ST23ZL48A / ST23ZL34A / ST23ZL18A
Security Target - Public Version
Common Criteria for IT security evaluation

SMD_ST23ZLxx_ST_09_001 Rev 01.00
1 Introduction

1.1 Security Target reference

1 Document identification: ST23ZL48A / ST23ZL34A / ST23ZL18A SECURITY TARGET -
PUBLIC VERSION.

2 Version number: Rev 01.00, issued November 2009.

3 Registration: registered at ST Microelectronics under number
SMD_ST23ZLxx_ST_09_001_V01.00.

1.2 Purpose

4 This document presents the Security Target - Public version (ST) of the ST23ZL48A,
ST23ZL34A, and ST23ZL18A, Security Integrated Circuits (IC), with Dedicated Software
(DSW), designed on the ST23 platform of STMicroelectronics.

5 This document is a sanitized version of the Security Target used for the evaluation. It is
classified as public information.

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

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

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

2 Context ........................................................................ 9

3 TOE description .......................................................... 10
  3.1 TOE overview ............................................................ 10
  3.2 TOE life cycle ............................................................ 12
  3.3 TOE environment ........................................................ 12
    3.3.1 TOE Development Environment ............................. 13
    3.3.2 TOE production environment ................................. 13
    3.3.3 TOE operational environment ................................. 13

4 Conformance claims ...................................................... 15
  4.1 Common Criteria conformance claims ............................... 15
  4.2 PP Claims ................................................................. 15
    4.2.1 PP Reference ...................................................... 15
    4.2.2 PP Refinements ................................................... 15
    4.2.3 PP Additions ...................................................... 15
    4.2.4 PP Claims rationale .............................................. 15

5 Security problem definition ........................................... 17
  5.1 Description of assets .................................................. 17
  5.2 Threats ................................................................. 18
  5.3 Organisational security policies .................................... 19
  5.4 Assumptions ............................................................ 20

6 Security objectives ....................................................... 21
  6.1 Security objectives for the TOE .................................... 21
  6.2 Security objectives for the environment .......................... 22
  6.3 Security objectives rationale ....................................... 22
    6.3.1 TOE threat "Memory Access Violation" ....................... 23
6.3.2 Organisational security policy "Additional Specific Security Functionality"

7 Security requirements ........................................... 25

7.1 Security functional requirements for the TOE .................. 25
  7.1.1 Limited fault tolerance (FRUFLT.2) ......................... 26
  7.1.2 Failure with preservation of secure state (FPTFLS.1) ....... 26
  7.1.3 Limited capabilities (FMTLIM.1) .......................... 26
  7.1.4 Limited availability (FMTLIM.2) ........................... 27
  7.1.5 Audit storage (FAUSAS.1) .................................. 27
  7.1.6 Resistance to physical attack (FPTPHP.3) .................. 27
  7.1.7 Basic internal transfer protection (FDPITT.1) .............. 27
  7.1.8 Basic internal TSF data transfer protection (FPTITT.1) .... 27
  7.1.9 Subset information flow control (FDPIFC.1) ............... 27
  7.1.10 Random number generation (FCSRNG.1) .................... 28
  7.1.11 Cryptographic operation (FSCOP.1) ........................ 28
  7.1.12 Static attribute initialisation (FMTMSA.3) ............... 28
  7.1.13 Management of security attributes (FMTMSA.1) ......... 28
  7.1.14 Complete access control (FPDACC.2) ...................... 29
  7.1.15 Security attribute based access control (FPDACF.1) ...... 29

7.2 TOE security assurance requirements ........................ 29

7.3 Refinement of the security assurance requirements ............. 30
  7.3.1 Refinement regarding functional specification (ADV_FSP) ... 31
  7.3.2 Refinement regarding test coverage (ATE_COV) ............ 32

7.4 Security Requirements rationale ................................ 32
  7.4.1 Rationale for the Security Functional Requirements ........ 32
  7.4.2 Additional security objectives are suitably addressed ..... 33
  7.4.3 Additional security requirements are consistent .......... 33
  7.4.4 Dependencies of Security Functional Requirements .......... 34
  7.4.5 Rationale for the Assurance Requirements ................. 35

