STMicroelectronics

ST31 - K330A
version I (contact mode only), with optional cryptographic library NESLIB 3.2

SECURITY TARGET FOR COMPOSITION

Common Criteria for IT security evaluation

SMD_SC31Zxxx_ST_13_002 Rev 02.02

March 2017

www.st.com

BLANK

ST31 - K330A
Security Target for Composition

Common Criteria for IT security evaluation

1 Introduction

1.1 Security Target reference

1 Document identification: ST31 - K330A version I (contact mode only), with optional cryptographic library Neslib 3.2 SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev 02.02, issued March 2017.

3 Registration: registered at ST Microelectronics under number SMD_SC31Zxxx_ST_13_002.

1.2 Purpose

4 This document presents **the Security Target for Composition (ST)** of the **ST31 - K330A** Security Integrated Circuits (IC), designed on the **ST31 platform of STMicroelectronics**, with Dedicated Software (DSW), and optional cryptographic library **Neslib 3.2**.

5 The precise reference of the Target of Evaluation (TOE) and the security IC features are given in *Section 3: TOE description*.

6 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 . . . 9

3 TOE description . . . 10

3.1 TOE identification . . . 10

3.2 TOE overview . . . 11

3.3 TOE life cycle . . . 13

3.4 TOE environment . . . 14

3.4.1 TOE Development Environment . . . 14

3.4.2 TOE production environment . . . 15

3.4.3 TOE operational environment . . . 15

4 Conformance claims . . . 17

4.1 Common Criteria conformance claims . . . 17

4.2 PP Claims . . . 17

4.2.1 PP Reference . . . 17

4.2.2 PP Refinements . . . 17

4.2.3 PP Additions . . . 17

4.2.4 PP Claims rationale . . . 17

5 Security problem definition . . . 19

5.1 Description of assets . . . 19

5.2 Threats . . . 20

5.3 Organisational security policies . . . 21

5.4 Assumptions . . . 21

6 Security objectives . . . 22

6.1 Security objectives for the TOE . . . 22

6.2 Security objectives for the environment . . . 23

6.3 Security objectives rationale . . . 23

6.3.1 TOE threat "Memory Access Violation" 24
6.3.2 Organisational security policy "Additional Specific Security Functionality" 25

7 Security requirements 26
7.1 Security functional requirements for the TOE 26
7.1.1 Security Functional Requirements from the Protection Profile 27
7.1.2 Additional Security Functional Requirements for the cryptographic services 29
7.1.3 Additional Security Functional Requirements for the memories protection 31
7.2 TOE security assurance requirements 32
7.3 Refinement of the security assurance requirements 33
7.3.1 Refinement regarding functional specification (ADV_FSP) 34
7.3.2 Refinement regarding test coverage (ATE_COV) 34
7.4 Security Requirements rationale 35
7.4.1 Rationale for the Security Functional Requirements 35
7.4.2 Additional security objectives are suitably addressed 36
7.4.3 Additional security requirements are consistent 36
7.4.4 Dependencies of Security Functional Requirements 37
7.4.5 Rationale for the Assurance Requirements 38

8 TOE summary specification 40
8.1 Limited fault tolerance (FRU_FLT.2) 40
8.2 Failure with preservation of secure state (FPT_FLS.1) 40
8.3 Limited capabilities (FMT_LIM.1) 40
8.4 Limited availability (FMT_LIM.2) 40
8.5 Audit storage (FAU_SAS.1) 41
8.6 Resistance to physical attack (FPT_PHP.3) 41
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) 41
8.8 Random number generation (FCS_RNG.1) 41
8.9 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES]) . 41
8.10 Cryptographic operation: AES operation (FCS_COP.1 [AES]) 42
8.11 Cryptographic operation: RSA operation (FCS_COP.1 [RSA]) if Neslib only 42

