STMicroelectronics

ST23YR80A Security Target - Public Version

Common Criteria for IT security evaluation

SMD_ST23YR80_ST_09_001 Rev 01.00

February 2009

BLANK

ST23YR80A
Security Target - Public Version

Common Criteria for IT security evaluation

1 Introduction

1.1 Security Target reference

1 Document identification: ST23YR80A SECURITY TARGET - PUBLIC VERSION.

2 Version number: Rev 01.00, issued February 2009.

3 Registration: registered at ST Microelectronics under number SMD_ST23YR80_ST_09_001_V01.00.

1.2 Purpose

4 This document presents **the Security Target - Public version (ST)** of the **ST23YR80A,** a Security Integrated Circuits (ICs), with its 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: ST23YR80A TOE description*.

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

Contents

List of tables

List of figures

2 Context

8 The Target of Evaluation (TOE) referred to in *Section 3: ST23YR80A TOE description*, is evaluated under the French IT Security Evaluation and Certification Scheme and is developed by the Smartcard Division of STMicroelectronics (ST).

9 The Target of Evaluation (TOE) is the ST23YR80A.

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 ST23YR80A 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 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.

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*, ***AUG1*** for Addition #1 of *AUG* and ***AUG4*** for Addition #4 of *AUG*.

3 ST23YR80A TOE description

3.1 TOE overview

15 The Target of Evaluation (TOE) is the ST23YR80A. This product is a dual contact/contactless Smartcard IC based on the 8/16-bit ST23 CPU core, with 80 Kbytes EEPROM, an internally generated clock, an MPU, an internal True Random Number Generator (TRNG) and accelerators dedicated to cryptographic algorithms.

16 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 interfaces with the on-chip RAM, ROM and EEPROM memories via an internal bus offering 16 MBytes of linear addressing space, protected by the memory protection unit (MPU) without performance loss.

17 An RF interface including an RF Universal Asynchronous Receiver Transmitter (RF UART) enables contactless communication up to 848 Kbits/s compatible with the ISO 14443-B standard.

18 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 coutermeasures 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 ST23YR80A features a highly reliable True Random Number Generator (TRNG), compliant with P2 Class of AIS-31 *[1]* and directly accessible through dedicated registers.

19 In a few words, the ST23YR80A offers a unique combination of high performances and very powerful features for high level security:

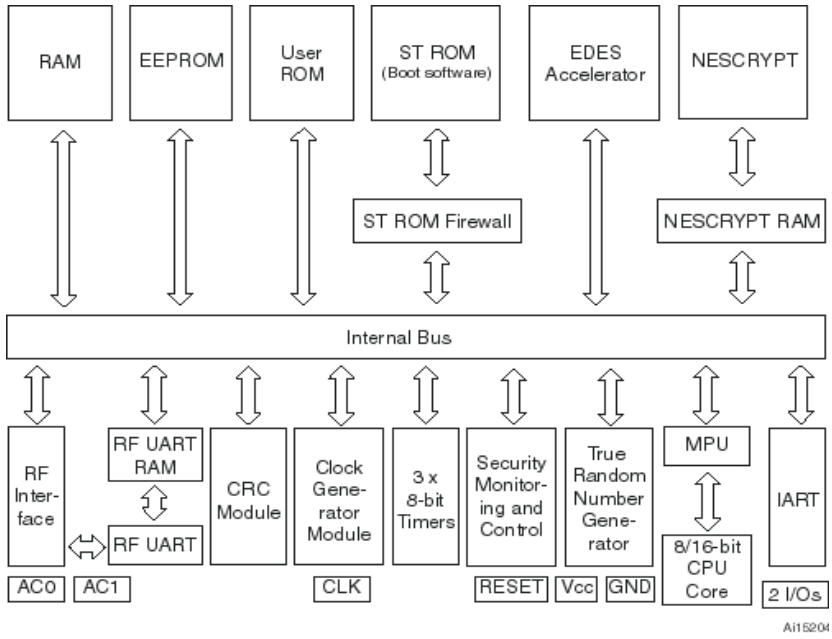
- Die integrity,
- Monitoring of environmental parameters,
- Protection mechanisms against faults,
- Hardware Security Enhanced DES accelerator,
- AIS-31 class P2 compliant True Random Number Generator,
- ISO 3309 CRC calculation block,
- Memory Protection Unit,
- Next Step Cryptography accelerator (NESCRYPT).

