STMicroelectronics

ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G with firmware revision 1.3.2 optional cryptographic library NESLIB 4.2.10 Security Target for composition

Common Criteria for IT security evaluation

SMD_ST33G_ST_16_001 Rev 01.02

January 2017

www.st.com
1 Introduction

1.1 Security Target reference

Document identification: ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G, with firmware revision 1.3.2, and optional cryptographic library Neslib 4.2.10 - SECURITY TARGET FOR COMPOSITION.

Version number: Rev 01.02, issued January 2017.

Registration: registered at ST Microelectronics under number SMD_ST33G_ST_16_001_V01.02.

1.2 Purpose

This document presents the Security Target for composition (ST) of the ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G Security Integrated Circuit (IC), designed on the ST33 platform of STMicroelectronics, with Firmware rev 1.3.2, and optional cryptographic library Neslib 4.2.10.

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

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

1 Introduction ................................................. 3
   1.1 Security Target reference .............................. 3
   1.2 Purpose .............................................. 3

2 Context ..................................................... 11

3 TOE description ........................................... 12
   3.1 TOE identification .................................... 12
   3.2 TOE overview ......................................... 13
   3.3 TOE life cycle ....................................... 16
   3.4 TOE environment ..................................... 18
      3.4.1 TOE Development Environment .................... 18
      3.4.2 TOE production environment ....................... 19
      3.4.3 TOE operational environment ..................... 19

4 Conformance claims ....................................... 20
   4.1 Common Criteria conformance claims ................. 20
   4.2 PP Claims ........................................... 20
      4.2.1 PP Reference .................................. 20
      4.2.2 PP Refinements ................................ 20
      4.2.3 PP Additions .................................. 20
      4.2.4 PP Claims rationale .............................. 20

5 Security problem definition ............................. 22
   5.1 Description of assets ................................ 22
   5.2 Threats ............................................. 24
   5.3 Organisational security policies ..................... 25
   5.4 Assumptions ......................................... 26
      5.4.1 Assumptions from the PP ......................... 26

6 Security objectives ....................................... 27
   6.1 Security objectives for the TOE ...................... 28
      6.1.1 Objectives from the PP: .......................... 28
6.1.2 Additional objectives: ............................................................ 28

6.2 Security objectives for the environment ........................................ 29

6.3 Security objectives rationale ....................................................... 29

6.3.1 TOE threat "Memory Access Violation" .................................... 31

6.3.2 TOE threat "Application code confidentiality" .......................... 31

6.3.3 TOE threat "Application data confidentiality" .......................... 31

6.3.4 TOE threat "Application code integrity" .................................. 31

6.3.5 TOE threat "Application data integrity" ............................... 31

6.3.6 Organisational security policy "Additional Specific Security Functionality" .......................................................... 32

6.3.7 Organisational security policy "Controlled loading of the Security IC Embedded Software" .................................................. 32

6.3.8 Organisational security policy "Usage of hardware platform" .......... 32

6.3.9 Organisational security policy "Treatment of user data" ............... 32

7 Security requirements ............................................................ 34

7.1 Security functional requirements for the TOE ................................. 34

7.1.1 Security Functional Requirements from the Protection Profile ........ 36

Limited fault tolerance (FRU_FLT.2) .............................................. 36

Failure with preservation of secure state (FPT_FLS.1) ......................... 36

Limited capabilities (FMT_LIM.1) [Test] ........................................ 36

Limited availability (FMT_LIM.2) [Test] ....................................... 36

Audit storage (FAU_SAS.1) ......................................................... 36

Resistance to physical attack (FPT_PHP.3) .................................... 36

Basic internal transfer protection (FDP_ITT.1) ................................ 37

Basic internal TSF data transfer protection (FPT_ITT.1) ....................... 37

Subset information flow control (FDP_IFC.1) .................................. 37

Random number generation (FCS_RNG.1) ................................... 37

7.1.2 Additional Security Functional Requirements for the cryptographic services .................................................. 38

Cryptographic operation (FCS_COP.1) ....................................... 38

Cryptographic key generation (FCS_CKM.1) .................................. 39

7.1.3 Additional Security Functional Requirements for the memories protection. .................................................. 40

Static attribute initialisation (FMT_MSA.3) [Memories] .................... 40

Management of security attributes (FMT_MSA.1) [Memories] .......... 40

Complete access control (FDP_ACC.2) [Memories] .......................... 40

Security attribute based access control (FDP_ACF.1) [Memories] ........ 41
7.1.4 Additional Security Functional Requirements related to the Admin configuration

Limited capabilities (FMT_LIM.1) [Admin]

Limited availability (FMT_LIM.2) [Admin]

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

7.1.5 Additional Security Functional Requirements related to the Application Firewall

Subset access control (FDP_ACC.1) [APPLI_FWLO]

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

Static attribute initialisation (FMT_MSA.3) [APPLI_FWLO]

7.2 TOE security assurance requirements

7.3 Refinement of the security assurance requirements

7.3.1 Refinement regarding functional specification (ADV_FSP)

7.3.2 Refinement regarding test coverage (ATE_COV)

7.4 Security Requirements rationale

7.4.1 Rationale for the Security Functional Requirements

7.4.2 Additional security objectives are suitably addressed

7.4.3 Additional security requirements are consistent

7.4.4 Dependencies of Security Functional Requirements

7.4.5 Rationale for the Assurance Requirements

8 TOE summary specification

8.1 Limited fault tolerance (FRU_FLT.2)

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

8.3 Limited capabilities (FMT_LIM.1) [Test]

8.4 Limited capabilities (FMT_LIM.1) [Admin]

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

8.6 Audit storage (FAU_SAS.1)

8.7 Resistance to physical attack (FPT_PHP.3)
8.8 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1) ................................................................. 56
8.9 Random number generation (FCS_RNG.1) ......................................................... 56
8.10 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES]) .......... 56
8.11 Cryptographic operation: AES operation (FCS_COP.1 [AES]) ....................... 57
8.12 Cryptographic operation: RSA operation (FCS_COP.1 [RSA]) if Neslib only ................................................................. 57
8.13 Cryptographic operation: Elliptic Curves Cryptography operation (FCS_COP.1 [ECC]) if Neslib only ................................................................. 57
8.14 Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only .......... 58
8.15 Cryptographic operation: DRBG operation (FCS_COP.1 [DRBG]) if Neslib only ................. 58
8.16 Cryptographic key generation: Prime generation (FCS_CKM.1 [Prime_generation]) if Neslib only ................................................................. 58
8.17 Cryptographic key generation: RSA key generation (FCS_CKM.1 [RSA_key_generation]) if Neslib only ................................................................. 58
8.18 Static attribute initialisation (FMT_MSA.3) [Memories] ................................. 58
8.19 Management of security attributes (FMT_MSA.1) [Memories] & Specification of management functions (FMT_SMF.1) [Memories] ............... 59
8.20 Complete access control (FDP_ACC.2) [Memories] & Security attribute based access control (FDP_ACF.1) [Memories] ................................. 59
8.21 Import of user data without security attributes (FDP_ITC.1) [Loader] .................. 59
8.22 Static attribute initialisation (FMT_MSA.3) [Loader] ........................................ 59
8.23 Management of security attributes (FMT_MSA.1) [Loader] & Specification of management functions (FMT_SMF.1) [Loader] ....................... 59
8.24 Subset access control (FDP_ACC.1) [Loader] & Security attribute based access control (FDP_ACF.1) [Loader] ................................................................. 59
8.25 Subset access control (FDP_ACC.1) [APPLI_FWL] & Security attribute based access control (FDP_ACF.1) [APPLI_FWL] ................................................................. 60
8.26 Static attribute initialisation (FMT_MSA.3) [APPLI_FWL] .................................. 60

9 References ................................................................. 61

Appendix A Glossary ................................................................. 64
A.1 Terms ................................................................. 64
A.2 Abbreviations ................................................................. 66
Contents

ST33G Platform Security Target for composition

10 Revision history .......................................................... 68
List of tables

Table 1. TOE identification ................................................................. 12
Table 2. Derivative devices configuration possibilities ............................. 12
Table 3. Composite product life cycle phases ...................................... 17
Table 4. Summary of security environment ......................................... 23
Table 5. Summary of security objectives ............................................. 27
Table 6. Security Objectives versus Assumptions, Threats or Policies ...... 30
Table 7. Summary of functional security requirements for the TOE .......... 34
Table 8. FCS_COP.1 iterations (cryptographic operations) .................... 38
Table 9. FCS_CKM.1 iterations (cryptographic key generation) .............. 40
Table 10. TOE security assurance requirements .................................... 44
Table 11. Impact of EAL5 selection on BSI-PP-0035 refinements ............ 45
Table 12. Security Requirements versus Security Objectives ................ 47
Table 13. Dependencies of security functional requirements .................. 52
Table 14. List of abbreviations ............................................................ 66
Table 15. Document revision history .................................................. 68
List of figures

Figure 1. ST33G Platform block diagram ................................................. 16
Figure 2. Security IC life cycle ................................................................. 18
2 Context

The Target of Evaluation (TOE) referred to in Section 3: TOE description, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Secure Microcontrollers Division of STMicroelectronics (ST).

