STMicroelectronics

ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A Security Target - Public Version

Common Criteria for IT security evaluation

SMD_ST23ZRCxx_ST_11_001 Rev 01.01

May 2012

BLANK

1 Introduction

1.1 Security Target reference

1 Document identification: ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A SECURITY TARGET - PUBLIC VERSION.

2 Version number: Rev 01.01, issued May 2012.

3 Registration: registered at ST Microelectronics under number SMD_ST23ZRCxx_ST_11_001_V01.01.

1.2 Purpose

4 This document presents **the Security Target - Public version (ST)** of the **ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A,** 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 . . . 13

3.3.1 TOE development environment . . . 13

3.3.2 TOE production environment . . . 14

3.3.3 TOE operational environment . . . 14

4 **Conformance claims . . . 16**

4.1 Common Criteria conformance claims . . . 16

4.2 PP Claims . . . 16

4.2.1 PP Reference . . . 16

4.2.2 PP Refinements . . . 16

4.2.3 PP Additions . . . 16

4.2.4 PP Claims rationale . . . 16

5 **Security problem definition . . . 18**

5.1 Description of assets . . . 18

5.2 Threats . . . 19

5.3 Organisational security policies . . . 20

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 Organisational security policy "Additional Specific Security Functionality" 23

7 Security requirements 24

7.1 Security functional requirements for the TOE 24

7.1.1 Limited fault tolerance (FRU_FLT.2) 25

7.1.2 Failure with preservation of secure state (FPT_FLS.1) 25

7.1.3 Limited capabilities (FMT_LIM.1) 25

7.1.4 Limited availability (FMT_LIM.2) 26

7.1.5 Audit storage (FAU_SAS.1) 26

7.1.6 Resistance to physical attack (FPT_PHP.3) 26

7.1.7 Basic internal transfer protection (FDP_ITT.1) 26

7.1.8 Basic internal TSF data transfer protection (FPT_ITT.1) 26

7.1.9 Subset information flow control (FDP_IFC.1) 26

7.1.10 Random number generation (FCS_RNG.1) 27

7.1.11 Cryptographic operation (FCS_COP.1) 27

7.2 TOE security assurance requirements 27

7.3 Refinement of the security assurance requirements 28

7.3.1 Refinement regarding functional specification (ADV_FSP) 29

7.3.2 Refinement regarding test coverage (ATE_COV) 30

7.4 Security Requirements rationale 30

7.4.1 Rationale for the Security Functional Requirements 30

7.4.2 Additional security objectives are suitably addressed 31

7.4.3 Additional security requirements are consistent 31

7.4.4 Dependencies of Security Functional Requirements 31

7.4.5 Rationale for the Assurance Requirements 32

8 TOE summary specification 34

8.1 Limited fault tolerance (FRU_FLT.2) 34

8.2 Failure with preservation of secure state (FPT_FLS.1) 34

8.3 Limited capabilities (FMT_LIM.1) 34

8.4 Limited availability (FMT_LIM.2) 34

8.5 Audit storage (FAU_SAS.1) 35

8.6 Resistance to physical attack (FPT_PHP.3) 35

8.7 Basic internal transfer protection (FDP_ITT.1), Basic internal TSF data transfer protection (FPT_ITT.1) & Subset information flow control (FDP_IFC.1) 35

8.8 Random number generation (FCS_RNG.1) 35
8.9 Cryptographic operation: DES / 3DES operation (FCS_COP.1 [EDES]) . 35
8.10 Cryptographic operation: AES operation (FCS_COP.1 [AES]) 36

9 References 37

Appendix A Glossary 39
A.1 Terms 39
A.2 Abbreviations. 41

10 Revision history 43

List of tables

Table 1. Master product and derivatives common characteristics . . . 10
Table 2. Master product and derivatives specific characteristics . . . 10
Table 3. Composite product life cycle phases . . . 12
Table 4. Summary of security environment . . . 19
Table 5. Summary of security objectives . . . 21
Table 6. Security Objectives versus Assumptions, Threats or Policies . . . 23
Table 7. Summary of functional security requirements for the TOE . . . 24
Table 8. FCS_COP.1 iterations (cryptographic operations) . . . 27
Table 9. TOE security assurance requirements . . . 28
Table 10. Impact of EAL5 selection on *BSI-PP-0035* refinements . . . 29
Table 11. Dependencies of security functional requirements . . . 31
Table 12. List of abbreviations . . . 41
Table 13. Document revision history . . . 43

List of figures

Figure 1. ST23ZRCxx block diagram 12

2 Context

8 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).