8 TOE summary specification ........................................ 36

8.1 Statement of TOE security functionality ....................... 36
  8.1.1 TSF_INIT_A: Hardware initialisation & TOE attribute initialisation 36
  8.1.2 TSF_CONFIG_A: TOE configuration switching and control .... 36
  8.1.3 TSF_INT_A: TOE logical integrity .......................... 36
  8.1.4 TSF_TEST_A: Test of the TOE .............................. 36
8.1.5 TSF_FWL_A: Memory Firewall ........................................ 37
8.1.6 TSF_PHT_A: Physical tampering protection ..................... 37
8.1.7 TSF_ADMINIS_A: Security violation administrator .............. 37
8.1.8 TSF_OBS_A: Unobservability ....................................... 38
8.1.9 TSF_SKCS_A: Symmetric Key Cryptography Support .......... 38
8.1.10 TSF_ALEAS_A: Unpredictable Number Generation Support .. 38

8.2 TOE summary specification rationale ................................ 38
8.2.1 TSF rationale ......................................................... 39

9 References ....................................................................... 40

Appendix A Glossary ............................................................ 42
A.1 Terms ........................................................................ 42
A.2 Abbreviations ............................................................. 44

10 Revision history .............................................................. 46
List of tables

Table 1. Products of the TOE ................................................................. 10
Table 2. Composite product life cycle phases ........................................ 12
Table 3. Summary of security environment ........................................... 18
Table 4. Summary of security objectives ............................................... 21
Table 5. Security Objectives versus Assumptions, Threats or Policies .......... 23
Table 6. Summary of functional security requirements for the TOE ............... 25
Table 7. FCS_COP.1 iterations (cryptographic operations) ......................... 28
Table 8. TOE security assurance requirements ....................................... 30
Table 9. Impact of EAL5 selection on BSI-PP-0035 refinements .................. 31
Table 10. Dependencies of security functional requirements ...................... 34
Table 11. Mapping of TSF services and SFRs .......................................... 39
Table 12. List of abbreviations .............................................................. 44
Table 13. Document revision history ....................................................... 46
List of figures

Figure 1. ST23ZL48A / ST23ZL34A / ST23ZL18A block diagram .......................... 11
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 Smartcard Division of STMicroelectronics (ST).

The Target of Evaluation (TOE) comprises the ST23ZL48A, ST23ZL34A, and ST23ZL18A.

The assurance level of the performed Common Criteria (CC) IT Security Evaluation is EAL 5 augmented.

The intent of this Security Target is to specify the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) applicable to the ST23ZL48A, ST23ZL34A, and ST23ZL18A security ICs, and to summarise their 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

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 overview

The Target of Evaluation (TOE) comprises three products: the ST23ZL48A, ST23ZL34A, and ST23ZL18A.

All those products share the same hardware design, and the same maskset. The different derivates differ only on the available memories size, as detailed here below:

<table>
<thead>
<tr>
<th>Product name</th>
<th>EEPROM size</th>
<th>Identification number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST23ZL48A</td>
<td>48 KBytes</td>
<td>0001h</td>
</tr>
<tr>
<td>ST23ZL34A</td>
<td>34 KBytes</td>
<td>000Ch</td>
</tr>
<tr>
<td>ST23ZL18A</td>
<td>18 KBytes</td>
<td>000Bh</td>
</tr>
</tbody>
</table>

The products having different NVM sizes can be distinguished by their product identification number, included in the traceability number, as detailed in their Data Sheets.

In this Security Target, the terms "TOE" or "ST23ZL48A / ST23ZL34A / ST23ZL18A" mean all 3 products.

The rest of this document applies to all products, except when a particular mention to one of the products is added. For easier reading, the restrictions corresponding to a particular product are typeset as indicated here.