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

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

This ST claims to be an instantiation of the "Security IC Platform Protection Profile" (PP) registered and certified under the reference BSI-PP-0035 in the German IT Security Evaluation and Certification Scheme, with the following augmentations:

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

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

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

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

3.1 TOE identification

13 The Target of Evaluation (TOE) is the ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G, with firmware rev 1.3.2, and the optional cryptographic library Neslib 4.2.10, with guidance documentation.

14 The IC maskset name is the product hardware identification. The maskset major version is updated when the full maskset is changed (i.e. all layers of the maskset are changed at the same time). The IC version is updated for any change in hardware (i.e. part of the layers of the maskset) or in the OST. The Product name, IC version (i.e. ST33G platform version G), Firmware version and libraries versions fully identify the TOE.

15 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 personalisation process.

16 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.

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

Table 2. Derivative devices configuration possibilities

<table>
<thead>
<tr>
<th>Features</th>
<th>Possible values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVM size</td>
<td>Selectable by 128 Kbytes granularity from 1280 Kbytes to 384 Kbytes</td>
</tr>
<tr>
<td>Operational temperature range</td>
<td>See Datasheet referenced in Section 9</td>
</tr>
</tbody>
</table>

18 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.

19 All along the product life, the marking on the die, a set of accessible registers and a set of specific instructions allow the customer to check the product information, providing the identification elements, as listed in Table 1: TOE identification, and the configuration elements as detailed in the Data Sheet and in the Firmware User Manual, referenced in Section 9.
The rest of this document applies to all possible configurations of the TOE, with or without Neslib, except when a restriction is mentioned. For easier reading, the restrictions are typeset as indicated here.

### 3.2 TOE overview

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.

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.

The TOE features hardware accelerators for advanced cryptographic functions, with built-in countermeasures against side channel attacks. The AES (Advanced Encryption Standard) accelerator provides a high-performance implementation of AES-128, AES-192 and AES-256 algorithms. The 3-key triple DES accelerator (EDES+) supports efficiently the Data Encryption Standard (TDES [2]), enabling Cipher Block Chaining (CBC) mode, fast DES and triple DES computation. The NESCRIPT crypto-processor allows fast and secure implementation of the most popular public key cryptosystems with a high level of performance ([7], [9], [15],[16], [17], [18]).

As randomness is a key stone in many applications, the ST33G Platform features a highly reliable True Random Number Generator (TRNG), compliant with PTG.2 Class of AIS20/AIS31 [1] and directly accessible through dedicated registers.

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

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.
In a few words, the ST33G Platform, offers a unique combination of high performances and very powerful features for high level security:

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

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.

The System ROM and ST NVM of the TOE contain a Dedicated Software which provides a 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.

The System ROM and ST NVM of the TOE contain a Dedicated Software which provides a set of protected commands for diagnosis purpose, reserved to STMicroelectronics.

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

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.

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 developper in his applicative code.

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

- an asymmetric key cryptographic support module, supporting secure modular arithmetic with large integers, with specialized functions for Rivest, Shamir & Adleman Standard cryptographic algorithm (RSA [17]),
- 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).
[15], and provides support for ECDH key agreement [22] and ECDSA generation and verification [5].

- an asymmetric key cryptographic support module that provides secure hash algorithm functions (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 [4]),
- prime number generation and RSA key pairs generation [3],
- support for a Deterministic Random Bit Generator [20].

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

The ES is not part of the TOE and is out of scope of the evaluation, except Neslib when it is embedded.

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

- the product Data Sheet and die description,
- optionally the ST33G1M2 platform Technical Notes,
- the product family Security Guidance,
- the AIS31 user manuals,
- the Cortex M3 SC300 Technical Reference Manuals,
- the Firmware user manual,
- the Flash loader installation guide,
- optionally the Neslib user manual.

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

35 Figure 1 provides an overview of the ST33G Platform.
3.3 TOE life cycle

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

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.

The life cycle phases are summarized in Table 3.

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

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.

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

The TOE is only delivered in ADMIN or USER configuration, depending on the customer’s request.

### Table 3. Composite product life cycle phases

<table>
<thead>
<tr>
<th>Phase</th>
<th>Name</th>
<th>Description</th>
<th>Responsible party</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IC embedded software development</td>
<td>security IC embedded software development specification of IC pre-personalization requirements</td>
<td>IC embedded software developer</td>
</tr>
<tr>
<td>2</td>
<td>IC development</td>
<td>IC design IC dedicated software development</td>
<td>IC developer: ST</td>
</tr>
<tr>
<td>3</td>
<td>IC manufacturing</td>
<td>integration and photomask fabrication IC production IC testing pre-personalisation</td>
<td>IC manufacturer: ST or TSMC</td>
</tr>
<tr>
<td>4</td>
<td>IC packaging</td>
<td>security IC packaging (and testing) pre-personalisation if necessary</td>
<td>IC packaging manufacturer: ST or AMKOR or CHIPBOND or NEDCARD or SMARTFLEX or STATS CHIPPAC</td>
</tr>
<tr>
<td>5</td>
<td>Composite product integration</td>
<td>composite product finishing process composite product testing</td>
<td>Composite product manufacturer</td>
</tr>
<tr>
<td>6</td>
<td>Personalisation</td>
<td>composite product personalisation composite product testing</td>
<td>Personaliser</td>
</tr>
<tr>
<td>7</td>
<td>Operational usage</td>
<td>composite product usage by its issuers and consumers</td>
<td>End-consumer</td>
</tr>
</tbody>
</table>

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

Considering the TOE, three types of environments are defined:

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

### 3.4.1 TOE Development Environment

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.

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

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).

The development centres involved in the development of the TOE can be the following: **ST ROUSSET (FRANCE), ST SOPHIA (FRANCE), ST GRENOBLE (FRANCE), ST RENNES (FRANCE), ST ANG MO KIO 1 (SINGAPORE), ST ZAVENTEM (BELGIUM).**
Reticules and photomasks are generated from the verified IC databases; the former are used in the silicon Wafer-fab processing. As reticules and photomasks are generated off-site, they are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrive only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

The authorized sub-contractors involved in the TOE mask manufacturing can be DNP (JAPAN), DPE (ITALY), or TSMC (TAIWAN).

3.4.2 TOE production environment

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.

Production starts within the Wafer-fab; here the silicon wafers undergo the diffusion processing. Computer tracking at wafer level throughout the process is commonplace. The wafers are then taken into the test area. Testing of each TOE occurs to assure conformance with the device specification. The wafers are then delivered for assembly onto the composite products.

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

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

Wafers are then scribed and broken such as to separate the functional from the non-functional ICs. The latter is discarded in a controlled accountable manner. The good ICs are then packaged in phase 4, in a back-end plant. When testing, programming or deliveries are done offsite, ICs are transported and worked on in a secure environment with accountability and traceability of all (good and bad) products.

When the product is delivered after phase 4, the authorized back-end plants involved in the packaging of the TOE can be ST ANG MO KIO 6 (SINGAPORE), ST BOUSKOURA (MOROCCO), ST CALAMBA (THE PHILIPPINES), ST MUAR (MALAYSIA), ST SHENZHEN (CHINA), AMKOR (THE PHILIPPINES or TAIWAN), CHIPBOND (TAIWAN), NEDCARD (THE NETHERLANDS), SMARTFLEX (SINGAPORE), STATS CHIPPAC (SINGAPORE or TAIWAN or CHINA).

All ST back-end plants, ST LOYANG (SINGAPORE) and ST ROUSSET (FRANCE) can also be involved for the logistics.

3.4.3 TOE operational environment

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

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

End-user environments (phase 7): composite products are used in a wide range of applications to assure authorised conditional access. Examples of such are Automotive and Machine to Machine (M2M). The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid any attempt to abuse the TOE.
4 Conformance claims

4.1 Common Criteria conformance claims

62 The ST33G Platform Security Target claims to be conformant to the Common Criteria version 3.1 revision 4.

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

64 The assurance level for the ST33G Platform Security Target is EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

65 The ST33G Platform Security Target claims strict conformance to the Security IC Platform Protection Profile (BSI-PP-0035), for the part of the TOE covered by this PP (Security IC), as required by this Protection Profile.

4.2.2 PP Refinements

66 The main refinements operated on the BSI-PP-0035 are:

• Addition #1: “Support of Cipher Schemes” from AUG,
• Addition #4: “Area based Memory Access Control” from AUG,
• Specific additions for the Secure Flash Loader
• Specific additions for the LPU
• Refinement of assurance requirements.

67 All refinements versus the PP are indicated with type setting text as indicated here, original text from the BSI-PP-0035 being typeset as indicated here. Text originating in AUG is typeset as indicated here.

4.2.3 PP Additions

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

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

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

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

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

4.2.4 PP Claims rationale

73 The differences between this Security Target security objectives and requirements and those of BSI-PP-0035, to which conformance is claimed, have been identified and justified in Section 6 and in Section 7. They have been recalled in the previous section.
In the following, the statements of the security problem definition, the security objectives, and the security requirements are consistent with those of the BSI-PP-0035.

