

SC23Z018 and 7
derivative products
with optional
cryptographic library
Neslib 3.1
Security Target - Public
Version

Common Criteria for IT security
evaluation

SMD_SC23Z018_ST_13_001 Rev 01.04

September 2013



BLANK



1 Introduction

1.1 Security Target reference

- 1 Document identification: SC23Z018A and 7 derivative products, with optional cryptographic library Neslib 3.1 SECURITY TARGET - PUBLIC VERSION.
- 2 Version number: Rev 01.04, issued September 2013.
- 3 Registration: registered at ST Microelectronics under number SMD_SC23Z018_ST_13_001_V01.04.

1.2 Purpose

- 4 This document presents **the Security Target - Public version (ST)** of the **SC23Z018A, SC23ZD12A, SC23ZD08A, SC23ZD04A, SB23ZD18A, SB23ZD12A, SB23ZD08A, SB23ZD04A**, Security Integrated Circuits (IC), with Dedicated Software (DSW), and optional cryptographic library Neslib 3.1, designed on the **ST23 platform of STMicroelectronics**.
- 5 This document is a sanitized version of the Security Target used for the evaluation. It is classified as public information.
- 6 The precise reference of the Target of Evaluation (TOE) and the security IC features are given in [Section 3: TOE description](#).
- 7 A glossary of terms and abbreviations used in this document is given in [Appendix A: Glossary](#).

Contents

- 1 Introduction 3**
 - 1.1 Security Target reference 3
 - 1.2 Purpose 3

- 2 Context 10**

- 3 TOE description 11**
 - 3.1 TOE overview 11
 - 3.2 TOE life cycle 14
 - 3.3 TOE environment 15
 - 3.3.1 TOE development environment 15
 - 3.3.2 TOE production environment 16
 - 3.3.3 TOE operational environment 16

- 4 Conformance claims 18**
 - 4.1 Common Criteria conformance claims 18
 - 4.2 PP Claims 18
 - 4.2.1 PP Reference 18
 - 4.2.2 PP Refinements 18
 - 4.2.3 PP Additions 18
 - 4.2.4 PP Claims rationale 18

- 5 Security problem definition 20**
 - 5.1 Description of assets 20
 - 5.2 Threats 21
 - 5.3 Organisational security policies 22
 - 5.4 Assumptions 23

- 6 Security objectives 24**
 - 6.1 Security objectives for the TOE 24
 - 6.2 Security objectives for the environment 25
 - 6.3 Security objectives rationale 25

6.3.1	Organisational security policy "Additional Specific Security Functionality"	26
6.3.2	Organisational security policy "Additional Specific Security Functionality"	27
7	Security requirements	28
7.1	Security functional requirements for the TOE	28
7.1.1	Limited fault tolerance (FRU_FLT.2)	29
7.1.2	Failure with preservation of secure state (FPT_FLS.1)	29
7.1.3	Limited capabilities (FMT_LIM.1)	30
7.1.4	Limited availability (FMT_LIM.2)	30
7.1.5	Audit storage (FAU_SAS.1)	30
7.1.6	Resistance to physical attack (FPT_PHP.3)	30
7.1.7	Basic internal transfer protection (FDP_ITT.1)	30
7.1.8	Basic internal TSF data transfer protection (FPT_ITT.1)	30
7.1.9	Subset information flow control (FDP_IFC.1)	31
7.1.10	Random number generation (FCS_RNG.1)	31
7.1.11	Cryptographic operation (FCS_COP.1)	31
7.1.12	Cryptographic key generation (FCS_CKM.1)	32
7.1.13	Static attribute initialisation (FMT_MSA.3)	32
7.1.14	Management of security attributes (MSA.1)	33
7.1.15	Complete access control (FDP_ACC.2)	33
7.1.16	Security attribute based access control (FDP_ACF.1)	33
7.1.17	Specification of management functions (FMT_SMF.1)	34
7.2	TOE security assurance requirements	34
7.3	Refinement of the security assurance requirements	35
7.3.1	Refinement regarding functional specification (ADV_FSP)	35
7.3.2	Refinement regarding test coverage (ATE_COV)	36
7.4	Security Requirements rationale	36
7.4.1	Rationale for the Security Functional Requirements	36
7.4.2	Additional security objectives are suitably addressed	37
7.4.3	Additional security requirements are consistent	38
7.4.4	Dependencies of Security Functional Requirements	38
7.4.5	Rationale for the Assurance Requirements	40
8	TOE summary specification	41
8.1	Limited fault tolerance (FRU_FLT.2)	41

8.2	Failure with preservation of secure state (FPT_FLS.1)	41
8.3	Limited capabilities (FMT_LIM.1)	41
8.4	Limited availability (FMT_LIM.2)	41
8.5	Audit storage (FAU_SAS.1)	42
8.6	Resistance to physical attack (FPT_PHP.3)	42
8.7	Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1)	42
8.8	Random number generation (FCS_RNG.1)	42
8.9	Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES]) .	42
8.10	Cryptographic operation: RSA operation (FCS_COP.1 [RSA]) if Neslib only	43
8.11	Cryptographic operation: AES operation (FCS_COP.1 [AES]) if Neslib only	43
8.12	Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1 [ECC]) if Neslib only	43
8.13	Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only	43
8.14	Cryptographic key generation: Prime generation (FCS_CKM.1 [Prime_generation]) if Neslib only	44
8.15	Cryptographic key generation: Protected Prime generation (FCS_CKM.1 [PROTECTED_Prime_generation]) if Neslib only	44
8.16	Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_Key_generation]) if Neslib only	44
8.17	Cryptographic key generation: PROTECTED RSA key generation (FCS_CKM.1 [PROTECTED_RSA_Key_generation]) if Neslib only	44
8.18	Static attribute initialisation (FMT_MSA.3)	44
8.19	Management of security attributes (FMT_MSA.1) & Specification of management functions (FMT_SMF.1)	44
8.20	Complete access control (FDP_ACC.2) & Security attribute based access control (FDP_ACF.1)	45
9	References	46
Appendix A	Glossary	49
A.1	Terms	49
A.2	Abbreviations.	51

10	Revision history	54
-----------	-------------------------------	-----------

List of tables

Table 1.	Master product and derivatives common characteristics	11
Table 2.	Master product and derivatives specific characteristics	11
Table 3.	Composite product life cycle phases	14
Table 4.	Summary of security environment	21
Table 5.	Summary of security objectives	24
Table 6.	Security Objectives versus Assumptions, Threats or Policies	26
Table 7.	Summary of functional security requirements for the TOE	28
Table 8.	FCS_COP.1 iterations (cryptographic operations)	31
Table 9.	FCS_CKM.1 iterations (cryptographic key generation)	32
Table 10.	TOE security assurance requirements	34
Table 11.	Impact of EAL5 selection on BSI-PP-0035 refinements	35
Table 12.	Dependencies of security functional requirements	38
Table 13.	List of abbreviations	51
Table 14.	Document revision history	54

List of figures

Figure 1. Sx23Zxxx block diagram. 14

2 Context

- 8 The Target of Evaluation (TOE) referred to in [Section 3: TOE description](#), is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Secure Microcontrollers Division of STMicroelectronics (ST).
- 9 The Target of Evaluation (TOE) is the SC23Z018A with 7 commercial derivative products: SC23ZD12A, SC23ZD08A, SC23ZD04A, SB23ZD18A, SB23ZD12A, SB23ZD08A, and SB23ZD04A, with or without the cryptographic library Neslib 3.1.
- 10 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented.
- 11 The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the TOE security IC, and to summarise its chosen TSF services and assurance measures.
- 12 This ST claims to be an instantiation of the "[Security IC Platform Protection Profile](#)" (PP) registered and certified under the reference [BSI-PP-0035](#) 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](#).
- The original text of this PP is typeset as [indicated here](#), its augmentation from [AUG](#) is [indicated here](#), when they are reproduced in this document.
- 13 Extensions introduced in this ST to the SFRs of the Protection Profile (PP) are **exclusively** drawn from the Common Criteria part 2 standard SFRs.
- 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**. 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-PP-0035](#), **AUG1** for Addition #1 of [AUG](#), and **AUG4** for Addition #4 of [AUG](#).