9 The Target of Evaluation (TOE) is the ST23ZR08A with 5 commercial derivatives: ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, and ST23ZC02A.

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

11 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.

12 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 augmentation***:

- Addition #1: “Support of Cipher Schemes” from *AUG*.

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

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

14 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*, and ***AUG1*** for Addition #1 of *AUG*.

3 TOE description

3.1 TOE overview

15 The Target of Evaluation (TOE) comprises the ST23ZR08A with 5 commercial derivatives: the ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, and ST23ZC02A.

The master product is the ST23ZR08A. All based on the same hardware design, the different derivatives are configured during the manufacturing or packaging process, in conformance with the customer's order.

16 All products of the TOE share the same hardware design, and the same maskset, thus mainly share the same characteristics:

Table 1. Master product and derivatives common characteristics

Maskset	Commercial version	Product version	OST name	OST revision
K340A	A	H	YBC	61h

17 The different derivatives differ from the master product, only on the available NVM memory size, and on the available I/O modes, as detailed here below:

Table 2. Master product and derivatives specific characteristics

Commercial name	Product ID	NVM size	I/O modes
ST23ZR08	0015h	8 KBytes	Dual mode (RF + contact)
ST23ZR04	0020h	4 KBytes	Dual mode (RF + contact)
ST23ZR02	0021h	2 KBytes	Dual mode (RF + contact)
ST23ZC08	0022h	8 KBytes	Contactless only
ST23ZC04	0023h	4 KBytes	Contactless only
ST23ZC02	0024h	2 KBytes	Contactless only

18 The master product and the different derivatives can be distinguished thanks to the product identification number, included in the traceability number, as detailed in *Table 2: Master product and derivatives specific characteristics*.

19 In this Security Target, the terms:

- "TOE" or "ST23ZRCxx" mean all products listed in *Table 2: Master product and derivatives specific characteristics*,
- "ST23ZRxx" means the subset of products ST23ZR08 / ST23ZR04 / ST23ZR02,
- "ST23ZCxx" means the subset of products ST23ZC08 / ST23ZC04 / ST23ZC02.

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

21 The ST23ZRxx is a dual contact/contactless Secure IC with 8, 4 or 2 Kbytes EEPROM (see *Table 2.*), enhanced security and optimized RF performance.

22 The ST23ZCxx is a contactless Secure IC with 8, 4 or 2 Kbytes EEPROM (see *Table 2.*), enhanced security and optimized RF performance.

23 The TOE is a serial access IC based on a 8/16-bit CPU core. 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 28 MHz). The CPU interfaces with the on-chip RAM, ROM and EEPROM memories via a 24-bit internal bus offering 16 MBytes of linear addressing space.

24 An RF interface including an RF Universal Asynchronous Receiver Transmitter (RF UART) enables contactless communication up to 848 Kbits/s compatible with the ISO/IEC 14443 Type A, B and B', and Paypass™ standards.

25 The CPU includes the Arithmetic Logic Unit (ALU) and the control logic.

26 The 3-key Triple DES accelerator (EDES+) enablesCipher Block Chaining (CBC) *[8]*, fast DES and triple DES computation *[2]*. This module provides an enhanced protection against side channel attacks (DPA and DEMA).

27 The device includes an AES (Advanced Encryption Standard) accelerator supporting AES-128, AES-192 and AES-256 ciphers (*[5]*). The AES accelerator can operate in ECB (Electronic Code Book) and CBC (Cipher Block Chaining) modes.

