STMicroelectronics

ST33G1M2A1 C06
including optional cryptographic library NesLib, including optional library SFM
Security Target for composition

Common Criteria for IT security evaluation

SMD_ST33G1M2A1_ST_19_002 Rev C06.1

June 2026



www.st.com

BLANK

ST33G1M2A1 C06 platform Security Target for composition

Common Criteria for IT security evaluation

1 Introduction (ASE_INT)

1.1 Security Target reference

1 Document identification: ST33G1M2A1 C06, including optional cryptographic library NesLib and optional library SFM - SECURITY TARGET FOR COMPOSITION.

2 Version number: Rev C06.1, issued in June 2026.

3 Registration: registered at ST Microelectronics under number SMD_ST33G1M2A1_ST_19_002.

1.2 TOE reference

4 This document presents **the Security Target (ST)** of the **ST33G1M2A1 C06** (ST33G1M2A and ST33G1M2M) Security Integrated Circuit (IC), designed on the **ST33G platform of STMicroelectronics**, with firmware version 1.3.2, optional cryptographic library NesLib version 6.3.4 and optional library SFM version1.0.8.

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

6 A glossary of terms and abbreviations used in this document is given in *Appendix A: Glossary*.

Contents

1 Introduction (ASE_INT) 3

1.1 Security Target reference 3

1.2 TOE reference 3

1.3 Context 10

1.4 TOE identification 11

1.5 TOE overview 11

1.6 TOE description 12

1.6.1 TOE hardware description 12

1.6.2 TOE software description 13

1.6.3 TOE documentation 15

1.6.4 TOE delivery format and method 15

1.7 TOE life cycle 15

1.8 TOE environment 16

1.8.1 TOE Development Environment 17

1.8.2 TOE production environment 17

1.8.3 TOE operational environment 18

2 Conformance claims (ASE_CCL) 19

2.1 Common Criteria conformance claims 19

2.2 Package Claims 19

2.3 PP Claims 19

2.3.1 PP Claims rationale 20

2.3.2 Rationale regarding CC:2022 and PP-0084 20

3 Security problem definition (ASE_SPD) 23

3.1 Description of assets 24

3.2 Threats 25

3.3 Organisational security policies 26

3.4 Assumptions 27

4 Security objectives (ASE_OBJ) 29

4.1 Security objectives for the TOE 30

4.2 Security objectives for the environment 31

4.3 Security objectives rationale 31
4.3.1 TOE threat "Memory Access Violation" 33
4.3.2 TOE threat "Application code confidentiality" 33
4.3.3 TOE threat "Application data confidentiality" 33
4.3.4 TOE threat "Application code integrity" 33
4.3.5 TOE threat "Application data integrity" 33
4.3.6 Organisational security policy "Additional Specific Security Functionality" 34
4.3.7 Organisational security policy "Controlled loading of the Security IC Embedded Software" 34
4.3.8 Organisational security policy "Treatment of user data" 34

5 Extended Components (ASE_ECD) 35

6 Security requirements (ASE_REQ) 36

6.1 Security functional requirements for the TOE 36
6.1.1 Security Functional Requirements from the Protection Profile 39
6.1.2 Additional Security Functional Requirements for the cryptographic services 41
6.1.3 Additional Security Functional Requirements for the memories protection 45
6.1.4 Additional Security Functional Requirements related to the possible availability of loading capabilities in phases 4 to 6 of the TOE life-cycle 47
6.1.5 Additional Security Functional Requirements related to the Application Firewall 48
6.2 TOE security assurance requirements 49
6.3 Refinement of the security assurance requirements 50
6.3.1 Refinement regarding functional specification (ADV_FSP) 51
6.3.2 Refinement regarding test coverage (ATE_COV) 52
6.4 Security Requirements rationale 52
6.4.1 Rationale for the Security Functional Requirements 52
6.4.2 Additional security objectives are suitably addressed 55
6.4.3 Additional security requirements are consistent 56
6.4.4 Dependencies of Security Functional Requirements 57
6.4.5 Rationale for the Assurance Requirements 60

7 TOE summary specification (ASE_TSS) 62

7.1 Limited fault tolerance (FRU_FLT.2) 62

7.2 Failure with preservation of secure state (FPT_FLS.1) 62
7.3 Limited capabilities (FMT_LIM.1) / Test 63
7.4 Limited capabilities (FMT_LIM.1) / Loader 63
7.5 Limited availability (FMT_LIM.2) / Test & (FMT_LIM.2) / Loader 63
7.6 Stored data confidentiality (FDP_SDC.1) 63
7.7 Stored data integrity monitoring and action (FDP_SDI.2) 63
7.8 Audit storage (FAU_SAS.1) 63
7.9 Resistance to physical attack (FPT_PHP.3) 64
7.10 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1) 64
7.11 Random number generation (FCS_RNG.1) 64
7.12 Cryptographic operation: TDES operation (FCS_COP.1) / TDES 64
7.13 Cryptographic operation: AES operation (FCS_COP.1) / AES 64
7.14 Cryptographic operation: RSA operation (FCS_COP.1) / RSA, only if NesLib 65
7.15 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC, only if NesLib 65
7.16 Cryptographic operation: SHA-1 & SHA-2 operation (FCS_COP.1) / SHA, only if NesLib 66
7.17 Cryptographic operation: Keccak & SHA-3 operation (FCS_COP.1) / Keccak, only if NesLib 66
7.18 Cryptographic operation: Keccak-p operation (FCS_COP.1) / Keccak-p, only if NesLib 67
7.19 Cryptographic operation: Diffie-Hellman operation (FCS_COP.1) / Diffie-Hellman, only if NesLib 67
7.20 Cryptographic operation: DRBG operation (FCS_COP.1) / DRBG, only if NesLib 67
7.21 Cryptographic key generation: Prime generation (FCS_CKM.1) / Prime_generation, only if NesLib 67
7.22 Cryptographic key generation: RSA key generation (FCS_CKM.1) / RSA_key_generation, only if NesLib 67
7.23 Static attribute initialisation (FMT_MSA.3) / Memories 68
7.24 Management of security attributes (FMT_MSA.1) / Memories & Specification of management functions (FMT_SMF.1) / Memories 68
7.25 Complete access control (FDP_ACC.2) / Memories & Security attribute based access control (FDP_ACF.1) / Memories 68

7.26 Static attribute initialisation (FMT_MSA.3) / Loader 68
7.27 Management of security attributes (FMT_MSA.1) / Loader & Specification of management functions (FMT_SMF.1) / Loader 68
7.28 Subset access control (FDP_ACC.1) / Loader, Security attribute based access control (FDP_ACF.1) / Loader, Security roles (FMT_SMR.1) / Loader & Timing of identification (FIA_UID.1) / Loader 68
7.29 Import of user data without security attributes (FDP_ITC.1) / Loader . . . 69
7.30 Subset access control (FDP_ACC.1) / APPLI_FWL & Security attribute based access control (FDP_ACF.1) / APPLI_FWL 69
7.31 Static attribute initialisation (FMT_MSA.3) / APPLI_FWL 69

8 Identification 70

9 References 76

Appendix A Glossary 80

A.1 Terms. 80
A.2 Abbreviations. 82

List of tables

Table 1. TOE components . . . 11
Table 2. Derivative devices configuration possibilities . . . 12
Table 3. Composite product life cycle phases . . . 16
Table 4. CC:2022 rationale . . . 20
Table 5. Summary of security aspects . . . 23
Table 6. Summary of security objectives . . . 29
Table 7. Security Objectives versus Assumptions, Threats or Policies . . . 32
Table 8. Summary of functional security requirements for the TOE . . . 37
Table 9. FCS_COP.1 iterations (cryptographic operations) . . . 42
Table 10. FCS_CKM.1 iterations (cryptographic key generation) . . . 45
Table 11. TOE security assurance requirements . . . 50
Table 12. Impact of EAL5 selection on BSI-CC-PP-0084-2014 refinements . . . 51
Table 13. Security Requirements versus Security Objectives . . . 53
Table 14. Dependencies of security functional requirements . . . 57
Table 15. TOE components . . . 70
Table 16. Guidance documentation . . . 70
Table 17. Sites list . . . 71
Table 18. Common Criteria . . . 76
Table 19. Protection Profile . . . 76
Table 20. Other standards . . . 76
Table 21. List of abbreviations . . . 82

List of figures

Figure 1. ST33G1M2A1 C06 platform block diagram 13

1.3 Context

7 The Target of Evaluation (TOE) referred to in *Section 1.4: TOE identification*, is certified under EUCC by the French National Cybersecurity Certification Authority (NCCA) and is developed by the Connected Security division of STMicroelectronics (ST).

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

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

10 This ST claims to be an instantiation of the "*Eurosmart - Security IC Platform Protection Profile with Augmentation Packages*" (PP) registered and certified under the reference *BSI-CC-PP-0084-2014* in the German IT Security Evaluation and Certification Scheme, ***with the following augmentations***:

- Addition #1: “Support of Cipher Schemes” from *AUG*
- Addition #4: “Area based Memory Access Control” from *AUG*
- Additions specific to this Security Target.

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

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

- Loader dedicated for usage in secured environment only.

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

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

1.4 TOE identification

13 The Target of Evaluation (TOE) is the ST33G1M2A1 C06 platform.

14 "ST33G1M2A1 C06" completely identifies the TOE including its components listed in *Table 1: TOE components*, its guidance documentation detailed in *Table 16: Guidance documentation*, and its development and production sites indicated in *Table 17: Sites list*.