8.12 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1 [ECC]) if Neslib only 42
8.13 Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only 42
8.14 Cryptographic key generation: Prime generation (FCS_CKM.1 [Prime_generation]) & Cryptographic key generation: Protected prime generation (FCS_CKM.1 [Protected_prime_generation]) if Neslib only . . 43
8.15 Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_key_generation]) & Cryptographic key generation: Protected RSA key generation (FCS_CKM.1 [Protected_RSA_key_generation]) if Neslib only 43
8.16 Static attribute initialisation (FMT_MSA.3) [Memories] 43
8.17 Management of security attributes (FMT_MSA.1) [Memories] & Specification of management functions (FMT_SMF.1) [Memories] 43
8.18 Complete access control (FDP_ACC.2) [Memories] & Security attribute based access control (FDP_ACF.1) [Memories] 43

9 References 44

Appendix A Glossary 47

A.1 Terms. 47
A.2 Abbreviations. 49

10 Revision history 51

List of tables

Table 1. TOE identification . . . 10
Table 2. Derivative devices configuration possibilities . . . 10
Table 3. Composite product life cycle phases . . . 14
Table 4. Summary of security environment . . . 19
Table 5. Summary of security objectives . . . 22
Table 6. Security Objectives versus Assumptions, Threats or Policies . . . 24
Table 7. Summary of functional security requirements for the TOE . . . 26
Table 8. FCS_COP.1 iterations (cryptographic operations) . . . 29
Table 9. FCS_CKM.1 iterations (cryptographic key generation). . . . 30
Table 10. TOE security assurance requirements . . . 32
Table 11. Impact of EAL5 selection on *BSI-PP-0035* refinements . . . 33
Table 12. Dependencies of security functional requirements . . . 37
Table 13. List of abbreviations . . . 49
Table 14. Document revision history . . . 51

List of figures

Figure 1. ST31 - K330A block diagram 13

2 Context

7 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).

8 The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

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

10 This ST claims to be an instantiation of the "*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 augmentations from *AUG* as indicated here, when they are reproduced in this document.

11 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 identification

12 The Target of Evaluation (TOE) is the ST31 - K330A version I (contact mode only), with the optional cryptographic library Neslib 3.2, with guidance documentation.

Table 1. TOE identification

IC Maskset name	Maskset Major version	IC version	Master identification number (1)	OST name(1)	OST version (1)	Optional crypto library name & version(2)
K330A	A	I	0033h	YGE	0014h	Neslib 3.2 1320h

1. Part of the product information.
2. See the Neslib User Manual referenced in *Section 9* .

13 The IC maskset name is the product hardware identification.
The maskset major version is updated when the full maskset is changed (i.e. all layers of the maskset are changed at the same time).
The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST software.
The maskset name with major version and IC version (i.e. K330A version I) fully identify the IC (hardware and OST).

14 The K330A version I, is dedicated to contact mode only. Its antenna pads are deactivated.

15 Different derivative devices may be configured by ST during the manufacturing or packaging process, depending on the customer needs. They all share the same hardware design and the same maskset.

16 The configuration of the derivative devices can impact the available NVM memory size,and the availability of Nescrypt, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
NVM size	52 Kbytes, 38 Kbytes, 22 Kbytes, 16 Kbytes
Nescrypt	Active, Inactive

17 All combinations of different features values are possible and covered by this certification. All possible configurations can vary under a unique IC (i.e. K330A), and without impact on security.

18 The Master identification number is unique for all product configurations.
Each derivative device has a specific Child product identification number, also part of the product information, and specified in the Data Sheet, referenced in *Section 9*.

19 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: TOE identification*, and the configuration elements as detailed in the Data Sheet, referenced in *Section 9*.

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

3.2 TOE overview

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

22 The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks. The AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. The 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (DES *[2]*), enabling Cipher Block Chaining (CBC) mode, fast DES and triple DES computation. If Nescrypt is active, the NESCRYPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance (*[4]*, *[8]*, *[12]*, *[18]*,*[19]*, *[20]*, *[21]*).

As randomness is a key stone in many applications, the ST31 - K330A features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS31 *[1]* and directly accessible thru dedicated registers.

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

23 The TOE offers a contact serial communication interface fully compatible with the ISO/IEC 7816-3 standard. The contactless interface is deactivated.

24 In a few words, the ST31 - K330A 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,
- Hardware Security Enhanced DES accelerator,
- True Random Number Generator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- optional NExt Step CRYPTography accelerator (NESCRYPT),
- optional cryptographic library.

25 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.

26 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.

