STMicroelectronics

ST33H768 D01
Security Target for composition

Common Criteria for IT security evaluation

SMD_ST33H768_ST_19_002 D01.0

April 2020

www.st.com

BLANK

ST33H768 D01
Security Target for composition

Common Criteria for IT security evaluation

1 Introduction

1.1 Security Target reference

1 Document identification: ST33H768 D01 - SECURITY TARGET FOR COMPOSITION.

2 Version number: D01.0, issued in April 2020.

3 Registration: registered at ST Microelectronics under number SMD_ST33H768_ST_19_002_D01.0.

1.2 Purpose

4 This document presents **the Security Target for composition (ST)** of the **ST33H768 D01** maskset K8K0A version C Security Integrated Circuit (IC), designed on the **ST33 platform of STMicroelectronics**, with Dedicated Software (DSW) rev 5.

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

List of tables

List of figures

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 IC, and to summarise its 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*
- Additions specific to this Security Target.

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

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

12 This ST makes various refinements to the above mentioned PP and *AUG*. They are all properly identified in the text typeset as ***indicated here***. The original text of the PP is repeated as scarcely as possible in this document for reading convenience. All PP identifiers have been however prefixed by their respective origin label: ***BSI*** for *BSI-PP-0035*, ***AUG1*** for Addition #1 of *AUG* and ***AUG4*** for Addition #4 of *AUG*.

3 TOE description

3.1 TOE identification

13 The Target of Evaluation (TOE) is the ST33H768 D01 platform.

14 “ST33H768 D01” completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Section 9*, and its development and production sites indicated in *Section 9*.

15 D01 is the version of the evaluated platform. Any change in the TOE components, the guidance documentation and the list of sites leads to a new version of the evaluated platform, thus a new TOE.

Table 1. TOE components

IC Maskset name & major version	IC version	Master identification number [1]	Firmware revision	OST revision
K8K0A	C	0098h	5	2.2

[1] Part of the product information. Depending on family extension, see Datasheet and related Technical Notes referenced in *Section 9*.

16 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.

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

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

18 They all share the same hardware design and the same maskset. The Master identification number is unique for all product configurations depending on family extension.

19 The configuration of the derivative devices can impact the available IOs, the available NVM memory size, the availability of the crypto processors and the availability of the LPU, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
SWP	Active, Inactive
SPI	Active, Inactive
IART	Active, Inactive
NVM size	Selectable by 128 Kbytes granularity from 768 Kbytes to 384 Kbytes
Nescrypt	Active, Inactive
EDES+ accelerator	Active, Inactive
AES accelerator	Active, Inactive

Table 2. Derivative devices configuration possibilities

Features	Possible values
Library Protection Unit (LPU)	Active, Inactive
Crypto1	Active, Inactive

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

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

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

3.2 TOE overview

23 The TOE is a serial access Smartcard IC designed for secure mobile applications, based on the most recent generation of ARM® processors for embedded secure systems. Its SecurCore® SC300™ 32-bit RISC core is built on the Cortex™ M3 core with additional security features to help to protect against advanced forms of attacks.

24 The TOE offers a high-speed User Flash memory, an internally generated clock, an MPU, an internal true random number generator (TRNG) and hardware accelerators for advanced cryptographic functions.

25 The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks.
If AES is active, the AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in ECB (Electronic Code Book) and CBC (Cipher Block Chaining) mode.
If EDES+ is active, the 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (DES *[2]*), enabling Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes, 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 (*[6]*, *[11]*,*[12]*, *[13]*, *[14]*).

As randomness is a key stone in many applications, the ST33H768 D01 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 *[1]* and directly accessible through dedicated registers.

This device includes the ARM® SecurCore® SC300™ memory protection unit (MPU), which enables the user to define its own region organization with specific protection and access permissions. The MPU can be used to enforce various protection models, ranging from a basic code dump prevention model up to a full application confinement model.

26 The TOE offers 3 communication channels to the external world: a serial communication interface fully compatible with the ISO/IEC 7816-3 standard, a single-wire protocol (SWP) interface for communication with a near-field communication (NFC) router in SIM/NFC

applications, and an alternative and exclusive SPI Slave interface for communication in non-SIM applications.

27 In a few words, the ST33H768 D01, offers a unique combination of high performances and very powerful features for high level security:

- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- AIS20/AIS31 class PTG.2 compliant True Random Number Generator,
- Memory protections,
- ISO 3309 CRC calculation block,
- optional EDES+ accelerator,
- optional AES accelerator,
- optional Library Protection Unit,
- optional Next Step Cryptography accelerator (NESCRYPT).

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

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

30 The System ROM and ST NVM of the TOE contain a Dedicated Support Software called Secure Flash Loader, enabling to securely and efficiently download the Security IC Embedded Software into the NVM. It also allows the evaluator to load software into the TOE for test purpose. The Secure Flash Loader is not available in User configuration.

31 The System ROM and ST NVM of the TOE contain a Dedicated Support Software, which provides low-level functions (called Flash Drivers), enabling the Security IC Embedded Software (ES) to modify and manage the NVM contents. The Flash Drivers are available all through the product life-cycle.

32 The Security IC Embedded Software (ES) is in User NVM.

The ES is not part of the TOE and is out of scope of the evaluation.