3 TOE description

3.1 TOE overview

15 The Target of Evaluation (TOE) comprises the SC23Z018A with 7 commercial derivatives: the SC23ZD12A, SC23ZD08A, SC23ZD04A, SB23ZD18A, SB23ZD12A, SB23ZD08A, and SB23ZD04A. Some of them may include the optional cryptographic library Neslib 3.1.

The master product is the SC23Z018A. All based on the same hardware design, the different derivatives are configured during the manufacturing or packaging process, in conformance with the customer's order.

16 All products of the TOE share the same hardware design, and the same maskset, thus mainly share the same characteristics:

Table 1. Master product and derivatives common characteristics

Maskset	Commercial version	Product version	OST name	OST revision	Optional crypto library name	Crypto library revision ⁽¹⁾
K390A	A	C	YIB	0063h	Neslib 3.1	1310h

1. See the Neslib User Manual referenced in [Chapter 9](#).

17 The commercial version (aka external version) is updated when hardware or OST modification has a visible impact for the customer.

18 The product version (aka internal version) is updated when hardware or OST is modified. This letter completely identifies the product version.

19 The different derivative products differ from the master product, only on the available NVM size, and on the availability of the cryptographic co-processor (NESCRIPT), as detailed here below:

Table 2. Master product and derivatives specific characteristics

Commercial name	Product identification ⁽¹⁾	NVM size	NESCRIPT
SC23Z018	003Ah	18 Kbytes	Yes
SC23ZD12	003Bh	12 Kbytes	Yes
SC23ZD08	003Ch	8 Kbytes	Yes
SC23ZD04	003Dh	4 Kbytes	Yes
SB23ZD18	003Eh	18 Kbytes	No
SB23ZD12	003Fh	12 Kbytes	No
SB23ZD08	0040h	8 Kbytes	No
SB23ZD04	0041h	4 Kbytes	No

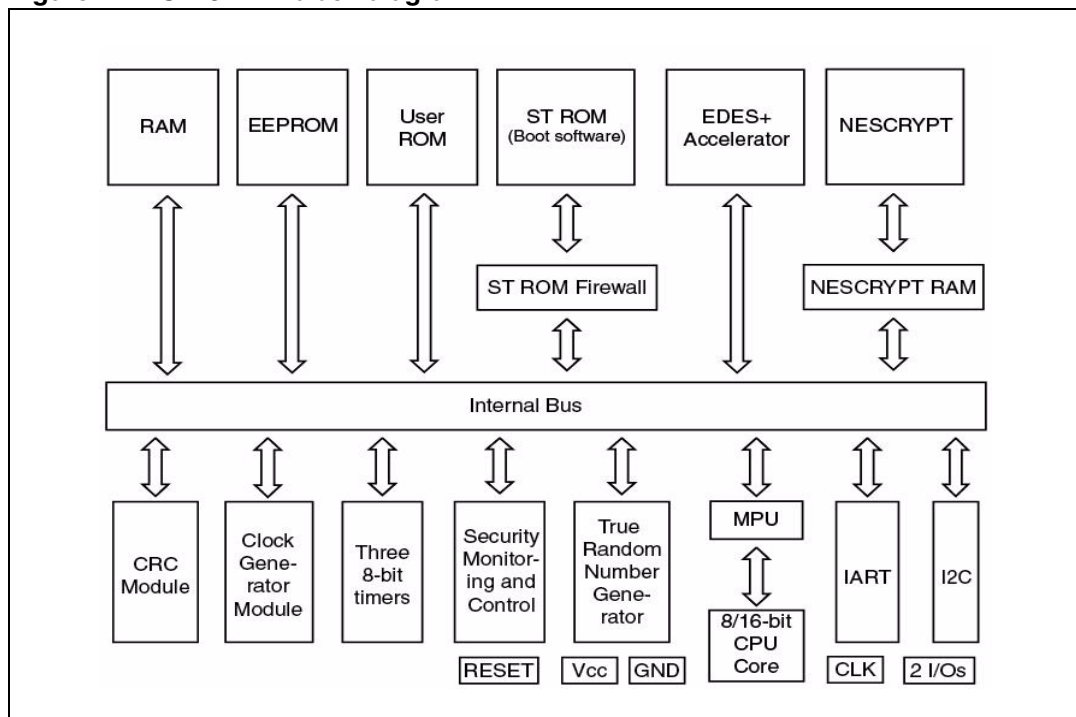
1. Part of the product information.

20 The master product and the different derivative products can be distinguished thanks to the product identification number, included in the traceability number, as detailed in [Table 2: Master product and derivatives specific characteristics](#) and in the data sheet.

- 21 In this Security Target, the terms:
- "TOE" or "Sx23Zxxx" or "SC23Z018A and 7 derivative products" mean all products listed in [Table 2: Master product and derivatives specific characteristics](#),
 - "SC23Zxxx" means the subset of products SC23Z018, SC23ZD12, SC23Z08, SC23Z04,
 - "SB23Zxxx" means the subset of products SB23ZD18, SB23ZD12, SB23ZD08, SB23ZD04.
- 22 The rest of this document applies to all products, with or without Neslib, except when a restriction is mentioned. For easier reading, the restrictions are typeset as [indicated here](#).
- 23 The SC23Zxxx is a Secure IC with 18, 12, 8 or 4 Kbytes EEPROM (see [Table 2: Master product and derivatives specific characteristics](#)), with Nescrypt cryptoprocessor.
- 24 The SB23Zxxx is a Secure IC with 18, 12, 8 or 4 Kbytes EEPROM (see [Table 2: Master product and derivatives specific characteristics](#)), without Nescrypt cryptoprocessor.
- 25 The TOE is a serial access IC based on a 8/16-bit CPU core. Operations are synchronized with an internally generated clock issued by the Clock Generator module. The internal speed of the device is fully software programmable. High performance can be reached by using high speed internal clock frequency (up to 28 MHz). The CPU interfaces with the on-chip RAM, ROM and EEPROM memories via a 24-bit internal bus offering 16 MBytes of linear addressing space.
- 26 The CPU includes the Arithmetic Logic Unit (ALU) and the control logic.
- 27 This device includes a flexible memory protection unit (MPU), which enables a fully dynamic memory segmentation and protection without downgrading the CPU performance. The MPU enables the software to control the addressable space and registers available to any given program, thanks to a flexible and software-friendly interface. As a result, the MPU allows the software developers to enforce a wide range of memory protection policies.
- 28 The 3-key Triple DES accelerator (EDES+) enables Cipher Block Chaining (CBC) [\[10\]](#), fast DES and triple DES computation [\[2\]](#). This module provides an enhanced protection against side channel attacks (DPA and DEMA).
- 29 For the SC23Zxxx, the NEXt Step CRYPTography accelerator (NESCRIPT) enables efficient computation for both GF(p) and GF(2ⁿ) with a very high level of performance. NESCRIPT also includes dedicated instructions to accelerate hash function SHA-1 and SHA-2 family. NESCRIPT allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([\[4\]](#), [\[8\]](#), [\[12\]](#), [\[18\]](#), [\[19\]](#), [\[20\]](#), [\[21\]](#)).
- 30 As randomness is a key stone in many applications, the SC23Z018 and 7 derivative products features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS-31 [\[1\]](#) and directly accessible through dedicated registers.
- 31 In a few words, the Sx23Zxxx offers a unique combination of high performances and very powerful features for high level security:
- Die integrity,
 - Monitoring of environmental parameters,
 - Protection mechanisms against faults,
 - AIS-31 class P2 compliant True Random Number Generator,
 - EDES+ accelerator,
 - NESCRIPT accelerator in the SC23Zxxx.