28 As randomness is a key stone in many applications, the ST23ZRCxx features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS-31 *[1]* and directly accessible through dedicated registers.

29 In a few words, the ST23ZRCxx 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,
- AIS-31 class P2 compliant True Random Number Generator,
- ISO 3309 CRC calculation block,
- EDES+ accelerator,
- AES accelerator.

30 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.

31 In addition, the ROM of the tested samples contains an operating system called "Card Manager" that allows the evaluators to use a set of commands with the I/O, and to load in EEPROM (or in RAM) test software. The card manager is not part of the TOE, and not in the scope of this evaluation.

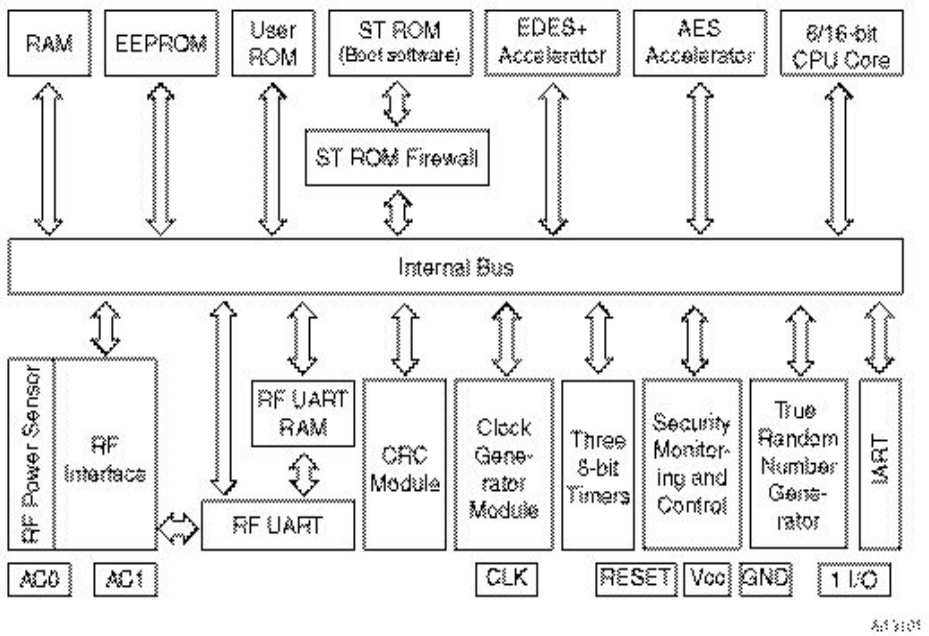
32 The user guidance documentation, part of the TOE, consists of:

- The product Data Sheet,
- The product family Security Guidance,
- The AIS31 user manuals,
- The product family programming manual.

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

33 *Figure 1* provides an overview of the ST23ZRCxx.

Figure 1. ST23ZRCxx block diagram



34 The IART interface is not operational in the ST23ZCxx.

3.2 TOE life cycle

35 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.

36 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.

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

38 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.

Table 3. Composite product life cycle phases

Phase	Name	Description	Responsible party
1	IC embedded software development	Security IC embedded software development	IC embedded software developer
2	IC development	IC design IC dedicated software development	IC developer: **ST**

Table 3. Composite product life cycle phases (continued)

Phase	Name	Description	Responsible party
3	IC manufacturing	integration and photomask fabrication IC production IC testing preparation pre-personalisation	IC manufacturer: **ST**
4	IC packaging	security IC packaging (and testing) pre-personalisation if necessary	IC packaging manufacturer: **ST** or **NEDCARD** or **SMARTFLEX**
5	Composite product integration	composite product finishing process composite product preparation composite product shipping	Composite product integrator
6	Personalisation	composite product personalisation composite product testing	Personaliser
7	Operational usage	composite product usage by its issuers and consumers	End-consumer

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

40 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.

41 The TOE is only delivered in USER configuration.

3.3 TOE environment

42 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.