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

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

The security requirements rationale presented in Section 7.4 has been updated with respect to the Protection Profile.

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

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.

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

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

5.1 Description of assets

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.

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.

According to the Protection Profile there is the following high-level security concern related to security service:
- SC4 deficiency of random numbers.

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.
The information and material produced and/or processed by ST in the TOE development and production environment (Phases 2 up to TOE delivery) can be grouped as follows:

- logical design data,
- physical design data,
- IC Dedicated Software, Security IC Embedded Software, Initialisation Data and pre-personalisation Data,
- specific development aids,
- test and characterisation related data,
- material for software development support, and
- photomasks and products in any form as long as they are generated, stored, or processed by ST.

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

Table 4. Summary of security environment

<table>
<thead>
<tr>
<th>Label</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI.T.Leak-Inherent</td>
<td>Inherent Information Leakage</td>
</tr>
<tr>
<td>BSI.T.Phys-Probing</td>
<td>Physical Probing</td>
</tr>
<tr>
<td>BSI.T.Malfunction</td>
<td>Malfunction due to Environmental Stress</td>
</tr>
<tr>
<td>BSI.T.Phys-Manipulation</td>
<td>Physical Manipulation</td>
</tr>
<tr>
<td>BSI.T.Leak-Forced</td>
<td>Forced Information Leakage</td>
</tr>
<tr>
<td>BSI.T.Abuse-Func</td>
<td>Abuse of Functionality</td>
</tr>
<tr>
<td>BSI.T.RND</td>
<td>Deficiency of Random Numbers</td>
</tr>
<tr>
<td>AUG4.T.Mem-Access</td>
<td>Memory Access Violation</td>
</tr>
<tr>
<td>T.Confid-Applic-Code</td>
<td>Application code confidentiality</td>
</tr>
<tr>
<td>T.Confid-Applic-Data</td>
<td>Application data confidentiality</td>
</tr>
<tr>
<td>T.Integ-Applic-Code</td>
<td>Application code integrity</td>
</tr>
<tr>
<td>T.Integ-Applic-Data</td>
<td>Application data integrity</td>
</tr>
<tr>
<td>BSI.P.Process-TOE</td>
<td>Protection during TOE Development and Production</td>
</tr>
<tr>
<td>AUG1.P.Add-Functions</td>
<td>Additional Specific Security Functionality (Cipher Scheme Support)</td>
</tr>
<tr>
<td>P.Controlled-ES-Loading</td>
<td>Controlled loading of the Security IC Embedded Software</td>
</tr>
<tr>
<td>P.Plat-Appl</td>
<td>Usage of hardware platform</td>
</tr>
<tr>
<td>P.Resp-Appl</td>
<td>Treatment of user data</td>
</tr>
<tr>
<td>BSI.A.Process-Sec-IC</td>
<td>Protection during Packaging, Finishing and Personalisation</td>
</tr>
<tr>
<td>BSI.A.Plat-Appl</td>
<td>Usage of Hardware Platform</td>
</tr>
<tr>
<td>BSI.A.Resp-Appl</td>
<td>Treatment of User Data</td>
</tr>
</tbody>
</table>
5.2 Threats

The threats are described in the BSI-PP-0035, section 3.2. Only those originating in AUG are detailed in the following section.

BSI.T.Leak-Inherent  Inherent Information Leakage
BSI.T.Phys-Probing   Physical Probing
BSI.T.Malfunction    Malfunction due to Environmental Stress
BSI.T.Phys-Manipulation Physical Manipulation
BSI.T.Leak-Forced    Forced Information Leakage
BSI.T.Abuse-Func     Abuse of Functionality
BSI.T.RND            Deficiency of Random Numbers
AUG4.T.Mem-Access    Memory Access Violation:

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

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

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

The following additional threats are related to Application protection.

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

T.Confid-Applic-Data Application data confidentiality:
A sensitive application data may need to be protected against unauthorized disclosure. This relates to attacks at runtime to gain read or compare access to the sensitive application data by another application. For example, the attacker executes an application that tries to read data belonging to the sensitive application.
5.3 Organisational security policies

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.

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

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

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

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.

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

BSI.P.Process-TOE Protection during TOE Development and Production:

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

5.4.1 Assumptions from the PP

The assumptions are described in the *BSI-PP-0035*, section 3.4.

**BSI.A.Process-Sec-IC** Protection during Packaging, Finishing and Personalisation

**BSI.A.Plat-Appl** Usage of Hardware Platform

**BSI.A.Resp-Appl** Treatment of User Data
6 Security objectives

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.

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

Note that the origin of each objective is clearly identified in the prefix of its label. Most of these security aspects can therefore be easily found in the protection profile. Only those originating in AUG, and the one introduced in this Security Target, are detailed in the following sections.

Table 5. Summary of security objectives

<table>
<thead>
<tr>
<th>Label</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI.O.Leak-Inherent</td>
<td>Protection against Inherent Information Leakage</td>
</tr>
<tr>
<td>BSI.O.Phys-Probing</td>
<td>Protection against Physical Probing</td>
</tr>
<tr>
<td>BSI.O.Malfunction</td>
<td>Protection against Malfunctions</td>
</tr>
<tr>
<td>BSI.O.Phys-Manipulation</td>
<td>Protection against Physical Manipulation</td>
</tr>
<tr>
<td>BSI.O.Leak-Forced</td>
<td>Protection against Forced Information Leakage</td>
</tr>
<tr>
<td>BSI.O.Abuse-Func</td>
<td>Protection against Abuse of Functionality</td>
</tr>
<tr>
<td>BSI.O.Identification</td>
<td>TOE Identification</td>
</tr>
<tr>
<td>BSI.O.RND</td>
<td>Random Numbers</td>
</tr>
<tr>
<td>AUG1.O.Add-Functions</td>
<td>Additional Specific Security Functionality</td>
</tr>
<tr>
<td>AUG4.O.Mem-Access</td>
<td>Dynamic Area based Memory Access Control</td>
</tr>
<tr>
<td>O.Controlled-ES-Loading</td>
<td>Controlled loading of the Security IC Embedded Software</td>
</tr>
<tr>
<td>O.Plat-App</td>
<td>Usage of hardware platform</td>
</tr>
<tr>
<td>O.Resp-App</td>
<td>Treatment of user data</td>
</tr>
<tr>
<td>O.Firewall</td>
<td>Application firewall</td>
</tr>
<tr>
<td>BSI.OE.Plat-App</td>
<td>Usage of Hardware Platform</td>
</tr>
<tr>
<td>BSI.OE.Resp-App</td>
<td>Treatment of User Data</td>
</tr>
<tr>
<td>BSI.OE.Process-Sec-IC</td>
<td>Protection during composite product manufacturing</td>
</tr>
</tbody>
</table>
6.1 Security objectives for the TOE

6.1.1 Objectives from the PP:

- BSI.O.Leak-Inherent: Protection against Inherent Information Leakage
- BSI.O.Phys-Probing: Protection against Physical Probing
- BSI.O.Malfunction: Protection against Malfunctions
- BSI.O.Phys-Manipulation: Protection against Physical Manipulation
- BSI.O.Leak-Forced: Protection against Forced Information Leakage
- BSI.O.Abuse-Func: Protection against Abuse of Functionality
- BSI.O.Identification: TOE Identification
- BSI.O.RND: Random Numbers

6.1.2 Additional objectives:

- AUG1.O.Add-Functions: Additional Specific Security Functionality:
  - The TOE must provide the following specific security functionality to the Security IC Embedded Software:
    - Data Encryption Standard (DES),
    - Triple Data Encryption Standard (3DES),
    - Advanced Encryption Standard (AES),
  - Elliptic Curves Cryptography on GF(p): when Neslib is embedded only,
  - Secure Hashing (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512): when Neslib is embedded only,
  - Rivest-Shamir-Adleman (RSA): when Neslib is embedded only,
  - Prime Number Generation: when Neslib is embedded only,
  - Deterministic Random Bit Generator: when Neslib is embedded only.

- AUG4.O.Mem-Access: Dynamic Area based Memory Access Control:
  - The TOE must provide the Security IC Embedded Software with the capability to define dynamic memory segmentation and protection. The TOE must then enforce the defined access restrictions so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

- O.Controlled-ES-Loading: Controlled loading of the Security IC Embedded Software:
  - The TOE must provide the capability to load the Security IC Embedded Software into the NVM, either before TOE delivery, under ST authority, or 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.
6.2 Security objectives for the environment

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

BSI.OE.Platform-App Usage of Hardware Platform

BSI.OE.Resp-App Treatment of User Data

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

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

6.3 Security objectives rationale

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

103 Thus, it is necessary to show that:

- security environment aspects from AUG, and from this ST, are addressed by security objectives stated in this chapter,
- security objectives from AUG, and from this ST, are suitable (i.e. they address security environment aspects),
- security objectives from AUG, and from this ST, are consistent with the other security objectives stated in this chapter (i.e. no contradictions).
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, ($AUG1.P.Add-Functions$)".