- 32 The TOE includes in the ST protected ROM a Dedicated Software which provides full test capabilities (operating system for test, called “OST”), not accessible by the Security IC Embedded Software (ES), after TOE delivery.
- 33 The Security IC Embedded Software (ES) is in User ROM.
The ES is not part of the TOE and is out of scope of the evaluation, except Neslib when it is embedded.
- 34 The [SC23Zxxx](#) optionally comprises a specific application in User ROM: this applicative Embedded Software is a cryptographic library called Neslib. Neslib is a cutting edge cryptographic library in terms of security and performance.
- 35 Neslib is embedded by the ES developer in his applicative code.
- 36 Neslib provides the most useful operations in public key algorithms and protocols, thanks to:
- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA [\[20\]](#)),
 - 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) [\[18\]](#),
 - an asymmetric key cryptographic support module that provides secure hash algorithm functions (SHA) [\[4\]](#),
 - a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES [\[7\]](#)),
 - prime number generation.
- 37 In addition, the ROM of the tested samples contains an operating system called “Card Manager” that allows the evaluators to use a set of commands with the I/O, and to load in EEPROM (or in RAM) test software. The card manager is not part of the TOE, and not in the scope of this evaluation.
- 38 The user guidance documentation, part of the TOE, consists of:
- The product Data Sheet,
 - The product family Security Guidance,
 - The AIS31 user manuals,
 - The product family programming manual,
 - Optionally the Neslib user manual.
- The complete list of guidance documents is detailed in [Chapter 9](#).
- 39 [Figure 1](#) provides an overview of the Sx23zxxx.

Figure 1. Sx23Zxxx block diagram



3.2 TOE life cycle

40 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 Security IC Platform Protection Profile (BSI-PP-0035), section 1.2.3.

41 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.

42 The life cycle phases are summarized in [Table 3](#).

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

Table 3. Composite product life cycle phases

Phase	Name	Description	Responsible party
1	IC embedded software development	Security IC embedded software development	IC embedded software developer
2	IC development	IC design IC dedicated software development	IC developer: ST

Table 3. Composite product life cycle phases (continued)

Phase	Name	Description	Responsible party
3	IC manufacturing	integration and photomask fabrication IC production IC testing preparation pre-personalisation	IC manufacturer: ST or GLOBAL FOUNDRIES
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary	IC packaging manufacturer: ST or NEDCARD or SMARTFLEX
5	Composite product integration	composite product finishing process composite product preparation composite product shipping	Composite product integrator
6	Personalisation	composite product personalisation composite product testing	Personaliser
7	Operational usage	composite product usage by its issuers and consumers	End-consumer

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

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

- after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or
- after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

46 The TOE is only delivered in USER configuration.

3.3 TOE environment

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

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

3.3.1 TOE development environment

48 To ensure security, the environment in which the development takes place is secured with controllable accesses having traceability. Furthermore, all authorised personnel involved fully understand the importance and the strict implementation of defined security procedures.

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

50 Design and development of the IC then follows, together with the dedicated and engineering software and tools development. The engineers use secure computer systems (preventing unauthorised access) to make their developments, simulations, verifications and generation of the TOE's databases. Sensitive documents, files and tools, databases on tapes, and

printed circuit layout information are stored in appropriate locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

- 51 The development centres involved in the development of the TOE are the following: **ST ROUSSET (FRANCE)** and **ST ANG MO KIO (SINGAPORE)**, for the design activities, **ST ROUSSET (FRANCE)**, for the engineering activities, **ST ROUSSET (FRANCE)** and **ST ZAVENTEM (BELGIUM)** for the software development activities.
- 52 Reticules and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. As reticules and photomasks are generated off-site, they are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).
- 53 The authorized sub-contractors involved in the TOE mask manufacturing can be **DNP (JAPAN)** and **DPE (ITALY)**.

3.3.2 TOE production environment

- 54 As high volumes of product commonly go through such environments, adequate control procedures are necessary to account for all product at all stages of production.
- 55 Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing of each TOE occurs to assure conformance with the device specification.
- 56 The authorized front-end plant involved in the manufacturing of the TOE can be **ST ROUSSET (FRANCE)** or **GLOBAL FOUNDRIES FAB 2 & 6 (SINGAPORE)**.
- 57 The authorized EWS plant involved in the testing of the TOE can be **ST ROUSSET (FRANCE)** or **ST TOA PAYOH (SINGAPORE)**.
- 58 Wafers are then scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged in phase 4, in a back-end plant. When testing, programming or deliveries are done offsite, ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.
- 59 When the product is delivered after phase 4, the authorized back-end plant involved in the packaging of the TOE can be **ST BOUSKOURA (MOROCCO)**, **ST CALAMBA (PHILIPPINES)**, **NEDCARD (THE NETHERLANDS)** or **SMARTFLEX (SINGAPORE)**.
- 60 The other sites that can be involved during the production of the TOE are **ST LOYANG (SINGAPORE)** for the logistics, and **ST SHENZEN (CHINA)** or **DISCO (GERMANY)** for the wafers backlap and sawing.

3.3.3 TOE operational environment

- 61 A TOE operational environment is the environment of phases 1, optionally 4, then 5 to 7.
- 62 At phases 1, 4, 5 and 6, the TOE operational environment is a controlled environment.
- 63 End-user environments (phase 7): composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are pay-TV, banking

cards, portable communication SIM cards, brand protection, health cards, transportation cards, identity and passport cards. The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.

4 Conformance claims

4.1 Common Criteria conformance claims

64 The Sx23Zxxx Security Target claims to be conformant to the Common Criteria version 3.1.
65 Furthermore it claims to be CC Part 2 ([CCMB-2009-07-002](#)) extended and CC Part 3 ([CCMB-2009-07-003](#)) conformant. The extended Security Functional Requirements are those defined in the [Security IC Platform Protection Profile \(BSI-PP-0035\)](#).
66 The assurance level for this Security Target is **EAL 5** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

67 This Security Target claims strict conformance to the [Security IC Platform Protection Profile \(BSI-PP-0035\)](#), as required by this Protection Profile.

4.2.2 PP Refinements

68 The main refinements operated on the [BSI-PP-0035](#) are:

- Addition #1: “Support of Cipher Schemes” from [AUG](#),
- Addition #4: “Area based Memory Access Control” from [AUG](#),
- Refinement of assurance requirements.

69 All refinements are indicated with type setting text **as indicated here**, original text from the [BSI-PP-0035](#) being typeset [as indicated here](#). Text originating in [AUG](#) is typeset [as indicated here](#).

4.2.3 PP Additions

70 The security environment additions relative to the PP are summarized in [Table 4](#).

71 The additional security objectives relative to the PP are summarized in [Table 5](#).

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

73 The additional SFRs for the TOE relative to the PP are summarized in [Table 7](#).

74 The additional SARs relative to the PP are summarized in [Table 10](#).

4.2.4 PP Claims rationale

75 The differences between this Security Target security objectives and requirements and those of [BSI-PP-0035](#), to which conformance is claimed, have been identified and justified in [Section 6](#) and in [Section 7](#). They have been recalled in the previous section.