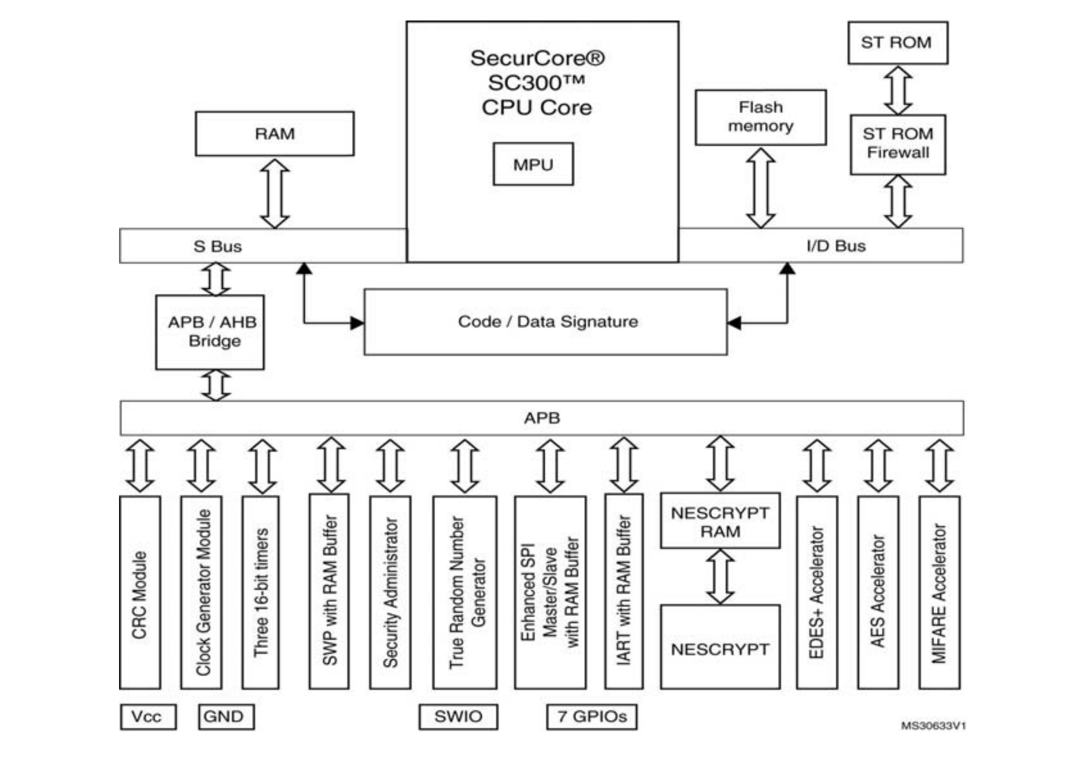
33 The user guidance documentation, part of the TOE, consists of:

- the product Data Sheet and die description,
- optionally the ST33H768 platform Technical Notes,
- the product family Security Guidance,
- the AIS31 user manuals,
- the Cortex M3 SC300 Technical Reference Manuals,
- the Firmware user manual,
- the Flash loader installation guide.

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

35 *Figure 1* provides an overview of the ST33H768 D01.

Figure 1. ST33H768 D01 block diagram



3.3 TOE life cycle

36 This Security Target is fully conform to the claimed PP. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to the *Security IC Platform Protection Profile* (*BSI-PP-0035*), section 1.2.3.

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

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

39 The sites potentially involved in the TOE life cycle are listed in table “Sites list” in *Section 9*.

40 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.

41 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.

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

43 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.

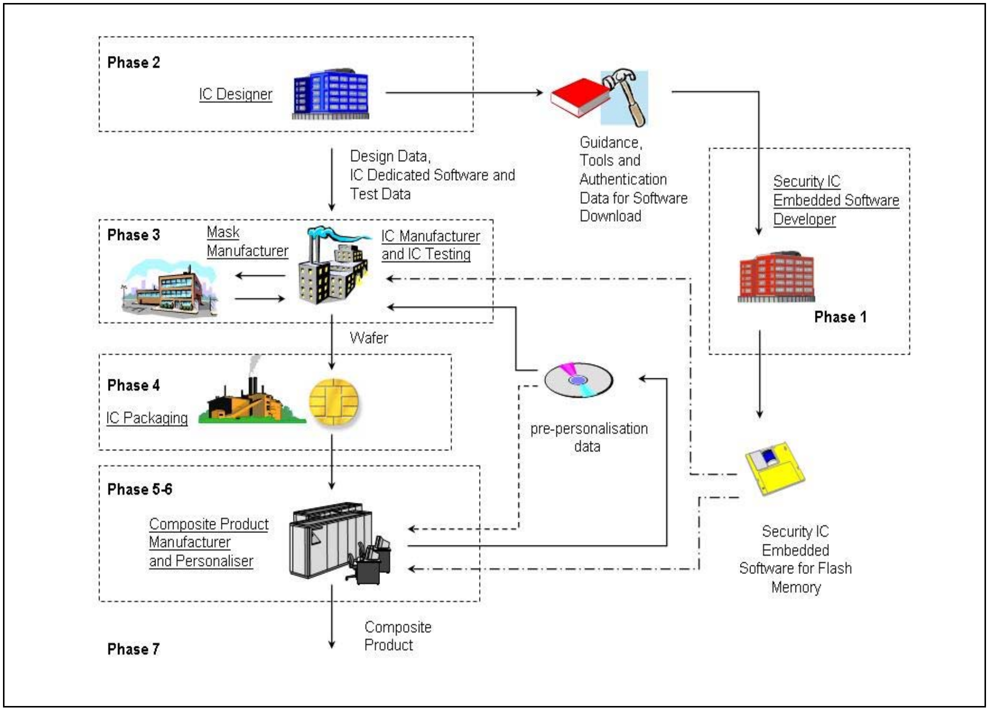
44 The TOE is only delivered in ADMIN (aka ISSUER) or USER configuration, depending on the customer’s request.