3.3.1 TOE development environment

43 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.

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

45 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).

46 The development centres involved in the development of the TOE are the following: **ST ROUSSET (FRANCE)** and **ST ANG MO KIO (SINGAPORE)**, for the design activities, **ST ROUSSET (FRANCE)**, for the engineering activities, **ST ROUSSET (FRANCE)** for the software development activities.

47 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).

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

3.3.2 TOE production environment

49 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.

50 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.

51 The authorized front-end plant involved in the manufacturing of the TOE is **ST ROUSSET (FRANCE)**.

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

53 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.

54 When the product is delivered after phase 4, the authorized back-end plant involved in the packaging of the TOE can be **ST BOUSKOURA (MOROCCO)** or **NEDCARD (THE NETHERLANDS)** or **SMARTFLEX (SINGAPORE)**.

55 The other sites that can be involved during the production of the TOE are **ST LOYANG (SINGAPORE)** for the logistics, and **ST SHENZEN (CHINA)** or **DISCO (GERMANY)** for the wafers backlap and sawing.

3.3.3 TOE operational environment

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

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

58 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, brand protection, 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

59 The ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A Security Target claims to be conformant to the Common Criteria version 3.1.

60 Furthermore it claims to be CC Part 2 (*CCMB-2009-07-002*) extended and CC Part 3 (*CCMB-2009-07-003*) conformant. The extended Security Functional Requirements are those defined in the *Security IC Platform Protection Profile* (*BSI-PP-0035*).

61 The assurance level for this Security Target is ***EAL 5*** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

62 This 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

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

- Addition #1: “Support of Cipher Schemes” from *AUG*,
- Refinement of assurance requirements.

64 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

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

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

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

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

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

4.2.4 PP Claims rationale

70 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.

71 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*.

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

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

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

75 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

76 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.

77 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.

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

5.1 Description of assets

79 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.

80 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.

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

SC4 deficiency of random numbers.

82 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.

83 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***.

Table 4. Summary of security environment

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
OSPs	BSI.P.Process-TOE	Protection during TOE Development and Production
	AUG1.P.Add-Functions	Additional Specific Security Functionality (Cipher Scheme Support)
Assumptions	BSI.A.Process-Sec-IC	Protection during Packaging, Finishing and Personalisation
	BSI.A.Plat-Appl	Usage of Hardware Platform
	BSI.A.Resp-Appl	Treatment of User Data

5.2 Threats

84 The threats are described in the *BSI-PP-0035*, section 3.2.

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

5.3 Organisational security policies

85 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.

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

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

88 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), – Advanced Encryption Standard (AES). 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

89 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

90 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.

91 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.

92 Most of these security aspects can therefore be easily found in the protection profile. Only the one originating in *AUG* is detailed in the following sections.

Table 5. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	AUG1.O.Add-Functions	Additional Specific Security Functionality
Environments	BSI.OE.Plat-Appl	Usage of Hardware Platform
	BSI.OE.Resp-Appl	Treatment of User Data
	BSI.OE.Process-Sec-IC	Protection during composite product manufacturing

6.1 Security objectives for the TOE

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

BSI.O.RND	Random Numbers
AUG1.O.Add-Functions	Additional Specific Security Functionality: The TOE must provide the following specific security functionality to the ***Security IC*** Embedded Software: – Data Encryption Standard (DES), – Triple Data Encryption Standard (3DES), – Advanced Encryption Standard (AES).

6.2 Security objectives for the environment

93 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

94 Security Objectives for the operational Environment (TOE delivery up to end of phase 6):

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

6.3 Security objectives rationale

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

96 Thus, it is necessary to show that:

- the security objective from *AUG* is suitable (i.e. it addresses security environment aspects),
- the security objective from *AUG* is consistent with the other security objectives stated in this chapter (i.e. no contradiction).

97 The selected augmentation from *AUG* introduces the following security environment aspect:

- organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add-Functions*)".