20 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.

21 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.

22 *Figure 1* provides an overview of the ST23YR80A.

Figure 1. ST23YR80A block diagram



3.2 TOE life cycle

23 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.

24 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.

25 The life cycle phases are summarized in *Table 1*.

26 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.

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

28 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 1. 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**
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
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

3.3 TOE environment

29 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

30 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.

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

32 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, diskettes, 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).

33 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.

34 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).

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

3.3.2 TOE production environment

36 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.

37 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.

38 The authorized front-end plant involved in the manufacturing of the TOE is **ST ROUSSET**.

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

3.3.3 TOE operational environment

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

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

42 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

43 The ST23YR80A Security Target claims to be conformant to the Common Criteria version 3.1.

44 Furthermore it claims to be CC Part2 (*CCMB-2007-09-002*) extended and CC Part 3 (*CCMB-2007-09-003*) conformant. The extended Security Functional Requirements are those defined in the *Security IC Platform Protection Profile* (*BSI-PP-0035*).

45 The assurance level for the ST23YR80A Security Target is ***EAL 5*** augmented by ALC_DVS.2 and AVA_VAN.5.

4.2 PP Claims

4.2.1 PP Reference

46 The ST23YR80A 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

47 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.

48 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

49 The security environment additions relative to the PP are summarized in *Table 2*.

50 The additional security objectives relative to the PP are summarized in *Table 3*.

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

52 The additional SFRs for the TOE relative to the PP are summarized in *Table 5*.

53 The additional SARs relative to the PP are summarized in *Table 7*.

4.2.4 PP Claims rationale

54 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.

55 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*.

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

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

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

59 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

60 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.

61 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.

62 A summary of all these security aspects and their respective conditions is provided in *Table 2*.

5.1 Description of assets

63 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.

64 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.

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

SC4 deficiency of random numbers.

66 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.

67 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 2. Summary of security environment

	Label	Title
TOE threats	BSI.T.Leak-Inherent	Inherent Information Leakage
	BSI.T.Phys-Probing	Physical Probing
	BSI.T.Malfunction	Malfunction due to Environmental Stress
	BSI.T.Phys-Manipulation	Physical Manipulation
	BSI.T.Leak-Forced	Forced Information Leakage
	BSI.T.Abuse-Func	Abuse of Functionality
	BSI.T.RND	Deficiency of Random Numbers
	AUG4.T.Mem-Access	Memory Access Violation
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
	AUG1.A.Key-Function	Usage of key-dependent functions

5.2 Threats

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

BSI.T.Leak-Inherent Inherent Information Leakage

BSI.T.Phys-Probing Physical Probing

BSI.T.Malfunction Malfunction due to Environmental Stress

BSI.T.Phys-Manipulation Physical Manipulation

BSI.T.Leak-Forced Forced Information Leakage

BSI.T.Abuse-Func	Abuse of Functionality
BSI.T.RND	Deficiency of Random Numbers
AUG4.T.Mem-Access	Memory Access Violation: Parts of the ***Security IC*** Embedded Software may cause security violations by accidentally or deliberately accessing restricted data (which may include code). Any restrictions are defined by the security policy of the specific application context and must be implemented by the ***Security IC*** Embedded Software. Clarification: This threat does not address the proper definition and management of the security rules implemented by the Security IC Embedded Software, this being a software design and correctness issue. This threat addresses the reliability of the abstract machine targeted by the software implementation. To avert the threat, the set of access rules provided by this TOE should be undefeated if operated according to the provided guidance. The threat is not realized if the Security IC Embedded Software is designed or implemented to grant access to restricted information. It is realized if an implemented access denial is granted under unexpected conditions or if the execution machinery does not effectively control a controlled access. Here the attacker is expected to (i) take advantage of flaws in the design and/or the implementation of the TOE memory access rules (refer to BSI.T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to BSI.T.Malfunction) and/or by physical manipulation (refer to BSI.T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

5.3 Organisational security policies

69 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.