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

- organisational security policies "Controlled loading of the Security IC Embedded Software, ($P.Controlled-ES-Loading$)", "Usage of hardware platform, ($P.Plat-Appl$)", and "Treatment of user data, ($P.Resp-Appl$)".

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-PP-0035 for the assumptions, policy and threats defined there.

**Table 6. Security Objectives versus Assumptions, Threats or Policies**

<table>
<thead>
<tr>
<th>Assumption, Threat or Organisational Security Policy</th>
<th>Security Objective</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI.A.Plat-Appl</td>
<td>BSI.OE.Plat-Appl</td>
<td>Phase 1</td>
</tr>
<tr>
<td>BSI.A.Resp-Appl</td>
<td>BSI.OE.Resp-Appl</td>
<td>Phase 1</td>
</tr>
<tr>
<td>BSI.P.Process-TOE</td>
<td>BSI.O.Identification</td>
<td>Phase 2-3</td>
</tr>
<tr>
<td>BSI.A.Process-Sec-IC</td>
<td>BSI.OE.Process-Sec-IC</td>
<td>Phase 4-6</td>
</tr>
<tr>
<td>P.Controlled-ES-Loading</td>
<td>O.Controlled-ES-Loading</td>
<td>Phase 4-6</td>
</tr>
<tr>
<td>AUG1.P.Add-Functions</td>
<td>AUG1.O.Add-Functions</td>
<td></td>
</tr>
<tr>
<td>P.Plat-Appl</td>
<td>O.Plat-Appl</td>
<td></td>
</tr>
<tr>
<td>P.Resp-Appl</td>
<td>O.Resp-Appl</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Leak-Inherent</td>
<td>BSI.O.Leak-Inherent</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Phys-Probing</td>
<td>BSI.O.Phys-Probing</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Malfunction</td>
<td>BSI.O.Malfunction</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Phys-Manipulation</td>
<td>BSI.O.Phys-Manipulation</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Leak-Forced</td>
<td>BSI.O.Leak-Forced</td>
<td></td>
</tr>
<tr>
<td>BSI.T.Abuse-Func</td>
<td>BSI.O.Abuse-Func</td>
<td></td>
</tr>
<tr>
<td>BSI.T.RND</td>
<td>BSI.O.RND</td>
<td></td>
</tr>
<tr>
<td>T.Confid-Applic-Code</td>
<td>O.Firewall</td>
<td></td>
</tr>
<tr>
<td>T.Confid-Applic-Data</td>
<td>O.Firewall</td>
<td></td>
</tr>
<tr>
<td>T.Integ-Applic-Code</td>
<td>O.Firewall</td>
<td></td>
</tr>
<tr>
<td>T.Integ-Applic-Data</td>
<td>O.Firewall</td>
<td></td>
</tr>
</tbody>
</table>
6.3.1 TOE threat "Memory Access Violation"

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

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.

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

6.3.2 TOE threat "Application code confidentiality"

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

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.

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

6.3.3 TOE threat "Application data confidentiality"

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

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.

6.3.4 TOE threat "Application code integrity"

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

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.

6.3.5 TOE threat "Application data integrity"

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

The threat is related to the alteration of the data of 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.
6.3.6 Organisational security policy "Additional Specific Security Functionality"

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

119 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.

120 Nevertheless the security objectives BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation and BSI.O.Leak-Forced define how to implement the specific security functionality required by AUG1.P.Add-Functions. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from AUG1.P.Add-Functions.) Especially BSI.O.Leak-Inherent and BSI.O.Leak-Forced refer to the protection of confidential data (User Data or TSF data) in general. User Data are also processed by the specific security functionality required by AUG1.P.Add-Functions.

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

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

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

123 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.

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

6.3.8 Organisational security policy "Usage of hardware platform"

The justification related to the organisational security policy "Usage of hardware platform, (P.Plat-Appl)" is as follows:

126 The policy states that the Security IC Embedded Software included in the TOE, uses the TOE hardware according to the respective PP assumption BSI.A.Plat-Appl. O.Plat-Appl has the same objective as BSI.OE.Plat-Appl defined in the PP. Thus, the objective O.Plat-Appl covers the policy P.Plat-Appl.

128 The added objective for the TOE O.Plat-Appl does not introduce any contradiction in the security objectives.

6.3.9 Organisational security policy "Treatment of user data"

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

129 In analogy to P.Plat-Appl, the policy P.Resp-Appl is covered in the same way by the objective O.Resp-Appl.
The added objective for the TOE O.Resp-Appl does not introduce any contradiction in the security objectives.
7 Security requirements

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

7.1 Security functional requirements for the TOE

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

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

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

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

All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of CCMB-2012-09-001. They are easily identified in the following text as they appear as indicated here. Note that in order to improve readability, iterations are sometimes expressed within tables.

The selected security functional requirements for the TOE, their respective origin and type are summarized in Table 7.

<table>
<thead>
<tr>
<th>Label</th>
<th>Title</th>
<th>Addressing</th>
<th>Origin</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRU_FLT.2</td>
<td>Limited fault tolerance</td>
<td></td>
<td>BSI-PP-0035</td>
<td></td>
</tr>
<tr>
<td>FPT_FLS.1</td>
<td>Failure with preservation of secure state</td>
<td>Malfunction</td>
<td></td>
<td>CCMB-2012-09-002</td>
</tr>
<tr>
<td>FMT_LIM.1</td>
<td>Limited capabilities</td>
<td>Abuse of TEST</td>
<td>BSI-PP-0035</td>
<td></td>
</tr>
<tr>
<td>FMT_LIM.2</td>
<td>Limited availability</td>
<td>Abuse of ADMIN</td>
<td>Security Target</td>
<td>Extended</td>
</tr>
<tr>
<td>FMT_LIM.1</td>
<td>Limited capabilities</td>
<td>Abuse of ADMIN</td>
<td>Operated</td>
<td></td>
</tr>
<tr>
<td>FAU_SAS.1</td>
<td>Audit storage</td>
<td>Lack of TOE identification</td>
<td>BSI-PP-0035</td>
<td>Operated</td>
</tr>
<tr>
<td>Label</td>
<td>Title</td>
<td>Addressing</td>
<td>Origin</td>
<td>Type</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>FPT_PHP.3</td>
<td>Resistance to physical attack</td>
<td>Physical manipulation &amp; probing</td>
<td>BSI-PP-0035</td>
<td></td>
</tr>
<tr>
<td>FDP_ITT.1</td>
<td>Basic internal transfer protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPT_ITT.1</td>
<td>Basic internal TSF data transfer protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_IFC.1</td>
<td>Subset information flow control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCS_RNG.1</td>
<td>Random number generation</td>
<td>Weak cryptographic quality of random numbers</td>
<td>BSI-PP-0035 Operated</td>
<td>Extended</td>
</tr>
<tr>
<td>FCS_COP.1</td>
<td>Cryptographic operation</td>
<td></td>
<td>AUG #1 Operated</td>
<td></td>
</tr>
<tr>
<td>FCS_CKM.1</td>
<td>Cryptographic key generation</td>
<td>Cipher scheme support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.2</td>
<td>Complete access control</td>
<td>Memory access violation</td>
<td>Security Target Operated</td>
<td></td>
</tr>
<tr>
<td>FDP_ACF.1</td>
<td>Security attribute based access control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.3</td>
<td>Static attribute initialisation</td>
<td></td>
<td>AUG #4 Operated</td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.1</td>
<td>Management of security attribute</td>
<td>Correct operation</td>
<td>Security Target Operated</td>
<td></td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>Specification of management functions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ITC.1</td>
<td>Import of user data without security attributes</td>
<td>User data loading access violation</td>
<td>Security Target Operated</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1</td>
<td>Subset access control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ACF.1</td>
<td>Security attribute based access control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.3</td>
<td>Static attribute initialisation</td>
<td>Correct operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.1</td>
<td>Management of security attribute</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>Specification of management functions</td>
<td>Abuse of ADMIN functionality</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1</td>
<td>Subset access control</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ACF.1</td>
<td>Security attribute based access control</td>
<td>Protected Application intrinsic confidentiality and integrity</td>
<td>Security Target Operated</td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.3</td>
<td>Static attribute initialisation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7. Summary of functional security requirements for the TOE (continued)
7.1.1 Security Functional Requirements from the Protection Profile

Limited fault tolerance (FRU_FLT.2)

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)

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.**

Refinement:

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

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

Limited capabilities (FMT_LIM.1) [Test]

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

Limited availability (FMT_LIM.2) [Test]

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

SFP_1: Limited capability and availability Policy [Test]

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

Audit storage (FAU_SAS.1)

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

Resistance to physical attack (FPT_PHP.3)

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

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)

146 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)

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

148 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)

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

150 SFP_2: Data Processing Policy
User Data and TSF data shall not be accessible from the TOE except when the Security IC Embedded Software decides to communicate the User Data via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the Security IC Embedded Software.

Random number generation (FCS_RNG.1)

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

• A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.

• If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

• The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.

• The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.

• The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-
tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.

152 The TSF shall provide octets of bits that meet
- Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.
- The average Shannon entropy per internal random bit exceeds 0.997.