Table 3. Composite product life cycle phases

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

45 The following figure shows the possible organization of the life cycle, adapted to the TOE which comprises programmable NVM. Thus, the Security IC Embedded Software may be loaded onto the TOE in phase 3, 4, 5 or 6, depending on customer’s choice.

Figure 2. Security IC life cycle



3.4 TOE environment

46 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

47 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.

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

49 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).

50 The development centres possibly involved in the development of the TOE are denoted by the activity “DEV” in table “Sites list” in *Section 9*.

3.4.2 TOE production environment

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

52 The authorized sub-contractors potentially involved in the TOE mask manufacturing are denoted by the activity “MASK” in table “Sites list” in *Section 9*.

53 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.

54 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. The wafers are then delivered for assembly onto the composite products.

55 The authorized front-end plant possibly involved in the manufacturing of the TOE are denoted by the activity “FE” in table “Sites list” in *Section 9*.

56 The authorized EWS (Electrical Wafer Sort) plants potentially involved in the testing of the TOE are denoted by the activity “EWS” in table “Sites list” in *Section 9*.

57 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.

58 When the product is delivered after phase 4, the authorized back-end plants possibly involved in the packaging of the TOE are denoted by the activity “BE” in table “Sites list” in *Section 9*.

59 All sites denoted by the activity “WHS” in table “Sites list” in *Section 9* can be involved for the logistics.

3.4.3 TOE operational environment

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

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

62 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

63 The ST33H768 D01 Security Target claims to be conformant to the Common Criteria version 3.1 revision 5.

64 Furthermore it claims to be CC Part 2 (*CCMB-2017-04-002*) extended and CC Part 3 (*CCMB-2017-04-003*) conformant. The extended Security Functional Requirements are those defined in the *Security IC Platform Protection Profile* (*BSI-PP-0035*).

65 The assurance level for the ST33H768 D01 Security Target is ***EAL 5*** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

66 The ST33H768 D01 Security Target claims strict conformance to the *Security IC Platform Protection Profile* (*BSI-PP-0035*), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

4.2.2 PP Refinements

67 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*,
- Specific additions for the Secure Flash Loader
- Refinement of assurance requirements.

68 All refinements versus the PP 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

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

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

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

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

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

4.2.4 PP Claims rationale

74 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.

75 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*.

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

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

78 The security requirements rationale presented in *Section 7.4* has been updated with respect to the protection profile.

79 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

80 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.

81 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*, and the one introduced in this Security Target, are detailed in the following sections.

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

5.1 Description of assets

83 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.

84 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.

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

SC4 deficiency of random numbers.

86 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.

87 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***.

88 Application note:
The TOE providing a functionality for Security IC Embedded Software secure loading into NVM, the ES is considered as User Data being stored in the TOE's memories at this step, and the Protection Profile security concerns are extended accordingly.

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
	T.Confid-Applic-Code	Application code confidentiality
	T.Confid-Applic-Data	Application data confidentiality
	T.Integ-Applic-Code	Application code integrity
	T.Integ-Applic-Data	Application data integrity
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
	P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.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.

90 The following additional threats are related to Application protection.

T.Confid-Applic-Code Application code confidentiality:

A sensitive application code may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to memory area where the sensitive application executable code is stored. The attacker executes an application to disclose code belonging to the sensitive application.

T.Confid-Applic-Data Application data confidentiality:

A sensitive application data may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the sensitive application data by another application.
For example, the attacker executes an application that tries to read data belonging to the sensitive application.

T.Integ-Applic-Code

Application code integrity:

A sensitive application code may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to memory area where the sensitive application executable code is stored.
The attacker executes an application that tries to alter (part of) the sensitive application code.

T.Integ-Applic-Data

Application data integrity:

A sensitive application data may need to be protected against unauthorized modification. This relates to attacks at runtime to gain write access to the sensitive application data by another application.
The attacker executes an application that tries to alter (part of) the sensitive application data.

5.3 Organisational security policies

91 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.

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

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

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

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

BSI.P.Process-TOE

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): if EDES+ is active,

– Triple Data Encryption Standard (3DES): if EDES+ is active,

– Advanced Encryption Standard (AES): if AES is active.

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

P.Controlled-ES-Loading

Controlled loading of the Security IC Embedded Software:

The TOE shall provide the capability to import the Security IC Embedded Software into the NVM, in a controlled manner, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority.
This capability is not available in User configuration.

5.4 Assumptions

5.4.1 Assumptions from the PP

96 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

97 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.

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

99 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*, and the one introduced in this Security Target, are detailed in the following sections.

Table 5. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
	O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
	O.Firewall	Application firewall
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

6.1.1 Objectives from the PP:

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

6.1.2 Additional objectives:

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): if EDES+ is active, – Triple Data Encryption Standard (3DES): if EDES+ is active, – Advanced Encryption Standard (AES): if AES is active.
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 restrictions*** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.
O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE must provide the capability to load the Security IC Embedded Software into the NVM, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. The TOE must restrict the access to these features. The TOE must provide control means to check the integrity of the loaded user data. This capability is not available in User configuration.
O.Firewall	Application firewall: The TOE shall ensure isolation of data and code between a Protected Application and the other applications. An application shall not read, write, compare any piece of data or code belonging to the Protected Application.

6.2 Security objectives for the environment

100 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

101 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

102 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*, and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 5* are addressed by the security objectives stated in this chapter.

103 Thus, it is necessary to show that:

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

104 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*)".