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

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

72 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, see *AUG1.A.Key-Function*.

5.4 Assumptions

73 The assumptions are described in the *BSI-PP-0035*, section 3.4. Only those originating in *AUG* are detailed in this document.

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
AUG1.A.Key-Function	Usage of key-dependent functions: Key-dependent functions, if any, shall be implemented in the ***Security IC*** Embedded Software in a way that they are not susceptible to leakage attacks (as described under *BSI.T.Leak-Inherent* and *BSI.T.Leak-Forced*). Note that here the routines that may compromise keys when being executed are part of the ***Security IC*** Embedded Software. In contrast to this, the threats *BSI.T.Leak-Inherent* and *BSI.T.Leak-Forced* address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

6 Security objectives

74 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.

75 A summary of all security objectives is provided in *Table 3*. Note that the origin of each objective is clearly identified in the prefix of its label.

76 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 3. Summary of security objectives

	Label	Title
TOE	BSI.O.Leak-Inherent	Protection against Inherent Information Leakage
	BSI.O.Phys-Probing	Protection against Physical Probing
	BSI.O.Malfunction	Protection against Malfunctions
	BSI.O.Phys-Manipulation	Protection against Physical Manipulation
	BSI.O.Leak-Forced	Protection against Forced Information Leakage
	BSI.O.Abuse-Func	Protection against Abuse of Functionality
	BSI.O.Identification	TOE Identification
	BSI.O.RND	Random Numbers
	AUG1.O.Add-Functions	Additional Specific Security Functionality
	AUG4.O.Mem Access	***Dynamic*** Area based Memory Access Control
Environments	BSI.OE.Plat-Appl	Usage of Hardware Platform ***with AUG1.Clarification & AUG4.Clarification***
	BSI.OE.Resp-Appl	Treatment of User Data ***with AUG1.Clarification & AUG4.Clarification***
	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).
AUG4.O.Mem Access	***Dynamic*** Area based Memory Access Control: The TOE must provide the ***Security IC*** Embedded Software with the capability to define ***dynamic memory segmentation and protection***. The TOE must then enforce ***the defined access rules*** so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

6.2 Security objectives for the environment

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

BSI.OE.Plat-Appl	Usage of Hardware Platform: To ensure that the TOE is used in a secure manner the Security IC Embedded Software shall be designed so that the requirements from the following documents are met: – (i) hardware data sheet for the TOE, – (ii) data sheet of the IC Dedicated Software of the TOE, – (iii) TOE application notes, other guidance documents, and – (iii) findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report. **AUG1.Clarification:** When the TOE supports cipher schemes as additional specific security functionality and if required, the ***Security IC*** Embedded Software shall use these cryptographic services of the TOE and their interface as specified. When key-dependent functions implemented in the ***Security IC*** Embedded Software are just being executed, the ***Security IC*** Embedded Software must provide protection against disclosure of confidential data (User Data) stored and/or processed in the TOE by using the methods described under "Inherent Information Leakage" (*BSI.T.Leak-Inherent*) and "Forced Information Leakage" (*BSI.T.Leak-Forced*). **AUG4.Clarification:** For the separation of different applications, the ***Security IC*** Embedded Software may implement a memory management scheme based upon security mechanisms of the TOE as required by the security policy defined for the specific application context.

BSI.OE.Resp-Appl	Treatment of User Data: Security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context. For example the Security IC Embedded Software will not disclose security relevant User Data to unauthorised users or processes when communicating with a terminal. **AUG1.Clarification:** By definition cipher or plain text data and cryptographic keys are User Data. The ***Security IC*** Embedded Software shall treat these data appropriately, use only proper secret keys (chosen from a large key space) as input for the cryptographic function of the TOE and use keys and functions appropriately in order to ensure the strength of cryptographic operation. This means that keys are treated as confidential as soon as they are generated. The keys must be unique with a very high probability, as well as cryptographically strong. For example, it must be ensured that it is beyond practicality to derive the private key from a public key if asymmetric algorithms are used. If keys are imported into the TOE and/or derived from other keys, quality and confidentiality must be maintained. This implies that appropriate key management has to be realised in the environment. **AUG4.Clarification:** The treatment of User Data is still required when a multi-application operating system is implemented as part of the ***Security IC*** Embedded Software on the TOE. In this case the multi-application operating system should not disclose security relevant user data of one application to another application when it is processed or stored on the TOE.