7.1.2 Additional Security Functional Requirements for the cryptographic services.

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

Cryptographic operation (FCS_COP.1)

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

Table 8. FCS_COP.1 iterations (cryptographic operations)

<table>
<thead>
<tr>
<th>Restrict</th>
<th>Iteration label</th>
<th>[assignment: list of cryptographic operations]</th>
<th>[assignment: cryptographic algorithm]</th>
<th>[assignment: cryptographic key sizes]</th>
<th>[assignment: list of standards]</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDES</td>
<td>* encryption</td>
<td>Data Encryption Standard (DES)</td>
<td>56 bits</td>
<td></td>
<td>NIST SP 800-67 NIST SP 800-38A</td>
</tr>
<tr>
<td></td>
<td>* decryption</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in Cipher Block Chaining (CBC) mode</td>
<td>Triple Data Encryption Standard (3DES)</td>
<td>168 bits</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in Electronic Code Book (ECB) mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td>* encryption (cipher)</td>
<td>Advanced Encryption Standard</td>
<td>128, 192 and 256 bits</td>
<td></td>
<td>FIPS PUB 197</td>
</tr>
<tr>
<td></td>
<td>* decryption (inverse cipher)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* key expansion</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* randomize</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td>* RSA public key operation</td>
<td>Rivest, Shamir &amp; Adleman’s</td>
<td>up to 4096 bits</td>
<td></td>
<td>PKCS #1 V2.1</td>
</tr>
<tr>
<td>If Neslib</td>
<td>* RSA private key operation without the Chinese Remainder Theorem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* RSA private key operation with the Chinese Remainder Theorem</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>* EMSA PSS and PKCS1 signature scheme coding</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ST33G Platform Security Target for composition

Security requirements

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

<table>
<thead>
<tr>
<th>Restrict</th>
<th>Iteration label</th>
<th>[assignment: list of cryptographic operations]</th>
<th>[assignment: cryptographic algorithm]</th>
<th>[assignment: cryptographic key sizes]</th>
<th>[assignment: list of standards]</th>
</tr>
</thead>
</table>
| If NESL | ECC             | * private scalar multiplication  
* prepare Jacobian  
* public scalar multiplication  
* point validity check  
* convert Jacobian to affine coordinates  
* general point addition  
* point expansion  
* point compression  
* Diffie-Hellman (ECDH) key agreement computation  
* digital signature algorithm (ECDSA) generation and verification | Elliptic Curves Cryptography on GF(p) | up to 640 bits | IEEE 1363-2000, chapter 7  
IEEE 1363a-2004 |
| If NESL | SHA             | * SHA-1  
* SHA-224  
* SHA-256  
* SHA-384  
* SHA-512  
* Protected SHA-1  
* Protected SHA-256  
* HMAC | Secure Hash Algorithm | assignment pointless because algorithm has no key | FIPS PUB 180-2  
FIPS PUB 198-1 |
| If NESL | DRBG            | * SHA-1  
* SHA-224  
* SHA-256  
* SHA-384  
* SHA-512 | Hash-DRBG | None | NIST SP 800-90  
FIPS PUB 180-2  
FIPS PUB 197 |

AES  
CTR-DRBG  
128, 192 and 256 bits  
NIST SP 800-90  
FIPS PUB 197

155 Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

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

Cryptographic key generation (FCS_CKM.1)

157 If NESL is embedded only, the TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm, in Table 9, and specified cryptographic key sizes of Table 9 that meet the following standards in Table 9.
### 7.1.3 Additional Security Functional Requirements for the memories protection.

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

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

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

- **159** 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]**

- **161** 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]**

- **162** 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.

- **163** 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.

---

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

<table>
<thead>
<tr>
<th>Iteration label</th>
<th>[assignment: cryptographic key generation algorithm]</th>
<th>[assignment: cryptographic key sizes]</th>
<th>[assignment: list of standards]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prime generation</td>
<td>prime generation and RSA prime generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions</td>
<td>up to 2048 bits</td>
<td>FIPS PUB 140-2, FIPS 186-4</td>
</tr>
<tr>
<td>RSA key generation</td>
<td>RSA key pair generation algorithm, optionally protected against side channel attacks, and/or optionally with conditions</td>
<td>up to 4096 bits</td>
<td>FIPS PUB 140-2</td>
</tr>
</tbody>
</table>

---

**Note:**

- **a.** See the Datasheet referenced in Section 9 for actual values.
Security attribute based access control (FDP_ACF.1) [Memories]

164 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.**

165 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.**

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

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

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

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

169 **SFP_3: Dynamic Memory Access Control Policy**

170 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]

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

7.1.4 Additional Security Functional Requirements related to the Admin configuration

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

Limited capabilities (FMT_LIM.1) [Admin]

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

Limited availability (FMT_LIM.2) [Admin]

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

ST33G Platform Security Target for composition

175  
SFP_4: Limited capability and availability Policy [Admin]

176  
Deploying Loading or Final Test Artifacts after TOE Delivery to final user (phase 7 / USER configuration) does not allow User Data to be disclosed or manipulated, TSF data to be disclosed or manipulated, stored software to be reconstructed or altered, and no substantial information about construction of TSF to be gathered which may enable other attacks.

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

177  
The TSF shall enforce the Loading Access Control Policy when importing user data, controlled under the SFP, from outside of the TOE.

178  
The TSF shall ignore any security attributes associated with the User data when imported from outside of the TOE.

179  
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]

180  
The TSF shall enforce the Loading Access Control Policy to provide restrictive default values for security attributes that are used to enforce the SFP.

181  
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]

182  
The TSF shall enforce the Loading Access Control Policy to restrict the ability to modify the security attributes password to the Standard Loader.

Subset access control (FDP_ACC.1) [Loader]

183  
The TSF shall enforce the Loading Access Control Policy on the execution of the Standard Loader instructions and/or the Advanced Loader instructions.

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

184  
The TSF shall enforce the Loading Access Control Policy to objects based on the following: an external process may execute the Standard Loader instructions and/or the Advanced Loader instructions, depending on the presentation of valid passwords.

185  
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: the Standard Loader instructions and/or Advanced Loader instructions can be executed only if valid passwords have been presented.

186  
The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none.

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

**SFP_5: Loading Access Control Policy**

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

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

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

**7.1.5 Additional Security Functional Requirements related to the Application Firewall**

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

**Subset access control (FDP_ACC.1) [APPLI_FWL]**

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]**

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

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.*

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

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.*

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

**SFP_6: Protected Application Firewall Access Control Policy**

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]**

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

### 7.2 TOE security assurance requirements

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

- ALC_DVS.2 and AVA_VAN.5.

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

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

<table>
<thead>
<tr>
<th>Label</th>
<th>Title</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV_ARC.1</td>
<td>Security architecture description</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ADV_FSP.5</td>
<td>Complete semi-formal functional specification with additional error information</td>
<td>EAL5</td>
</tr>
<tr>
<td>ADV_IMP.1</td>
<td>Implementation representation of the TSF</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ADV_INT.2</td>
<td>Well-structured internals</td>
<td>EAL5</td>
</tr>
<tr>
<td>ADV_TDS.4</td>
<td>Semiformal modular design</td>
<td>EAL5</td>
</tr>
<tr>
<td>AGD_OPE.1</td>
<td>Operational user guidance</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>AGD_PRE.1</td>
<td>Preparative procedures</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ALC_CMC.4</td>
<td>Production support, acceptance procedures and automation</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ALC_CMS.5</td>
<td>Development tools CM coverage</td>
<td>EAL5</td>
</tr>
<tr>
<td>ALC_DEL.1</td>
<td>Delivery procedures</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ALC_DVS.2</td>
<td>Sufficiency of security measures</td>
<td>BSI-PP-0035</td>
</tr>
<tr>
<td>ALC_LCD.1</td>
<td>Developer defined life-cycle model</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ALC_TAT.2</td>
<td>Compliance with implementation standards</td>
<td>EAL5</td>
</tr>
<tr>
<td>ASE_CCL.1</td>
<td>Conformance claims</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_ECD.1</td>
<td>Extended components definition</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_INT.1</td>
<td>ST introduction</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_OBJ.2</td>
<td>Security objectives</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_REQ.2</td>
<td>Derived security requirements</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_SPD.1</td>
<td>Security problem definition</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ASE_TSS.1</td>
<td>TOE summary specification</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ATE_COV.2</td>
<td>Analysis of coverage</td>
<td>EAL5/BSI-PP-0035</td>
</tr>
<tr>
<td>ATE_DPT.3</td>
<td>Testing: modular design</td>
<td>EAL5</td>
</tr>
</tbody>
</table>
7.3 Refinement of the security assurance requirements

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

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

Regarding application note 22 of *BSI-PP-0035*, the refinements for all the assurance families have been reviewed for the hierarchically higher-level assurance components selected in this Security Target.

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

For reader’s ease, an impact summary is provided in *Table 11:*

### Table 11. Impact of EAL5 selection on *BSI-PP-0035* refinements

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

7.3.1 Refinement regarding functional specification (ADV_FSP)

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.*
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.