98 As required by CC Part 1 (*CCMB-2009-07-001*), 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.

99 The justification of the additional policy, provided in the next subsection shows that it does not contradict to the rationale already given in the protection profile *BSI-PP-0035* for the assumptions, policy and threats defined there.

Table 6. Security Objectives versus Assumptions, Threats or Policies

Assumption, Threat or Organisational Security Policy	Security Objective	Notes
BSI.A.Plat-Appl	*BSI.OE.Plat-Appl*	Phase 1
BSI.A.Resp-Appl	*BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3 optional Phase 4
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 5-6 optional Phase 4
BSI.T.Leak-Inherent	*BSI.O.Leak-Inherent*	
BSI.T.Phys-Probing	*BSI.O.Phys-Probing*	
BSI.T.Malfunction	*BSI.O.Malfunction*	
BSI.T.Phys-Manipulation	*BSI.O.Phys-Manipulation*	
BSI.T.Leak-Forced	*BSI.O.Leak-Forced*	
BSI.T.Abuse-Func	*BSI.O.Abuse-Func*	
BSI.T.RND	*BSI.O.RND*	
AUG1.P.Add-Functions	*AUG1.O.Add-Functions*	

6.3.1 Organisational security policy "Additional Specific Security Functionality"

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

101 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.

102 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*.

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

7 Security requirements

104 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

105 Security Functional Requirements (SFRs) from the "*BSI-PP-0035*" Protection Profile (PP) are drawn from *CCMB-2009-07-002*, except the following SFRs, that are **extensions** to *CCMB-2009-07-002*:

- **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.

106 All extensions to the SFRs of the "*BSI-PP-0035*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2009-07-002*.

107 All iterations, assignments, selections, or refinements on SFRs have been performed according to section C.4 of *CCMB-2009-07-001*. 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.

108 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.

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

Table 7. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-PP-0035*	*CCMB-2009-07-002*
FPT_FLS.1	Failure with preservation of secure state			
FMT_LIM.1	Limited capabilities	Abuse of functionality	*BSI-PP-0035*	Extended
FMT_LIM.2	Limited availability			
FAU_SAS.1	Audit storage	Lack of TOE identification	*BSI-PP-0035* Operated	

Table 7. Summary of functional security requirements for the TOE (continued)

Label	Title	Addressing	Origin	Type
FPT_PHP.3	Resistance to physical attack	Physical manipulation & probing	*BSI-PP-0035*	*CCMB-2009-07-002*
FDP_ITT.1	Basic internal transfer protection	Leakage		
FPT_ITT.1	Basic internal TSF data transfer protection			
FDP_IFC.1	Subset information flow control			
FCS_RNG.1	Random number generation	Weak cryptographic quality of random numbers	*BSI-PP-0035* Operated	Extended
FCS_COP.1	Cryptographic operation	Cipher scheme support	*AUG* #1 Operated	*CCMB-2009-07-002*

7.1.1 Limited fault tolerance (FRU_FLT.2)

110 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)

111 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.***

112 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)

113 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)

114 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.

115 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)

116 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)

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

118 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)

119 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)

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

121 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)

122 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***.

123 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)

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

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

7.1.11 Cryptographic operation (FCS_COP.1)

126 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*.

Table 8. FCS_COP.1 iterations (cryptographic operations)

Iteration label	[assignment: list of cryptographic operations]	[assignment: cryptographic algorithm]	[assignment: cryptographic key sizes]	[assignment: list of standards]
DES / 3DES operation	encryption decryption in Cipher Block Chaining (CBC) mode	Data Encryption Standard (DES)	56 bits	*FIPS PUB 46-3* *ISO/IEC 9797-1* *ISO/IEC 10116*
		Triple Data Encryption Standard (3DES)	112 bits	
AES operation	encryption (cipher) decryption (inverse cipher) - in Electronic Code Book (ECB) mode - in Cipher Block Chaining (CBC) mode	Advanced Encryption Standard	128, 192, and 256 bits	*FIPS PUB 197*

7.2 TOE security assurance requirements

127 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.