27 The TOE 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.

Neslib is embedded by the ES developper in his applicative code.
Note that Neslib can only be used if Nescrypt is active.

Neslib provides the most useful operations in public key algorithms and protocols:

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[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 functions (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 *[4]*),
- prime number generation *[6]*.

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

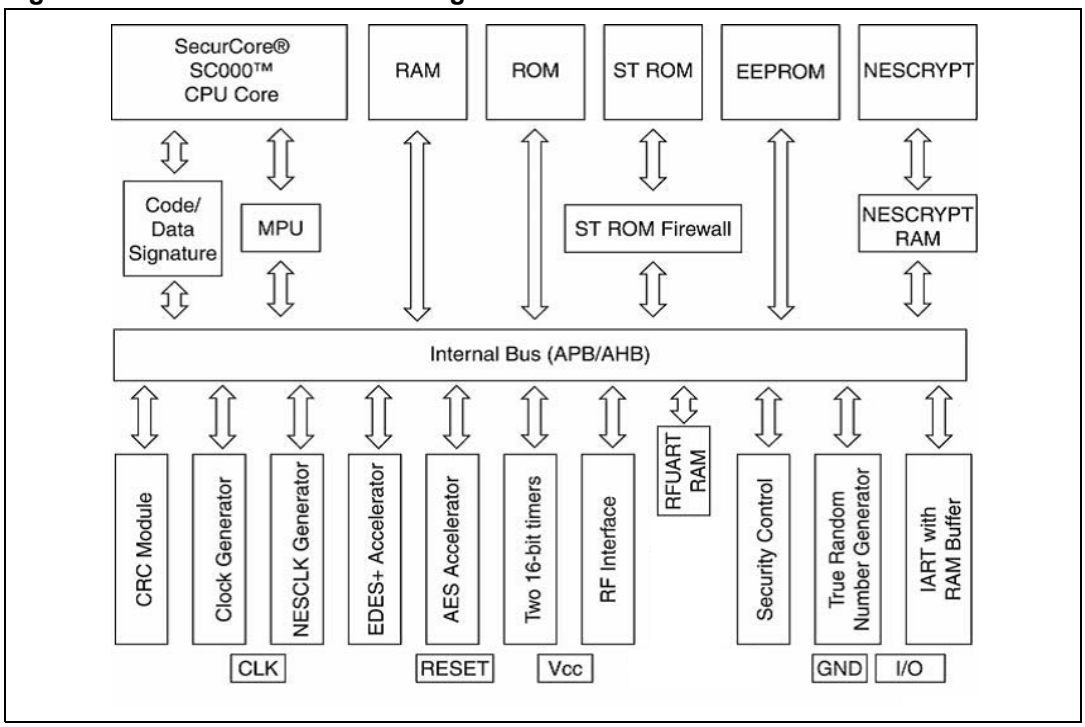
- the product Data Sheet and die description,
- the product family Security Guidance,
- the AIS31 user manuals,
- the product family programming manual,
- the ARM SC000 Technical Reference Manual,
- optionally the Neslib user manual.

29 The complete list of guidance documents is detailed in *Section 9*.

30 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. It will not be present on the field (Phase 7).

31 *Figure 1* provides an overview of the ST31 - K330A.

Figure 1. ST31 - K330A block diagram



3.3 TOE life cycle

32 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.

33 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.

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

35 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.

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

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

38 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.

39 The TOE is delivered in USER configuration.

Table 3. Composite product life cycle phases

Phase	Name	Description	Responsible party
1	IC embedded software development	security IC embedded software development specification of IC pre-personalization requirements	IC embedded software developer
2	IC development	IC design IC dedicated software development	IC developer: **ST**
3	IC manufacturing	integration and photomask fabrication IC production IC testing pre-personalisation	IC manufacturer: **ST**
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary	IC packaging manufacturer: **ST** or **SMARTFLEX**
5	Composite product integration	composite product finishing process composite product testing	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

3.4 TOE environment

40 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.

3.4.1 TOE Development Environment

41 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.

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

43 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).