76 In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the [BSI-PP-0035](#).

77 The security problem definition presented in [Section 5](#), clearly shows the additions to the security problem statement of the PP.

- 78 The security objectives rationale presented in [Section 6.3](#) clearly identifies modifications and additions made to the rationale presented in the [BSI-PP-0035](#).
- 79 Similarly, the security requirements rationale presented in [Section 7.4](#) has been updated with respect to the protection profile.
- 80 All PP requirements have been shown to be satisfied in the extended set of requirements whose completeness, consistency and soundness has been argued in the rationale sections of the present document.

5 Security problem definition

81 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.

82 This Security Target being fully conform to the claimed PP, in the following, just a summary and some useful explanations are given. For complete details on the security problem definition please refer to the [Security IC Platform Protection Profile \(BSI-PP-0035\)](#), section 3.

83 A summary of all these security aspects and their respective conditions is provided in [Table 4](#).

5.1 Description of assets

84 The assets (related to standard functionality) to be protected are:

- the User Data,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software.

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

- SC1 integrity of User Data and of the Security IC Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- SC2 confidentiality of User Data and of the Security IC Embedded Software (while being processed and while being stored in the TOE's memories)
- SC3 correct operation of the security services provided by the TOE for the Security IC Embedded Software.

86 According to the Protection Profile there is the following high-level security concern related to security service:

- SC4 deficiency of random numbers.

87 To be able to protect these assets the TOE shall protect its security functionality. Therefore critical information about the TOE shall be protected. Critical information includes:

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

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

- 88 The information and material produced and/or processed by **ST** in the TOE development and production environment (Phases 2 up to TOE delivery) can be grouped as follows:
- logical design data,
 - physical design data,
 - IC Dedicated Software, Security IC Embedded Software, Initialisation Data and pre-personalisation Data,
 - specific development aids,
 - test and characterisation related data,
 - material for software development support, and
 - photomasks and products in any form
- as long as they are generated, stored, or processed by **ST**.

Table 4. Summary of security environment

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
	AUG4.T.Mem-Access	Memory Access Violation
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Plat-Appl	Usage of Hardware Platform
	BSI.A.Resp-Appl	Treatment of User Data

5.2 Threats

89 The threats are described in the [BSI-PP-0035](#), section 3.2. Only those originating in [AUG](#) are detailed in the following section.

- BSI.T.Leak-Inherent Inherent Information Leakage
- BSI.T.Phys-Probing Physical Probing
- BSI.T.Malfunction Malfunction due to Environmental Stress
- BSI.T.Phys-Manipulation Physical Manipulation
- BSI.T.Leak-Forced Forced Information Leakage
- BSI.T.Abuse-Func Abuse of Functionality

BSI.T.RND

Deficiency of Random Numbers

AUG4.T.Mem-Access

Memory Access Violation:

Parts of the **Security IC** Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the **Security IC** Embedded Software.

Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access.

Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

5.3 Organisational security policies

- 90 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.
- 91 ST applies the Protection policy during TOE Development and Production (*BSI.P.Process-TOE*) as specified below.
- 92 **ST** applies the Additional Specific Security Functionality policy (*AUG1.P.Add-Functions*) as specified below.
- 93 No other Organisational Security Policy (OSP) has been defined in this ST since their specifications depend heavily on the applications in which the TOE will be integrated. The Security Targets for the applications embedded in this TOE should further define them.

BSI.P.Process-TOE

Protection during TOE Development and Production:

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

- AUG1.P.Add-Functions Additional Specific Security Functionality:
The TOE shall provide the following specific security functionality to the Security IC Embedded Software:
- Data Encryption Standard (DES),
 - Triple Data Encryption Standard (3DES),
 - Advanced Encryption Standard (AES): when Neslib is embedded only,
 - **Elliptic Curves Cryptography on $GF(p)$** : when Neslib is embedded only,
 - **Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512)**: when Neslib is embedded only,
 - Rivest-Shamir-Adleman (RSA): when Neslib is embedded only,
 - **Prime Number Generation**: when Neslib is embedded only.
- Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

5.4 Assumptions

94 The assumptions are described in the [BSI-PP-0035](#), section 3.4.

- BSI.A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation
- BSI.A.Plat-Appl Usage of Hardware Platform
- BSI.A.Resp-Appl Treatment of User Data

6 Security objectives

- 95 The security objectives of the TOE cover principally the following aspects:
- integrity and confidentiality of assets,
 - protection of the TOE and associated documentation during development and production phases,
 - provide random numbers,
 - provide cryptographic support and access control functionality.
- 96 A summary of all security objectives is provided in [Table 5](#). Note that the origin of each objective is clearly identified in the prefix of its label.
- 97 Most of these security aspects can therefore be easily found in the protection profile. Only those originating in [AUG](#) are detailed in the following sections.

Table 5. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem Access	Dynamic Area based Memory Access Control
Environments	BSI.OE.Plat-Appl	Usage of Hardware Platform
	BSI.OE.Resp-Appl	Treatment of User Data
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing

6.1 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
AUG1.O.Add-Functions	<p>Additional Specific Security Functionality:</p> <p>The TOE must provide the following specific security functionality to the Security IC Embedded Software:</p> <ul style="list-style-type: none"> – Data Encryption Standard (DES), – Triple Data Encryption Standard (3DES), – Advanced Encryption Standard (AES): when Neslib is embedded only, – Elliptic Curves Cryptography on GF(p): when Neslib is embedded only, – Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512): when Neslib is embedded only, – Rivest-Shamir-Adleman (RSA): when Neslib is embedded only, – Prime Number Generation: when Neslib is embedded only.
AUG4.O.Mem Access	<p>Dynamic Area based Memory Access Control:</p> <p>The TOE must provide the Security IC Embedded Software with the capability to define dynamic memory segmentation and protection. The TOE must then enforce the defined access rules so that access of software to memory areas is controlled as required, for example, in a multi-application environment.</p>

6.2 Security objectives for the environment

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

BSI.OE.Plat-Appl Usage of Hardware Platform

BSI.OE.Resp-Appl Treatment of User Data

99 Security Objectives for the operational Environment (TOE delivery up to end of phase 6):

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

6.3 Security objectives rationale

100 The main line of this rationale is that the inclusion of all the security objectives of the **BSI-PP-0035** protection profile, together with those in **AUG**, guarantees that all the security environment aspects identified in **Section 5** are addressed by the security objectives stated in this chapter.

- 101 Thus, it is necessary to show that:
 - security environment aspects from *AUG* are addressed by security objectives stated in this chapter,
 - the security objectives from *AUG* are suitable (i.e. they address security environment aspects),
 - the security objectives from *AUG* are consistent with the other security objectives stated in this chapter (i.e. no contradiction).
- 102 The selected augmentations from *AUG* introduce the following security environment aspect:
 - TOE threat "Memory Access Violation, (*AUG4.T.Mem-Access*)",
 - organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)".
- 103 As required by CC Part 1 (*CCMB-2009-07-001*), no assumption nor objective for the environment has been added to those of the *BSI-PP-0035* Protection Profile to which strict conformance is claimed.
- 104 The justification of the additional policy and the additional threat provided in the next subsections shows that they do not contradict to the rationale already given in the protection profile *BSI-PP-0035* for the assumptions, policy and threats defined there.