15 C06 is the version of the evaluated platform. Any change in the TOE components, the guidance documentation and the list of sites leads to a new version of the evaluated platform, thus a new TOE.

Table 1. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	OST version	Optional NesLib crypto library version(2)	Optional SFM library version
K8H0A (3)	H	01BCh (ST33G1M2)	1.3.2	2.2	6.3.4	1.0.8

1. Part of the product information.
2. See the NesLib User Manual referenced in *Table 16: Guidance documentation*
3. This maskset K8H0A rev H corresponds to product line K8M0.

16 The IC maskset name is the product hardware identification.
The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST software.

17 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in *Table 1: TOE components*, and the configuration elements as detailed in the Data Sheet, referenced in *Table 16: Guidance documentation*.

1.5 TOE overview

18 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.

19 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.

20 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 personnalisation process.

21 They all share the same hardware design and the same maskset (denoted by the Master identification number). The Master identification number is unique for all product configurations.

22 The configuration of the derivative devices can impact the available NVM memory size, and the operational temperature range, as detailed here below:

Table 2. Derivative devices configuration possibilities

Features	Possible values
NVM size	Selectable by 128 Kbytes granularity from 1280 Kbytes to 384 Kbytes
Operational temperature range	See Data Sheet, referenced in *Table 16: Guidance documentation*

23 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.

24 The Master identification number is unique for all product configurations.
Each derivative device has a specific Child product identification number, also part of the product information, and specified in the Data Sheet and in the Firmware User Manual, referenced in *Table 16*.

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

26 In a few words, the ST33G1M2A1 C06, 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 Protection Unit,
- ISO/IEC 13239 CRC calculation block,
- Hardware Security Enhanced DES accelerator (EDES+),
- AES accelerator (HW-AES),
- Library Protection Unit,
- Next Step Cryptography accelerator (NESCRYPT),
- Optional cryptographic library NesLib,
- Optional SFM library.

1.6 TOE description

1.6.1 TOE hardware description

27 The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks.
The AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. It can operate in Electronic CodeBook (ECB) or Cipher Block Chaining (CBC) modes.

28 The 3-key triple DES accelerator (EDES+) supports efficiently the Triple Data Encryption Standard (TDES *[2]*), enabling Electronic Code Book (ECB) and Cipher Block Chaining (CBC) modes, and Triple DES computation.
Note that a triple DES can be performed by a triple DES computation or by 3 single DES computations.

29 The NESCRYPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([7], [12], [15],[16], [17], [18]).

30 As randomness is a key stone in many applications, the ST33G1M2A1 C06 features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 [1] and directly accessible thru dedicated registers.

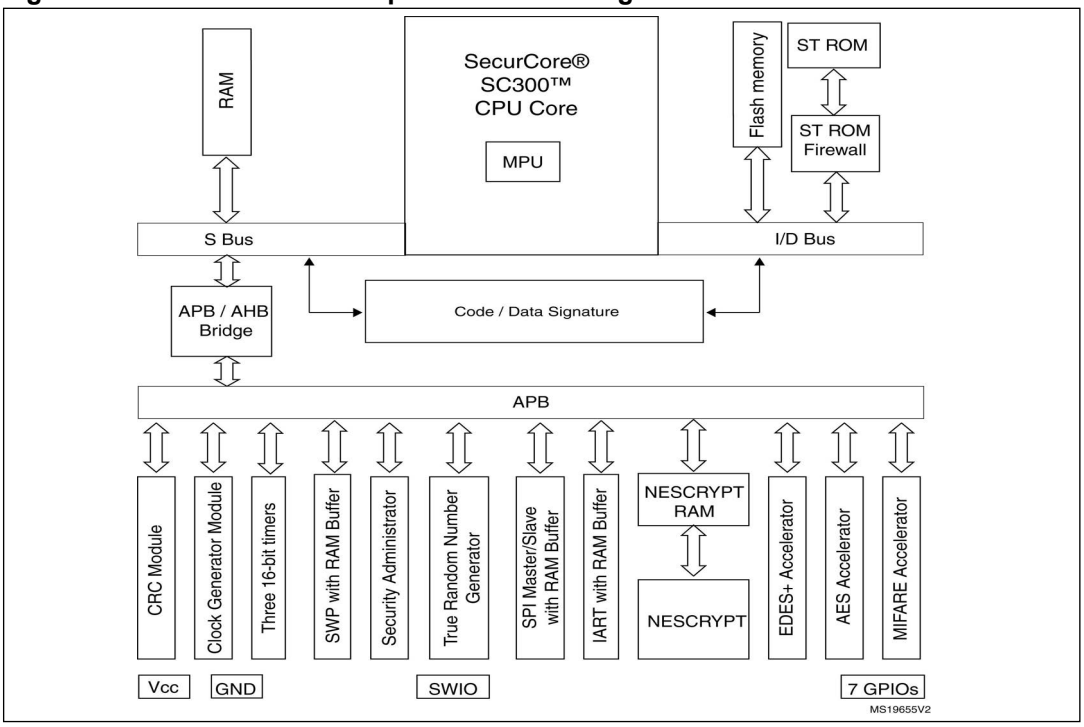
This device includes the ARM® SecurCore® SC300™ memory protection unit (MPU), which enables the user to define its own region organization with specific protection and access permissions. The MPU can be used to enforce various protection models, ranging from a basic code dump prevention model up to a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

31 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.

32 The detailed features of this TOE are described in the Data Sheet and in the Cortex SC300 Technical Reference Manual, referenced in Table 16.

33 Figure 1 provides an overview of the ST33G1M2A1 C06 platform.

Figure 1. ST33G1M2A1 C06 platform block diagram



1.6.2 TOE software description

34 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.

35 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.

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

37 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.

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

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

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

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA *[17]*), and Diffie-Hellman *[23]*,
- an asymmetric key cryptographic support module that provides very efficient basic functions to build up protocols using Elliptic Curves Cryptography on prime fields GF(p) with elliptic curves in short Weierstrass form *[15]*, and provides support for ECDH key agreement *[21]* and ECDSA generation and verification *[5]*.
- a module for supporting elliptic curve cryptography on Edwards curve 25519, in particular ed25519 signature generation, verification and point decompression *[26]*.
- a cryptographic support module that provides hash functions (SHA-1[a], SHA-2 *[4]*), SHA-3, Keccak and a toolbox for cryptography based on Keccak-p, the permutation underlying SHA-3 *[25]*,
- a symmetric key cryptographic support module whose base algorithm is the Data Encryption Standard cryptographic algorithm (DES) *[2]*,
- a symmetric key cryptographic support module whose base algorithm is the Advanced Encryption Standard cryptographic algorithm (AES) *[6]*,
- support for Deterministic Random Bit Generators *[19]*,
- prime number generation and RSA key pairs generation *[3]*.

39 NesLib also provides basic services for memory access such as read, write, integrity checking, copy, exception management, protection against faults and random generation.

40 The TOE optionally comprises a specific application in User NVM: this applicative Embedded Software is a NVM management library called StoreKeeper Flash Management (SFM). SFM provides a specific convenient interface to the physical NVM.

41 SFM is embedded by the ES developer in his applicative code.

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

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

43 **Note:** the ES is not part of the TOE and is out of scope of the evaluation, except NesLib when it is embedded.

1.6.3 TOE documentation

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

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

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

1.6.4 TOE delivery format and method

46 The ST33G1M2A1 C06 is delivered in forms of wafers, micromodules or packages, as described in the Data Sheet referenced in *Table 16*. It is shipped to the customer with monitoring of the delivery activity.
The firmware is integrated on the IC before delivery.

47 Guidance documents in pdf format have a reference identifier. Each delivery is registered and done encrypted for each customer by email or using a secure file transfer system.

48 All the possible forms of delivery are equivalent from a security point of view.

1.7 TOE life cycle

49 This Security Target is fully conform to the claimed PP. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 1.2.3.

50 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.

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

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

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

54 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.

55 The TOE, except the NesLib and SFM, is delivered after Phase 3 in form of wafers or after Phase 4 in packaged form, depending on the customer's order.

56 NesLib and SFM are delivered as part of Phase 1, each as a software package part of the dedicated support software, downloaded by ST entitled employees, from a controlled centralized system, then sent encrypted to the customer. NesLib and SFM are intended to be used in support to the development of secure embedded software in phase 1. So the ES developers embeds one of them (resp. both) and links it (resp. them) to its applicative code.

57 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.
- NesLib and SFM are part of the TOE and specifically delivered for each of them as part of phase 1 in form of ciphered and signed binary file, so that the ES developer embeds one of them (resp. both) and links it (resp. both) to its applicative code.

58 The TOE is delivered in Admin (aka Issuer) or User configuration.

Table 3. Composite product life cycle phases

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

1.8 TOE environment

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

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

1.8.1 TOE Development Environment

60 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.

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

62 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).

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

1.8.2 TOE production environment

64 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.

65 Phase 3

66 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).

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

68 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 and pre-personalization of each TOE occurs to assure conformance with the device specification.

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

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

71 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.

72 Phase 4

73 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.

74 When the product is delivered after phase 4, the authorized back-end plants possibly involved in the packaging of the TOE are denoted by the activity “BE” in *Table 17*.

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

1.8.3 TOE operational environment

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

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

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

2 Conformance claims (ASE_CCL)

2.1 Common Criteria conformance claims

79 The ST33G1M2A1 C06 platform Security Target claims to be conformant to the Common Criteria version 2022 revision 1. More precisely the ST33G1M2A1 C06 platform Security Target is:

- CC Part 2 extended, where *CCMB-2022-11-002 R1* is extended with FAU_SAS.1 and,
- CC Part 3 conformant, cf. *CCMB-2022-11-003 R1* and,
- CC Part 5 conformant, cf. *CCMB-2022-11-005 R1* with,
- Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), cf. *Reference 001*.