78 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

79 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.

80 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).

81 The selected augmentations from *AUG* introduce the following security environment aspects:

- assumption "Usage of key-dependent functions, (*AUG1.A.Key-Function*)" in phase 1,
- TOE threat "Memory Access Violation, (*AUG4.T.Mem-Access*)",
- organisational security policy "Additional Specific Security Functionality, (*AUG1.P.Add Functions*)".

82 The justification of the additional policy, additional threat and the additional assumption 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 4. 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
AUG1.A.Key-Function	*BSI.OE.Plat-Appl* *BSI.OE.Resp-Appl*	Phase 1
BSI.P.Process-TOE	*BSI.O.Identification*	Phase 2-3
BSI.A.Process-Sec-IC	*BSI.OE.Process-Sec-IC*	Phase 4-6
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*	
AUG4.T.Mem-Access	*AUG4.O.Mem Access*	

6.3.1 Assumption "Usage of key-dependent functions"

83 The justification related to the assumption "Usage of key-dependent functions, (*AUG1.A.Key-Function*)" in phase 1 is as follows:

84 Compared to *BSI-PP-0035* a clarification has been made for the security objective “Usage of Hardware Platform (*BSI.OE.Plat-Appl*)", (AUG1.Clarification): If required the ***Security IC*** Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the ***Security IC*** Embedded Software must implement functions, which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. This addition ensures that the assumption *AUG1.A.Key-Function* is addressed by the objective *BSI.OE.Plat-Appl*.

85 Compared to *BSI-PP-0035* a clarification has been made for the security objective “Treatment of User Data (*BSI.OE.Resp-Appl*)” (AUG1.Clarification): By definition cipher or

plain text data and cryptographic keys are User Data. So, the ***Security IC*** Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realized in the environment. These measures make sure that the assumption *AUG1.A.Key-Function* is addressed by the security objective *BSI.OE.Resp-Appl*.

86 The added clarifications (AUG1.Clarification) do not introduce any contradiction in the security objectives applicable during phase 1.

6.3.2 TOE threat "Memory Access Violation"

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

88 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.

89 The clarification of “Usage of Hardware Platform, (*BSI.OE.Plat-Appl*)” (AUG4.Clarification) makes clear that it is up to the ***Security IC*** Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in *AUG4.T.Mem-Access* and *AUG4.O.Mem Access*. The TOE shall provide access control functions as a means to be used by the ***Security IC*** Embedded Software. This is further emphasised by the clarification of “Treatment of User Data, (*BSI.OE.Resp-Appl*)” (AUG4.Clarification) which reminds that the ***Security IC*** Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat *AUG4.T.Mem-Access*.

90 The added clarifications (AUG4.Clarification) do not introduce any contradiction in the security objectives applicable during phase 1.

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

6.3.3 Organisational security policy "Additional Specific Security Functionality"

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

93 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.

94 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*.

95 Compared to *BSI-PP-0035* a clarification has been made for the security objective “Usage of Hardware Platform (*BSI.OE.Plat-Appl*), (AUG1.Clarification)”: If required the ***Security IC*** Embedded Software shall use these cryptographic services of the TOE and their interface as specified. In addition, the ***Security IC*** Embedded Software must implement functions which perform operations on keys (if any) in such a manner that they do not disclose information about confidential data. This addition ensures that the assumption *BSI.OE.Plat-Appl* is still covered by the objective *BSI.OE.Plat-Appl* although additional functions are being supported according to *AUG1.P.Add Functions*.

96 Compared to *BSI-PP-0035* a clarification has been made for the security objective “Treatment of User Data (*BSI.OE.Resp-Appl*), (AUG1.Clarification)”: By definition cipher or plain text data and cryptographic keys are User Data. So, the ***Security IC*** Embedded Software will protect such data if required and use keys and functions appropriately in order to ensure the strength of cryptographic operation. Quality and confidentiality must be maintained for keys that are imported and/or derived from other keys. This implies that appropriate key management has to be realised in the environment. These measures make sure that the assumption *BSI.OE.Resp-Appl* is still covered by the security objective *BSI.OE.Resp-Appl* although additional functions are being supported according to *AUG1.P.Add Functions*.