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
<i>BSI.A.Plat-Appl</i>	<i>BSI.OE.Plat-Appl</i>	Phase 1
<i>BSI.A.Resp-Appl</i>	<i>BSI.OE.Resp-Appl</i>	Phase 1
<i>BSI.P.Process-TOE</i>	<i>BSI.O.Identification</i>	Phase 2-3 optional Phase 4
<i>BSI.A.Process-Sec-IC</i>	<i>BSI.OE.Process-Sec-IC</i>	Phase 5-6 optional Phase 4
<i>BSI.T.Leak-Inherent</i>	<i>BSI.O.Leak-Inherent</i>	
<i>BSI.T.Phys-Probing</i>	<i>BSI.O.Phys-Probing</i>	
<i>BSI.T.Malfunction</i>	<i>BSI.O.Malfunction</i>	
<i>BSI.T.Phys-Manipulation</i>	<i>BSI.O.Phys-Manipulation</i>	
<i>BSI.T.Leak-Forced</i>	<i>BSI.O.Leak-Forced</i>	
<i>BSI.T.Abuse-Func</i>	<i>BSI.O.Abuse-Func</i>	
<i>BSI.T.RND</i>	<i>BSI.O.RND</i>	
<i>AUG1.P.Add-Functions</i>	<i>AUG1.O.Add-Functions</i>	
<i>AUG4.T.Mem-Access</i>	<i>AUG4.O.Mem Access</i>	

6.3.1 TOE threat "Memory Access Violation"

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

- 106 According to [AUG4.O.Mem Access](#) the TOE must enforce the **dynamic memory segmentation and protection** so that access of software to memory areas is controlled. Any restrictions are to be defined by the **Security IC** Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data (which may include code) can be prevented (refer to [AUG4.T.Mem-Access](#)). The threat [AUG4.T.Mem-Access](#) is therefore removed if the objective is met.
- 107 The added objective for the TOE [AUG4.O.Mem Access](#) does not introduce any contradiction in the security objectives for the TOE.

6.3.2 Organisational security policy "Additional Specific Security Functionality"

- 108 The justification related to the organisational security policy "Additional Specific Security Functionality, ([AUG1.P.Add-Functions](#))" is as follows:
- 109 Since [AUG1.O.Add-Functions](#) requires the TOE to implement exactly the same specific security functionality as required by [AUG1.P.Add-Functions](#), **and in the very same conditions**, the organisational security policy is covered by the objective.
- 110 Nevertheless the security objectives [BSI.O.Leak-Inherent](#), [BSI.O.Phys-Probing](#), , [BSI.O.Malfunction](#), [BSI.O.Phys-Manipulation](#) and [BSI.O.Leak-Forced](#) define how to implement the specific security functionality required by [AUG1.P.Add-Functions](#). (Note that these objectives support that the specific security functionality is provided in a secure way as expected from [AUG1.P.Add-Functions](#).) Especially [BSI.O.Leak-Inherent](#) and [BSI.O.Leak-Forced](#) refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by [AUG1.P.Add-Functions](#).
- 111 The added objective for the TOE [AUG1.O.Add-Functions](#) does not introduce any contradiction in the security objectives for the TOE.

7 Security requirements

112 This chapter on security requirements contains a section on security functional requirements (SFRs) for the TOE ([Section 7.1](#)), a section on security assurance requirements (SARs) for the TOE ([Section 7.2](#)), a section on the refinements of these SARs ([Section 7.3](#)) as required by the "BSI-PP-0035" Protection Profile. This chapter includes a section with the security requirements rationale ([Section 7.4](#)).

7.1 Security functional requirements for the TOE

113 Security Functional Requirements (SFRs) from the "BSI-PP-0035" Protection Profile (PP) are drawn from [CCMB-2009-07-002](#), except the following SFRs, that are **extensions** to [CCMB-2009-07-002](#):

- **FCS_RNG** Generation of random numbers,
- **FMT_LIM** Limited capabilities and availability,
- **FAU_SAS** Audit data storage.

The reader can find their certified definitions in the text of the "BSI-PP-0035" Protection Profile.

114 All extensions to the SFRs of the "BSI-PP-0035" Protection Profiles (PPs) are **exclusively** drawn from [CCMB-2009-07-002](#).

115 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of [CCMB-2009-07-001](#). 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.

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

117 The selected security functional requirements for the TOE, their respective origin and type are summarized in [Table 7](#).

Table 7. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	BSI-PP-0035	CCMB-2009-07-002
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1	Limited capabilities	Abuse of functionality	BSI-PP-0035	Extended
FMT_LIM.2	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	BSI-PP-0035 Operated	

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

Label	Title	Addressing	Origin	Type
FPT_PHP.3	Resistance to physical attack	Physical manipulation & probing	BSI-PP-0035	CCMB-2009-07-002
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1	Random number generation	Weak cryptographic quality of random numbers	BSI-PP-0035 Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	AUG #1 Operated	CCMB-2009-07-002
FCS_CKM.1 (if Neslib is embedded only)	Cryptographic key generation		Security Target Operated	
FDP_ACC.2	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1	Security attribute based access control			
FMT_MSA.3	Static attribute initialisation	Correct operation	AUG #4 Operated	
FMT_MSA.1	Management of security attribute			
FMT_SMF.1	Specification of management functions		Security Target Operated	

7.1.1 Limited fault tolerance (FRU_FLT.2)

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

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

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

120 Refinement:

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

Regarding application note 15 of [BSI-PP-0035](#), the TOE provides information on the operating conditions monitored during Security IC Embedded Software execution and after a warm reset. No audit requirement is however selected in this Security Target.

7.1.3 Limited capabilities (FMT_LIM.1)

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

7.1.4 Limited availability (FMT_LIM.2)

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

123 SFP_1: Limited capability and availability Policy

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

7.1.5 Audit storage (FAU_SAS.1)

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

7.1.6 Resistance to physical attack (FPT_PHP.3)

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

126 Refinement:

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

7.1.7 Basic internal transfer protection (FDP_ITT.1)

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

7.1.8 Basic internal TSF data transfer protection (FPT_ITT.1)

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

129 Refinement:

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

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

7.1.9 Subset information flow control (FDP_IFC.1)

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

131 SFP_2: Data Processing Policy

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

7.1.10 Random number generation (FCS_RNG.1)

132 The TSF shall provide a **physical** random number generator that implements a **total failure test of the random source**.

133 The TSF shall provide random numbers that meet **P2 class of BSI-AIS31**.

7.1.11 Cryptographic operation (FCS_COP.1)

134 The TSF shall perform **the operations in Table 8** in accordance with a specified cryptographic algorithm **in Table 8** and cryptographic key sizes **of Table 8** that meet the **standards in Table 8**. **The list of operations depends on the presence of Neslib, as indicated in Table 8 (Restrict)**.

Table 8. FCS_COP.1 iterations (cryptographic operations)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
Even without Neslib	EDES	encryption decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode MAC computation in CBC-MAC	Data Encryption Standard (DES)	56 bits	FIPS PUB 46-3 ISO/IEC 9797-1 ISO/IEC 10116
			Triple Data Encryption Standard (3DES)	168 bits	
If Neslib	AES	encryption (cipher) decryption (inverse cipher) key expansion andomize	Advanced Encryption Standard	128, 192 and 256 bits	FIPS PUB 197
If Neslib	RSA	RSA public key operation RSA private key operation without the Chinese Remainder Theorem RSA private key operation with the Chinese Remainder Theorem	Rivest, Shamir & Adleman's	up to 4096 bits	PKCS #1 V2.1

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

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
If Neslib	ECC	private scalar multiplication prepare Jacobian public scalar multiplication point validity check convert Jacobian to affine coordinates general point addition, point expansion point compression	Elliptic Curves Cryptography on GF(p)	up to 640 bits	IEEE 1363-2000, chapter 7 IEEE 1363a-2004
If Neslib	SHA	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	Secure Hash Algorithm	assignment pointless because algorithm has no key	FIPS PUB 180-1 FIPS PUB 180-2 ISO/IEC 10118-3:1998

7.1.12 Cryptographic key generation (FCS_CKM.1)

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

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

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

7.1.13 Static attribute initialisation (FMT_MSA.3)

136 The TSF shall enforce the **Dynamic Memory Access Control Policy** to provide *minimally protective*^(a) default values for security attributes that are used to enforce the SFP.