105 The augmentations made in this ST introduce the following security environment aspects:

- TOE threats "Application code confidentiality, (*T.Confid-Applic-Code*)", "Application data confidentiality, (*T.Confid-Applic-Data*)", "Application code integrity, (*T.Integ-Applic-Code*)", and "Application data integrity, (*T.Integ-Applic-Data*)".
- organisational security policy "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)".

106 The justification of the additional policy, and additional threats 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
P.Controlled-ES-Loading	*O.Controlled-ES-Loading*	Phase 4-6
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	

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

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
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*	
T.Confid-Applic-Code	*O.Firewall*	
T.Confid-Applic-Data	*O.Firewall*	
T.Integ-Applic-Code	*O.Firewall*	
T.Integ-Applic-Data	*O.Firewall*	

6.3.1 TOE threat "Memory Access Violation"

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

108 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.

109 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 TOE threat "Application code confidentiality"

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

111 Since *O.Firewall* requires that the TOE ensures isolation of code between the Protected Application and the other applications, the code of he Protected Application is protected against unauthorised disclosure, therefore *T.Confid-Applic-Code* is covered by *O.Firewall*.

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

6.3.3 TOE threat "Application data confidentiality"

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

114 Since *O.Firewall* requires that the TOE ensures isolation of data between he Protected Application and the other applications, the data of he Protected Application is protected against unauthorised disclosure, therefore *T.Confid-Applic-Data* is covered by *O.Firewall*.

6.3.4 TOE threat "Application code integrity"

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

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

6.3.5 TOE threat "Application data integrity"

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

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

6.3.6 Organisational security policy "Additional Specific Security Functionality"

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

120 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.

121 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*.

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

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

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

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

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

7 Security requirements

126 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

127 Security Functional Requirements (SFRs) from the "*BSI-PP-0035*" Protection Profile (PP) are drawn from *CCMB-2017-04-002*, except the following SFRs, that are **extensions** to *CCMB-2017-04-002*:

- **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.

128 All extensions to the SFRs of the "*BSI-PP-0035*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2017-04-002*.

129 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2017-04-001*. 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.

130 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-2017-04-002*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1 [Test]	Limited capabilities	Abuse of TEST functionality	*BSI-PP-0035*	Extended
FMT_LIM.2 [Test]	Limited availability			
FMT_LIM.1 [Admin]	Limited capabilities	Abuse of ADMIN functionality	Security Target Operated	
FMT_LIM.2 [Admin]	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-2017-04-002*
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-2017-04-002*
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	
FDP_ITC.1 [Loader]	Import of user data without security attributes	User data loading access violation	Security Target Operated	
FDP_ACC.1 [Loader]	Subset access control			
FDP_ACF.1 [Loader]	Security attribute based access control			
FMT_MSA.3 [Loader]	Static attribute initialisation	Correct operation		
FMT_MSA.1 [Loader]	Management of security attribute			
FMT_SMF.1 [Loader]	Specification of management functions	Abuse of ADMIN functionality		
FDP_ACC.1 [APPLI_FWL]	Subset access control	Protected Application intrinsic confidentiality and integrity		
FDP_ACF.1 [APPLI_FWL]	Security attribute based access control			
FMT_MSA.3 [APPLI_FWL]	Static attribute initialisation			

7.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

131 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)

132 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.***

133 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) [Test]

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

Limited availability (FMT_LIM.2) [Test]

135 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 [Test].

136 SFP_1: Limited capability and availability Policy [Test]

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)

137 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)

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

139 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)

140 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)

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

142 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)

143 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***.

144 *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)

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

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

tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

146 The TSF shall provide ***octets of bits*** that meet

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

7.1.2 Additional Security Functional Requirements for the cryptographic services.

147 The following SFRs are extensions to "*BSI-PP-0035*" Protection Profile (PP), related to the cryptographic services.

Cryptographic operation (FCS_COP.1)

148 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 crypto accelerators, 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]
If EDES+	EDES	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Data Encryption Standard (DES)	56 bits	*NIST SP 800-67* *NIST SP 800-38A*
			Triple Data Encryption Standard (3DES)	168 bits	
If AES	AES	* encryption (cipher) * decryption (inverse cipher) - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Advanced Encryption Standard	128, 192 and 256 bits	*FIPS PUB 197*

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

7.1.3 Additional Security Functional Requirements for the memories protection.

150 The following SFRs are extensions to "*BSI-PP-0035*" Protection Profile (PP), related to the memories protection.

Static attribute initialisation (FMT_MSA.3) [Memories]

151 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.

152 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]

153 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]

154 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.

155 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]

156 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.***

157 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.***

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

159 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***in Admin or 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.

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

161 SFP_3: Dynamic Memory Access Control Policy

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

162 *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]

163 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.***

7.1.4 Additional Security Functional Requirements related to the Admin configuration

164 The following SFRs are extensions to "*BSI-PP-0035*" Protection Profile (PP), related to the possible availability of final test and loading capabilities in phases 4 to 6 of the TOE life-cycle.

Limited capabilities (FMT_LIM.1) [Admin]

165 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 [Admin]***.

Limited availability (FMT_LIM.2) [Admin]

166 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 [Admin]***.

167 *SFP_4: Limited capability and availability Policy [Admin]*

168 *Deploying Loading or Final Test Artifacts after TOE Delivery to final user (phase 7 / USER configuration) does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, stored software to be reconstructed or altered, and no substantial information about construction of TSF to be gathered which may enable other attacks.*

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

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

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

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

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

Static attribute initialisation (FMT_MSA.3) [Loader]

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

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

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

174 The TSF shall enforce the ***Loading Access Control Policy*** to restrict the ability to ***modify*** the security attributes ***password*** to ***the Standard Loader.***

Subset access control (FDP_ACC.1) [Loader]

175 The TSF shall enforce the ***Loading Access Control Policy*** on ***the execution of the Standard Loader instructions and/or the Advanced Loader instructions***.