44 The development centres involved in the development of the TOE are the following: **ST ROUSSET (FRANCE), ST ANG MO KIO (SINGAPORE)**, **ST SOPHIA (FRANCE)**, **ST GRENOBLE (FRANCE)**, **ST RENNES (FRANCE), ST GARDANNE (FRANCE)** and **ST ZAVENTEM (BELGIUM)**.

45 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).

46 The authorized sub-contractors involved in the TOE mask manufacturing can be **DNP (JAPAN)** and **DPE (ITALY)**.

3.4.2 TOE production environment

47 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.

48 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.

49 The authorized front-end plant involved in the manufacturing of the TOE can be **ST ROUSSET (FRANCE)** or **ST CROLLES (FRANCE)**.

50 The authorized EWS plant involved in the testing of the TOE can be **ST ROUSSET (FRANCE)** or **ST TOA PAYOH (SINGAPORE)**.

51 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.

52 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 (THE PHILIPPINES), ST SHENZEN (CHINA), ST ANG MO KIO (SINGAPORE)**, or **SMARTFLEX (SINGAPORE)**.

53 All ST back-end plants listed above, plus **ST LOYANG (SINGAPORE)** and **ST ROUSSET (FRANCE)** can be involved for the logistics.

54 **ST TUNIS (TUNISIA)** can be involved as an IT center.

3.4.3 TOE operational environment

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

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

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

4 Conformance claims

4.1 Common Criteria conformance claims

58 The ST31 - K330A Security Target claims to be conformant to the Common Criteria version 3.1 revision 4.

59 Furthermore it claims to be CC Part 2 (*CCMB-2012-09-002*) extended and CC Part 3 (*CCMB-2012-09-003*) conformant. The extended Security Functional Requirements are those defined in the *Security IC Platform Protection Profile* (*BSI-PP-0035*).

60 The assurance level for the ST31 - K330A Security Target is ***EAL 5*** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

61 The ST31 - K330A 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

62 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.

63 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

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

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

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

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

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

4.2.4 PP Claims rationale

69 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.

70 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*.

71 The security problem definition presented in *Section 5*, clearly shows the additions to the security problem statement of the PP.

72 The security objectives rationale presented in *Section 6.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-PP-0035*.

73 Similarly, the security requirements rationale presented in *Section 7.4* has been updated with respect to the protection profile.

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

5 Security problem definition

75 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.

76 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Security IC Platform Protection Profile* (*BSI-PP-0035*), section 3. Only those originating in *AUG* are detailed in the following sections.

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

5.1 Description of assets

78 Since this Security Target claims strict conformance to the *Security IC Platform Protection Profile* (*BSI-PP-0035*), the assets defined in section 3.1 of the Protection Profile are applied and the assets regarding threats are clarified in this Security Target.

79 The assets regarding the threats are:

- logical design data, physical design data, IC Dedicated Software, and configuration data,
- Initialisation data and pre-personalisation data, specific development aids, test and characterisation related data, material for software development support, and photomasks and product in any form,
- the TOE correct operation,
- the Security IC Embedded Software, stored and in operation,
- the security services provided by the TOE for the Security IC Embedded Software,
- the cryptographic co-processors for Triple-DES and AES, the random number generator,
- the TSF Data.

80 This Security Target includes optionally Security IC Embedded Software and therefore does contain more assets compared to *BSI-PP-0035*. These assets are described above.

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

Table 4. Summary of security environment

	Label	Title
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

81 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

82 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.

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

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

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),
- ***Elliptic Curves Cryptography on GF(p),*** if Neslib is embedded only***,***
- ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if Neslib is embedded only***,***
- Rivest-Shamir-Adleman (RSA)***,*** if Neslib is embedded only,
- ***Prime Number Generation,*** if 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

85 The following 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

86 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.

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

88 Note that the origin of each objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the 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	Additional Specific Security Functionality: The TOE must 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), – ***Elliptic Curves Cryptography on GF(p),*** if Neslib is embedded only***,*** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if Neslib is embedded only***,*** – Rivest-Shamir-Adleman (RSA)***,*** if Neslib is embedded only, – ***Prime Number Generation,*** if Neslib is embedded only***.***
AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control: The TOE must provide the ***Security IC*** Embedded Software with the capability to define ***dynamic memory segmentation and protection***. The TOE must then enforce ***the defined access rules*** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

6.2 Security objectives for the environment

89 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

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

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

6.3 Security objectives rationale

91 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.