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

Application note:

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

7.1.14 Management of security attributes (MSA.1)

138 The TSF shall enforce the **Dynamic Memory Access Control Policy** to restrict the ability to **modify** the current set of access rights security attributes to **software running in supervisor level**.

7.1.15 Complete access control (FDP_ACC.2)

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

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

7.1.16 Security attribute based access control (FDP_ACF.1)

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

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

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

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

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

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

146 SFP_3: *Dynamic Memory Access Control Policy*

147 The TSF must control read, write, execute accesses of software to data (including code stored in memory areas), based on their respective clearance levels and on the current set of access rights.

a. See the Datasheet referenced in [Section 9](#) for actual values.

7.1.17 Specification of management functions (FMT_SMF.1)

148 The TSF will be able to perform the following management functions: **modification of the current set of access rights security attributes by software running in supervisor level, supporting the Dynamic Memory Access Control Policy.**

7.2 TOE security assurance requirements

149 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 and AVA_VAN.5.

150 Regarding application note 21 of [BSI-PP-0035](#), the continuously increasing maturity level of evaluations of Security ICs justifies the selection of a higher-level assurance package.

151 The set of security assurance requirements (SARs) is presented in [Table 10](#), indicating the origin of the requirement.

Table 10. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/ BSI-PP-0035
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/ BSI-PP-0035
ADV_INT.2	Well-structured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/ BSI-PP-0035
AGD_PRE.1	Preparative procedures	EAL5/ BSI-PP-0035
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/ BSI-PP-0035
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/ BSI-PP-0035
ALC_DVS.2	Sufficiency of security measures	BSI-PP-0035
ALC_LCD.1	Developer defined life-cycle model	EAL5/ BSI-PP-0035
ALC_TAT.2	Compliance with implementation standards	EAL5
ATE_COV.2	Analysis of coverage	EAL5/ BSI-PP-0035
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/ BSI-PP-0035
ATE_IND.2	Independent testing - sample	EAL5/ BSI-PP-0035
AVA_VAN.5	Advanced methodical vulnerability analysis	BSI-PP-0035

7.3 Refinement of the security assurance requirements

- 152 As [BSI-PP-0035](#) defines refinements for selected SARs, these refinements are also claimed in this Security Target.
- 153 The main customizing is that the IC Dedicated Software is an operational part of the TOE after delivery, although it is not available to the user.
- 154 Regarding application note 22 of [BSI-PP-0035](#), the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.
- 155 The text of the impacted refinements of [BSI-PP-0035](#) is reproduced in the next sections.
- 156 For reader's ease, an impact summary is provided in [Table 11](#).

Table 11. Impact of EAL5 selection on [BSI-PP-0035](#) refinements

Assurance Family	BSI-PP-0035 Level	ST Level	Impact on refinement
ADO_DEL	1	1	None
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	4	None
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, IC Dedicated Software is included
ADV_IMP	1	1	None
ATE_COV	2	2	IC Dedicated Software is included
AGD_OPE	1	1	None
AGD_PRE	1	1	None
AVA_VAN	5	5	None

7.3.1 Refinement regarding functional specification (ADV_FSP)

- 157 ~~Although the IC Dedicated Test Software is a part of the TOE, the test functions of the IC Dedicated Test Software are not described in the Functional Specification because the IC Dedicated Test Software is considered as a test tool delivered with the TOE but not providing security functions for the operational phase of the TOE. The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are properly identified in the delivered documentation.~~
- 158 The Functional Specification **refers to datasheet to trace security features that do not provide any external interface but that contribute to fulfil the SFRs e.g. like physical protection. Thereby they are part of the complete instantiation of the SFRs.**
- 159 The Functional Specification **refers to design specifications to detail the mechanisms against physical attacks described in a more general way only, but detailed enough to be able to support Test Coverage Analysis also for those mechanisms where inspection of the layout is of relevance or tests beside the TSFI may be needed.**

- 160 The Functional Specification *refers to data sheet to* specify operating conditions of the TOE. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature.
- 161 All functions and mechanisms which control access to the functions provided by the IC Dedicated Test Software (refer to the security functional requirement (FMT_LIM.2)) **are part of the** Functional Specification. Details will be given in the document for ADV_ARC, ~~refer to Section 6.2.1.5~~. In addition, all these functions and mechanisms **are** subsequently be refined according to all relevant requirements of the Common Criteria assurance class ADV because these functions and mechanisms are active after TOE Delivery and need to be part of the assurance aspects Tests (class ATE) and Vulnerability Assessment (class AVA). Therefore, all necessary information **is** provided to allow tests and vulnerability assessment.
- 162 Since the selected higher-level assurance component requires a security functional specification presented in a “semi-formal style” (ADV_FSP.5.2C) the changes affect the style of description, the *BSI-PP-0035* refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

7.3.2 Refinement regarding test coverage (ATE_COV)

- 163 The TOE **is** tested under different operating conditions within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that “Fault tolerance (FRU_FLT.2)” **is** proven for the complete TSF. The tests ~~must~~ also cover functions which may be affected by “ageing” (such as EEPROM writing).
- 164 The existence and effectiveness of measures against physical attacks (as specified by the functional requirement FPT_PHP.3) cannot be tested in a straightforward way. Instead **STMicroelectronics provides** evidence that the TOE actually has the particular physical characteristics (especially layout design principles). This **is** done by checking the layout (implementation or actual) in an appropriate way. The required evidence pertains to the existence of mechanisms against physical attacks (unless being obvious).
- 165 ~~The IC Dedicated Test Software is seen as a “test tool” being delivered as part of the TOE. However, the Test Features do not provide security functionality. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis. The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are part of the Test Coverage Analysis.~~

7.4 Security Requirements rationale

7.4.1 Rationale for the Security Functional Requirements

- 166 Just as for the security objectives rationale of *Section 6.3*, the main line of this rationale is that the inclusion of all the security requirements of the *BSI-PP-0035* protection profile, together with those in *AUG*, guarantees that all the security objectives identified in *Section 6* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.
- 167 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 7* and *Table 10*, it can be

verified that the justifications provided by the *BSI-PP-0035* protection profile and *AUG* can just be carried forward to their union.

168 From *Table 5*, it is straightforward to identify two additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem Access*), all tracing back to *AUG*. This rationale must show that security requirements suitably address these too.

169 Furthermore, a more careful observation of the requirements listed in *Table 7* and *Table 10* shows that:

- there are additional security requirements introduced by this Security Target (*FCS_CKM.1 (if Neslib is embedded only)* and various assurance requirements of EAL5),
- there are security requirements introduced from *AUG* (*FCS_COP.1*, *FDP_ACC.2*, *FDP_ACF.1*, *FMT_MSA.3*, *FMT_MSA.1* and *FMT_SMF.1*).

170 Though it remains to show that:

- security objectives from *AUG* are addressed by security requirements stated in this chapter,
- additional security requirements from this Security Target and from *AUG* are mutually supportive to the security requirements from the *BSI-PP-0035* protection profile, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

171 The justification that the additional security objective is suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in *BSI-PP-0035*, they form an internally consistent whole, is provided in the next subsections.

