SCR400L revF

SECURITY TARGET (LITE)

SEC100 v1

SAFRAN
Starchip

0 Table Of Content

1 Introduction

1.1 ST Reference

This document is the SCR400L security target (ST) "Public Version" of the Security target referenced **SEC104** version **5.**

1.2 TOE Reference

The Target of evaluation (TOE) is the SCR400L version **F.**

Means to check TOE label for hardware:

- Physical label on the die ➔ C
- HW label obtained by reading product ID: OTP @ 0x40000014 ➔ **0x0D** for SCR400L
- HW version obtained by reading product revision: OTP @ 0x40000016 ➔ **0x06** corresponding to version **F**
- Configuration CRC value ➔ **0xBEFB4AAF**

1.3 TOE Overview

1.3.1 TOE Type

The SCR400L is a powerful, low-power 32-bit microcontroller, based on APS3sf-ARX core, and SST SuperFlash technology.

APS3sf-ARX is a High-performance 32-bit RISC Secure Core combining Cortus' APS3 CPU and Starchip' ARX core security technologies. APS3sf-ARX will use the same means of development as APS3. Thanks to this 32-bit Harvard RISC architecture, SCR400L achieves **30MIPS** @30MHz.

SCR400L embeds the state-of-the-art security peripherals and global architecture, StarChip® technology.

1.3.2 TOE Usage

SCR400L has been designed to address ID, passport and payment markets together with only one micro-controller.

SCR400L is a contact **or** RF Interface smartcard, communicating through ISO7816 or ISO14443 protocols.

1.3.3 TOE Features

General:

- APS3s-ARX Secured 32-bit core based on CORTUS and StarChip® technologies
  Harvard RISC Architecture
  Fully compatible with APS3s Core
- Advanced Low power modes
- Internal Clock oscillator (VFO) at 30MHz

- ESD Protection
  6kV for ISO7816 interface (Human Body Model)
  2kV for ISO14443 interface (Human Body Model)
- Class A, B supported with Class Indicator
- Interrupt Controller with up to 15 vectors

Memories:

- SST SuperFlash® Non-volatile Memory
- 400K Bytes of Flash Memory
  Sector: 256 bytes
  <2.5ms Sector Erase
  <17.6µs Byte program
  208 Bytes OTP Memory
- 8K Bytes RAM Memory
  including 1 KByte crypto-RAM
- Endurance Capability: 500K Cycles per sectors
- 25 years Data Retention
- Full Memory Personalization Time: down to 6 seconds

Security:

- GAIA Technology for EAL5+ security level
- Cryptographic peripherals:
  TDES 2K/3K
  AES 128/192/256
  GF(p) PKI Accelerator (with Montgomery support method)
  DMA access to RAM for fast PKI operations
- Secured Memories
  Data Encryption
  Address Bus Scrambling
- True Random Number Generator
- Code Signature Unit
- Control Flow Unit
- Unpredictable Index Generator
- Patch Module, to help the development of code update
- Random Process Interrupt
- Environmental Protection System
  Frequency and Power Supply monitors
  Active Shield
- Unique Serial Number per chip
- Memory Protection Unit:
  Configurable data access rights: read/write

Peripherals:

- Smart Card ISO7816 Controller
  625 Kbits/s at 5MHz
  Specific DMA for easy data management
  ISO7816 dedicated timer for ETU and cycle counter
  Waiting Time & Guard Time automatic management
  Compliant with T=0 and T=1 Protocols
- Contact Less RF ISO14443 Controller
  Type A - 13.56Mhz carrier frequency
  Power Saving modes
  106, 212, 424 and 848 Kbits/s support in both reception and transmission
  up to 4096 Bytes Frame Size management
  Internal dedicated timer
  ICAO Compliant
  EMV Compliant
- Multiple DMA: 2 channels
- CRC-16/32 Engine
- 32-bit Timer

1.3.4 Non-TOE hardware/software/firmware required by the TOE.

None.

1.4 TOE Description

1.4.1 Physical Scope

The TOE physical scope is the die.