92 Thus, it is necessary to show that:

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

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

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

94 As required by CC part 1 (*CCMB-2012-09-001*), 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.

95 The justification of the additional policies, additional threats, and additional assumptions 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
BSI.A.Plat-Appl	*BSI.OE.Plat-Appl*	Phase 1
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 4-6
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func*	
BSI.T.RND	*BSI.O.RND*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	

6.3.1 TOE threat "Memory Access Violation"

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

97 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.

98 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"

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

100 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.

101 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*.

102 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

103 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

104 Security Functional Requirements (SFRs) from the "*BSI-PP-0035*" Protection Profile (PP) are drawn from *CCMB-2012-09-002*, except the following SFRs, that are **extensions** to *CCMB-2012-09-002*:

- **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.

105 All extensions to the SFRs of the "*BSI-PP-0035*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2012-09-002*.

106 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2012-09-001*. 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.

107 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.

108 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-2012-09-002*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1	Limited capabilities	Abuse of TEST 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-2012-09-002*
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-2012-09-002*
FCS_CKM.1 (if Neslib is embedded only)	Cryptographic key generation		Security Target Operated	
FDP_ACC.2 [Memories]	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1 [Memories]	Security attribute based access control		*AUG* #4 Operated	
FMT_MSA.3 [Memories]	Static attribute initialisation	Correct operation		
FMT_MSA.1 [Memories]	Management of security attribute			
FMT_SMF.1 [Memories]	Specification of management functions		Security Target Operated	

7.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

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

Failure with preservation of secure state (FPT_FLS.1)

110 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.***

111 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.

Limited capabilities (FMT_LIM.1)

112 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.

Limited availability (FMT_LIM.2)

113 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.

114 *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.

Audit storage (FAU_SAS.1)

115 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***.

Resistance to physical attack (FPT_PHP.3)

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

117 Refinement:

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

Basic internal transfer protection (FDP_ITT.1)

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

Basic internal TSF data transfer protection (FPT_ITT.1)

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

120 Refinement:

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

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

Subset information flow control (FDP_IFC.1)

121 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***.

122 *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.

Random number generation (FCS_RNG.1)

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

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

7.1.2 Additional Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

125 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	
Even without Neslib	AES	* encryption (cipher) * decryption (inverse cipher) * key expansion * randomize	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS PUB 197*

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	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*
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 * Protected SHA-1	Secure Hash Algorithm	assignment pointless because algorithm has no key	*FIPS PUB 180-1* *FIPS PUB 180-2* *ISO/IEC 10118-3:1998*

Cryptographic key generation (FCS_CKM.1)

126 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*

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

Iteration label	[assignment: cryptographic key generation algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
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*

7.1.3 Additional Security Functional Requirements for the memories protection

Static attribute initialisation (FMT_MSA.3) [Memories]

127 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.

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

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

Management of security attributes (FMT_MSA.1) [Memories]

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

Complete access control (FDP_ACC.2) [Memories]

130 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.

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

Security attribute based access control (FDP_ACF.1) [Memories]

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

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

a. See the Datasheet referenced in *Section 9* for actual values.

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

135 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***in User configuration, any access (read, write, execute) to the OST ROM is denied, and in User configuration, any write access to the ST NVM is denied.***

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.

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

137 SFP_3: Dynamic Memory Access Control Policy

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

Specification of management functions (FMT_SMF.1) [Memories]

139 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 privileged mode, supporting the Dynamic Memory Access Control Policy.***

7.2 TOE security assurance requirements

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

- ALC_DVS.2 and AVA_VAN.5.

141 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.

142 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-stuctured 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*

Table 10. TOE security assurance requirements (continued)

Label	Title	Origin
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

143 As *BSI-PP-0035* defines refinements for selected SARs, these refinements are also claimed in this Security Target.

144 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.

145 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.

146 The text of the impacted refinements of *BSI-PP-0035* is reproduced in the next sections.

147 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

Table 11. Impact of EAL5 selection on *BSI-PP-0035* refinements (continued)

Assurance Family	*BSI-PP-0035* Level	ST Level	Impact on refinement
AGD_PRE	1	1	None
AVA_VAN	5	5	None

7.3.1 Refinement regarding functional specification (ADV_FSP)

148 ~~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.***

149 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.