7.4.2 Additional security objectives are suitably addressed

Security objective “Dynamic Area based Memory Access Control (*AUG4.O.Mem Access*)”

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

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

174 The security functional requirement “*Static attribute initialisation (FMT_MSA.3)*” requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) **as further detailed in the security functional requirements “Management of security attributes (MSA.1)”**. These management functions **together with “Specification of management functions (FMT_SMF.1)”** ensure that the required access control can be realised using the functions provided by the TOE.

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

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

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

7.4.3 Additional security requirements are consistent

“Cryptographic operation (*FCS_COP.1*) & key generation (*FCS_CKM.1* (if *Neslib is embedded only*))”

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

“Static attribute initialisation (*FMT_MSA.3*), Management of security attributes (*FMT_MSA.1*), Complete access control (*FDP_ACC.2*), Security attribute based access control (*FDP_ACF.1*), Specification of management functions (*FMT_SMF.1*)”

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

7.4.4 Dependencies of Security Functional Requirements

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

- those justified in the *BSI-PP-0035* protection profile security requirements rationale,
- those justified in *AUG* security requirements rationale (except on *FMT_MSA.2*, see discussion below),
- the dependency of *FCS_COP.1* and *FCS_CKM.1* (if *Neslib is embedded only*) on *FCS_CKM.4* (see discussion below).

180 Details are provided in *Table 12* below.

Table 12. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FRU_FLT.2	FPT_FLS.1	Yes	Yes, <i>BSI-PP-0035</i>
FPT_FLS.1	None	No dependency	Yes, <i>BSI-PP-0035</i>
FMT_LIM.1	FMT_LIM.2	Yes	Yes, <i>BSI-PP-0035</i>
FMT_LIM.2	FMT_LIM.1	Yes	Yes, <i>BSI-PP-0035</i>
FAU_SAS.1	None	No dependency	Yes, <i>BSI-PP-0035</i>

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in <i>BSI-PP-0035</i> or in <i>AUG</i>
FPT_PHP.3	None	No dependency	Yes, <i>BSI-PP-0035</i>
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, <i>BSI-PP-0035</i>
FPT_ITT.1	None	No dependency	Yes, <i>BSI-PP-0035</i>
FDP_IFC.1	FDP_IFF.1	No, see <i>BSI-PP-0035</i>	Yes, <i>BSI-PP-0035</i>
FCS_RNG.1	None	No dependency	Yes, <i>BSI-PP-0035</i>
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FCS_CKM.1, see discussion below	Yes, <i>AUG #1</i>
	FCS_CKM.4	No, see discussion below	
FCS_CKM.1	[FDP_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.1	No , <i>CCMB-2009-07-002</i>
	FCS_CKM.4	No, see discussion below	
FDP_ACC.2	FDP_ACF.1	Yes	No , <i>CCMB-2009-07-002</i>
FDP_ACF.1	FDP_ACC.1	Yes, by FDP_ACC.2	Yes, <i>AUG #4</i>
	FMT_MSA.3	Yes	
FMT_MSA.3	FMT_MSA.1	Yes	Yes, <i>AUG #4</i>
	FMT_SMR.1	No, see <i>AUG #4</i>	
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes, by FDP_ACC.2	Yes, <i>AUG #4</i>
	FMT_SMF.1	Yes	No , <i>CCMB-2009-07-002</i>
	FMT_SMR.1	No, see <i>AUG #4</i>	Yes, <i>AUG #4</i>
FMT_SMF.1	None	No dependency	No , <i>CCMB-2009-07-002</i>

181 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.

182 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. This is why FCS_CKM.4 is not defined in this ST.

7.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5 ([Table 10](#))

- 183 Regarding application note 21 of [BSI-PP-0035](#), 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.
- 184 EAL5 represents a meaningful increase in assurance from EAL4 by requiring semiformal design descriptions, a more structured (and hence analyzable) architecture, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered during development.
- 185 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.
- 186 Note that detailed and updated refinements for assurance requirements are given in [Section 7.3](#).

Dependencies of assurance requirements

- 187 Dependencies of security assurance requirements are fulfilled by the EAL5 package selection.
- 188 Augmentation to this package are identified in paragraph [149](#) and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

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

190 The complete TOE summary specification has been presented in the [SC23Z018A and 7 derivative products with optional cryptographic library NESLIB 3.1 Security Target](#).

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

8.1 Limited fault tolerance (FRU_FLT.2)

192 The TSF provides limited fault tolerance, by managing a certain number of faults or errors that may happen, related to memory contents, random number generation and cryptographic operations, thus preventing risk of malfunction.

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

193 The TSF provides preservation of secure state by managing the following events, resulting in an immediate reset:

- Die integrity violation detection,
- Errors on memories,
- Bus integrity error,
- Glitches,
- High voltage supply,
- CPU error,
- Clock tree error,
- etc..

194 The ES can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1)

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

8.4 Limited availability (FMT_LIM.2)

196 The TOE is either in TEST or in USER configuration.

197 The only authorised TOE configuration modification is:

- TEST to USER configuration.

198 The TSF ensures the switching and the control of TOE configuration and mode.

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

8.5 Audit storage (FAU_SAS.1)

200 The TOE provides commands to store data and/or pre-personalisation data and/or supplements of the ES in the NVM. These commands are only available to authorised processes, and only until end of phase 4.

8.6 Resistance to physical attack (FPT_PHP.3)

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

- The TOE implements counter-measures that reduce the exploitability of physical probing.
- The TOE is physically protected by an active shield that commands an automatic reaction on die integrity violation detection.

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

202 The TSF prevents the disclosure of internal and user data thanks to the following features:

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

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

8.8 Random number generation (FCS_RNG.1)

204 The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the [BSI-AIS31](#) standard for a P2 class device.

8.9 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES])

205 The TOE provides an EDES+ accelerator that has the capability to perform the following standard DES cryptographic operations, conformant to [FIPS PUB 46-3](#), with intrinsic counter-measures against fault attacks (FA), DEMA and DPA attacks:

- DES encryption,
- DES decryption,
- Triple DES encryption,
- Triple DES decryption.

206 The EDES+ accelerator offers a Cipher Block Chaining (CBC) mode conformant to [ISO/IEC 10116](#).

8.10 Cryptographic operation: RSA operation (FCS_COP.1 [RSA]) if Neslib only

- 207 The cryptographic library Neslib provides the RSA public key cryptographic operation for modulus sizes up to 4096 bits, conformant to [PKCS #1 V2.1](#).
- 208 The cryptographic library Neslib provides the RSA private key cryptographic operation with or without CRT for modulus sizes up to 4096 bits, conformant to [PKCS #1 V2.1](#).

8.11 Cryptographic operation: AES operation (FCS_COP.1 [AES]) if Neslib only

- 209 The cryptographic library Neslib provides an AES the following standard AES cryptographic operations for key sizes of 128, 192 and 256 bits, conformant to [FIPS PUB 197](#) with intrinsic counter-measures against attacks:
- randomize,
 - key expansion,
 - cipher,
 - inverse cipher.

8.12 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1 [ECC]) if Neslib only

- 210 The cryptographic library Neslib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields, all conformant to [IEEE 1363-2000](#) and [IEEE 1363a-2004](#):
- private scalar multiplication,
 - preparation of Elliptic Curve computations in affine coordinates,
 - public scalar multiplication,
 - point validity check,
 - Jacobian conversion to affine coordinates,
 - general point addition,
 - point expansion and compression.

8.13 Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only

- 211 The cryptographic library Neslib provides the SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 secure hash functions conformant to [FIPS PUB 180-1](#), [FIPS PUB 180-2](#), [ISO/IEC 10118-3:1998](#).