2.2 Package Claims

80 EAL packages are described in *CCMB-2022-11-005 R1*.

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

82 Some of the SARs are refined as required by the *BSI-CC-PP-0084-2014*.

2.3 PP Claims

83 The ST33G1M2A1 C06 platform Security Target claims strict conformance to the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

84 The following packages have been selected from the *BSI-CC-PP-0084-2014*:

- Package “Loader dedicated for usage in secured environment only.”

85 The ST33G1M2A1 C06 Security Target for composition includes the following additional elements:

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

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

87 The security environment additions relative to the PP are summarized in *Table 5*.

88 The additional security objectives relative to the PP are summarized in *Table 6*.

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

90 The additional SFRs for the TOE relative to the PP are summarized in *Table 8*.

91 The additional SARs relative to the PP are summarized in *Table 11*.

2.3.1 PP Claims rationale

92 The differences between this Security Target security objectives and requirements and those of *BSI-CC-PP-0084-2014*, to which conformance is claimed, have been identified and justified in *Section 4* and in *Section 6*. They have been recalled in the previous section.

93 In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the *BSI-CC-PP-0084-2014*.

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

95 The security objectives rationale presented in *Section 4.3* clearly identifies modifications and additions made to the rationale presented in the *BSI-CC-PP-0084-2014*.

96 Similarly, the security requirements rationale presented in *Section 6.4* has been updated with respect to the Protection Profile.

97 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.

2.3.2 Rationale regarding CC:2022 and PP-0084

98 The SFRs defined in *BSI-CC-PP-0084-2014*, including the functional packages, were conformant to the CC version 3.1. Since this Security Target conforms to the CC:2022, the SFRs have been updated to both comply with CC:2022 and meet *BSI-CC-PP-0084-2014*.

99 The *Table 4* provides the rationale of the changes.

Table 4. CC:2022 rationale

SFR	*BSI-CC-PP-0084-2014* and *CCMB-2017-04-002 R5* definition	*CCMB-2022-11-002 R1* definition	Change
FMT_LIM.1	The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: Limited capability policy].	The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced [assignment: Limited capability and availability policy].	The CC:2022 definition modifies the wording of the SFR to emphasize that the TSF shall limit its capabilities. The new SFR modifies the assignment to limit availability. The CC:2022 version explicitly links the limited capability and limited availability policies, not only at the level of the dependencies. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.

Table 4. CC:2022 rationale (continued)

SFR	*BSI-CC-PP-0084-2014* and *CCMB-2017-04-002 R5* definition	*CCMB-2022-11-002 R1* definition	Change
FMT_LIM.2	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited availability policy].	The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced [assignment: Limited capability and availability policy].	The new SFR modifies the assignment to limit capability. The CC:2022 version explicitly links the limited capability and limited availability policies, not only at the level of the dependencies. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.
FDP_SDC.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*].	The TSF shall ensure the confidentiality of [selection: *all user data, the following user data* [assignment: *list of user data*]] while it is stored in the [selection: *temporary memory, persistent memory, any memory*].	The new SFR provides the option to select the type of data and memory type. Any instantiation to the CC:2022 SFR meets the CC3.1 SFR.
FIA_API.1	The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [selection: *TOE,* [assignment: *object, authorized user or role*]] to an external entity.	The TSF shall provide an [assignment: *authentication mechanism*] to prove the identity of [assignment: *entity*] by including the following properties [assignment: *list of properties*] to an external entity.	A selection is replaced by an assignment: the SFR in CC:2022 is more flexible than in CC 3.1. Nevertheless, the instantiation made in this Security Target meets the SFR defined in the PP.
FAU_SAR.1	The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.	The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit data.	The new definition changes the term "record" with the term "data". The change does not have any impact.
	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.	The TSF shall provide the audit data in a manner suitable for the user to interpret the information.	

Table 4. CC:2022 rationale (continued)

SFR	*BSI-CC-PP-0084-2014* and *CCMB-2017-04-002 R5* definition	*CCMB-2022-11-002 R1* definition	Change
FCS_RNG.1	The TSF shall provide a [selection: *physical, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].	The first selection add the terms “non physical true” and “deterministic”. The change does not have any impact.
	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].	The TSF shall provide [selection: *bits, octets of bits, numbers* [assignment: *format of the numbers*]] that meet [assignment: *a defined quality metric*].	
FCS_CKM.4	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].	Removed SFR.	FCS_CKM.6 is replacing FCS_CKM.4. FCS_COP.1 has a dependency on FCS_CKM.6. FCS_CKM.6 in CC:2022 is more flexible than FCS_CKM.4 in CC 3.1. Nevertheless, although no instantiation is made in this Security Target, the dependency is discussed later and this change has no impact.
FCS_CKM.6	Not present.	The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*].	
		The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].	

3 Security problem definition (ASE_SPD)

100 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.

101 Note that the origin of each security aspect is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*), section 3. Only those originating in *AUG*, and the ones introduced in this Security Target, are detailed in the following sections.

102 A summary of all these security aspects and their respective conditions is provided in *Table 5*.

Table 5. Summary of security aspects

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
	AUG4.T.Mem-Access	Memory Access Violation
	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
	BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
	P.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
	P.Resp-Appl	Treatment of user data
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Resp-Appl	Treatment of User Data

3.1 Description of assets

103 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.

104 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.

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

SC4 deficiency of random numbers.

106 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.

107 The information and material produced and/or processed by the TOE manufacturer 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 the TOE manufacturer.

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

3.2 Threats

109 The threats are described in the *BSI-CC-PP-0084-2014*, section 3.2.
Only those originating in *AUG* and those introduced in this Security Target are detailed in the following section.

110

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.
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.

3.3 Organisational security policies

111 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.

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

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

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

115 New Organisational Security Policies (OSPs) are defined here below:

116 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.

117 P.Resp-Appl is related to the ES that is part of the evaluation, and valid in case NesLib is embedded in the TOE.

BSI.P.Process-TOE	Identification during TOE Development and Production: An accurate identification ***is*** established for the TOE. This requires that each instantiation of the TOE carries this unique identification.
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality: The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. He limits the capability and blocks the availability of the Loader in order to protect stored data from disclosure and manipulation.
AUG1.P.Add-Functions	Additional Specific Security Functionality: The TOE shall provide the following specific security functionality to the Security IC Embedded Software: – Triple Data Encryption Standard (TDES), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded***,*** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded***,*** – Rivest-Shamir-Adleman (RSA)***,*** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, – ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded.
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.
P.Resp-Appl	Treatment of user data: The Security IC Embedded Software, part of the TOE, treats user data according to the assumption A.Resp-Appl defined in *BSI-CC-PP-0084-2014*.

3.4 Assumptions

118 The following assumptions are described in the *BSI-CC-PP-0084-2014*, section 3.4.

BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
BSI.A.Resp-Appl	Treatment of User Data of the Composite TOE

4 Security objectives (ASE_OBJ)

119 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.

120 A summary of all security objectives is provided in *Table 6*.

121 Note that the origin of each objective is clearly identified in the prefix of its label.
Most of these security aspects can therefore be easily found in the *BSI-CC-PP-0084-2014*, sections 4.1 and 7.3. Only those originating in *AUG*, and the ones introduced in this Security Target, are detailed in the following sections.

Table 6. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control
	O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software
	O.Resp-Appl	Treatment of user data
	O.Firewall	Application firewall
Environments	BSI.OE.Resp-Appl	Treatment of User Data of the Composite TOE
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing
	BSI.OE.Lim-Block-Loader	Limitation of capability and blocking the Loader

4.1 Security objectives for the TOE

BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
BSI.O.Phys-Probing	Protection against Physical Probing
BSI.O.Malfunction	Protection against Malfunctions
BSI.O.Phys-Manipulation	Protection against Physical Manipulation
BSI.O.Leak-Forced	Protection against Forced Information Leakage
BSI.O.Abuse-Func	Protection against Abuse of Functionality
BSI.O.Identification	TOE Identification
BSI.O.RND	Random Numbers
BSI.O.Cap-Avail-Loader	Capability and Availability of the Loader
AUG1.O.Add-Functions	Additional Specific Security Functionality: The TOE must provide the following specific security functionality to the ***Security IC*** Embedded Software: – Triple Data Encryption Standard (TDES), – Advanced Encryption Standard (AES), – ***Elliptic Curves Cryptography on GF(p),*** if NesLib is embedded***,*** – ***Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512),*** if NesLib is embedded***,*** – Rivest-Shamir-Adleman (RSA)***,*** if NesLib is embedded, – ***Deterministic Random Bit Generator (DRBG),*** if NesLib is embedded, – ***Keccak,*** if NesLib is embedded, – ***Keccak-p,*** if NesLib is embedded, – ***Diffie-Hellman,*** if NesLib is embedded, – ***Prime Number Generation,*** if NesLib is embedded***.***
AUG4.O.Mem-Access	***Dynamic*** Area based Memory Access Control: The TOE must provide the ***Security IC*** Embedded Software with the capability to define ***dynamic memory segmentation and protection***. The TOE must then enforce ***the defined access rules*** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.
O.Controlled-ES-Loading	Controlled loading of the Security IC Embedded Software: The TOE must provide the capability to load the Security IC Embedded Software into the NVM, either before TOE delivery, under ST authority, either after TOE delivery, under the composite product manufacturer authority. The TOE must restrict the access to these features. The TOE must provide control means to check the integrity of the loaded user data. This capability is not available in User configuration.