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.

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.

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.

Since the selected higher-level assurance component requires a security functional specification presented in a "semi-formal style" (ADV_FSP.5.2C) the changes affect the style of description, the BSI-PP-0035 refinements can be applied with changes covering the IC Dedicated Test Software and are valid for ADV_FSP.5.

### 7.3.2 Refinement regarding test coverage (ATE_COV)

The TOE is tested under different operating conditions within the specified ranges. These conditions include but are not limited to the frequency of the clock, the power supply, and the temperature. This means that “Fault tolerance (FRU_FLT.2)” is proven for the complete TSF. The tests must also cover functions which may be affected by “ageing” (such as EEPROM writing).

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).

The IC Dedicated Test Software is seen as a “test tool” being delivered as part of the TOE. However, the Test Features do not provide security functionality. Therefore, Test Features need not to be covered by the Test Coverage Analysis but all functions and mechanisms which limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the IC Dedicated Test Software must be part of the Test Coverage Analysis. The IC Dedicated Software provides security functionalities as soon as the TOE becomes operational (boot software). These are part of the Test Coverage Analysis.
7.4 Security Requirements rationale

7.4.1 Rationale for the Security Functional Requirements

Just as for the security objectives rationale of Section 6.3, the main line of this rationale is that the inclusion of all the security requirements of the BSI-PP-0035 protection profile, together with those in AUG, and with those introduced in this Security Target, guarantees that all the security objectives identified in Section 6 are suitably addressed by the security requirements stated in this chapter, and that the latter together form an internally consistent whole.

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>TOE Security Functional and Assurance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSI.O.Leak-Inherent</td>
<td>FDP_ITT.1 Basic internal transfer protection</td>
</tr>
<tr>
<td></td>
<td>FPT_ITT.1 Basic internal TSF data transfer protection</td>
</tr>
<tr>
<td></td>
<td>FDP_IFC.1 Subset information flow control</td>
</tr>
<tr>
<td>BSI.O.Phys-Probing</td>
<td>FPT_PHP.3 Resistance to physical attack</td>
</tr>
<tr>
<td>BSI.O.Malfunction</td>
<td>FRU_FLT.2 Limited fault tolerance</td>
</tr>
<tr>
<td></td>
<td>FPT_FLS.1 Failure with preservation of secure state</td>
</tr>
<tr>
<td>BSI.O.Phys-Manipulation</td>
<td>FPT_PHP.3 Resistance to physical attack</td>
</tr>
<tr>
<td>BSI.O.Leak-Forced</td>
<td>All requirements listed for BSI.O.Leak-Inherent</td>
</tr>
<tr>
<td></td>
<td>FDP_ITT.1, FPT_ITT.1, FDP_IFC.1</td>
</tr>
<tr>
<td></td>
<td>plus those listed for BSI.O.Malfunction and BSI.O.Phys-Manipulation</td>
</tr>
<tr>
<td></td>
<td>FRU_FLT.2, FPT_FLS.1, FPT_PHP.3</td>
</tr>
<tr>
<td>BSI.O.Abuse-Func</td>
<td>FMT_LIM.1 [Test] Limited capabilities</td>
</tr>
<tr>
<td></td>
<td>FMT_LIM.2 [Test] Limited availability</td>
</tr>
<tr>
<td></td>
<td>FMT_LIM.1 [Admin] Limited capabilities</td>
</tr>
<tr>
<td></td>
<td>FMT_LIM.2 [Admin] Limited availability</td>
</tr>
<tr>
<td></td>
<td>plus those for BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced</td>
</tr>
<tr>
<td></td>
<td>FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1</td>
</tr>
<tr>
<td>BSI.O.Identification</td>
<td>FAU_SAS.1 Audit storage</td>
</tr>
<tr>
<td>BSI.O.RND</td>
<td>FCS_RNG.1 Random number generation</td>
</tr>
<tr>
<td></td>
<td>plus those for BSI.O.Leak-Inherent, BSI.O.Phys-Probing, BSI.O.Malfunction, BSI.O.Phys-Manipulation, BSI.O.Leak-Forced</td>
</tr>
<tr>
<td></td>
<td>FDP_ITT.1, FPT_ITT.1, FDP_IFC.1, FPT_PHP.3, FRU_FLT.2, FPT_FLS.1</td>
</tr>
<tr>
<td>BSI.OE.Plat-Appl</td>
<td>Not applicable</td>
</tr>
<tr>
<td>BSI.OE.Resp-Appl</td>
<td>Not applicable</td>
</tr>
<tr>
<td>BSI.OE.Process-Sec-IC</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in Table 7 and Table 10, it can be verified that the justifications provided by the BSI-PP-0035 protection profile and AUG can just be carried forward to their union.

From Table 5, it is straightforward to identify two additional security objectives for the TOE (AUG1.O.Add-Functions and AUG4.O.Mem-Access) tracing back to AUG, and four additional objectives (O.Controlled-ES-Loading, O.Plat-App, O.Resp-App, and O.Firewall) introduced in this Security Target. This rationale must show that security requirements suitably address them.

Furthermore, a more careful observation of the requirements listed in Table 7 and Table 10 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_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).
Though it remains to show that:

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

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

### 7.4.2 Additional security objectives are suitably addressed

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

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

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.

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)”**

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

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)”**

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

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.

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

Security objective “Usage of hardware platform (O.Plat-Appl)”

The justification related to the security objective “Usage of hardware platform (O.Plat-Appl)” is as follows:

The objective was translated from an environment objective in the PP into a TOE objective in this ST. Its goal is to ensure that the hardware platform is used in a secure manner, which is based on the insight that hardware and software have to supplement each other in order to build a secure whole. The ST claims conformance to the PP and the PP SFRs do cover the PP TOE objectives. The PP uses the environment objective OE.Plat-Appl to ensure appropriate software support for its SFRs, but since the TOE does now consist of hardware and software, the PP SFRs do also apply to the Security IC Embedded Software included in the TOE, and thereby all PP SFRs fulfil the objective O.Plat-Appl. In other words: the software support required by the hardware-focused PP is now included in this combined hardware-software TOE and both hardware and software fulfil the PP SFRs.

Security objective “Treatment of user data (O.Resp-Appl)”

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

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)”

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

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

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

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])"

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])"

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])"

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

7.4.4 Dependencies of Security Functional Requirements

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

- those justified in the BSI-PP-0035 protection profile security requirements rationale,
- those justified in AUG security requirements rationale (except on FMT_MSA.2, see discussion below),
- the dependency of FCS_COP.1 and FCS_CKM.1 on FCS_CKM.4 (see discussion below),
- the dependency of FMT_MSA.1 [Loader] and FMT_MSA.3 [Loader] on FMT_SMR.1 (see discussion below),
- the dependency of FMT_MSA.3 [APPLI_FWL] on FMT_MSA.1 and FMT_SMR.1 (see discussion below).

Details are provided in Table 13 below.
<table>
<thead>
<tr>
<th>Label</th>
<th>Dependencies</th>
<th>Fulfilled by security requirements in this Security Target</th>
<th>Dependency already in BSI-PP-0035 or in AUG</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRU_FLT.2</td>
<td>FPT_FLS.1</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FPT_FLS.1</td>
<td>None</td>
<td>No dependency</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FMT_LIM.1</td>
<td>FMT_LIM.2 [Test]</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FMT_LIM.2</td>
<td>FMT_LIM.1 [Test]</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FMT_LIM.1</td>
<td>FMT_LIM.2 [Admin]</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FMT_LIM.2</td>
<td>FMT_LIM.1 [Admin]</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FAU_SAS.1</td>
<td>None</td>
<td>No dependency</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FPT_PHP.3</td>
<td>None</td>
<td>No dependency</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FDP_ITT.1</td>
<td>FDP_ACC.1 or FDP_IFC.1</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FPT_ITT.1</td>
<td>None</td>
<td>No dependency</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FDP_IFC.1</td>
<td>FDP_IFF.1</td>
<td>No, see BSI-PP-0035</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FCS_RNG.1</td>
<td>None</td>
<td>No dependency</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FCS_COP.1</td>
<td>[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4]</td>
<td>No, see discussion below</td>
<td>Yes, AUG #1</td>
</tr>
<tr>
<td>FCS_CKM.1</td>
<td>[FDP_CKM.2 or FCS_COP.1]</td>
<td>Yes, by FCS_COP.1</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FDP_ACC.2</td>
<td>FDP_ACF.1 [Memories]</td>
<td>No, see discussion below</td>
<td>Yes, CCMB-2012-09-002</td>
</tr>
<tr>
<td>FDP_ACF.1</td>
<td>FDP_ACC.1 [Memories]</td>
<td>Yes, by FDP_ACC.2 [Memories]</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_MSA.3</td>
<td>FMT_MSA.1 [Memories]</td>
<td>Yes</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_SMR.1</td>
<td>FMT_MSA.1 [Memories]</td>
<td>No, see AUG #4</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_SMR.1</td>
<td>[FDP_ACC.1 or FDP_IFC.1]</td>
<td>Yes, by FDP_ACC.2 [Memories] and FDP_IFC.1</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_MSA.1</td>
<td>[Memories]</td>
<td>No, see AUG #4</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_SMF.1</td>
<td>FMT_MSA.1 [Memories]</td>
<td>Yes</td>
<td>No, CCMB-2012-09-002</td>
</tr>
</tbody>
</table>
### Table 13. Dependencies of security functional requirements (continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Dependencies</th>
<th>Fulfilled by security requirements in this Security Target</th>
<th>Dependency already in BSI-PP-0035 or AUG</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMT_SMF.1 [Memories]</td>
<td>None</td>
<td>No dependency</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_ITC.1 [Loader]</td>
<td>[FDP_ACC.1 [Loader] or FDP_IFC.1]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_MSA.3 [Loader]</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1 [Loader]</td>
<td>FDP_ACF.1 [Loader]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FDP_ACF.1 [Loader]</td>
<td>FDP_ACC.1 [Loader]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_MSA.3 [Loader]</td>
<td>FMT_MSA.1 [Loader]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_SMR.1 [Loader]</td>
<td>FMT_SMR.1 [Loader]</td>
<td>No, see discussion below</td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.1 [Loader]</td>
<td>[FDP_ACC.1 [Loader] or FDP_IFC.1]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FDP_SMF.1 [Loader]</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_SMF.1 [Loader]</td>
<td>FDP_SMR.1 [Loader]</td>
<td>No, see discussion below</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1 [APPLI_FWIL]</td>
<td>FDP_ACF.1 [APPLI_FWIL]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FDP_ACF.1 [APPLI_FWIL]</td>
<td>FDP_ACC.1 [APPLI_FWIL]</td>
<td>Yes</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_MSA.3 [APPLI_FWIL]</td>
<td>FMT_MSA.1 [APPLI_FWIL]</td>
<td>No, see discussion below</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
<tr>
<td>FMT_MSA.3 [APPLI_FWIL]</td>
<td>FMT_SMR.1</td>
<td>No, see discussion below</td>
<td><strong>No, CCMB-2012-09-002</strong></td>
</tr>
</tbody>
</table>