8.14 Cryptographic key generation: Prime generation (FCS_CKM.1 [Prime_generation]) if Neslib only

212 The cryptographic library Neslib provides prime numbers generation for key sizes up to 2048 bits conformant to [FIPS PUB 140-2](#) and [FIPS PUB 186](#).

8.15 Cryptographic key generation: Protected Prime generation (FCS_CKM.1 [PROTECTED_Prime_generation]) if Neslib only

213 The cryptographic library Neslib provides prime numbers generation for key sizes up to 2048 bits conformant to [FIPS PUB 140-2](#) and [FIPS PUB 186](#), and offering resistance against side channel and fault attacks.

8.16 Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_Key_generation]) if Neslib only

214 The cryptographic library Neslib provides standard RSA public and private key computation for key sizes upto 4096 bits conformant to [FIPS PUB 140-2](#), [ISO/IEC 9796-2](#) and [PKCS #1 V2.1](#).

8.17 Cryptographic key generation: PROTECTED RSA key generation (FCS_CKM.1 [PROTECTED_RSA_Key_generation]) if Neslib only

215 The cryptographic library Neslib provides standard RSA public and private key computation for key sizes upto 4096 bits conformant to [FIPS PUB 140-2](#), [ISO/IEC 9796-2](#) and [PKCS #1 V2.1](#), and offering resistance against side channel and fault attacks.

8.18 Static attribute initialisation (FMT_MSA.3)

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

8.19 Management of security attributes (FMT_MSA.1) & Specification of management functions (FMT_SMF.1)

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

8.20 Complete access control (FDP_ACC.2) & Security attribute based access control (FDP_ACF.1)

- 218 The TOE enforces the dynamic memory protection policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), programmed by the ES. Overriding the MPU set of access rights, the TOE enforces:
- an additional protection of the NVM sectors against modification (write and erase), programmed by the ES,
 - a permanent protection of the OST ROM and, in User configuration, a protection of the ST NVM against write accesses.

9 References

219 Protection Profile reference

Component description	Reference	Revision
Security IC Platform Protection Profile	BSI-PP-0035	1.0

220 Security Target references

Component description	Reference
SC23Z018A and 7 derivative products with optional cryptographic library NESLIB 3.1 Security Target	SMD_SC23Z018_ST_12_001

221 Guidance documentation references

Component description	Reference	Revision
SC23Z018: Smartcard MCU with enhanced security, crypto-processor, 18 KByte EEPROM - Datasheet	DS_23Z018	0.4
SB23Z012/SC23Z018 and derivative devices - Security guidance	AN_SECU_Sx23Z0xx	1
ST23 AIS31 compliant random number user manual	UM_23_AIS31	2
ST23 AIS31 Reference implementation - Startup, online and total failure tests - User manual	AN_23_AIS31	2
ST21/23 programming manual	PM_21_23	3
ST23 NesLib 3.1 cryptographic library user manual	UM_23_NESLIB_3.1	5
How to identify certified HW devices using additional ST traceability information	AN_TRACE	2
Application Note - Recommendations for use of EEPROM in SC23Z018, SB23Z012 and derivative devices	AN_Sx23Z01x_EEPROM	1

222 Standards references

Ref	Identifier	Description
[1]	BSI-AIS31	A proposal for Functionality classes and evaluation methodology for true (physical) random number generators, W. Killmann & W. Schindler BSI, Version 3.1, 25-09-2001
[2]	FIPS PUB 46-3	FIPS PUB 46-3, Data encryption standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, 1999

Ref	Identifier	Description
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, U.S. Department of Commerce, 1999
[4]	FIPS PUB 180-1	FIPS PUB 180-1 Secure Hash Standard, National Institute of Standards and Technology, U.S. Department of Commerce, 1995
[5]	FIPS PUB 180-2	FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004
[6]	FIPS PUB 186	FIPS PUB 186 Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S.A., 1994
[7]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, 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]	ISO/IEC 9797-1	ISO/IEC 9797, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, ISO, 1999
[10]	ISO/IEC 10116	ISO/IEC 10116, Information technology - Security techniques - Modes of operation of an n-bit block cipher algorithm, ISO, 1997
[11]	ISO/IEC 10118-3:1998	Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions
[12]	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
[13]	CCMB-2009-07-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009, version 3.1 Revision 3
[14]	CCMB-2009-07-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009, version 3.1 Revision 3
[15]	CCMB-2009-07-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, version 3.1 Revision 3
[16]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[17]	MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
[18]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[19]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004

Ref	Identifiant	Description
[20]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[21]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[22]	NOTE 12.1	Note d'application: Modélisation formelle des politiques de sécurité d'une cible d'évaluation NOTE/12.1, N°587/SGDN/DCSSI/SDR DCSSI, 25-03-2008

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.

Differential Power Analysis (DPA)

An analysis in variations of the electrical power consumption of a device, using advanced statistical methods and/or error correction techniques, for the purpose of extracting information correlated to secrets processed in the device. When several consumption traces are recombined during analysis to remove counter-measures adding random, the analysis is known as Higher Order DPA (HODPA).

Dual mode

Contact and contactless I/O modes.

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

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

IC Dedicated Software

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

IC Dedicated Test Software

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

IC developer

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

IC manufacturer

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

IC packaging manufacturer

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

Initialisation data

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

Object

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

Packaged IC

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

Pre-personalization data

Any data supplied by the Card Manufacturer that is injected into the non-volatile memory by the Integrated Circuits manufacturer (Phase 3). These data are for instance used for traceability and/or to secure shipment between phases.

Secret

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

Security IC

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

Security IC Embedded SoftWare (ES)

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

Security IC embedded software (ES) developer

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

Security attribute

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

Sensitive information

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

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

Secure Microcontroller

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

Simple Power Analysis (SPA)

A direct analysis, primarily visual, of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a device, for the purpose of revealing the features and implementations of (cryptographic) algorithms and subsequently the values of the secrets they process in the device.

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 either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

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.

Warm reset

Reset operation on the TOE without lowering power under the Power on Reset (POR) level.

A.2 Abbreviations

Table 13. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI)
ALU	Arithmetical and Logical Unit.
API	Application Programming Interface.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Securite des Systemes d'Information.
DEMA	Differential Electromagnetic Analysis.
DES	Data Encryption Standard.
DIP	Dual-In-Line Package.
DPA	Differential Power Analysis.
DSW	IC Proprietary Dedicated Software.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
ECC	Elliptic Curves Cryptography or Error Correcting Code.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.

Table 13. List of abbreviations (continued)

Term	Meaning
EMA	Electromagnetic Analysis.
ES	Security IC Embedded Software.
FIPS	Federal Information Processing Standard.
HODPA	High Order Differential Power Analysis.
I2C	Inter-integrated circuit.
I/O	Input / Output.
IART	ISO-7816 Asynchronous Receiver Transmitter.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
OST	Operating System for Test.
OTP	One Time Programmable.
POR	Power On Reset.
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.
SMD	Secure Microcontrollers Division.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or Security Target.
ST-ROM	ST reserved ROM.
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.

Table 13. List of abbreviations (continued)

Term	Meaning
TSFI	TSF Interface.
TSP	TOE Security Policy.
USR_ROM	User reserved ROM.

10 Revision history

Table 14. Document revision history

Date	Revision	Changes
08-Jan-2013	01.00	Initial release.
18-Feb-2013	01.01	Reference documents updated.
26-Feb-2013	01.02	Reference documents updated.
02-Apr-2013	01.03	Reference documents updated.
03-Sep-2013	01.04	Reference documents updated.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries ("ST") reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST's terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST'S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY AN AUTHORIZED ST REPRESENTATIVE, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER'S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2013 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com