O.Resp-Appl	Treatment of user data: Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant user data to unauthorised users or processes when communicating with a terminal.
O.Firewall	Application firewall: The TOE provides a service to ensure isolation of data and code between a Protected Application and the other applications. Another application shall not read, write, compare any piece of data or code belonging to the Protected Application.

4.2 Security objectives for the environment

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

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

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

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

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

4.3 Security objectives rationale

124 The main line of this rationale is that the inclusion of all the security objectives of the *BSI-CC-PP-0084-2014* Protection Profile, together with those in *AUG*, and those introduced in this ST, guarantees that all the security environment aspects identified in *Section 3* are addressed by the security objectives stated in this chapter.

125 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).

126 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*)".

127 The augmentation made in this ST introduces 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 policies "Controlled loading of the Security IC Embedded Software, (*P.Controlled-ES-Loading*)", and "Treatment of user data, (*P.Resp-Appl*)".

128 The justification of the additional policies, and additional threats provided in the next subsections shows that they do not contradict to the rationale already given in the Protection Profile *BSI-CC-PP-0084-2014* for the assumptions, policy and threats defined there.

Table 7. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.P.Lim-Block-Loader	*BSI.O.Cap-Avail-Loader* *BSI.OE.Lim-Block-Loader*	Phase 5-6 optional Phase 4
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
P.Controlled-ES-Loading	*O.Controlled-ES-Loading*	Phase 4-6
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	
P.Resp-Appl	*O.Resp-Appl*	
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func*	
BSI.T.RND	*BSI.O.RND*	
AUG4.T.Mem-Access	*AUG4.O.Mem-Access*	
T.Confid-Applic-Code	*O.Firewall*	
T.Confid-Applic-Data	*O.Firewall*	
T.Integ-Applic-Code	*O.Firewall*	
T.Integ-Applic-Data	*O.Firewall*	

4.3.1 TOE threat "Memory Access Violation"

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

130 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.

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

4.3.2 TOE threat "Application code confidentiality"

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

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

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

4.3.3 TOE threat "Application data confidentiality"

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

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

4.3.4 TOE threat "Application code integrity"

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

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

4.3.5 TOE threat "Application data integrity"

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

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

4.3.6 Organisational security policy "Additional Specific Security Functionality"

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

142 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.

143 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*.

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

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

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

146 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.

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

4.3.8 Organisational security policy "Treatment of user data"

148 The justification related to the organisational security policy "Treatment of user data, (*P.Resp-Appl*)" is as follows:

149 The policy states that the Security IC Embedded Software included in the TOE, treats user data according to the PP assumption *BSI.A.Resp-Appl*. *O.Resp-Appl* has the same objective as *BSI.OE.Resp-Appl* defined in the PP. Thus, the objectives *O.Resp-Appl* covers the policy *P.Resp-Appl*.

150 The added objective for the TOE *O.Resp-Appl* does not introduce any contradiction in the security objectives.

5 Extended Components (ASE_ECD)

151 This Security Target uses the extended Security Functional Requirements **FAU_SAS.1** Audit data storage defined in the *Eurosmart - Security IC Platform Protection Profile with Augmentation Packages* (*BSI-CC-PP-0084-2014*).

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

6 Security requirements (ASE_REQ)

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

6.1 Security functional requirements for the TOE

154 Security Functional Requirements (SFRs) from the "*BSI-CC-PP-0084-2014*" Protection Profile (PP) have been updated as necessary to meet *CCMB-2022-11-002 R1* (see rationale *Section 2.3.2*)

155 All iterations, assignments, selections, or refinements on SFRs have been performed according to section 8.2 of *CCMB-2022-11-001 R1*. 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.

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

157 The selected security functional requirements for the TOE, their respective origin and type are summarized in *Table 8*.

Table 8. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-CC-PP-0084-2014*	*CCMB-2022-11-002 R1*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1 / Test	Limited capabilities	Abuse of Test functionality	*BSI-CC-PP-0084-2014*	
FMT_LIM.2 / Test	Limited availability			
FMT_LIM.1 / Loader	Limited capabilities	Abuse of Loader functionality	*BSI-CC-PP-0084-2014* Operated	
FMT_LIM.2 / Loader	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification		Extended
FDP_SDC.1	Stored data confidentiality	Physical manipulation & probing		*CCMB-2022-11-002 R1*
FDP_SDI.2	Stored data integrity monitoring and action			
FPT_PHP.3	Resistance to physical attack		*BSI-CC-PP-0084-2014*	
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1	Random number generation	Weak cryptographic quality of random numbers	*BSI-CC-PP-0084-2014* Operated	

Table 8. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	CCMB-2022-11-002 R1
FCS_CKM.1 (if NesLib is embedded)	Cryptographic key generation		Security Target Operated	
FDP_ACC.2 / Memories	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1 / Memories	Security attribute based access control		*AUG* #4 Operated	
FMT_MSA.3 / Memories	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Memories	Management of security attribute			
FMT_SMF.1 / Memories	Specification of management functions		Security Target Operated	
FDP_ITC.1 / Loader	Import of user data without security attributes	User data loading access violation	Security Target Operated	CCMB-2022-11-002 R1
FDP_ACC.1 / Loader	Subset access control			
FDP_ACF.1 / Loader	Security attribute based access control			
FMT_MSA.3 / Loader	Static attribute initialisation	Correct operation		
FMT_MSA.1 / Loader	Management of security attribute			
FMT_SMR.1 / Loader	Security roles	Abuse of Admin functionality		
FIA_UID.1 / Loader	Timing of identification			
FMT_SMF.1 / Loader	Specification of management functions			
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			

6.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

158 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)

159 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.***

160 ***Refinements:***

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

Regarding application note 14 of BSI-CC-PP-0084-2014, the secure state is reached by an immediate interrupt or by a reset, depending on the current context.

Regarding application note 15 of BSI-CC-PP-0084-2014, the TOE provides information on the operating conditions monitored during Security IC Embedded Software execution and after a warm reset. No audit requirement is however selected in this Security Target.

Limited capabilities (FMT_LIM.1) / Test

161 The TSF shall limit its 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

162 The TSF shall be designed in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1) / Test" the following policy is enforced: ***Limited capability and availability Policy / Test***.

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

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

Audit storage (FAU_SAS.1)

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

Stored data confidentiality (FDP_SDC.1)

165 The TSF shall ensure the confidentiality of the information of ***all user data*** while it is stored in ***any memory***.

Stored data integrity monitoring and action (FDP_SDI.2)

166 The TSF shall monitor user data stored in containers controlled by the TSF for ***integrity errors*** on all objects, based on the following attributes: ***user data stored in all possible memory areas, depending on the integrity control attributes***.

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

Resistance to physical attack (FPT_PHP.3)

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

169 ***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)

170 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)

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

172 ***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)

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

174 *SFP_2: Data Processing Policy*

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

Random number generation (FCS_RNG.1)

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

- ***(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.***
- ***(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.***
- ***(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.***
- ***(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.***
- ***(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.***

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

- ***(PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.***
- ***(PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.***

6.1.2 Additional Security Functional Requirements for the cryptographic services

Cryptographic operation (FCS_COP.1)

177 The TSF shall perform ***the operations in*** *Table 9* in accordance with a specified cryptographic algorithm ***in*** *Table 9* and cryptographic key sizes ***of*** *Table 9* that meet the ***standards in*** *Table 9*. ***The list of operations may depend on the presence of NesLib, as indicated in*** *Table 9* ***(Restrict).***

Table 9. FCS_COP.1 iterations (cryptographic operations)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm](1)	[assignment: cryptographic key sizes]	[assignment: list of standards]
	TDES(2)	* encryption * decryption - in Cipher Block Chaining (CBC) mode - in Electronic Code Book (ECB) mode	Triple Data Encryption Standard (TDES)	112 bits 168 bits	*NIST SP 800-67* *NIST SP 800-38A*
	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*
If NesLib		* Message authentication Code computation (CMAC) * Authenticated encryption/decryption in Galois Counter Mode (GCM) * Authenticated encryption/decryption in Counter with CBC-MAC (CCM)			*NIST SP 800-38B* *NIST SP 800-38A* *NIST SP 800-38D* *NIST SP 800-38C*
If NesLib	RSA(3)	* RSA public key operation * RSA private key operation without the Chinese Remainder Theorem * RSA private key operation with the Chinese Remainder Theorem * EMSA PSS and PKCS1 signature scheme coding * RSA Key Encapsulation Method (KEM)	Rivest, Shamir & Adleman's	up to 4096 bits	*PKCS #1 V2.1*

Table 9. FCS_COP.1 iterations (cryptographic operations) (continued)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm][1]	[assignment: cryptographic key sizes]	[assignment: list of standards]
If NesLib	ECC on Weierstrass curves	* private scalar multiplication * prepare Jacobian * public scalar multiplication * point validity check * convert Jacobian to affine coordinates * general point addition * point expansion * point compression	Elliptic Curves Cryptography on GF(p) on curves in Weierstrass form[4]	up to 640 bits	*IEEE 1363-2000, chapter 7* *IEEE 1363a-2004*
		* Diffie-Hellman (ECDH) key agreement computation			*NIST SP 800-56A*
		* digital signature algorithm (ECDSA) generation and verification			*FIPS PUB 186-4* *ANSI X9.62, section 7*
If NesLib	ECC on Edwards curves	* ed25519 generation * ed25519 verification * ed25519 point decompression	Elliptic Curves Cryptography on GF(p) on curves in Edwards form, with curve 25519	256 bits	*EdDSA rfc* *EDDSA* *EDDSA2*
If NesLib	SHA	* SHA-1[5] * SHA-224 * SHA-256 * SHA-384 * SHA-512 * Protected SHA-1[1] * Protected SHA-256 * Protected SHA-384 * Protected SHA-512	Secure Hash Algorithm	assignment pointless because algorithm has no key	*FIPS PUB 180-2*
		* HMAC using Protected SHA-1or Protected SHA-256[6]		up to 512 bits	*FIPS PUB 198-1*