The TOE is a serial access Smartcard IC based on the enhanced 8/16-bit ST23 CPU core, with 48 Kbytes EEPROM for the ST23ZL48A / 34 Kbytes EEPROM for the ST23ZL34A / 18 Kbytes EEPROM for the ST23ZL18A, an internally generated clock, an MPU, an internal True Random Number Generator (TRNG) and accelerators dedicated to cryptographic algorithms.

Operations are synchronized with an internally generated clock issued by the Clock Generator module. The internal speed of the device is fully software programmable. High performance can be reached by using high speed internal clock frequency (up to 29 MHz).

The CPU includes the Arithmetic Logic Unit (ALU) and the control logic. This device includes a flexible memory protection unit (MPU), which enables a fully dynamic memory segmentation and protection without downgrading the CPU performance. The MPU enables the software to control the addressable space and registers available to any given program, thanks to a flexible and software-friendly interface. As a result, the MPU allows the software developers to enforce a wide range of memory protection policies.

The E-DES (Enhanced DES) module supports efficiently the Data Encryption Standard (DES [2]) with built-in countermeasures against side channel attacks. Additionally, an extra feature allows fast implementation of CBC and CBC-MAC modes [10] [9].

The NESCRYPT (NExt Step CRYPTo-processor) is the latest generation of ST cryptographic accelerator providing native modular arithmetic for both GF(p) and GF(2^n) with a very high level of performance. NESCRYPT also includes dedicated instructions to accelerate SHA-1 and SHA-2 family hash functions. NESCRYPT allows efficient and secure
implementation of almost all known public key cryptosystems with a high level of performance ([4], [8], [12], [18],[19], [20], [21]).

As randomness is a key stone in many applications, the ST23ZL48A / ST23ZL34A / ST23ZL18A features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS-31 [1] and directly accessible through dedicated registers.

In a few words, the ST23ZL48A / ST23ZL34A / ST23ZL18A offer a unique combination of high performances and very powerful features for high level security:
- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- Hardware Security Enhanced DES accelerator,
- AIS-31 class P2 compliant True Random Number Generator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- NExt Step CRYPTography accelerator (NESCRIPT).

The TOE includes in the ST protected ROM a Dedicated Software which provides full test capabilities (operating system for test, called “OST”), not accessible by the Security IC Embedded SoftWare (SICESW), after delivery.

In addition, the ROM of the tested samples contains an operating system called “Card Manager” that allows the evaluators to use a set of commands with the I/O, and to load in EEPROM (or in RAM) test softwares.

Figure 1 provides an overview of the ST23ZL48A / ST23ZL34A / ST23ZL18A.
3.2 TOE life cycle

26 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.

27 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.

28 The life cycle phases are summarized in Table 2.

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

30 The TOE Manufacturer, as defined in [BSI-PP-0035], is STMicroelectronics.

31 In the following, the term "TOE delivery" is uniquely used to indicate after phase 3 (or before phase 4). The TOE is delivered after phase 3, in USER configuration.

<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</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 preparation pre-personalisation</td>
<td>IC manufacturer: ST</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</td>
</tr>
<tr>
<td>5</td>
<td>Composite product integration</td>
<td>composite product finishing process composite product preparation composite product shipping</td>
<td>Composite product integrator</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>

3.3 TOE environment

32 Considering the TOE, three types of environments are defined:
- Development environment corresponding to phase 2,
- Production environment corresponding to phase 3,
- Operational environment, including phase 1 and from phase 4 to phase 7.
3.3.1 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 are the following: ST ROUSSET and ST ANG MO KIO, for the design activities, ST ROUSSET, for the engineering activities, ST ROUSSET for the software development activities.

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 and DPE ITALY.

3.3.2 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 is ST ROUSSET.

The authorized EWS plant involved in the testing of the TOE is ST ROUSSET.

3.3.3 TOE operational environment

A TOE operational environment is the environment of phases 1, then 4 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 pay-TV, banking cards, portable communication SIM cards, health cards, transportation cards, identity and
passport cards. The end-user environment therefore covers a wide range of very different functions, thus making it difficult to avoid and monitor any abuse of the TOE.
4 Conformance claims

4.1 Common Criteria conformance claims

The ST23ZL48A / ST23ZL34A / ST23ZL18A Security Target claims to be conformant to the Common Criteria version 3.1.