97 The added objective for the TOE *AUG1.O.Add-Functions* does not introduce any contradiction in the security objectives. It merely extends the scope of the objectives identified above so that they cover the added functionality.

7 Security requirements

98 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

99 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.

100 All extensions to the SFRs of the "*BSI-PP-0035*" Protection Profiles (PPs) are **exclusively** drawn from *CCMB-2007-09-002*.

101 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.

102 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.

103 The selected security functional requirements for the TOEs, their respective origin and type are summarized in *Table 5*.

Table 5. Summary of functional security requirements for the TOE

Label	Title	Addressing	Origin	Type
FRU_FLT.2	Limited fault tolerance	Malfunction	*BSI-PP-0035*	*CCMB-2007-09-002*
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 5. 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-2007-09-002*
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-2007-09-002*
FDP_ACC.2	Complete access control	Memory access violation	Security Target Operated	
FDP_ACF.1	Security attribute based access control		*AUG* #4 Operated	
FMT_MSA.3	Static attribute initialisation	Correct operation		
FMT_MSA.1	Management of security attribute			

7.1.1 Limited fault tolerance (FRU_FLT.2)

104 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)

105 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.***

106 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)

107 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)

108 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.

109 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)

110 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)

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

112 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)

113 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)

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

115 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)

116 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***.

117 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)

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

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

7.1.11 Cryptographic operation (FCS_COP.1)

120 The TSF shall perform ***the operations in*** *Table 6* in accordance with a specified cryptographic algorithm ***in*** *Table 6* and cryptographic key sizes ***of*** *Table 6* that meet the ***standards in*** *Table 6****.***

Table 6. 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 - in Electronic Code Book (ECB) mode - in CBC-MAC operating modes	Data Encryption Standard (DES)	56 effective bits	*FIPS PUB 46-3* *ISO/IEC 9797-1* *ISO/IEC 10116*
		Triple Data Encryption Standard (3DES)	112 effective bits	

7.1.12 Static attribute initialisation (FMT_MSA.3)

121 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.

122 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)

123 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)

124 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.

125 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)

126 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.***

127 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.***

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

129 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.

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

131 SFP_3: *Dynamic Memory Access Control Policy*

132 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

133 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.

134 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.

135 The set of security assurance requirements (SARs) is presented in *Table 7*, indicating the origin of the requirement.

Table 7. 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

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

137 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.

138 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.

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

140 For reader's ease, an impact summary is provided in *Table 8*.

Table 8. 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)

141 ~~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.***

142 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.

143 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.

144 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.

145 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.

146 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)

147 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).

148 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).

149 ~~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

150 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.

151 As origins of security objectives have been carefully kept in their labelling, and origins of security requirements have been carefully identified in *Table 5* and *Table 7*, 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.

152 From *Table 3*, it is straightforward to identify two additional security objectives for the TOE (*AUG1.O.Add-Functions* and *AUG4.O.Mem Access*), and two clarifications on two security objectives for the environment (*BSI.OE.Plat-Appl* and *BSI.OE.Resp-Appl*), all tracing back to *AUG*. This rationale must show that security requirements suitably address these too.

153 Furthermore, a more careful observation of the requirements listed in *Table 5* and *Table 7* 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*).

154 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.

155 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*)”

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

157 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 ~~an~~ ***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.

158 The security functional requirement "*Static attribute initialisation (FMT_MSA.3)*" requires that the TOE provides default values for security attributes. ~~These default values can be overwritten by any subject (software) provided that the necessary access is allowed what is further detailed in the security functional requirement "Management of security attributes (FMT_MSA.1)".~~ 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.