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

176 The TSF shall enforce the ***Loading Access Control Policy*** to objects based on the following: ***an external process may execute the Standard Loader instructions and/or the Advanced Loader instructions, depending on the presentation of valid passwords.***

177 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***the Standard Loader instructions and/or Advanced Loader instructions can be executed only if valid passwords have been presented.***

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

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

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

181 SFP_5: Loading Access Control Policy

182 According to a password control, the TSF grants execution of the instructions of the Standard Loader, Advanced Loader or none.

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

183 The TSF will be able to perform the following management functions: ***modification of the Standard Loader behaviour, by the Advanced Loader, under the Loading Access Control Policy.***

7.1.5 Additional Security Functional Requirements related to the Application Firewall

184 The following SFRs are extensions to "*BSI-PP-0035*" Protection Profile (PP), related to the protections by the Application Firewall.

Subset access control (FDP_ACC.1) [APPLI_FWL]

185 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** on ***the Protected Application code and data.***

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

186 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** to objects based on the following: ***Protected Application code and data***.

187 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***Another application cannot read, write, compare any piece of data or code belonging to the Protected Application.***

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

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

- ***Another application cannot read, write, compare any piece of data or code belonging to the Protected Application.***

190 The following SFP ***Protected Application Firewall Access Control Policy*** is defined for the requirement "Security attribute based access control (FDP_ACF.1) [APPLI_FWL]":

191 SFP_6: Protected Application Firewall Access Control Policy

192 Another application cannot read, write, compare any piece of data or code belonging to the Protected Application.

Static attribute initialisation (FMT_MSA.3) [APPLI_FWL]

193 The TSF shall enforce the ***Protected Application Firewall Access Control Policy*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

194 The TSF shall allow ***no subject*** to specify alternative initial values to override the default values when an object or information is created.

7.2 TOE security assurance requirements

195 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.

196 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.

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

Table 9. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-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

Table 9. TOE security assurance requirements (continued)

Label	Title	Origin
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
ASE_CCL.1	Conformance claims	EAL5/*BSI-PP-0035*
ASE_ECD.1	Extended components definition	EAL5/*BSI-PP-0035*
ASE_INT.1	ST introduction	EAL5/*BSI-PP-0035*
ASE_OBJ.2	Security objectives	EAL5/*BSI-PP-0035*
ASE_REQ.2	Derived security requirements	EAL5/*BSI-PP-0035*
ASE_SPD.1	Security problem definition	EAL5/*BSI-PP-0035*
ASE_TSS.1	TOE summary specification	EAL5/*BSI-PP-0035*
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

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

199 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.

200 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.

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

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

Table 10. 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)

203 ~~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.***

204 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.

205 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.

206 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.

207 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.

208 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)

209 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).

210 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).

211 ~~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

212 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*, and with those introduced in this Security Target, 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.

.

Table 11. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Inherent	FDP_ITT.1 Basic internal transfer protection FPT_ITT.1 Basic internal TSF data transfer protection FDP_IFC.1 Subset information flow control
BSI.O.Phys-Probing	FPT_PHP.3 Resistance to physical attack
BSI.O.Malfunction	FRU_FLT.2 Limited fault tolerance FPT_FLS.1 Failure with preservation of secure state
BSI.O.Phys-Manipulation	FPT_PHP.3 Resistance to physical attack

Table 11. Security Requirements versus Security Objectives (continued)

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Forced	All requirements listed for BSI.O.Leak-Inherent FDP_ITT.1, FPT_ITT.1, FDP_IFC.1 plus those listed for BSI.O.Malfunction and BSI.O.Phys-Manipulation FRU_FLT.2, FPT_FLS.1, FPT_PHP.3
BSI.O.Abuse-Func	FMT_LIM.1 [Test] Limited capabilities FMT_LIM.2 [Test] Limited availability FMT_LIM.1 [Admin] Limited capabilities FMT_LIM.2 [Admin] Limited availability plus those for BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
BSI.O.Identification	FAU_SAS.1 Audit storage
BSI.O.RND	FCS_RNG.1 Random number generation plus those for BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1
BSI.OE.Plat-Appl	Not applicable
BSI.OE.Resp-Appl	Not applicable
BSI.OE.Process-Sec-IC	Not applicable
AUG1.O.Add-Functions	FCS_COP.1 Cryptographic operation
AUG4.O.Mem-Access	FDP_ACC.2 [Memories] Complete access control FDP_ACF.1 [Memories] Security attribute based access control FMT_MSA.3 [Memories] Static attribute initialisation FMT_MSA.1 [Memories] Management of security attribute FMT_SMF.1 [Memories] Specification of management functions
O.Controlled-ES-Loading	FDP_ITC.1 [Loader] Import of user data without security attributes FDP_ACC.1 [Loader] Subset access control FDP_ACF.1 [Loader] Security attribute based access control FMT_MSA.3 [Loader] Static attribute initialisation FMT_MSA.1 [Loader] Management of security attribute FMT_SMF.1 [Loader] Specification of management functions
O.Firewall	FDP_ACC.1 [APPLI_FWL] Subset access control FDP_ACF.1 [APPLI_FWL] Security attribute based access control FMT_MSA.3 [APPLI_FWL] Static attribute initialisation

213 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 9*, 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.