128 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.

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

Table 9. TOE security assurance requirements

Label	Title	Origin
ADV_ARC.1	Security architecture description	EAL5/*BSI-PP-0035*
ADV_FSP.5	Complete semi-formal functional specification with additional error information	EAL5
ADV_IMP.1	Implementation representation of the TSF	EAL5/*BSI-PP-0035*
ADV_INT.2	Well-stuctured internals	EAL5
ADV_TDS.4	Semiformal modular design	EAL5
AGD_OPE.1	Operational user guidance	EAL5/*BSI-PP-0035*
AGD_PRE.1	Preparative procedures	EAL5/*BSI-PP-0035*
ALC_CMC.4	Production support, acceptance procedures and automation	EAL5/*BSI-PP-0035*
ALC_CMS.5	Development tools CM coverage	EAL5
ALC_DEL.1	Delivery procedures	EAL5/*BSI-PP-0035*
ALC_DVS.2	Sufficiency of security measures	*BSI-PP-0035*
ALC_LCD.1	Developer defined life-cycle model	EAL5/*BSI-PP-0035*
ALC_TAT.2	Compliance with implementation standards	EAL5
ATE_COV.2	Analysis of coverage	EAL5/*BSI-PP-0035*
ATE_DPT.3	Testing: modular design	EAL5
ATE_FUN.1	Functional testing	EAL5/*BSI-PP-0035*
ATE_IND.2	Independent testing - sample	EAL5/*BSI-PP-0035*
AVA_VAN.5	Advanced methodical vulnerability analysis	*BSI-PP-0035*

7.3 Refinement of the security assurance requirements

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

131 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.

132 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.

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

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

Table 10. Impact of EAL5 selection on *BSI-PP-0035* refinements

Assurance Family	*BSI-PP-0035* Level	ST Level	Impact on refinement
ADO_DEL	1	1	None
ALC_DVS	2	2	None
ALC_CMS	4	5	None, refinement is still valid
ALC_CMC	4	4	None
ADV_ARC	1	1	None
ADV_FSP	4	5	Presentation style changes, IC Dedicated Software is included
ADV_IMP	1	1	None
ATE_COV	2	2	IC Dedicated Software is included
AGD_OPE	1	1	None
AGD_PRE	1	1	None
AVA_VAN	5	5	None

7.3.1 Refinement regarding functional specification (ADV_FSP)

135 ~~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.***

136 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.

137 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.

138 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.

139 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.

140 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)

141 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).

142 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).

143 ~~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

144 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.

145 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 7* and *Table 9*, it can be verified that the justifications provided by the *BSI-PP-0035* protection profile and *AUG* can just be carried forward to their union.

146 From *Table 5*, it is straightforward to identify an additional security objective for the TOE (*AUG1.O.Add-Functions*), tracing back to *AUG*. This rationale must show that security requirements suitably address it too.

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

- there are additional security requirements introduced by this Security Target (various assurance requirements of EAL5),
- there is a security requirement introduced from *AUG* (*FCS_COP.1*).

148 Though it remains to show that:

- the security objective from *AUG* is 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.

149 The justification that the additional security objective is 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 “Additional Specific Security Functionality (*AUG1.O.Add-Functions*)”

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

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

7.4.3 Additional security requirements are consistent

"Cryptographic operation (*FCS_COP.1*)"

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

7.4.4 Dependencies of Security Functional Requirements

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

- those justified in the *BSI-PP-0035* protection profile security requirements rationale,
- those justifed in *AUG* security requirements rationale (except on FMT_MSA.2, see discussion below).