Security objective “Additional Specific Security Functionality (*AUG1.O.Add-Functions*)”

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

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

7.4.3 Additional security requirements are consistent

"Cryptographic operation (***FCS_COP.1***)"

161 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*)"

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

7.4.4 Dependencies of Security Functional Requirements

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

- those justified in the *BSI-PP-0035* protection profile security requirements rationale,
- those justifed in *AUG* security requirements rationale (except on FMT_MSA.2, see discussion below),
- the dependency of *FMT_MSA.1* on FMT_SMF.1 (see discussion below).

164 Details are provided in *Table 9* below.

Table 9. 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*
FAU_SAS.1	None	No dependency	Yes, *BSI-PP-0035*
FPT_PHP.3	None	No dependency	Yes, *BSI-PP-0035*
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Yes	Yes, *BSI-PP-0035*
FPT_ITT.1	None	No dependency	Yes, *BSI-PP-0035*
FDP_IFC.1	FDP_IFF.1	No, see *BSI-PP-0035*	Yes, *BSI-PP-0035*
FCS_RNG.1	None	No dependency	Yes, *BSI-PP-0035*
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes	Yes, *AUG* ***#1*** (adapted to CC V3.1 R2, see discussion below)
	FCS_CKM.4	Yes (by the environment)	
FDP_ACC.2	FDP_ACF.1	Yes	***No,*** *CCMB-2007-09-002*
FDP_ACF.1	FDP_ACC.1	Yes	Yes, *AUG* ***#4***
	FMT_MSA.3	Yes	
FMT_MSA.3	FMT_MSA.1	Yes	Yes, *AUG* ***#4***
	FMT_SMR.1	No, see *AUG* ***#4***	

Table 9. Dependencies of security functional requirements (continued)

Label	Dependencies	Fulfilled by security requirements in this Security Target	Dependency already in *BSI-PP-0035* or in *AUG*
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	Yes	Yes, *AUG* ***#4***
	FMT_SMF.1	No, see discussion below	***No,*** *CCMB-2007-09-002*
	FMT_SMR.1	No, see *AUG* ***#4***	Yes, *AUG* ***#4***

165 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.

166 *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 7*)

167 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.

168 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.

169 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.

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

Dependencies of assurance requirements

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

172 Augmentation to this package are identified in paragraph *133* and do not introduce dependencies not already satisfied by the EAL5 package.

8 TOE summary specification

173 This section demonstrates how the TOE meets each Security Functional Requirement.

174 The following TSS relies on the refinement of the TSF security elements, as detailed in the TOE Functional Specification referenced in the *ST23YR80/SA23YR80 Documentation Report* (see *Section 9*, paragraph *211*).

8.1 Statement of TOE security functionality

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

8.1.1 TSF_INIT_A: Hardware initialisation & TOE attribute initialisation

176 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

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

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

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

180 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

181 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.

182 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

183 This functionality is responsible for restricting access of the TOE TEST functionality to the TEST process in TEST configuration.

184 In TEST configuration, this functionality ensures that the only allowed TOE user is an authorized TEST process.

185 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...).

186 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).

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

8.1.5 TSF_FWL_A: Memory Firewall

188 In TEST and USER configurations, this security functionality monitors:

- access from memory locations to other locations for ROM, RAM and NVM,
- register access.

189 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.

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

191 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.

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

8.1.6 TSF_PHT_A: Physical tampering protection

193 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.

194 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

195 In TEST and USER configurations, this functionality ensures the management of security violations attempts.

196 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

197 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.

198 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

199 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

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

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

202 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

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

8.2.1 TSF rationale

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

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

206 The complete rationale has been presented and evaluated in the *ST23YR80 Security Target*.

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

208 *Table 10* below summarises which TOE security functional requirements (SFRs) are addressed by each TSF service (TSFs).