214 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*, and four additional objectives (*O.Controlled-ES-Loading* and *O.Firewall*) introduced in this Security Target. This rationale must show that security requirements suitably address them.

215 Furthermore, a more careful observation of the requirements listed in *Table 7* and *Table 9* shows that:

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

216 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.

217 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*)”

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

219 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.

220 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*)”

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

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

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

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

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

225 The security functional requirement "*Static attribute initialisation (FMT_MSA.3) [Loader]*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) [Loader]*". The security functional requirement "*Specification of management functions (FMT_SMF.1) [Loader]*" provides additional controlled facility for adapting the loader behaviour to the user’s needs. These management functions ensure that the required access control, associated to the loading feature, can be realised using the functions provided by the TOE.

Security objective “Application firewall (*O.Firewall*)”

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

227 The security functional requirements "Subset access control (FDP_ACC.1) [APPLI_FWL]" and "Security attribute based access control (FDP_ACF.1) [APPLI_FWL]", supported by "Static attribute initialisation (FMT_MSA.3) [APPLI_FWL]", require that no application can read, write, compare any piece of data or code belonging to a Protected Application. This meets the objective *O.Firewall*.

7.4.3 Additional security requirements are consistent

"Cryptographic operation (*FCS_COP.1*)"

228 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]*)"

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

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

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

"Subset access control (*FDP_ACC.1 [APPLI_FWL]*),
Security attribute based access control (*FDP_ACF.1 [APPLI_FWL]*),
Static attribute initialisation (*FMT_MSA.3 [APPLI_FWL]*),

231 These security requirements have already been argued in *Section : Security objective "Application firewall (O.Firewall)"* above.

7.4.4 Dependencies of Security Functional Requirements

232 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* on FCS_CKM.4 (see discussion below),
- the dependency of *FMT_MSA.1 [Loader]* and *FMT_MSA.3 [Loader]* on FMT_SMR.1 (see discussion below),
- the dependency of *FMT_MSA.3 [APPLI_FWL]* on FMT_MSA.1 and FMT_SMR.1 (see discussion below).

233 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 [Test]	FMT_LIM.2 [Test]	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2 [Test]	FMT_LIM.1 [Test]	Yes	Yes, *BSI-PP-0035*

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_LIM.1 [Admin]	FMT_LIM.2 [Admin]	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2 [Admin]	FMT_LIM.1 [Admin]	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, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.4	No, see discussion below	
FDP_ACC.2 [Memories]	FDP_ACF.1 [Memories]	Yes	***No,*** *CCMB-2017-04-002*
FDP_ACF.1 [Memories]	FDP_ACC.1 [Memories]	Yes, by FDP_ACC.2 [Memories]	Yes, *AUG* ***#4***
	FMT_MSA.3 [Memories]	Yes	
FMT_MSA.3 [Memories]	FMT_MSA.1 [Memories]	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	
FMT_MSA.1 [Memories]	[FDP_ACC.1 [Memories] or FDP_IFC.1]	Yes, by FDP_ACC.2 [Memories] and FDP_IFC.1	Yes, *AUG* ***#4***
	FMT_SMF.1 [Memories]	Yes	***No,*** *CCMB-2017-04-002*
	FMT_SMR.1 [Memories]	No, see *AUG* ***#4***	Yes, *AUG* ***#4***
FMT_SMF.1 [Memories]	None	No dependency	***No,*** *CCMB-2017-04-002*
FMT_ITC.1 [Loader]	[FDP_ACC.1 [Loader] or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002*
	FMT_MSA.3 [Loader]	Yes	
FDP_ACC.1 [Loader]	FDP_ACF.1 [Loader]	Yes	***No,*** *CCMB-2017-04-002*

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*
FDP_ACF.1 [Loader]	FDP_ACC.1 [Loader]	Yes	***No,*** *CCMB-2017-04-002*
	FMT_MSA.3 [Loader]	Yes	
FMT_MSA.3 [Loader]	FMT_MSA.1 [Loader]	Yes	***No,*** *CCMB-2017-04-002*
	FMT_SMR.1 [Loader]	No, see discussion below	
FMT_MSA.1 [Loader]	[FDP_ACC.1 [Loader] or FDP_IFC.1]	Yes	***No,*** *CCMB-2017-04-002*
	FDP_SMF.1 [Loader]	Yes	
	FDP_SMR.1 [Loader]	No, see discussion below	
FDP_SMF.1 [Loader]	None	No dependency	***No,*** *CCMB-2017-04-002*
FDP_ACC.1 [APPLI_FWL]	FDP_ACF.1 [APPLI_FWL]	Yes	***No,*** *CCMB-2017-04-002*
FDP_ACF.1 [APPLI_FWL]	FDP_ACC.1 [APPLI_FWL]	Yes	***No,*** *CCMB-2017-04-002*
	FMT_MSA.3 [APPLI_FWL]	Yes	
FMT_MSA.3 [APPLI_FWL]	FMT_MSA.1	No, see discussion below	***No,*** *CCMB-2017-04-002*
	FMT_SMR.1	No, see discussion below	

234 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, "Import of user data without security attributes (FDP_ITC.1) [Loader]" may be used for the purpose of creating cryptographic keys, but also, the ES has all possibilities to implement its own creation function, in conformance with its security policy.

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

236 Part 2 of the Common Criteria defines the dependency of "Management of security attributes (FMT_MSA.1) [Loader]" and "Static attribute initialisation (FMT_MSA.3) [Loader]" on "Security roles (FMT_SMR.1) [Loader]". This dependency is considered to be satisfied, because the access control defined for the loader is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a Security Functional Requirement "FMT_SMR.1".