154 Details are provided in *Table 11* below.

Table 11. Dependencies of security functional requirements

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FRU_FLT.2	FPT_FLS.1	Yes	Yes, *BSI-PP-0035*
FPT_FLS.1	None	No dependency	Yes, *BSI-PP-0035*
FMT_LIM.1	FMT_LIM.2	Yes	Yes, *BSI-PP-0035*
FMT_LIM.2	FMT_LIM.1	Yes	Yes, *BSI-PP-0035*

Table 11. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FAU_SAS.1	None	No dependency	Yes, *BSI-PP-0035*
FPT_PHP.3	None	No dependency	Yes, *BSI-PP-0035*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, *BSI-PP-0035*
FPT_ITT.1	None	No dependency	Yes, *BSI-PP-0035*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-PP-0035*	Yes, *BSI-PP-0035*
FCS_RNG.1	None	No dependency	Yes, *BSI-PP-0035*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, see discussion below	Yes, *AUG* ***#1*** (adapted to CC V3.1 R2, see discussion below)
	FCS_CKM.4	No, see discussion below	

155 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, there is no specific function for the generation or import of the keys. The ES has all possibilities to implement its own creation function, in conformance with its security policy.

156 Part 2 of the Common Criteria defines the dependency of "*Cryptographic operation (FCS_COP.1)*" on "Cryptographic key destruction (FCS_CKM.4)". In this particular TOE, there is no specific function for the destruction of the keys. The ES has all possibilities to implement its own destruction function, in conformance with its security policy.

157 *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 9*)

158 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.

159 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.

160 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.

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

Dependencies of assurance requirements

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

163 Augmentation to this package are identified in paragraph *127* and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

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

165 The complete TOE summary specification has been presented in the *ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A Security Target*.

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

8.1 Limited fault tolerance (FRU_FLT.2)

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

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

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

- Die integrity violation detection,
- Errors on memories,
- Bus integrity error,
- Glitches,
- High voltage supply,
- CPU error,
- Clock tree error,
- etc..

169 The SICESW can generate a software reset.

8.3 Limited capabilities (FMT_LIM.1)

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

8.4 Limited availability (FMT_LIM.2)

171 The TOE is either in TEST or in USER configuration.

172 The only authorised TOE configuration modification is:

- TEST to USER configuration.

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

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

8.5 Audit storage (FAU_SAS.1)

175 The TOE provides commands to store data and/or pre-personalisation data and/or supplements of the SICESW in the NVM. These commands are only available to authorised processes, and only until end of phase 4.

8.6 Resistance to physical attack (FPT_PHP.3)

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

- The TOE implements counter-measures that reduce the exploitability of physical probing.
- The TOE is physically protected by an active shield that commands an automatic reaction on die integrity violation detection.

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

177 The TSF prevents the disclosure of internal and user data thanks to the following features:

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

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

8.8 Random number generation (FCS_RNG.1)

179 The TSF provides 8-bit true random numbers that can be qualified with the test metrics required by the *BSI-AIS31* standard for a P2 class device.

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

180 The TOE provides an EDES+ accelerator that has the capability to perform the following standard DES cryptographic operations, conformant to *FIPS PUB 46-3*, with intrinsic counter-measures against fault attacks (FA), DEMA and DPA attacks:

- DES encryption,
- DES decryption,
- Triple DES encryption,
- Triple DES decryption.

181 The EDES+ accelerator offers a Cipher Block Chaining (CBC) mode conformant to *ISO/IEC 10116*.

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

182 The TOE provides an AES accelerator that has the capability to perform 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 fault attacks (FA), SPA, DEMA and DPA attacks:

- randomize,
- encryption,
- decryption,
- decryption key derivation.

183 The AES accelerator offers a Electronic Code Book (ECB) and a Cipher Block Chaining (CBC) mode conformant to *ISO/IEC 10116*.

