

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

Composite product

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

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

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

IC Dedicated Software

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

IC Dedicated Test Software

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

IC developer

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

IC manufacturer

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

IC packaging manufacturer

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

Initialisation data

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

Object

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

Packaged IC

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

Pre-personalization data

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

Secret

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

Security IC

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

Security IC Embedded SoftWare (ES)

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

Security IC embedded software (ES) developer

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

Security attribute

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

Sensitive information

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

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

Smartcard

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

Subject

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

Test features

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

TOE Delivery

The period when the TOE is delivered which is after Phase 3 ***or Phase 1 for the NesLib, 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 23. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI).
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1. R5.
CFB	Cipher FeedBack.
CTR	Counter
DES	Data Encryption Standard.
DRBG	Deterministic Random Bit Generator.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
ES	Security IC Embedded Software.
ES-DEV	Embedded Software Development.
FIPS	Federal Information Processing Standard.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
NESCRYPT	Next Step Cryptography Accelerator.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OFB	Output FeedBack
OSP	Organisational Security Policy.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
ST	Context dependent : STMicroelectronics or Security Target.

Table 23. List of abbreviations (continued)

Term	Meaning
TDES	Triple Data Encryption Standard
TOE	Target of Evaluation.
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.

IMPORTANT NOTICE – PLEASE READ CAREFULLY