7.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5 (*Table 9*)

237 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.

238 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.

239 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.

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

Dependencies of assurance requirements

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

242 Augmentation to this package are identified in paragraph *195* and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

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

244 The complete TOE summary specification has been presentad and evaluated in the ST33H768 D01 - SECURITY TARGET.

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

8.1 Limited fault tolerance (FRU_FLT.2)

246 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)

247 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..

248 The ES can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1) [Test]

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

8.4 Limited capabilities (FMT_LIM.1) [Admin]

250 The TSF ensures that the Secure Flash Loader and the final test capabilities are unavailable in USER configuration, in accordance with SFP_4: Limited capability and availability Policy [Admin].

8.5 Limited availability (FMT_LIM.2) [Test] & [Admin]

251 The TOE is either in TEST, ADMIN or USER configuration.

252 The only authorised TOE configuration modifications are:

- TEST to ADMIN configuration,
- TEST to USER configuration,
- ADMIN to USER configuration.

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

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

8.6 Audit storage (FAU_SAS.1)

255 In Admin 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.

8.7 Resistance to physical attack (FPT_PHP.3)

256 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.

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

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

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

8.9 Random number generation (FCS_RNG.1)

258 The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the BSI-AIS20/AIS31 standard for a PTG.2 class device.

8.10 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES]) only if EDES+

259 If EDES+ is active, the TOE provides an EDES accelerator that has the capability to perform a DES encryption and a DES decryption conformant to NIST SP 800-67, and a Triple DES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes conformant to NIST SP 800-67 and NIST SP 800-38A.

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

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

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

- cipher,
- inverse cipher.

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

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

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

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

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

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

264 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.

8.15 Import of user data without security attributes (FDP_ITC.1) [Loader]

265 In Admin configuration, the System Firmware provides the capability of securely loading user data into the NVM (Secure Flash Loader). The ciphered data is automatically decrypted, before installation in the NVM.
The integrity of the loaded data is systematically checked, and the integrity of the NVM can also be checked by the ES.

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

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

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

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

8.18 Subset access control (FDP_ACC.1) [Loader] & Security attribute based access control (FDP_ACF.1) [Loader]

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

8.19 Subset access control (FDP_ACC.1) [APPLI_FWL] & Security attribute based access control (FDP_ACF.1) [APPLI_FWL]

269 The Library Protection Unit is used to isolate the Protected Application (code and data) from the rest of the code embedded in the device.

8.20 Static atttribute initialisation (FMT_MSA.3) [APPLI_FWL]

270 At product start, all the static attributes are initialised, which are needed to protect the segments where the Protected Application code and data are stored.

9 References and identification

271 Protection Profile references

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

272 ST33H768 D01 Security Target reference

Component description	Reference
ST33H768 D01 - SECURITY TARGET	SMD_ST33H768_ST_19_001

273 Guidance documentation references

Component description	Reference	Revision
ST33H768 Secure MCU with 32-bit ARM SecurCore SC300 - Datasheet	DS_ST33H768	4
ST33H768 platform: BP and BM specific product profiles - Technical note	TN_ST33H768_01	1
ST33H768: LS, LC and BS specific product profiles - Technical Note	TN_ST33H768_02	1
ST33H768: CMOS M10+ 80-nm technology die and wafer delivery description	DD_ST33H768	2
ARM® Cortex SC300 r0p0 Technical Reference Manual	ARM DDI 0337	F
ARM® Cortex M3 r2p0 Technical Reference Manual	ARM DDI 0337F3c	F3c
ARM® SC300 r0p0 SecurCore Technical Reference Manual Supplement 1A	ARM DDI 0337 Supp 1A	A
ARM® SecurCore SC300 technical limitations	ES_SC300	1
ST33H768 Firmware user manual	UM_ST33H768_FW	10
ST33H768 and derivatives Flash loader installation guide	UM_33H_FL	4
ST33G and ST33H Firmware support for LPU regions - Application Note	AN_33G_33H_LPU	1
ST33G and ST33H Secure MCU platforms - Security Guidance	AN_SECU_ST33	9
ST33G and ST33H Power supply glitch detector characteristics - application note	AN_33_GLITCH	2
ST33G and ST33H - AIS31 Compliant Random Number user manual	UM_33G_33H_AIS31	3
ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - User manual	AN_33G_33H_AIS31	1

Component description	Reference	Revision
ST33 ARM Execute-only memory support for SecurCore® SC300 devices - Application note	AN_33_EXE	2
ST33 uniform timing application note	AN_33_UT	2

274 Sites list

Site	Address	Activities[1]
Amkor ATP1	AMKOR ATP1 Km 22 East Service Road, South Superhighway, Muntinlupa City, 1771 Philippines	BE
Amkor ATP3/4	AMKOR ATP3/4 119 North Science Avenue, Laguna Technopark, Binan, Laguna, 4024 Philippines	BE
Amkor ATT1	AMKOR TECHNOLOGY TAIWAN, INC. (ATT) - T1 No. 1, Kao-Ping Sec, Chung-Feng Road., Longtan District, TAOYUAN City 325, Taiwan, R.O.C.	BE
Amkor ATT3	AMKOR TECHNOLOGY TAIWAN, INC. (ATT) - T3 No. 11, Guangfu Road., Hsinchu Industrial Park, Hukou Township, HSINCHU County 303, Taiwan, R.O.C.	BE
DNP Japan	DNP (Dai Nippon printing Co ltd.) 2-2-1 Kami-Fukuoka, Fujimino-shi, Saitama,356-8507, Japan	MASK
DPE Italy	DPE (Dai Printing Europe) Via C. Olivetti, 2/A, I-20041 Agrate, Italy	MASK
Feiliks	Feili Logistics (Shenzhen) CO., Ltd Zhongbao Logistics Building, No. 28 Taohua Road, FFTZ, Shenzhen, Guangdong 518038, China	WHS
Smartflex	Smartflex Technology 37A Tampines Street 92, Singapore 528886	BE
ST AMK1	STMicroelectronics 5A Serangoon North Avenue 5, Singapore 554574	DEV
ST AMK6	STMicroelectronics 18 Ang Mo Kio Industrial park 2, Singapore 569505	WHS