150 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.

151 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.

152 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.

153 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)

154 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).

155 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).

156 ~~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

157 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.

158 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 7*, 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.

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

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

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

161 Though it remains to show that:

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

162 The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those already in *BSI-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*)”

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

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

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

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

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

167 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*.

7.4.3 Additional security requirements are consistent

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

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

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

169 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

170 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 justifed in *AUG* security requirements rationale (except on FMT_MSA.2, see discussion below),
- the dependency of *FCS_COP.1* and *FCS_CKM.1* on FCS_CKM.4 (see discussion below).

171 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 *BSI-PP-0035* or in *AUG*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-PP-0035*
FPT_FLS.1	None	No dependency	Yes, *BSI-PP-0035*
FMT_LIM.1	FMT_LIM.2	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2	FMT_LIM.1	Yes	Yes, *BSI-PP-0035*
FAU_SAS.1	None	No dependency	Yes, *BSI-PP-0035*
FPT_PHP.3	None	No dependency	Yes, *BSI-PP-0035*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, *BSI-PP-0035*
FPT_ITT.1	None	No dependency	Yes, *BSI-PP-0035*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-PP-0035*	Yes, *BSI-PP-0035*
FCS_RNG.1	None	No dependency	Yes, *BSI-PP-0035*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes, by FDP_ITC.1 and FCS_CKM.1, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.4	No, see discussion below	
FCS_CKM.1	[FDP_CKM.2 or FCS_COP.1]	Yes, by FCS_COP.1	
	FCS_CKM.4	No, see discussion below	
FDP_ACC.2 [Memories]	FDP_ACF.1 [Memories]	Yes	***No,*** *CCMB-2012-09-002*
FDP_ACF.1 [Memories]	FDP_ACC.1 [Memories]	Yes, by FDP_ACC.2 [Memories]	Yes, *AUG* ***#4***
	FMT_MSA.3 [Memories]	Yes	
FMT_MSA.3 [Memories]	FMT_MSA.1 [Memories]	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	

Table 12. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FMT_MSA.1 [Memories]	[FDP_ACC.1 [Memories] or FDP_IFC.1]	Yes, by FDP_ACC.2 [Memories] and FDP_IFC.1	Yes, *AUG* ***#4***
	FMT_SMF.1 [Memories]	Yes	***No,*** *CCMB-2012-09-002*
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	Yes, *AUG* ***#4***
FMT_SMF.1 [Memories]	None	No dependency	***No,*** *CCMB-2012-09-002*

172 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.

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

7.4.5 Rationale for the Assurance Requirements

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

174 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.

175 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.

176 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.

177 Note that detailed and updated refinements for assurance requirements are given in *Section 7.3*.

Dependencies of assurance requirements

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

179 Augmentation to this package are identified in paragraph *139* and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

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

181 The complete TOE summary specification has been presentad and evaluated in the ST31 - K330A version I (contact mode only) with optional cryptographic library Neslib 3.2 SECURITY TARGET.

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

8.1 Limited fault tolerance (FRU_FLT.2)

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

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

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

- Die integrity violation detection,
- Errors on memories,
- Glitches,
- High voltage supply,
- CPU errors,
- MPU errors,
- External clock incorrect frequency,
- etc..

185 The ES can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1)

186 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)

187 The TOE is either in TEST,or USER configuration.

188 The only authorised TOE configuration modification is:

- TEST to USER configuration.

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

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

8.5 Audit storage (FAU_SAS.1)

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

8.6 Resistance to physical attack (FPT_PHP.3)

192 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)

193 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)

194 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])

195 The TOE provides an EDES accelerator that has the capability to perform DES and Triple DES encryption and decryption conformant to FIPS PUB 46-3.

196 The EDES accelerator offers a Cipher Block Chaining (CBC) mode conformant to ISO/IEC 10116, and a Cipher Block Chaining Message Authentication Code (CBC-MAC) mode conformant to ISO/IEC 9797-1.