Table 9. FCS_COP.1 iterations (cryptographic operations) (continued)

Restrict	Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm][1]	[assignment: cryptographic key sizes]	[assignment: list of standards]
If NesLib	Keccak and SHA-3	* SHAKE128, * SHAKE256, * SHA3-224, * SHA3-256, * SHA3-384, * SHA3-512, * Keccak[r,1600-r], * protected SHAKE128, * protected SHAKE256, * protected SHA3-224, * protected SHA3-256, * protected SHA3-384, * protected SHA3-512, * Protected Keccak[r,1600-r]	Keccak	no key for plain functions, variable key length up to security level for protected functions (security level is last number in function names and 1600-c for Keccak)	*FIPS PUB 202*
If NesLib	Keccak-p	* Keccak-p[1600,n_r = 24], * Keccak-p[1600, n_r=12], * protected Keccak-p[1600,n_r = 24], * protected Keccak-p[1600, n_r=12]	Keccak-p	no key for plain functions, any key length up to 256 bits for protected functions	*FIPS PUB 202*
If NesLib	Diffie-Hellman	Diffie-Hellman	Diffie-Hellman	up to 3968 bits	*ANSI X9.42*
If NesLib	DRBG(7)	* SHA-1 * SHA-224 * SHA-256 * SHA-384 * SHA-512	Hash-DRBG	None	*NIST SP 800-90* *FIPS PUB 180-2*
		*AES	CTR-DRBG	128, 192 and 256 bits	*NIST SP 800-90* *FIPS PUB 197*

1. Note that there is no claimed security beyond the algorithmic security of the implemented cryptographic algorithms. The security of cryptographic algorithms can change at any point in time following cryptanalysis results by the scientific community or advances in computation techniques. Recommendations for the use of TSF cryptographic mechanisms are provided in documents *ECCG ACM* for EUCC and *PG-083* for France.
Therefore it is up to the user to satisfy the requirements of these algorithms by respecting the recommendations and rules given in these documents, for instance regarding the secrecy, the length and the minimum entropy of keys and the uniqueness of nonces. Also, some algorithms are parameterized, and for these the choice of parameters and its consequences on the algorithmic security is left to the user's appreciation.

2. Single DES and triple DES with two keys are no longer recommended as encryption functions. Triple DES with three keys can be used until end 2027 as recommended in *ECCG ACM*. However depending on the context of use, the Embedded Software that may need to use triple DES with three keys might be submitted to a dedicated cryptographic analysis evaluation, for instance in France the use of triple DES with three keys is not recommended anymore since end 2025, cf. *PG-083*.
3. It is recommended for RSA primitive to use modulus of size equal or higher to 3000 bits and 16-bit long public exponent since 2026 in *ECCG ACM*.
4. Elliptic curve cryptographic algorithms should be used with elliptic curves that have no known weaknesses and preferably standard ones. Some recommended curves are given in *ECCG ACM*. More curves can be used, the composite product certification will determine the correct use of elliptic curves during the cryptographic analysis.
5. Note that SHA-1 and SHA-224 are no longer recommended as a cryptographic function. Hence, Security IC Embedded Software may need to use another SHA to achieve a suitable strength.
6. HMAC-SHA-1 is only recommended for use until end 2030 in *ECCG ACM*.
7. NesLib gives support to Hash-DRBG and CTR-DRBG as specified in Section 10 of *NIST SP 800-90*. The implementation is following the specification of the Section 10 of *NIST SP 800-90*.

Cryptographic key generation (FCS_CKM.1)

178 If NesLib is embedded only, the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm***, in*** *Table 10****,*** and specified cryptographic key sizes ***of*** *Table 10* that meet the following ***standards in*** *Table 10****.***

Table 10. FCS_CKM.1 iterations (cryptographic key generation)

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

1. As it is recommended for RSA primitive to use modulus of size equal or higher to 3000 bits and 16-bit long public exponent since 2026 in *ECCG ACM*, prime and RSA key generation methods shall be used to generate such proper key lengths.

6.1.3 Additional Security Functional Requirements for the memories protection

179 The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the memories protection.

Static attribute initialisation (FMT_MSA.3) / Memories

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

b. See the Datasheet referenced in *Section 8* for actual values.

181 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

182 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

183 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.

184 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

185 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.***

186 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.***

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

188 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.***

189 **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.

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

191 *SFP_3: Dynamic Memory Access Control Policy*

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

Specification of management functions (FMT_SMF.1) / Memories

192 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.***

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

Limited capabilities (FMT_LIM.1) / Loader

193 The TSF shall limit its capabilities so that in conjunction with “Limited availability (FMT_LIM.2)” the following policy is enforced: ***Loader Limited capability Policy.***

194 *SFP_4: Loader Limited capability Policy*

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

Limited availability (FMT_LIM.2) / Loader

196 The TSF shall be designed in a manner that limits its availability so that in conjunction with “Limited capabilities (FMT_LIM.1)” the following policy is enforced: ***Loader Limited availability Policy***.

197 *SFP_5: Loader Limited availability Policy*

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

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

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

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

201 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

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

203 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

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

Subset access control (FDP_ACC.1) / Loader

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

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

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

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

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

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

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

211 *SFP_6: Loading Access Control Policy*

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

Specification of management functions (FMT_SMF.1) / Loader

213 The TSF will be able to perform the following management functions: ***change the TOE mode, change the user role, change the remaining sessions.***

Security roles (FMT_SMR.1) / Loader

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

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

Timing of identification (FIA_UID.1) / Loader

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

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

6.1.5 Additional Security Functional Requirements related to the Application Firewall

218 The following SFRs are extensions to "*BSI-CC-PP-0084-2014*" Protection Profile (PP), related to the protections by the Application Firewall.

Subset access control (FDP_ACC.1) / APPLI_FWL

219 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

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

221 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.***

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

223 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.***

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

225 *SFP_7: Protected Application Firewall Access Control Policy*

226 *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

227 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.

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

6.2 TOE security assurance requirements

229 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.
- ***ALC_FLR.2.***

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

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

232 The set of security assurance requirements (SARs) is presented in *Table 11*, indicating the origin of the requirement.

Table 11. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-CC-PP-0084-2014*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-CC-PP-0084-2014*
ADV_INT.2	Well-stuctured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/*BSI-CC-PP-0084-2014*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/*BSI-CC-PP-0084-2014*
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-CC-PP-0084-2014*
ALC_DVS.2	Sufficiency of security measures	*BSI-CC-PP-0084-2014*
ALC_FLR.2	Flaw reporting procedures	Security Target
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-CC-PP-0084-2014*
ALC_TAT.2	Compliance with implementation standards	EAL5
ASE_CCL.1	Conformance claims	EAL5/*BSI-CC-PP-0084-2014*
ASE_ECD.1	Extended components definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_INT.1	ST introduction	EAL5/*BSI-CC-PP-0084-2014*
ASE_OBJ.2	Security objectives	EAL5/*BSI-CC-PP-0084-2014*
ASE_REQ.2	Derived security requirements	EAL5/*BSI-CC-PP-0084-2014*
ASE_SPD.1	Security problem definition	EAL5/*BSI-CC-PP-0084-2014*
ASE_TSS.1	TOE summary specification	EAL5/*BSI-CC-PP-0084-2014*
ATE_COV.2	Analysis of coverage	EAL5/*BSI-CC-PP-0084-2014*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-CC-PP-0084-2014*
ATE_IND.2	Independent testing - sample	EAL5/*BSI-CC-PP-0084-2014*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-CC-PP-0084-2014*

6.3 Refinement of the security assurance requirements

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

234 The main customizing is that the IC Dedicated Software is an operational part of the TOE after delivery, although it is mainly not available to the user.

235 Regarding application note 23 of *BSI-CC-PP-0084-2014*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

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

237 For reader's ease, an impact summary is provided in *Table 12*.

Table 12. Impact of EAL5 selection on *BSI-CC-PP-0084-2014* refinements

Assurance Family	*BSI-CC-PP-0084-2014* Level	ST Level	Impact on refinement
ADO_DEL	1	1	None
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	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

6.3.1 Refinement regarding functional specification (ADV_FSP)

238 ~~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.***

239 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.

240 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.

241 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.

242 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.

243 Since the selected higher-level assurance component requires a security functional specification presented in a “semi-formal style" (ADV_FSP.5.2C) the changes affect the style of description, the *BSI-CC-PP-0084-2014* refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

6.3.2 Refinement regarding test coverage (ATE_COV)

244 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~~ ***NVM*** writing).

245 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).