Site	Address	Activities[1]
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers – BP97, 20180 Bouskoura, Maroc	BE WHS
ST Calamba	STMicroelectronics 9 Mountain Drive, LISP II, Brgy La mesa, Calamba, Philippines 4027	BE WHS
ST Crolles	STMicroelectronics 850 rue Jean Monnet, 38926 Crolles, France	DEV MASK FE
ST Gardanne	CMP Georges Charpak 880 Avenue de Mimet, 13541 Gardanne, France	BE
ST Grenoble	STMicroelectronics 12 rue Jules Horowitz, BP 217, 38019 Grenoble Cedex, France	DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive, Singapore 508938	WHS
ST Rennes	STMicroelectronics 10 rue de Jouanet, ePark, 35700 Rennes, France	DEV
ST Rousset	STMicroelectronics 190 Avenue Célestin Coq, Z.I., 13106 Rousset Cedex, France	DEV EWS WHS FE
ST Shenzen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone, Shenzhen, P.R. China 518038	BE
ST Sophia	STMicroelectronics 635 route des lucioles, 06560 Valbonne, France	DEV

Site	Address	Activities[1]
ST Toa Payoh	STMicroelectronics 629 Lorong 4/6 Toa Payoh, Singapore 319521	EWS
ST Tunis	STMicroelectronics Tunis Elgazala Technopark, Raoued, Gouvernorat de l’Ariana, PB21, 2088 cedex, Ariana, Tunisia	IT
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B, 3d floor, 1831 Diegem/Machelen, Belgium	DEV
STATS JSCC	STATS ChipPAC Semiconductor Jiangyin CO. Ltd (JSCC) No. 78 Changshan Road, Jiangyin, Jiangsu, China, Postal code: 214437	BE
TSMC F2/F5	TSMC FAB 2-5 121 Park Avenue 3, Hsinchu science park, Hsinchu 300-77, Taiwan, ROC	MASK FE
TSMC F14	TSMC FAB 14 1-1 Nan Ke N. Rd. Tainan science park, Tainan 741_44, Taiwan, ROC	MASK FE
TSMC F8	TSMC FAB 8 25, Li-Hsin Road, Hsinchu Science Park, Hsinchu 300-78, Taiwan ROC	MASK FE
Winstek	WINSTEK STATS ChipPAC (SCT) No 176-5, 6 Ling, Hualung Chun, Chiung Lin, 307 Hsinchu, Taiwan	BE

1. DEV = development, FE = front end manufacturing, EWS = electrical wafer sort and pre-perso, BE = back end manufacturing, MASK = mask manufacturing, WHS = warehouse

275 **Standards references**

Ref	Identifier	Description
[1]	BSI-AIS20/AIS31	A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler BSI, Version 2.0, 18-09-2011
[2]	NIST SP 800-67	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology

Ref	Identifier	Description
[3]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[4]	ISO/IEC 9796-2	ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002
[5]	NIST SP 800-38A	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010
[6]	ISO/IEC 14888	Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[7]	CCMB-2017-04-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017, version 3.1 Revision 5
[8]	CCMB-2017-04-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017, version 3.1 Revision 5
[9]	CCMB-2017-04-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017, version 3.1 Revision 5
[10]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[11]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[12]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[13]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[14]	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 or Firmware

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
AES	Advanced Encryption Standard.
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.
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.
DSW	IC Proprietary Dedicated Software.
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.
FTOS	Final Test Operating System.
GPIO	General Purpose I/O.
I/O	Input / Output.
IART	ISO-7816 Asynchronous Receiver Transmitter.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
LPU	Library Protection Unit.
MAC	Message Authentication Code.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NFC	Near Field Communication.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OS	Operating System.

Table 13. List of abbreviations (continued)

Term	Meaning
OSP	Organisational Security Policy.
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
SAR	Security Assurance Requirement.
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SIM	Subscriber Identity Module.
SOIC	Small Outline IC.
SPI	Serial Peripheral Interface.
ST	Context dependent: STMicroelectronics or Security Target.
SWP	Single Wire Protocol.
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.
UID	User Identification.

IMPORTANT NOTICE – PLEASE READ CAREFULLY

STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, enhancements, modifications, and improvements to ST products and/or to this document at any time without notice. Purchasers should obtain the latest relevant information on ST products before placing orders. ST products are sold pursuant to ST’s terms and conditions of sale in place at the time of order acknowledgement.

Purchasers are solely responsible for the choice, selection, and use of ST products and ST assumes no liability for application assistance or the design of Purchasers’ products.

No license, express or implied, to any intellectual property right is granted by ST herein.

Resale of ST products with provisions different from the information set forth herein shall void any warranty granted by ST for such product.

ST and the ST logo are trademarks of ST. For additional information about ST trademarks, please refer to *www.st.com/trademarks*. All other product or service names are the property of their respective owners.

Information in this document supersedes and replaces information previously supplied in any prior versions of this document.