8.10 Cryptographic operation: AES operation (FCS_COP.1 [AES])

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

- randomize,
- key expansion,
- cipher,
- inverse cipher.

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

198 The cryptographic library Neslib provides the RSA public key cryptographic operation for modulus sizes up to 4096 bits, conformant to PKCS #1 V2.1.

199 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.

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

200 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, including:

- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check.

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

201 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.

202 The cryptographic library Neslib provides the SHA-1 secure hash function conformant to FIPS PUB 180-1, FIPS PUB 180-2, ISO/IEC 10118-3:1998, and offering resistance against side channel and fault attacks.

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

203 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.

8.15 Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_key_generation]) & Cryptographic key generation: Protected RSA key generation (FCS_CKM.1 [Protected_RSA_key_generation]) if Neslib only

204 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.

8.16 Static attribute initialisation (FMT_MSA.3) [Memories]

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

8.17 Management of security attributes (FMT_MSA.1) [Memories] & Specification of management functions (FMT_SMF.1) [Memories]

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

8.18 Complete access control (FDP_ACC.2) [Memories] & Security attribute based access control (FDP_ACF.1) [Memories]

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

9 References

208 Protection Profile references

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

209 ST31 - K330A Security Target reference

Component description	Reference
ST31 - K330A version I (contact mode only) with optional cryptographic library Neslib 3.2 SECURITY TARGET	SMD_SC31Zxxx_ST_13_001

210 Guidance documentation references

Component description	Reference	Revision
ST31 - K330 platform - Sx31Zxxx, Mx31Zxxx - Secure dual interface microcontrolleer with enhanced security and up to 52 Kbytes of EEPROM - Datasheet	DS_ST31Z052	7
ST31 - K330 platform 90nm F10 CMOS die description	DD_31Z052	5
ARM SC000 Technical Reference Manual - R0P0	ARM DDI 0456	A
ARM v6-M Architecture Reference Manual	ARM DDI 0419	C
ST31 - K330 Security guidance	AN_SECU_ST31_K330	4
ST31 - AIS31 Compliant Random Number user manual	UM_31_AIS31	2
ST31 - AIS31 Reference implementation - Startup, online and total failure tests - Application Note	AN_31_AIS31	2
ST31 NesLib cryptographic library User manual	UM_31_NESLIB_3.2	7
ST31-K330 and ST33-K8H0 secure microcontrollers - Power supply glitch detector characteristics	AN_31_GLITCH	2

211 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
[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

Ref	Identifier	Description
[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	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-2012-09-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012, version 3.1 Revision 4
[14]	CCMB-2012-09-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012, version 3.1 Revision 4
[15]	CCMB-2012-09-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012, version 3.1 Revision 4
[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	Identifier	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

Appendix A Glossary

A.1 Terms

Authorised user

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

Composite product

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

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

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

IC Dedicated Software

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

IC Dedicated Test Software

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

IC developer

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

IC manufacturer

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

IC packaging manufacturer

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

Initialisation data

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

Object

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

Packaged IC

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

Pre-personalization data

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

Secret

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

Security IC

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

Security IC Embedded SoftWare (ES)

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

Security IC embedded software (ES) developer

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

Security attribute

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

Sensitive information

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

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

Smartcard

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

Subject

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

Test features

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

TOE Delivery

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

TSF data

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

User

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

User data

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

A.2 Abbreviations

Table 13. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI)
ALU	Arithmetical and Logical Unit.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CBC-MAC	Cipher Block Chaining Message Authentication Code.
CC	Common Criteria Version 3.1.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DES	Data Encryption Standard.
DIP	Dual-In-Line Package.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
ES	Security IC Embedded SoftWare.
FIPS	Federal Information Processing Standard.
I/O	Input / Output.
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.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.

Table 13. List of abbreviations (continued)

Term	Meaning
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SOIC	Small Outline IC.
ST	Context dependent : STMicroelectronics or Security Target.
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.

10 Revision history

Table 14. Document revision history

Date	Revision	Changes
25-Mar-2013	01.00	Initial release.
03-Nov-2014	02.00	Change in title & sites list. Update of revisions.
06-Nov-2014	02.01	Modification following evaluator’s remarks
20-Mar-2017	02.02	Change in sites and guides.