246 ~~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.***

6.4 Security Requirements rationale

6.4.1 Rationale for the Security Functional Requirements

247 Just as for the security objectives rationale of *Section 4.3*, the main line of this rationale is that the inclusion of all the security requirements of the *BSI-CC-PP-0084-2014* Protection Profile, together with those in *AUG*, and with those introduced in this Security Target, guarantees that all the security objectives identified in *Section 4* are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

Table 13. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
BSI.O.Leak-Inherent	*Basic internal transfer protection FDP_ITT.1* *Basic internal TSF data transfer protection FPT_ITT.1* *Subset information flow control FDP_IFC.1*
BSI.O.Phys-Probing	*Stored data confidentiality FDP_SDC.1* *Resistance to physical attack FPT_PHP.3*
BSI.O.Malfunction	*Limited fault tolerance FRU_FLT.2* *Failure with preservation of secure state FPT_FLS.1*
BSI.O.Phys-Manipulation	*Stored data integrity monitoring and action FDP_SDI.2* *Resistance to physical attack FPT_PHP.3*
BSI.O.Leak-Forced	All requirements listed for *BSI.O.Leak-Inherent* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1* plus those listed for *BSI.O.Malfunction* and *BSI.O.Phys-Manipulation* *FRU_FLT.2*, *FPT_FLS.1*, *FDP_SDI.2*, *FPT_PHP.3*
BSI.O.Abuse-Func	*Limited capabilities FMT_LIM.1 / Test* *Limited availability FMT_LIM.2 / Test* plus those for *BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FDP_SDI.2*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.O.Identification	*Audit storage FAU_SAS.1*
BSI.O.RND	*Random number generation FCS_RNG.1* plus those for *BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced* *FDP_ITT.1*, *FPT_ITT.1*, *FDP_IFC.1*, *FDP_IFC.1*, *FDP_SDC.1*, *FPT_PHP.3*, *FRU_FLT.2*, *FPT_FLS.1*
BSI.OE.Resp-Appl	Not applicable
BSI.OE.Process-Sec-IC	Not applicable
AUG1.O.Add-Functions	*Cryptographic operation FCS_COP.1* *Cryptographic key generation FCS_CKM.1*
AUG4.O.Mem-Access	*Complete access control FDP_ACC.2 / Memories* *Security attribute based access control FDP_ACF.1 / Memories* *Static attribute initialisation FMT_MSA.3 / Memories* *Management of security attribute FMT_MSA.1 / Memories* *Specification of management functions FMT_SMF.1 / Memories*
BSI.O.Cap-Avail-Loader	*Limited capabilities FMT_LIM.1 / Loader* *Limited availability FMT_LIM.2 / Loader*

Table 13. Security Requirements versus Security Objectives

Security Objective	TOE Security Functional and Assurance Requirements
O.Controlled-ES-Loading	*Import of user data without security attributes FDP_ITC.1 / Loader* *Subset access control FDP_ACC.1 / Loader* *Security attribute based access control FDP_ACF.1 / Loader* *Static attribute initialisation FMT_MSA.3 / Loader* *Management of security attribute FMT_MSA.1 / Loader* *Specification of management functions FMT_SMF.1 / Loader* *Security roles FMT_SMR.1 / Loader* *Timing of identification FIA_UID.1 / Loader*
O.Resp-Appl	All SFRs defined additionnaly in the ST
O.Firewall	*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*

248 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 8* and *Table 13*, it can be verified that the justifications provided by the *BSI-CC-PP-0084-2014* Protection Profile and *AUG* can just be carried forward to their union.

249 From *Table 6*, it is straightforward to identify additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem-Access*) tracing back to *AUG*, and additional objectives (*O.Controlled-ES-Loading, O.Resp-Appl,* and *O.Firewall*) introduced in this Security Target. This rationale must show that security requirements suitably address them all.

250 Furthermore, a careful observation of the requirements listed in *Table 8* and *Table 13* shows that:

- there are security requirements introduced from *AUG* (*FCS_COP.1*, *FDP_ACC.2 / Memories*, *FDP_ACF.1 / Memories*, *FMT_MSA.3 / Memories* and *FMT_MSA.1 / Memories*),
- there are additional security requirements introduced by this Security Target (*FCS_CKM.1*, *FDP_ITC.1 / Loader*, *FDP_ACC.1 / Loader*, *FDP_ACF.1 / Loader*, *FMT_MSA.3 / Loader*, *FMT_MSA.1 / Loader*, *FMT_SMF.1 / Loader*, *FMT_SMR.1 / Loader*, *FIA_UID.1 / Loader*, *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+).

251 Though it remains to show that:

- security objectives from this Security Target and from *AUG* are addressed by security requirements stated in this chapter,
- additional security requirements from this Security Target and from *AUG* are mutually supportive with the security requirements from the *BSI-CC-PP-0084-2014* Protection Profile, and they do not introduce internal contradictions,
- all dependencies are still satisfied.

252 The justification that the additional security objectives are suitably addressed, that the additional security requirements are mutually supportive and that, together with those

already in *BSI-CC-PP-0084-2014*, they form an internally consistent whole, is provided in the next subsections.

6.4.2 Additional security objectives are suitably addressed

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

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

254 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.

255 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*)”

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

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

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

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

259 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.

260 The security functional requirement "*Static attribute initialisation (FMT_MSA.3) / Loader*" requires that the TOE provides default values for security attributes. The ability to update the security attributes is restricted to privileged subject(s) as further detailed in the security functional requirement "*Management of security attributes (FMT_MSA.1) / Loader*". The security functional requirements"*Security roles (FMT_SMR.1) / Loader*" and "*Timing of identification (FIA_UID.1) / Loader*" specifies the roles that the TSF recognises and the

actions authorised before their identification.The security functional requirement "*Specification of management functions (FMT_SMF.1) / Loader*" provides additional controlled facility for adapting the loader behaviour to the user's needs. These management functions ensure that the required access control, associated to the loading feature, can be realised using the functions provided by the TOE.

Security objective "Treatment of user data (*O.Resp-Appl*)"

261 The justification related to the security objective "Treatment of user data (*O.Resp-Appl*)" is as follows:

262 The objective was translated from an environment objective in the PP into a TOE objective in this ST. The objective is that "Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context." The application context is defined by the security environment described in this ST. The additional SFRs defined in this ST do address the additional TOE objectives of the ST based on the ST security environment, therefore *O.Resp-Appl* is fulfilled by the additional ST SFRs.

Security objective "Application firewall (*O.Firewall*)"

263 The justification related to the security objective "Application firewall (*O.Firewall*)" is as follows:

264 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*.

6.4.3 Additional security requirements are consistent

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

265 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*)"**

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

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

267 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*),**

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

6.4.4 Dependencies of Security Functional Requirements

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

- those justified in the *BSI-CC-PP-0084-2014* Protection Profile security requirements rationale,
- those justified in *AUG* security requirements rationale,
- the dependency of *FCS_COP.1* and *FCS_CKM.1* on FCS_CKM.6 (see discussion below).
- the dependency of *FMT_MSA.3 / APPLI_FWL* on FMT_MSA.1 and FMT_SMR.1 (see discussion below).

270 Details are provided in *Table 14* below.

Table 14. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-CC-PP-0084-2014*
FPT_FLS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Test	FMT_LIM.2 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Test	FMT_LIM.1 / Test	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.1 / Loader	FMT_LIM.2 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FMT_LIM.2 / Loader	FMT_LIM.1 / Loader	Yes	Yes, *BSI-CC-PP-0084-2014*
FAU_SAS.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_SDC.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*

Table 14. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FDP_SDI.2	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FPT_PHP.3	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, *BSI-CC-PP-0084-2014*
FPT_ITT.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-CC-PP-0084-2014*	Yes, *BSI-CC-PP-0084-2014*
FCS_RNG.1	None	No dependency	Yes, *BSI-CC-PP-0084-2014*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, or FCS_CKM.5]	Yes, by FDP_ITC.1 and FCS_CKM.1, see discussion below	Yes, *AUG* ***#1***
	FCS_CKM.6	No, see discussion below	
FCS_CKM.1	[FDP_CKM.2 or FCS_CKM.5 or FCS_COP.1]	Yes, by FCS_COP.1	
	[FCS_RBG.1 or FCS_RNG.1]	Yes, by FCS_RNG.1	
	FCS_CKM.6	No, see discussion below	
FDP_ACC.2 / Memories	FDP_ACF.1 / Memories	Yes	***No,*** *CCMB-2022-11-002 R1*
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-2022-11-002 R1*
	FMT_SMR.1 / Memories	No, see *AUG* ***#4***	Yes, *AUG* ***#4***

Table 14. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-CC-PP-0084-2014* or in *AUG*
FMT_SMF.1 / Memories	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FMT_ITC.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_MSA.3 / Loader	Yes	
FDP_ACC.1 / Loader	FDP_ACF.1 / Loader	Yes	***No,*** *CCMB-2022-11-002 R1*
FDP_ACF.1 / Loader	FDP_ACC.1 / Loader	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_MSA.3 / Loader	Yes	
FMT_MSA.3 / Loader	FMT_MSA.1 / Loader	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_SMR.1 / Loader	Yes	
FMT_MSA.1 / Loader	[FDP_ACC.1 / Loader or FDP_IFC.1]	Yes	***No,*** *CCMB-2022-11-002 R1*
	FDP_SMF.1 / Loader	Yes	
	FDP_SMR.1 / Loader	Yes	
FMT_SMR.1 / Loader	FIA_UID.1 / Loader	Yes	***No,*** *CCMB-2022-11-002 R1*
FIA_UID.1 / Loader	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FDP_SMF.1 / Loader	None	No dependency	***No,*** *CCMB-2022-11-002 R1*
FDP_ACC.1 / APPLI_FWL	FDP_ACF.1 / APPLI_FWL	Yes	***No,*** *CCMB-2022-11-002 R1*
FDP_ACF.1 / APPLI_FWL	FDP_ACC.1 / APPLI_FWL	Yes	***No,*** *CCMB-2022-11-002 R1*
	FMT_MSA.3 / APPLI_FWL	Yes	
FMT_MSA.3 / APPLI_FWL	FMT_MSA.1	No, see discussion below	***No,*** *CCMB-2022-11-002 R1*
	FMT_SMR.1	No, see discussion below	

271 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" on "Import of user data without security attributes (FDP_ITC.1)" or "Import of user data with security attributes (FDP_ITC.2)" or "Cryptographic key generation (FCS_CKM.1)". In this particular TOE, both "*Cryptographic key generation (FCS_CKM.1)*" and "*Import of user data without security attributes (FDP_ITC.1) / Loader*" may be used for the purpose of creating cryptographic keys, but also, the ES has all possibilities to implement its own creation function, in conformance with its security policy.