The assurance level for the ST23ZL48A / ST23ZL34A / ST23ZL18A Security Target is EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

The ST23ZL48A / ST23ZL34A / ST23ZL18A Security Target claims strict conformance to the Security IC Platform Protection Profile (BSI-PP-0035), as required by this Protection Profile.

4.2.2 PP Refinements

The main refinements operated on the BSI-PP-0035 are:
- Addition #1: “Support of Cipher Schemes” from AUG,
- Addition #4: “Area based Memory Access Control” from AUG,
- Refinement of assurance requirements.

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

4.2.3 PP Additions

The security environment additions relative to the PP are summarized in Table 3.

The additional security objectives relative to the PP are summarized in Table 4.

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

The additional SFRs for the TOE relative to the PP are summarized in Table 6.

The additional SARs relative to the PP are summarized in Table 8.

4.2.4 PP Claims rationale

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

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

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

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

63 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.

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

65 A summary of all these security aspects and their respective conditions is provided in Table 3.

5.1 Description of assets

66 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.

67 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.

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

SC4 deficiency of random numbers.

69 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 to 3) can be grouped as follows:

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

### Table 3. 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>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>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
5.3 Organisational security policies

72 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.

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

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

75 No other Organisational Security Policy (OSP) has been defined in this ST since their specifications depend heavily on the applications in which the TOE will be integrated. The Security Targets for the applications embedded in this TOE should further define them.

BSI.P.Process-TOE Protection during TOE Development and Production:
An accurate identification is established for the TOE. This requires that each instantiation of the TOE carries this unique identification.
AUG1.P.Add-Functions  Additional Specific Security Functionality:
The TOE shall provide the following specific security functionality to the Security IC Embedded Software:
– Data Encryption Standard (DES),
– Triple Data Encryption Standard (3DES).
Note that DES is no longer recommended as an encryption function in the context of smart card applications. Hence, Security IC Embedded Software may need to use triple DES to achieve a suitable strength.

5.4 Assumptions

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 4. Note that the origin of each objective is clearly identified in the prefix of its label.

Most of these security aspects can therefore be easily found in the protection profile. Only those originating in AUG are detailed in the following sections.

Table 4. 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><em>Dynamic</em> Area based Memory Access Control</td>
</tr>
<tr>
<td>BSI.OE.Plat-Appl</td>
<td>Usage of Hardware Platform</td>
</tr>
<tr>
<td>BSI.OE.Resp-Appl</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

- 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
6.2 Security objectives for the environment

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

BSI.OE.Plat-Appl Usage of Hardware Platform
BSI.OE.Resp-Appl Treatment of User Data

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

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

Thus, it is necessary to show that:

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

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)".
As required by CC Part 1 (CCMB-2006-09-001), no assumption nor objective for the environment has been added to those of the BSI-PP-0035 Protection Profile to which strict conformance is claimed.

The justification of the additional policy and the additional threat provided in the next subsections shows that they do not contradict to the rationale already given in the protection profile BSI-PP-0035 for the assumptions, policy and threats defined there.

### Table 5. 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>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>AUG1.P.Add-Functions</td>
<td>AUG1.O.Add-Functions</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 Organisational security policy "Additional Specific Security Functionality"

The justification related to the organisational security policy "Additional Specific Security Functionality, (AUG1.P.Add-Functions)" is as follows:
Since \textit{AUG1.O.Add-Functions} requires the TOE to implement exactly the same specific security functionality as required by \textit{AUG1.P.Add-Functions}, and in the very same conditions, the organisational security policy is covered by the objective.

Nevertheless the security objectives \textit{BSI.O.Leak-Inherent}, \textit{BSI.O.Phys-Probing}, \textit{BSI.O.Malfunction}, \textit{BSI.O.Phys-Manipulation} and \textit{BSI.O.Leak-Forced} define how to implement the specific security functionality required by \textit{AUG1.P.Add-Functions}. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from \textit{AUG1.P.Add-Functions}.) Especially \textit{BSI.O.Leak-Inherent} and \textit{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 \textit{AUG1.P.Add-Functions}.