NB: **The TOE is intended to be used for a Security IC composite product, this Security IC composite product comprises:**

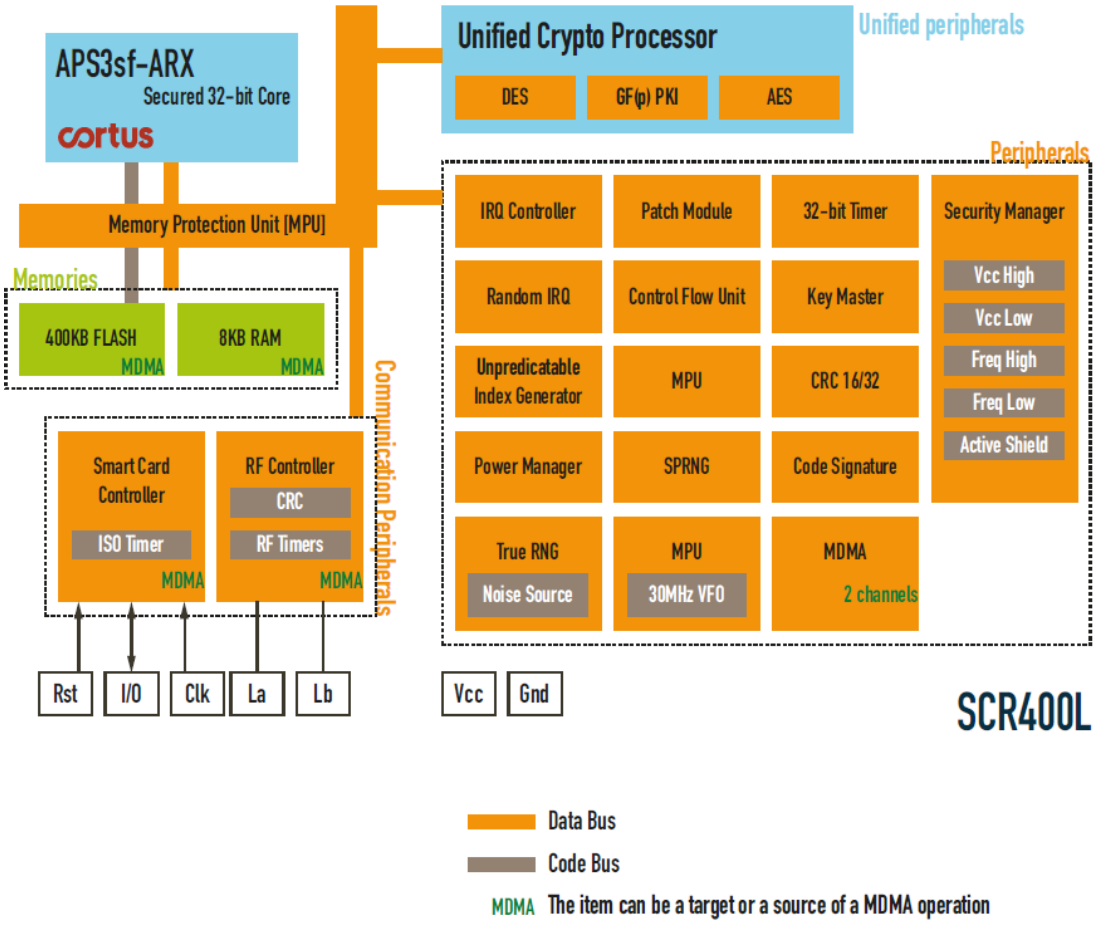
- the TOE (Hardware)
- the Security IC Embedded (Soft-coded Security IC Embedded Software stored in Flash Memory) and
- User Data (especially personalization data and other data generated and used by the Security IC Embedded Software).

Security Guidance for this TOE is:

- [TEP045] Security Guidance & Recommendations
- [TEP021] SCR400L Technical Datasheet
- [TEP044] SCR400L Errata Sheet

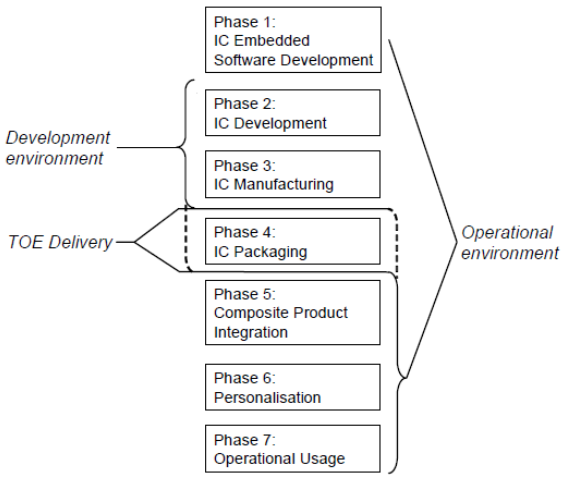
1.4.2 Logical Scope

All features listed in 1.3.3 are actually in the logical scope of the TOE. The following figure summarizes TOE logical scope for HW:



1.4.3 Development Life Cycle

The following figure details development life cycle from [BSI-PP-0084].