272 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" and "*Cryptographic key generation (FCS_CKM.1)*" on "Timing and event of cryptographic key destruction (FCS_CKM.6)". 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.

273 Part 2 of the Common Criteria defines the dependency of "*Static attribute initialisation (FMT_MSA.3) / APPLI_FWL*" on "Management of security attributes (FMT_MSA.1)" and "Security roles (FMT_SMR.1)". For this particular instantiation of the access control attributes aimed at protecting a Protected Application code and data from unauthorised accesses, the security attributes are only static, initialized at product start. Therefore, there is no need to identify management capabilities and associated roles in form of Security Functional Requirements "FMT_MSA.1" and "FMT_SMR.1".

6.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5 (*Table 11*)

274 Regarding application note 22 of *BSI-CC-PP-0084-2014*, this Security Target chooses EAL5 with augmentations because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

275 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.

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

277 The assurance components in an evaluation assurance level (EAL) are chosen in a way that they build a mutually supportive and complete set of components. All dependencies introduced by the requirements chosen for augmentation are fulfilled. Therefore, these components add additional assurance to EAL5, but the mutual support of the requirements and the internal consistency is still guaranteed.

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

Dependencies of assurance requirements

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

280 The augmentation to this package identified in paragraph *229* does not introduce dependencies not already satisfied by the EAL5 package, and is considered as consistent augmentation:

- ALC_FLR.2 has no dependency.

7 TOE summary specification (ASE_TSS)

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

7.1 Limited fault tolerance (FRU_FLT.2)

282 The TSF provides limited fault tolerance, by managing the following circumstances:

- NVM cell depletion: The TOE provides mechanisms and drivers to detect cell depletion in the NVM, and to repair the depleted cells.
- Faults attacks on code and/or data: The TOE provides the ES with the capability to sign code and/or data on the buses.
- TRNG failure: The TOE monitors the random source, implementing the total failure test, and provides a TRNG with enough entropy at each read-out.
- Fault attacks on the cryptographic library: The Cryptographic library NesLib provides protection against fault attacks on those functions sensitive to such attacks (if NesLib is embedded only).
- Fault attack on the enhanced DES: The TOE provides the ES with the capability to check the blinded SBoxes value.
- SFM single-bit errors: the SFM library automatically corrects a single-bit error within a byte upon a NVM read (if SFM is embedded only).

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

283 The TSF provides preservation of secure state by detecting and managing the following failures:

- High voltage supply,
- Glitches,
- Die integrity violation detection,
- Illegal scan attempt,
- Incorrect NVM access attempt,
- Double read error on NVM,
- NVM protect,
- NVM hard fail,
- NVM, ROM or RAM parity errors,
- MPU error,
- Register integrity,
- SC300 parity,
- SC300 error,
- Watchdog reset,
- Fault attack to NesLib (if NesLib is embedded only).
- SFM 2-bits error on NVM (if SFM is embedded only).

284 The secure state is reached by an immediate reset and run.

285 The ES can generate a software reset, either simple or infinite (reset and wait).

7.3 Limited capabilities (FMT_LIM.1) / Test

286 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.

7.4 Limited capabilities (FMT_LIM.1) / Loader

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

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

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

289 In Admin configuration, the TOE is either in Final Test OS, Install Mode, User Emulation Mode or Diagnostic Mode.

290 In User configuration, the TOE is either in User Mode or Diagnostic Mode.

7.6 Stored data confidentiality (FDP_SDC.1)

291 The TSF ensures confidentiality of the User Data, thanks to the following features:

- Memories scrambling and encryption,
- Protection of NVM sectors,
- MPU,
- LPU.

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

292 The TSF ensures stored data integrity, thanks to the following features:

- Memories parity control,
- Protection of NVM sectors,
- MPU,
- LPU.

7.8 Audit storage (FAU_SAS.1)

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

7.9 Resistance to physical attack (FPT_PHP.3)

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

- The TOE implements a set of countermeasures that reduce the exploitability of physical probing.
- The TOE is physically protected by active shields that command an automatic reaction on die integrity violation detection.

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

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

- Memories scrambling and encryption,
- Bus encryption,
- RAM content destruction and register cleaning upon reset,
- Clocks jittering,
- Mechanisms for operation execution concealment.

7.11 Random number generation (FCS_RNG.1)

296 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.

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

297 The TOE provides an EDES+ accelerator that has the capability to perform 3-key Triple DES encryption and decryption in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode conformant to *NIST SP 800-67* and *NIST SP 800-38A*.

If NesLib is embedded, the cryptographic library NesLib instantiates the same standard DES cryptographic operations, in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode.

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

298 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.

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

300 If NesLib is embedded, the cryptographic library NesLib instantiates the same standard AES cryptographic operations, in Electronic Code Book (ECB) and Cipher Block Chaining (CBC) mode, and additionally provides:

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

7.14 Cryptographic operation: RSA operation (FCS_COP.1) / RSA, only if NesLib

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

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

7.15 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1) / ECC, only if NesLib

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

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

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

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

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

- generation,
- verification,
- point decompression.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Hash-DRBG,
- CTR-DRBG.

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

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

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

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

7.23 Static attribute initialisation (FMT_MSA.3) / Memories

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

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

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

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

320 The TOE enforces the dynamic memory protection policy for data access and code access thanks to a dynamic Memory Protection Unit (MPU), programmed by the ES.
Overriding the MPU set of access rights, the TOE enforces:

- an additional protection of the NVM sectors against modification (write and erase), programmed by the ES,
- a permanent protection of the OST ROM and, in User configuration, a protection of the ST NVM against write accesses.

7.26 Static attribute initialisation (FMT_MSA.3) / Loader

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

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

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

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

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

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

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

7.30 Subset access control (FDP_ACC.1) / APPLI_FWL & Security attribute based access control (FDP_ACF.1) / APPLI_FWL

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

7.31 Static attribute initialisation (FMT_MSA.3) / APPLI_FWL

326 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.

8 Identification

Table 15. TOE components

IC Maskset name	IC version	Master identification number (1)	Firmware version	OST version	Optional NesLib crypto library version(2)	Optional SFM library version
K8H0A(3)	H	01BCh (ST33G1M2)	1.3.2	2.2	6.3.4	1.0.8

1. Part of the product information.
2. See the NesLib User Manual referenced in *Table 16: Guidance documentation*.
3. This maskset K8H0A rev H corresponds to product line K8M0.

Table 16. Guidance documentation

Component description	Reference	Version
ST33G1M2A: Secure MCU with 32-bit ARM SecurCore SC300 - Datasheet	DS_ST33G1M2A	3
ST33G1M2A ST33G1M2M Die description: CMOS M10+ 80-nm technology die and wafer delivery description	DD_ST33G1M2	2
ARM® Cortex SC300 r0p0 Technical Reference Manual	ARM DDI 0337F	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
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
ST33G1M2A firmware - User manual	UM_ST33G1M2A_M_FW	11
Addendum for ST33G Firmware User Manual	TN_UM_ST33G_FW_Addendum	1
ST33G and ST33H Firmware support for LPU regions - application note	AN_33G_33H_LPU	1
NesLib cryptographic library NesLib 6.3 - User manual	UM_NesLib_6.3	4
ST33G and ST33H secure MCU platforms - NesLib 6.3 security recommendations - Application note	AN_SECU_ST33G_H_NESLIB_6.3	10
NesLib 6.3.4 for ST33G, ST33H and ST33I platforms - Release note	RN_ST33_NESLIB_6.3.4	7
StoreKeeper v1.0 - User manual	UM_StoreKeeper	3
Security recommendation Application Note SFM Library 1.0	AN_SECU_StoreKeeper	1

Table 16. Guidance documentation (continued)

Component description	Reference	Version
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 - Application note	AN_33G_33H_AIS31	1
ST33G and ST33H Secure MCU platforms - Security Guidance	AN_SECU_ST33	10
ST33G and ST33H Power supply glitch detector characteristics - application note	AN_33_GLITCH	2
Flash memory loader installation guide for the ST33G1M2A and ST33G1M2M platforms	UM_33GA_FL	3

Table 17. 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 Rd, Lungtan Township, TAOYUAN County, 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
Amkor ATT6	AMKOR TECHNOLOGY TAIWAN, INC. (ATT) - T6 No. 333, Longyuan 1st Rd., Hsinchu Science Park, Longtan Dist., Taoyuan City, Taiwan R.O.C.	BE
AMTC/TOPPAN Dresden	Advanced Mask Technology Center Gmbh & Co KG Rahnitzer Allee 9, 01109 Dresden, Germany	MASK

Table 17. Sites list (continued)