The added objective for the TOE \textit{AUG1.O.Add-Functions} does not introduce any contradiction in the security objectives for the TOE.
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-2007-09-002, except the following SFRs, that are extensions to CCMB-2007-09-002:

- 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-2007-09-002.

All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of CCMB-2006-09-001. 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.

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

The selected security functional requirements for the TOE, their respective origin and type are summarized in Table 6.

Table 6. Summary of functional security requirements for the TOE

<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></td>
<td></td>
</tr>
<tr>
<td>FPT_FLS.1</td>
<td>Failure with preservation of secure state</td>
<td>Malfunction</td>
<td>BSI-PP-0035</td>
<td></td>
</tr>
<tr>
<td>FMT_LIM.1</td>
<td>Limited capabilities</td>
<td>Abuse of functionality</td>
<td>BSI-PP-0035</td>
<td></td>
</tr>
<tr>
<td>FMT_LIM.2</td>
<td>Limited availability</td>
<td></td>
<td></td>
<td>Extended</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>
</tbody>
</table>
Table 6. Summary of functional security requirements for the TOE (continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Title</th>
<th>Addressing</th>
<th>Origin</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPT_PHP.3</td>
<td>Resistance to physical attack</td>
<td>Physical manipulation &amp; probing</td>
<td>BSI-PP-0035</td>
<td>Extended</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>Leakage</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</td>
<td>Operated</td>
</tr>
<tr>
<td>FCS_COP.1</td>
<td>Cryptographic operation</td>
<td>Cipher scheme support</td>
<td>AUG #1</td>
<td>Operated</td>
</tr>
<tr>
<td>FDP_ACC.2</td>
<td>Complete access control</td>
<td>Memory access violation</td>
<td>Security Target</td>
<td>Operated</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>AUG #4</td>
<td>Operated</td>
</tr>
<tr>
<td>FMT_MSA.1</td>
<td>Management of security attribute</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.1.1 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).

7.1.2 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.

7.1.3 Limited capabilities (FMT_LIM.1)

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

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.

SFP_1: Limited capability and availability Policy

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

7.1.5 **Audit storage (FAU_SAS.1)**

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

7.1.6 **Resistance to physical attack (FPT_PHP.3)**

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.

7.1.7 **Basic internal transfer protection (FDP_ITT.1)**

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

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

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

Refinement:

The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE. This requirement is equivalent to FDP_ITT.1 above but refers to TSF data instead of User Data. Therefore, it should be understood as to refer to the same Data Processing Policy defined under FDP_IFC.1 below.

7.1.9 **Subset information flow control (FDP_IFC.1)**

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.

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

7.1.10 Random number generation (FCS_RNG.1)

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

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

7.1.11 Cryptographic operation (FCS_COP.1)

The TSF shall perform the operations in Table 7 in accordance with a specified cryptographic algorithm in Table 7 and cryptographic key sizes of Table 7 that meet the standards in Table 7.

Table 7. FCS_COP.1 iterations (cryptographic operations)

<table>
<thead>
<tr>
<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>DES / 3DES</td>
<td>encryption decryption</td>
<td>Data Encryption Standard (DES)</td>
<td>56 effective bits</td>
<td>FIPS PUB 46-3 ISO/IEC 9797-1 ISO/IEC 10116</td>
</tr>
<tr>
<td>operation</td>
<td>- in Cipher Block Chaining (CBC) mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in Electronic Code Book (ECB) mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in CBC-MAC operating modes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DES / 3DES</td>
<td>encryption decryption</td>
<td>Triple Data Encryption Standard (3DES)</td>
<td>112 effective bits</td>
<td></td>
</tr>
<tr>
<td>operation</td>
<td>- in Cipher Block Chaining (CBC) mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in Electronic Code Book (ECB) mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- in CBC-MAC operating modes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.1.12 Static attribute initialisation (FMT_MSA.3)

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

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

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

7.1.13 Management of security attributes (FMT_MSA.1)

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

---

(a) See the Datasheet referenced in Section 9 for actual values.
7.1.14 Complete access control (FDP_ACC.2)

120 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.