246 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.

247 Part 2 of the Common Criteria defines the dependency of "Cryptographic operation (FCS_COP.1)" and "Cryptographic key generation (FCS_CKM.1)" on "Cryptographic key destruction (FCS_CKM.4)". In this particular TOE, there is no specific function for the destruction of the keys. The ES has all possibilities to implement its own destruction function, in conformance with its security policy. Therefore, FCS_CKM.4 is not defined in this ST.
Part 2 of the Common Criteria defines the dependency of "Management of security attributes (FMT_MSA.1) [Loader]" and "Static attribute initialisation (FMT_MSA.3) [Loader]" on "Security roles (FMT_SMR.1) [Loader]". This dependency is considered to be satisfied, because the access control defined for the loader is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a Security Functional Requirement "FMT_SMR.1".

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".

7.4.5 Rationale for the Assurance Requirements

Security assurance requirements added to reach EAL5 (Table 10)

Regarding application note 21 of BSI-PP-0035, this Security Target chooses EAL5 because developers and users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

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.

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

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

Dependencies of assurance requirements

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

Augmentation to this package are identified in paragraph 203 and do not introduce dependencies not already satisfied by the EAL5 package.
8 TOE summary specification

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

The complete TOE summary specification has been presented and evaluated in the ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G with firmware revision 1.3.2, optional cryptographic library Neslib 4.2.10 - SECURITY TARGET.

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

8.1 Limited fault tolerance (FRU_FLT.2)

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

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

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

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

The ES can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1) [Test]

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

8.4 Limited capabilities (FMT_LIM.1) [Admin]

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

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

The TOE is either in TEST, ADMIN or USER configuration.
The only authorised TOE configuration modifications are:
• TEST to ADMIN configuration,
• TEST to USER configuration,
• ADMIN to USER configuration.

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

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

8.6 Audit storage (FAU_SAS.1)

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

8.7 Resistance to physical attack (FPT_PHP.3)

The TSF ensures resistance to physical tampering, thanks to the following features:
• The TOE implements counter-measures that reduce the exploitability of physical probing.
• The TOE is physically protected by an active shield that commands an automatic reaction on die integrity violation detection.

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

The TSF prevents the disclosure of internal and user data thanks to:
• Memories scrambling and encryption,
• Bus encryption,
• Mechanisms for operation execution concealment,
• etc..

8.9 Random number generation (FCS_RNG.1)

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

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

The TOE provides an EDES accelerator that has the capability to perform DES and Triple DES encryption and decryption conformant to NIST SP 800-67. Note that DES is no longer recommended as an encryption function in the context of smart
card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

273 The EDES accelerator offers a Cipher Block Chaining (CBC) mode conformant to NIST SP 800-38A.

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

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

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

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

276 The cryptographic library Neslib provides the RSA private key cryptographic operation with or without CRT for modulus sizes up to 4096 bits, conformant to PKCS #1 V2.1.

277 The cryptographic library Neslib provides RSA signature formatting (EMSA) compliant with PKCS #1 V2.1.

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

278 The cryptographic library Neslib provides to the ES developer the following efficient basic functions for Elliptic Curves Cryptography over prime fields, all conformant to IEEE 1363-2000 chapter 7 and IEEE 1363a-2004:
- private scalar multiplication,
- preparation of Elliptic Curve computations in affine coordinates,
- public scalar multiplication,
- point validity check,
- Jacobian conversion to affine coordinates,
- general point addition,
- point expansion and compression.

279 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 and Elliptic Curve Digital Signature Algorithm (ECDSA) generation and verification, as stipulated in FIPS 186-4 and specified in ANSI X9.62, section 7.
8.14 **Cryptographic operation: SHA operation (FCS_COP.1 [SHA]) if Neslib only**

- 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.
- The cryptographic library Neslib provides the SHA-1 and SHA-256 secure hash function conformant to FIPS PUB 180-2 and offering resistance against side channel and fault attacks.
- 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 and SHA-256.

8.15 **Cryptographic operation: DRBG operation (FCS_COP.1 [DRBG]) if Neslib only**

- The cryptographic library Neslib gives support for a DRBG generator, based on cryptographic algorithms specified in NIST SP 800-90.
- The cryptographic library Neslib implements three of the DRBG specified in NIST SP 800-90:
  - Hash-DRBG,
  - CTR-DRBG.

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

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

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

- The cryptographic library Neslib provides standard RSA public and private key computation for key sizes up 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.

8.18 **Static attribute initialisation (FMT_MSA.3) [Memories]**

- The TOE enforces a default memory protection policy when none other is programmed by the ES.
8.19  **Management of security attributes (FMT_MSA.1) [Memories]** & **Specification of management functions (FMT_SMF.1) [Memories]**

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

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

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

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

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

8.22  **Static attribute initialisation (FMT_MSA.3) [Loader]**

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

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

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

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

In Admin configuration, the System Firmware grants access to the Flash Loader functions, only after presentation of the required valid passwords.
8.25 **Subset access control (FDP_ACC.1) [APPLI_FWL] & Security attribute based access control (FDP_ACF.1) [APPLI_FWL]**

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

8.26 **Static attribute initialisation (FMT_MSA.3) [APPLI_FWL]**

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.
# References

## Protection Profile references

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security IC Platform Protection Profile</td>
<td>BSI-PP-0035</td>
<td>1.0</td>
</tr>
</tbody>
</table>

## ST33G Platform Security Target reference

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST33G platform ST33G1M2A, ST33G1M2M maskset K8H0A version G with firmware revision 1.3.2, optional cryptographic library Neslib 4.2.10 - SECURITY TARGET</td>
<td>SMD_ST33G_ST_14_001</td>
</tr>
</tbody>
</table>

## Guidance documentation references

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST33G Platform - ST33G1M2A: M2M automotive-grade Secure MCU with 32-bit ARM® SecurCore® SC300TM CPU and high density Flash memory - Datasheet</td>
<td>DS_ST33G1M2A</td>
<td>0.1</td>
</tr>
<tr>
<td>ST33G Platform - ST33G1M2M: M2M Industrial Secure MCU with 32-bit ARM® SecurCore® SC300TM CPU and high density Flash memory - Datasheet</td>
<td>DS_ST33G1M2M</td>
<td>0.1</td>
</tr>
<tr>
<td>ST33G1M2A, ST33G1M2M: CMOS M10+ 80-nm technology die and wafer delivery description</td>
<td>DD_ST33G1M2A_M</td>
<td>1</td>
</tr>
<tr>
<td>ARM® Cortex SC300 r0p0 Technical Reference Manual</td>
<td>ARM DDI 0337</td>
<td>F</td>
</tr>
<tr>
<td>ARM® Cortex M3 r2p0 Technical Reference Manual</td>
<td>ARM DDI 0337F3c</td>
<td>F3c</td>
</tr>
<tr>
<td>ARM® SC300 r0p0 SecurCore Technical Reference Manual Supplement 1A</td>
<td>ARM DDI 0337 Supp 1A</td>
<td>A</td>
</tr>
<tr>
<td>ARM® SecurCore SC300 technical limitations</td>
<td>ES_SC300</td>
<td>1</td>
</tr>
<tr>
<td>STx ARM Execute-only memory support for SecurCore® SC000 and SC300</td>
<td>AN_33_EXE</td>
<td>2</td>
</tr>
<tr>
<td>ST33 uniform timing application note</td>
<td>AN_33_UT</td>
<td>2</td>
</tr>
<tr>
<td>ST33G1M2A Firmware user manual</td>
<td>UM_ST33G1M2A_FW</td>
<td>3</td>
</tr>
<tr>
<td>ST33G and ST33H Firmware support for LPU regions - Application Note</td>
<td>AN_33G_33H_LPU</td>
<td>1</td>
</tr>
<tr>
<td>ST33G and ST33H Secure MCU platforms - Security Guidance</td>
<td>AN_SECU_ST33</td>
<td>5</td>
</tr>
<tr>
<td>ST33G and ST33H Power supply glitch detector characteristics - application note</td>
<td>AN_33_GLITCH</td>
<td>2</td>
</tr>
<tr>
<td>ST33G and ST33H - AIS31 Compliant Random Number user manual</td>
<td>UM_33G_33H_AIS31</td>
<td>3</td>
</tr>
</tbody>
</table>
Reference