The following table details how phase 2 & 3 are implemented for this Security Target:

Phase	Process	Company	Site
Phase 2	RTL & SCH design	StarChip	Meyreuil (France)
	Synthesis	StarChip	Meyreuil (France)
	Place & Route	StarChip	Meyreuil (France)
Phase3	Mask Preparation	L-Foundry	Landshut (Germany)
	Generate Photo Mask	Compugraphics	Glenrothes Fife (Scotland)
	Manufacturing	L-Foundry	Avezzano (Italy)
	Test & NVM Loading	Nanium	Porto (Portugal)

NB: The customer embedded software will be loaded by StarChip before delivery (delivery from test house). The embedded software developer is responsible for the security of the composite TOE after delivery.

2 Conformance claims

2.1 CC conformance

This Security Target claims to be conformant to the Common Criteria version 3.1.

Furthermore it claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in chapter 5 of [BSI-PP-0084].

This Security Target has been built with the Common Criteria for Information Technology Security Evaluation; Version 3.1 which comprises:

- [CCpart1] Common Criteria for Information Technology Security Evaluation, Part 1:
- Introduction and General Model; Version 3.1, Revision 4, September 2012
- [CCpart2] Common Criteria for Information Technology Security Evaluation, Part 2:
- Security Functional Requirements; Version 3.1, Revision 4, September 2012
- [CCpart3] Common Criteria for Information Technology Security Evaluation, Part 3:

Security Assurance Requirements; Version 3.1, Revision 4, September 2012

The [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012 has been taken into account.

2.2 Package conformance

The package conformance in this Security Target is an assurance level as defined in chapter 8 of [CCpart3].

The assurance level conformance claimed is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5

2.3 PP conformance

This Security Target claims strict conformance to [BSI-PP-0084] protection profile.

The statement of security problem definition is a superset of the security problem definition in [BSI-PP-0084].

This superset is defined in:

- Addition #1 and #4 of [AUG], Cf. chapter 3 for details.

The statement of security objectives is a superset of objectives in [BSI-PP-0084].

This superset is defined in:

- Addition #1 and #4 of [AUG], Cf. chapter 4 for details.

The statement of security requirements is a superset of the security requirements in [BSI-PP-0084].

This superset is defined in:

- Addition #1 and #4 of [AUG], Cf. chapter 6 for details.

The following section explain impacts of Addition #1 on assumptions ("A.Key-Function" is added):

This new assumption does not mitigate any threat meant to be addressed by security objectives for the TOE. Indeed, this assumption is related to routines which may compromise keys when being executed as part of the Smartcard Embedded Software. In contrast to this the threats T.Leak-Inherent and T.Leak-Forced address (i) the cryptographic routines which are part of the TOE and (ii) the processing of User Data including cryptographic keys.

To cover this new assumption, the following clarifications are made on objective on the operational environment OE.Resp-Appl

Clarification of "Usage of Hardware Platform (OE.Plat-Appl)"

Since OE.Plat-Appl is removed from [BSI-PP-0084]. This Clarification taken from Addition 1 of [AUG] is not relevant anymore.

Clarification of "Treatment of User Data (OE.Resp-Appl)"

By definition cipher or plain text data and cryptographic keys are User Data. The Smartcard 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.

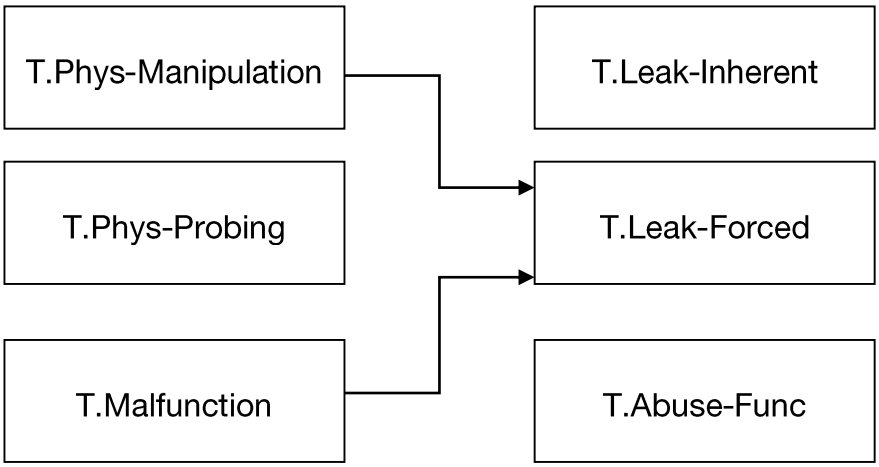
3 Security Problem Definition

3.1 Assets

Assets are defined in chapter 3.1 of [BSI-PP-0084]