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

7.1.15 Security attribute based access control (FDP_ACF.1)

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

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

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

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

*Note:* It should be noted that this level of policy detail is not needed at the application level. The composite Security Target writer should describe the SICESW access control and information flow control policies instead. Within the SICESW 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.

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

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

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

7.2 TOE security assurance requirements

129 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.*

130 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.

131 The set of security assurance requirements (SARs) is presented in *Table 8*, indicating the origin of the requirement.
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 9.
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 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

<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>
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)

143 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).

144 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).

145 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

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

147 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in Table 6 and Table 8, 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.

148 From Table 4, it is straightforward to identify two additional security objectives for the TOE (AUG1.O.Add-Functions and AUG4.O.Mem Access), all tracing back to AUG. This rationale must show that security requirements suitably address these too.

149 Furthermore, a more careful observation of the requirements listed in Table 6 and Table 8 shows that:

- there are additional security requirements introduced by this Security Target (various assurance requirements of EAL5),
- there are security requirements introduced from AUG (FCS_COP.1, FDP_ACC.2, FDP_ACF.1, FMT_MSA.3 and FMT_MSA.1).
Though it remains to show that:

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

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

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

7.4.3 Additional security requirements are consistent

“Cryptographic operation (FCS_COP.1)"

This security requirement has already been argued in Section : Security objective “Additional Specific Security Functionality (AUG1.O.Add-Functions)” above.
“Static attribute initialisation (FMT_MSA.3),
Management of security attributes (FMT_MSA.1),
Complete access control (FDP_ACC.2),
Security attribute based access control (FDP_ACF.1)”

These security requirements have already been argued in Section : Security objective

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 FMT_MSA.1 on FMT_SMF.1 (see discussion below).

Details are provided in Table 10 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</td>
<td>Yes</td>
<td>Yes, BSI-PP-0035</td>
</tr>
<tr>
<td>FMT_LIM.2</td>
<td>FMT_LIM.1</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]</td>
<td>Yes (by the environment)</td>
<td>Yes, AUG #1 (adapted to CC V3.1 R2, see discussion below)</td>
</tr>
<tr>
<td></td>
<td>FCS_CKM.4</td>
<td>Yes (by the environment)</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.2</td>
<td>FDP_ACF.1</td>
<td>Yes</td>
<td>No, CCMB-2007-09-002</td>
</tr>
<tr>
<td>FDP_ACF.1</td>
<td>FDP_ACC.1</td>
<td>Yes</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td></td>
<td>FMT_MSA.3</td>
<td>Yes</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td>FMT_MSA.3</td>
<td>FMT_MSA.1</td>
<td>Yes</td>
<td>Yes, AUG #4</td>
</tr>
<tr>
<td></td>
<td>FMT_SMR.1</td>
<td>No, see AUG #4</td>
<td></td>
</tr>
</tbody>
</table>
Part 2 of the Common Criteria defines the dependency of "Management of security attributes (FMT_MSA.1)" on "Specification of management functions (FMT_SMF.1)". In this particular ST, the specification of FMT_SMF.1 is useless. As stated in the Dynamic Memory Access Control Policy and in FMT_MSA.1, there is no specific function for the management of the memory access rights, it is just part of the Management of the security attributes.

**AUG #1** defines the dependency of "Cryptographic operation (FCS_COP.1)" on "Secure security attributes (FMT_MSA.2)". This dependency is not anymore defined in the Part 2 of the Common Criteria V3.1 Revision 2. Thus, it has not been retained in this Security Target.

### 7.4.5 Rationale for the Assurance Requirements

**Security assurance requirements added to reach EAL5** (Table 8)

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 129 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.

The following TSS relies on the refinement of the TSF security elements, as detailed in the TOE Functional Specification referenced in the ST/SB23ZL48/34/18 Documentation Report (see Section 9, paragraph 207).

8.1 Statement of TOE security functionality

The following TSF services are an abstraction of the TOE Functional Specification.