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST33G and ST33H - AIS31 Reference implementation - Startup, online and total failure tests - User manual</td>
<td>AN_33G_33H_AIS31</td>
<td>1</td>
</tr>
<tr>
<td>NesLib 4.2 library - User manual</td>
<td>UM_NESLIB_4_2</td>
<td>1</td>
</tr>
<tr>
<td>ST33G and ST33H Secure MCU platforms NesLib 4.2 security recommendations - Application note</td>
<td>AN_SECU_ST33_NESLIB_4_2</td>
<td>2</td>
</tr>
<tr>
<td>Neslib 4.2.10 Release Note</td>
<td>RN_ST33_NESLIB_4_2_10</td>
<td>4</td>
</tr>
<tr>
<td>Flash memory loader installation guide for the ST33G1M2A and ST33G1M2M platforms - User manual</td>
<td>UM_33GA_FL</td>
<td>3</td>
</tr>
</tbody>
</table>

Standards references

<table>
<thead>
<tr>
<th>Ref</th>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[2]</td>
<td>NIST SP 800-67</td>
<td>NIST SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, revised January 2012, National Institute of Standards and Technology</td>
</tr>
<tr>
<td>[3]</td>
<td>FIPS PUB 140-2</td>
<td>FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002</td>
</tr>
<tr>
<td>[5]</td>
<td>FIPS 186-4</td>
<td>FIPS PUB 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), July 2013</td>
</tr>
<tr>
<td>[8]</td>
<td>NIST SP 800-38A</td>
<td>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</td>
</tr>
<tr>
<td>Ref</td>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[17]</td>
<td>PKCS #1 V2.1</td>
<td>PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002</td>
</tr>
<tr>
<td>[19]</td>
<td>NIST SP 800-38B</td>
<td>NIST special publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, National Institute of Standards and Technology (NIST), May 2005</td>
</tr>
<tr>
<td>[20]</td>
<td>NIST SP 800-90</td>
<td>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</td>
</tr>
<tr>
<td>[22]</td>
<td>NIST SP 800-56A</td>
<td>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</td>
</tr>
</tbody>
</table>
Appendix A  Glossary

A.1  Terms

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

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

End-consumer
User of the Composite Product in Phase 7.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Sensitive information**
Any information identified as a security relevant element of the TOE such as:
- the application data of the TOE (such as IC pre-personalization requirements, IC and system specific data),
- the security IC embedded software,
- the IC dedicated software,
- the IC specification, design, development tools and technology.

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

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

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

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

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

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

**User data**
All data managed by the Smartcard Embedded Software in the application context. User data comprise all data in the final Smartcard IC except the TSF data.
## A.2 Abbreviations

Table 14. List of abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard.</td>
</tr>
<tr>
<td>AIS</td>
<td>Application notes and Interpretation of the Scheme (BSI).</td>
</tr>
<tr>
<td>ALU</td>
<td>Arithmetical and Logical Unit.</td>
</tr>
<tr>
<td>BSI</td>
<td>Bundesamt für Sicherheit in der Informationstechnik.</td>
</tr>
<tr>
<td>CBC</td>
<td>Cipher Block Chaining.</td>
</tr>
<tr>
<td>CBC-MAC</td>
<td>Cipher Block Chaining Message Authentication Code.</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria Version 3.1.</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit.</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check.</td>
</tr>
<tr>
<td>DCSSI</td>
<td>Direction Centrale de la Sécurité des Systèmes d’Information</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard.</td>
</tr>
<tr>
<td>DIP</td>
<td>Dual-In-Line Package.</td>
</tr>
<tr>
<td>DRBG</td>
<td>Deterministic Random Bit Generator.</td>
</tr>
<tr>
<td>EAL</td>
<td>Evaluation Assurance Level.</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book.</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography.</td>
</tr>
<tr>
<td>EDES</td>
<td>Enhanced DES.</td>
</tr>
<tr>
<td>EEPROM</td>
<td>Electrically Erasable Programmable Read Only Memory.</td>
</tr>
<tr>
<td>ES</td>
<td>Security IC Embedded SoftWare.</td>
</tr>
<tr>
<td>FTOS</td>
<td>Final Test Operating System.</td>
</tr>
<tr>
<td>GPIO</td>
<td>General Purpose I/O.</td>
</tr>
<tr>
<td>I/O</td>
<td>Input / Output.</td>
</tr>
<tr>
<td>IART</td>
<td>ISO-7816 Asynchronous Receiver Transmitter.</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit.</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organisation.</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology.</td>
</tr>
<tr>
<td>LPU</td>
<td>Library Protection Unit.</td>
</tr>
<tr>
<td>MAC</td>
<td>Message Authentication Code.</td>
</tr>
<tr>
<td>MPU</td>
<td>Memory Protection Unit.</td>
</tr>
<tr>
<td>NESCRIPT</td>
<td>Next Step Cryptography Accelerator.</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication.</td>
</tr>
</tbody>
</table>
### Table 14. List of abbreviations (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology.</td>
</tr>
<tr>
<td>NVM</td>
<td>Non Volatile Memory.</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System.</td>
</tr>
<tr>
<td>OSP</td>
<td>Organisational Security Policy.</td>
</tr>
<tr>
<td>OST</td>
<td>Operating System for Test.</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile.</td>
</tr>
<tr>
<td>PUB</td>
<td>Publication Series.</td>
</tr>
<tr>
<td>RAM</td>
<td>Random Access Memory.</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency.</td>
</tr>
<tr>
<td>RF UART</td>
<td>Radio Frequency Universal Asynchronous Receiver Transmitter.</td>
</tr>
<tr>
<td>ROM</td>
<td>Read Only Memory.</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir &amp; Adleman.</td>
</tr>
<tr>
<td>SAR</td>
<td>Security Assurance Requirement.</td>
</tr>
<tr>
<td>SFP</td>
<td>Security Function Policy.</td>
</tr>
<tr>
<td>SFR</td>
<td>Security Functional Requirement.</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm.</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module.</td>
</tr>
<tr>
<td>SOIC</td>
<td>Small Outline IC.</td>
</tr>
<tr>
<td>SPI</td>
<td>Serial Peripheral Interface.</td>
</tr>
<tr>
<td>ST</td>
<td>Context dependent : STMicroelectronics or Security Target.</td>
</tr>
<tr>
<td>SWP</td>
<td>Single Wire Protocol.</td>
</tr>
<tr>
<td>TOE</td>
<td>Target of Evaluation.</td>
</tr>
<tr>
<td>TQFP</td>
<td>Thin Quad Flat Package.</td>
</tr>
<tr>
<td>TRNG</td>
<td>True Random Number Generator.</td>
</tr>
<tr>
<td>TSC</td>
<td>TSF Scope of Control.</td>
</tr>
<tr>
<td>TSF</td>
<td>TOE Security Functionality.</td>
</tr>
<tr>
<td>TSFI</td>
<td>TSF Interface.</td>
</tr>
<tr>
<td>TSP</td>
<td>TOE Security Policy.</td>
</tr>
<tr>
<td>TSS</td>
<td>TOE Summary Specification.</td>
</tr>
<tr>
<td>UID</td>
<td>User Identification.</td>
</tr>
</tbody>
</table>

*Note: ST Context dependent : STMicroelectronics or Security Target.*
10 Revision history

Table 15. Document revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>26-Sep-2016</td>
<td>01.00</td>
<td>Initial release</td>
</tr>
<tr>
<td>09-Jan-2017</td>
<td>01.01</td>
<td>Changes in guidances</td>
</tr>
<tr>
<td>12-Jan-2017</td>
<td>01.02</td>
<td>Changes in guidances</td>
</tr>
</tbody>
</table>
Please Read Carefully:

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

All ST products are sold pursuant to ST's terms and conditions of sale. Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

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

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

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

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

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

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

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

© 2017 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

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

www.st.com