Table 10. Mapping of TSF services and SFRs

TSFs / SFRs	TSF_INIT_A (8.1.1)	TSF_CONFIG_A (8.1.2)	TSF_INT_A (8.1.3)	TSF_TEST_A (8.1.4)	TSF_FWL_A (8.1.5)	TSF_PHT_A (8.1.6)	TSF_ADMINIS_A (8.1.7)	TSF_OBS_A (8.1.8)	TSF_ALEAS_A (8.1.10)	TSF_SKCS_A (8.1.9)
FAU_SAS.1 (7.1.5)			X	X						
FRU_FLT.2 (7.1.1)			X			X				
FPT_FLS.1 (7.1.2)	X		X		X	X	X			
FMT_LIM.1 (7.1.3)		X		X						
FMT_LIM.2 (7.1.4)		X		X						
FPT_PHP.3 (7.1.6)	X					X	X			
FDP_ITT.1 (7.1.7)						X		X	X	X
FPT_ITT.1 (7.1.8)						X		X	X	X
FDP_IFC.1 (7.1.9)						X		X	X	X
FCS_RNG.1 (7.1.10)									X	
FDP_ACC.2 (7.1.14)					X					
FDP_ACF.1 (7.1.15)					X					
FMT_MSA.3 (7.1.12)					X					
FMT_MSA.1 (7.1.13)					X					
FCS_COP.1 (7.1.11)										X

9 References

209 Protection Profile references

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

210 ST23YR80 Security Target reference

Component description	Reference
ST23YR80 Security Target	SMD_ST23YR80_ST_08_001

211 Target of Evaluation referenced documents

212 For security reasons, all these documents are classified and their applicable revisions are referenced in the ST23YR80/SA23YR80 Documentation Report.

Component description	Reference
ST23YR80/SA23YR80 Documentation Report	SMD_SA23YR80_DR_08_001

213 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 180-1	FIPS PUB 180-1 Secure Hash Standard, National Institute of Standards and Technology, U.S. Department of Commerce,1995
[5]	FIPS PUB 180-2	FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004
[6]	FIPS PUB 186	FIPS PUB 186 Digital Signature Standard (DSS), National Institute of Standards and Technology, U.S.A., 1994
[7]	FIPS PUB 197	FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001
[8]	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

Ref	Identifier	Description
[9]	ISO/IEC 9797-1	ISO/IEC 9797, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, ISO, 1999
[10]	ISO/IEC 10116	ISO/IEC 10116, Information technology - Security techniques - Modes of operation of an n-bit block cipher algorithm, ISO, 1997
[11]	ISO/IEC 10118-3:1998	ISO/IEC 10118-3:1998, Information technology - Security techniques - Hash functions - Part 3: Dedicated hash functions
[12]	ISO/IEC 14888	ISO/IEC 14888, Information technology - Security techniques - Digital signatures with appendix - Part 1: General (1998), Part 2: Identity-based mechanisms (1999), Part 3: Certificate based mechanisms (2006), ISO
[13]	CCMB-2006-09-001	Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2006, version 3.1
[14]	CCMB-2007-09-002	Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2007, version 3.1 Revision 2
[15]	CCMB-2007-09-003	Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2007, version 3.1 Revision 2
[16]	AUG	Smartcard Integrated Circuit Platform Augmentations, Atmel, Hitachi Europe, Infineon Technologies, Philips Semiconductors, Version 1.0, March 2002.
[17]	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
[18]	IEEE 1363-2000	IEEE 1363-2000, Standard Specifications for Public Key Cryptography, IEEE, 2000
[19]	IEEE 1363a-2004	IEEE 1363a-2004, Standard Specifications for Public Key Cryptography - Amendment 1:Additional techniques, IEEE, 2004
[20]	PKCS #1 V2.1	PKCS #1 V2.1 RSA Cryptography Standard, RSA Laboratories, June 2002
[21]	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.

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 11. 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.
CBC-MAC	Cipher Block Chaining Message Authentication Code.
CC	Common Criteria Version 3.1.
CPU	Central Processing Unit.
CRC	Cyclic Redundancy Checkj.
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DEMA	Differential Electromagnetic Analysis.
DES	Data Encryption Standard.
DIP	Dual-In-Line Package.
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.
IC	Integrated Circuit.
ISO	International Standards Organisation.
IT	Information Technology.
MPU	Memory Protection Unit.
NESCRYPT	Next Step Cryptography Accelerator.
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.

Table 11. List of abbreviations (continued)

Term	Meaning
RSA	Rivest, Shamir & Adleman.
SAR	Security Assurance Requirement.
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.
TSS	TOE Summary Specification.

10 Revision history

Table 12. Document revision history

Date	Revision	Changes
10-Feb-2009	01.00	Initial release.

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.

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