8.1.1 TSF_INIT_A: Hardware initialisation & TOE attribute initialisation

In TEST and USER configurations, this functionality ensures the following:
- the TOE starts running in a secure state,
- the TOE is securely initialised,
- the reset operation is correctly managed.

8.1.2 TSF_CONFIG_A: TOE configuration switching and control

In TEST and USER configurations, this functionality ensures the switching and the control of TOE configuration.

This functionality ensures that the TOE is either in TEST or USER configuration.

The only authorised TOE configuration modification is TEST to USER configuration, by the TEST administrator.

This functionality is responsible for the TOE configuration detection and notification to the other resources of the TOE.

8.1.3 TSF_INT_A: TOE logical integrity

In TEST and USER configurations, this functionality is responsible for:
- correcting single bit fails upon a read operation on each NVM byte,
- verifying valid CPU usage,
- checking integrity loss when accessing NVM, ROM or RAM,
- providing a sign engine to check code and/or data integrity loss,
- monitoring various manifestations of fault injection attempts,
- providing a security timeout feature (watchdog timer),
- providing the SICESW with the traceability information of the TOE.

This functionality is responsible for reporting to TSF_ADMINIS_A all detected errors resulting from the above operations.

8.1.4 TSF_TEST_A: Test of the TOE

This functionality is responsible for restricting access of the TOE TEST functionality to the TEST process in TEST configuration.
In TEST configuration, this functionality ensures that the only allowed TOE user is an authorized TEST process.

In TEST configuration, this functionality ensures the test of TOE functionality with respect to the IC specification, including the TSF. This functionality is therefore responsible of the hardware functional integrity (CPU, RAM, ROM, NVM, Bus...).

In TEST configuration, this functionality provides commands to store data and/or pre-personalisation data and/or supplements of the Security IC Embedded Software (personalisation).

In USER configuration, this functionality ensures that the critical TOE TEST functionality is disabled.

**8.1.5 TSF_FWL_A: Memory Firewall**

In TEST and USER configurations, this security functionality monitors:
- access from memory locations to other locations for ROM, RAM and NVM,
- register access.

The TOE memories segmentation and protection can be dynamically defined, by the TOE user, thanks to the Memory Protection Unit (MPU), in order to implement various access control policies.

A default-TOE memories segmentation and protection is initially defined by ST.

In TEST and USER configurations, this security functionality relies on the MPU to ensure that only the Supervisor programs can change the TOE memories segmentation and protection in ROM, RAM and NVM.

This security functionality is responsible for the notification of violation attempts to TSF_ADMINIS_A.

**8.1.6 TSF_PHT_A: Physical tampering protection**

In TEST and USER configurations, this functionality ensures the following:
- the TOE detects clock and voltage supply operating changes by the environment,
- the TOE detects attempts to violate its physical integrity, and glitch attacks,
- the TOE is always clocked with shape and timing within specified operating conditions.

This functionality is responsible for the notification of physical tampering attempts and clock and voltage supply operating changes by the environment to TSF_ADMINIS_A.

**8.1.7 TSF_ADMINIS_A: Security violation administrator**

In TEST and USER configurations, this functionality ensures the management of security violations attempts.
The main security violations attempts which are managed are:

- incorrect CPU usage,
- integrity loss in NVM, ROM or RAM,
- code signature alarm,
- fault injection attempt,
- watchdog timeout.
- access attempt to unavailable or reserved memory areas,
- MPU errors,
- clock and voltage supply operating changes by the environment,
- TOE physical integrity abuse.

8.1.8 TSF_OBS_A: Unobservability

In USER configuration, this functionality addresses the Basic internal transfer protection (FDP_ITT.1), the Basic internal TSF data transfer protection (FPT_ITT.1) and the Subset information flow control (FDP_IFC.1) security functional requirements expressed in this document.

This functionality provides additional support mechanisms to the SICESW developer contributing to avoid information leakage.

8.1.9 TSF_SKCS_A: Symmetric Key Cryptography Support

In USER configuration, this functionality implements the following standard symmetric key cryptography algorithms:
- Data Encryption Standard (DES) with 64 bits long keys (56 effective bits).