9 References

184 Protection Profile reference

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

185 Security Target references

Component description	Reference
ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A Security Target	SMD_ST23Zxxx_ST_10_001

186 Guidance documentation references

Component description	Reference	Revision
ST23ZRxx/ST23ZCxx Secure microcontroller with enhanced security - Datasheet	DS_23ZR08	2.0
Application note - ST23ZRxx/ST23ZCxx Security guidance	AN_23ZRxx_SECU	2.0
ST23 AIS31 compliant random number user manual	UM_23_AIS31	2
ST23 AIS31 Reference implementation - Startup, online and total failure tests - User manual	AN_23_AIS31	2
ST21/23 programming manual	PM_21_23	3
ST23ZRxx/ST23ZCxx recommendations for contactless operations	AN_23Zx_RF_RCMD	1.0
How to identify certified HW devices using additional ST traceability information	AN_TRACE	1

187 Standards references

Ref	Identifier	Description
[1]	BSI-AIS31	A proposal for Functionality classes and evaluation methodology for true (physical) random number generators, W. Killmann & W. Schindler BSI, Version 3.1, 25-09-2001
[2]	FIPS PUB 46-3	FIPS PUB 46-3, Data encryption standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, 1999
[3]	FIPS PUB 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, U.S. Department of Commerce, 1999
[4]	FIPS PUB 186	FIPS PUB 186 Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S.A., 1994

Ref	Identifier	Description
[5]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[6]	ISO/IEC 9796-2	ISO/IEC 9796, Information technology - Security techniques - Digital signature scheme giving message recovery - Part 2: Integer factorization based mechanisms, ISO, 2002
[7]	ISO/IEC 9797-1	ISO/IEC 9797, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, ISO, 1999
[8]	ISO/IEC 10116	ISO/IEC 10116, Information technology - Security techniques - Modes of operation of an n-bit block cipher algorithm, ISO, 1997
[9]	ISO/IEC 14888	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[10]	CCMB-2009-07-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009, version 3.1 Revision 3
[11]	CCMB-2009-07-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009, version 3.1 Revision 3
[12]	CCMB-2009-07-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, version 3.1 Revision 3
[13]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[14]	MIT/LCS/TR-212	On digital signatures and public key cryptosystems, Rivest, Shamir & Adleman Technical report MIT/LCS/TR-212, MIT Laboratory for computer sciences, January 1979
[15]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[16]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[17]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[18]	MOV 97	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997

Appendix A Glossary

A.1 Terms

Authorised user

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

Composite product

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

End-consumer

User of the Composite Product in Phase 7.

Integrated Circuit (IC)

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

IC Dedicated Software

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

IC Dedicated Test Software

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

IC developer

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

IC manufacturer

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

IC packaging manufacturer

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

Initialisation data

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

Object

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

Packaged IC

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

Pre-personalization data

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

Secret

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

Security IC

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

Security IC Embedded SoftWare (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.

Secure Microcontroller

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 either (i) after Phase 3 (or before Phase 4) if the TOE is delivered in form of wafers or sawn wafers (dice) or (ii) after Phase 4 (or before Phase 5) if the TOE is delivered in form of packaged products.

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 12. List of abbreviations

Term	Meaning
AIS	Application notes and Interpretation of the Scheme (BSI)
ALU	Arithmetical and Logical Unit.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
CBC	Cipher Block Chaining.
CC	Common Criteria Version 3.1.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Check.
DEMA	Differential Electromagnetic Analysis.
DES	Data Encryption Standard.
DIP	Dual-In-Line Package.
DPA	Differential Power Analysis.
EAL	Evaluation Assurance Level.
ECB	Electronic Code Book.
EDES	Enhanced DES.
EEPROM	Electrically Erasable Programmable Read Only Memory.
FIPS	Federal Information Processing Standard.
I/O	Input / Output.
IART	ISO-7816 Asynchronous Receiver Transmitter.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
NIST	National Institute of Standards and Technology.
NVM	Non Volatile Memory.
OSP	Organisational Security Policy.
OST	Operating System for Test.
PP	Protection Profile.
PUB	Publication Series.
RAM	Random Access Memory.
RF	Radio Frequency.
RF UART	Radio Frequency Universal Asynchronous Receiver Transmitter.
ROM	Read Only Memory.
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.

Table 12. List of abbreviations (continued)

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

10 Revision history

Table 13. Document revision history

Date	Revision	Changes
08-Nov-2011	01.00	Initial release.
10-May-2012	01.01	Update of Guidance documents revisions.