Site	Address	Activities[1]
DNP	DNP (Dai Nippon printing Co ltd.) 2-2-1 Kami-Fukuoka, Fujimino-shi, Saitama,356-8507, Japan	MASK
DPE	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	WHSD
Pantos	LX Pantos Logistics (HK) Co Ltd. Unit 1001, 10/F, Mapletree Logistics Hub, 30 Tsing Yi Road, Tsing Yi, N.T. Hong Kong	WHSD
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
ST Bouskoura	STMicroelectronics 101 Boulevard des Muriers, 20180 Bouskoura, Maroc	BE WHSD
ST Catania	STMicroelectronics Str. Primosole, 50, 95121 Catania, Italy	DEV
ST Crolles	STMicroelectronics 850 rue Jean Monnet, 38926 Crolles, France	DEV MASK FE

Table 17. Sites list (continued)

Site	Address	Activities[1]
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	BE DEV ES-DEV
ST Ljubljana	STMicroelectronics d.o.o. Ljubljana Tehnoloski park 21, 1000 Ljubljana, Slovenia	DEV
ST Loyang	STMicroelectronics 7 Loyang Drive, Singapore 508938	WHSD
ST Palermo	STMicroelectronics Via Tommaso Marcellini, 8L, 90129 Palermo, Italy	DEV
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 ES_DEV MASK EWS WHSD FE
ST Sophia	STMicroelectronics Sky Sophia, Bât B, 776 Rue Albert Caquot, 06410 Biot, France	DEV
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

Table 17. Sites list (continued)

Site	Address	Activities[1]
ST Zaventem	STMicroelectronics Green Square, Lambroekstraat 5, Building B, 3d floor, 1831 Diegem/Machelen, Belgium	ES_DEV
STS Shenzhen	STS Microelectronics 16 Tao hua Rd., Futian free trade zone, Shenzhen, P.R. China 518038	BE
STS Shenzhen Lab	STS Microelectronics 17 Taohua Road., Futian Free trade zone, Shenzhen, P.R. China 518038	BE
Suzhou	STMicroelectronics C8-2/C9-2 warehouse, 8 Datong Road, Integrated Free Trade Zone, New District, Suzhou, 215151, P.R. China	WHSD
TSMC F14	TSMC FAB 14 1-1 Nan Ke N. Rd. Tainan science park, Tainan 741-44, Taiwan, ROC	MASK FE
TSMC F18	TSMC FAB 18 No.8 Beiyuan 2nd Rd., Tainan Science Park Tainan City 745-43, Taiwan, ROC	WHS
TSMC F2/F5	TSMC FAB 2-5 121 Park Avenue 3, Hsinchu science park, Hsinchu 300-77, Taiwan, ROC	MASK
TSMC F8	TSMC FAB 8 25, Li-Hsin Road, Hsinchu Science Park, Hsinchu 300-78, Taiwan ROC	MASK
UTAC UTL1	UTAC Thai Limited 1 237 Lasalle Road, Bangna, Bangkok, 10260 Thailand	BE

Table 17. Sites list (continued)

Site	Address	Activities[1]
UTAC UTL3	UTAC Thai Limited 3 73 Moo5, Bangsamak, Bangpakong, Chachoengsao, 24180 Thailand	BE
WINSTEK	Winstek Semiconductor Co., Ltd. No 176-5, Luliaokeng, 6th Ling, Qionglin, 307 Hsinchu County, Taiwan	BE

1. BE = back end
DEV = development,
ES_DEV = Libraries & OS development,
EWS = electrical wafer sort &/or pre-perso manufacturing
FE = front end manufacturing,
IT = Information Technology,
MASK = mask manufacturing,
WHS = warehouse,
WHSD = warehouse for delivery

9 References

Table 18. Common Criteria

Component description	Reference	Version
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2017-04-002 R5	3.1 Rev 5
Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, April 2017	CCMB-2022-11-001 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017	CCMB-2022-11-002 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017	CCMB-2022-11-003 R1	2022 Rev 1
Common Criteria for Information Technology Security Evaluation - Part 5: Pre-defined packages of security requirements, November 2022	CCMB-2022-11-005 R1	2022 Rev 1
Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), 15th October 2025	Reference 001	version 1.2

Table 19. Protection Profile

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

Table 20. Other standards

Ref	Identifier	Description
[1]	BSI-AIS20/AIS31	A proposal for: Functionality classes for random number generators, W. Killmann & W. Schindler BSI, Version 2.0, 18-09-2011
[2]	NIST SP 800-67	NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised November 2017, National Institute of Standards and Technology
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002
[4]	FIPS PUB 180-2	FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004

Table 20. Other standards

Ref	Identifier	Description
[5]	FIPS PUB 186-4	FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), July 2013
[6]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, updated May 2023
[7]	ISO/IEC 9796-2	ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002
[8]	NIST SP 800-38A	NIST SP 800-38A Recommendation for Block Cipher Modes of Operation, 2001, with Addendum Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode, October 2010
[9]	NIST SP 800-38B	NIST special publication 800-38B, Recommandation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), May 2005
[10]	NIST SP 800-38C	NIST special publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, National Institute of Standards and Technology (NIST), May 2004
[11]	NIST SP 800-38D	NIST special publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter mode (GCM) and GMAC, National Institute of Standards and Technology (NIST), November 2007
[12]	ISO/IEC 14888	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[13]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[14]	MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
[15]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[16]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[17]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002

Table 20. Other standards

Ref	Identifier	Description
[18]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997
[19]	NIST SP 800-90	NIST Special Publication 800-90, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), March 2007
[20]	FIPS PUB 198-1	FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology (NIST), July 2008
[21]	NIST SP 800-56A	NIST SP 800-90A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), May 2013
[22]	ANSI X9.31	ANSI X9.31, Digital Signature Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), American National Standard for Financial Services, 1998
[23]	ANSI X9.42	ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, American National Standard for Financial Services, 2003 (R2013)
[24]	ANSI X9.62	ANSI X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard for Financial Services, 2005
[25]	FIPS PUB 202	FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, August 2015
[26]	EdDSA rfc	S. Josefsson and I. Liusvaara,, Edwards-curve Digital Signature Algorithm (EdDSA) draft-irtf-cfrg-eddsa-08, Network Working Group Internet-Draft, IETF, August 19, 2016, available from *https://tools.ietf.org/html/draft-irtf-cfrg-eddsa-08*
[27]	EDDSA	Bernstein, D., Duif, N., Lange, T., Schwabe, P., and B. Yang, "High-speed high-security signatures", *http://ed25519.cr.yp.to/ed25519-20110926.pdf* September 2011
[28]	EDDSA2	Bernstein, D., Josefsson, S., Lange, T., Schwabe, P., and B. Yang, "EdDSA for more curves", WWW *http://ed25519.cr.yp.to/eddsa-20150704.pdf* July 2015

Table 20. Other standards

Ref	Identifier	Description
[29]	PG-083	Guide des Mécanismes Cryptographiques - Régles et recommendations concernant le choix et le dimensionnement des mécanismes cryptographiques - January 2020 - Version 2.04.
[30]	ECCG ACM	Agreed Cryptographic Mechanisms, European Cybersecurity Certification Group - Sub-group on Cryptography, Version 2.0, April 2025.

Appendix A Glossary

A.1 Terms

Authorised user

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

Composite product

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

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

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

IC Dedicated Software

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

IC Dedicated Test Software

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

IC developer

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

IC manufacturer

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

IC packaging manufacturer

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

Initialisation data

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

Object

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

Packaged IC

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

Pre-personalization data

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

Secret

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

Security IC

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

Security IC Embedded SoftWare (ES)

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

Security IC embedded software (ES) developer

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

Security attribute

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

Sensitive information

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

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

Smartcard

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

Subject

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

Test features

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

TOE Delivery

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

TSF data

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

User

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

User data

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

A.2 Abbreviations

Table 21. List of abbreviations

Term	Meaning
AES	Advanced Encryption Standard
AIS	Application notes and Interpretation of the Scheme (BSI).
ALU	Arithmetical and Logical Unit.
BE	Back End manufacturing.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CBC-MAC	Cipher Block Chaining Message Authentication Code.
CC	Common Criteria Version 3.1. R5.
CC:2022	Common Criteria Version 2022 R1.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information.
DES	Data Encryption Standard.
DEV	Development.
DIP	Dual-In-Line Package.
DRBG	Deterministic Random Bit Generator.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
ECC	Elliptic Curve Cryptography.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
ES	Security IC Embedded Software.
EWS	Electrical Wafer Sort.
FE	Front End manufacturing.
FIPS	Federal Information Processing Standard.
FTOS	Final Test Operating System.
GPIO	General Purpose I/O.
HMAC	Keyed-Hash Message Authentication Code.
I/O	Input / Output.
IC	Integrated Circuit.
ISO	International Standards Organisation.

Table 21. List of abbreviations (continued)

Term	Meaning
IT	Information Technology.
LPU	Library Protection Unit.
MASK	Mask manufacturing.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
NFC	Near Field Communication.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
SFM	StoreKeeper Flash Management
SFP	Security Function Policy.
SFR	Security Functional Requirement.
SHA	Secure Hash Algorithm.
SIM	Subscriber Identity Module.
SOIC	Small Outline IC.
SPI	Serial Peripheral Interface.
ST	Context dependent : STMicroelectronics or Security Target.
SWP	Single Wire Protocol.
TDES	Triple DES.
TOE	Target of Evaluation.
TQFP	Thin Quad Flat Package.
TRNG	True Random Number Generator.
TSC	TSF Scope of Control.
TSF	TOE Security Functionality.

Table 21. List of abbreviations (continued)

Term	Meaning
TSFI	TSF Interface.
TSP	TOE Security Policy.
TSS	TOE Summary Specification.
UID	User Identification.
WHS	Warehouse.
WHSD	Warehouse for delivery.

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.

© 2026 STMicroelectronics – All rights reserved