This functionality supports the following standard modes of operation, both for encryption and for decryption:
- DES by itself (fast DES),
- Triple DES.

Each of these modes of operation can be chained in the standard Cipher Block Chaining mode (CBC).

8.1.10 TSF_ALEAS_A: Unpredictable Number Generation Support

In all configurations, this functionality provides 8-bit true random numbers.

In USER configuration, this functionality supports the mitigation of information leakage.

This functionality can be qualified with the test metrics required by the BSI-AIS31 standard for a P2 class device.

8.2 TOE summary specification rationale

This section shows that the TSF and assurance measures are suitable to meet the TOE security requirements.
8.2.1 TSF rationale

This section demonstrates that the combination of the specified TSF work together so as to satisfy the TOE security functional requirements.

Each of the security functional requirements is addressed by at least one or a combination of TSF services.

The complete rationale has been presented and evaluated in the SB23ZL48, ST23ZL48, SB23ZL34, ST23ZL34, SB23ZL18, ST23ZL18 Security Target.

For confidentiality reasons, this rationale is not fully reproduced here.

Table 11 below summarises which TOE security functional requirements (SFRs) are addressed by each TSF service (TSFs).

<table>
<thead>
<tr>
<th>SFRs</th>
<th>TSFs</th>
<th>TSF_INIT_A</th>
<th>TSF_INIT_B</th>
<th>TSF_INIT_C</th>
<th>TSF_TEST_A</th>
<th>TSF_TEST_B</th>
<th>TSF_CONF_A</th>
<th>TSF_CONF_B</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAU_SAS.1 (7.1.5)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRU_FLT.2 (7.1.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPT_FLS.1 (7.1.2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_LIM.1 (7.1.3)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMT_LIM.2 (7.1.4)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPT_PHP.3 (7.1.6)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_ITT.1 (7.1.7)</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FPT_ITT.1 (7.1.8)</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDP_IFC.1 (7.1.9)</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FCS_RNG.1 (7.1.10)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FDP_ACC.2 (7.1.14)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FDP_ACF.1 (7.1.15)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FMT_MSA.3 (7.1.12)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FMT_MSA.1 (7.1.13)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FCS_COP.1 (7.1.11)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
9 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>

Sx23ZLxx Security Target reference

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>SB23ZL48, ST23ZL48, SB23ZL34, ST23ZL34, SB23ZL18, ST23ZL18 Security Target</td>
<td>SMD_Sx23ZLxx_ST_09_001</td>
</tr>
</tbody>
</table>

Target of Evaluation referenced documents

For security reasons, all these documents are classified and their applicable revisions are referenced in the ST/SB23ZL48/34/18 Documentation Report.

<table>
<thead>
<tr>
<th>Component description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST/SB23ZL48/34/18 Documentation Report</td>
<td>SMD_STSBS23ZL48_DR_09_001</td>
</tr>
</tbody>
</table>

Standards references

<table>
<thead>
<tr>
<th>Ref</th>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref</td>
<td>Identifier</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>[20]</td>
<td>PKCS #1 V2.1</td>
<td>PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002</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
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 (SICESW)
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 (SICESW) 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 before 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>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<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>EAL</td>
<td>Evaluation Assurance Level.</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Code Book.</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>I/O</td>
<td>Input / Output.</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>MPU</td>
<td>Memory Protection Unit.</td>
</tr>
<tr>
<td>NESCRYPT</td>
<td>Next Step Cryptography Accelerator.</td>
</tr>
<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>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>Term</td>
<td>Meaning</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------------------------------------</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>SICESW</td>
<td>Security IC Embedded SoftWare.</td>
</tr>
<tr>
<td>SOIC</td>
<td>Small Outline IC.</td>
</tr>
<tr>
<td>ST</td>
<td>Context dependent : STMicroelectronics or Security Target.</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>
</tbody>
</table>
10 Revision history

Table 13. Document revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Nov-2009</td>
<td>01.00</td>
<td>Initial release.</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.

© 2009 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