3.2 Threats

Standard threats are defined in section 3.2 of [BSI-PP-0084]:



In addition to threats defined above the following additional threats are identified

- In orange font, addition from Addition #4 of [AUG]

T.Mem-Access — Memory Access Violation

Parts of the Smartcard Embedded Software may cause security violations by accidentally or deliberately accessing restricted data. Any restrictions are defined by the security policy of the specific application context and must be implemented by the Smartcard Embedded Software.

3.3 Organizational security policies

Organizational security policies (OSPs) are defined in section 3.3 of [BSI-PP-0084].

P.Process-TOE

In addition to OSPs defined above the following additional OSPs are identified

- In orange font, addition from Addition #1 of [AUG] (detailed below)

P.Add-Functions_HW

P.Add-Functions_HW Hardware Additional Specific Security Functionality

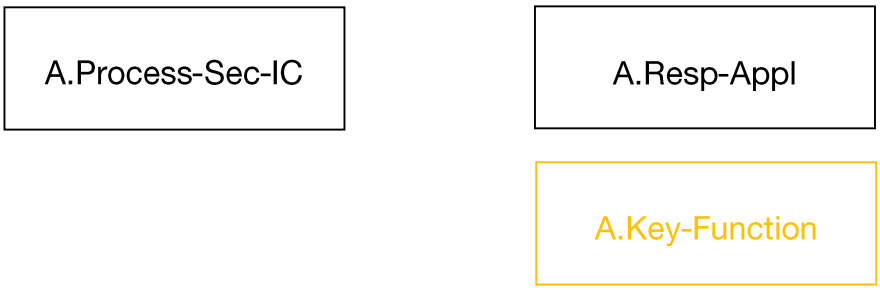
The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:

- Data Encryption Standard (DES) & (3DES with 112 & 168 bits key sizes), FIPS PUB 46-3, Data encryption standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, 1999
- Advanced Encryption Standard (AES with 128, 192 & 256 bits key sizes), FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001

3.4 Assumptions

Assumptions are defined in section 3.4 of [BSI-PP-0084]:

In addition the following assumption is added (This addition comes from Addition #1 of [AUG], it is identified in orange font):

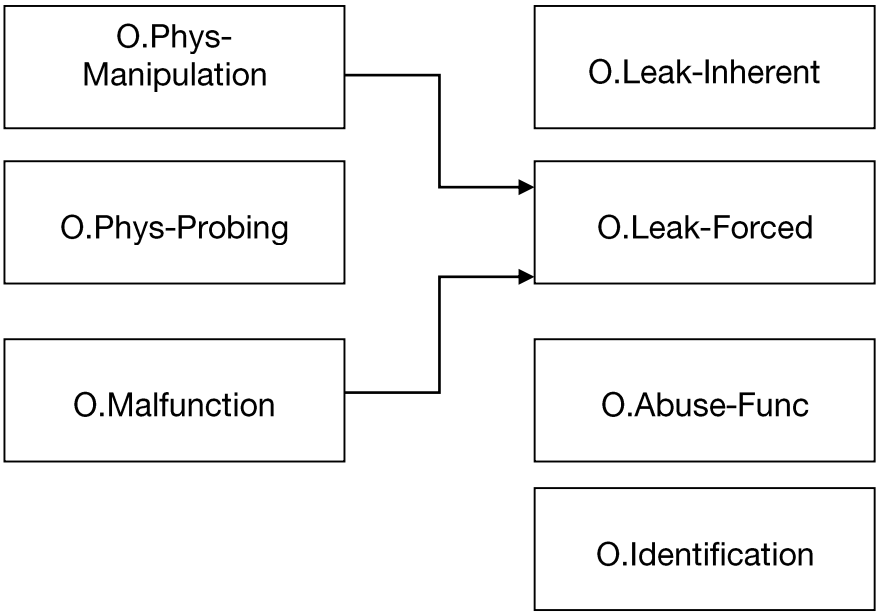


A.Key-Function	Usage of Key-dependent Functions Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys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

4 Security Objectives

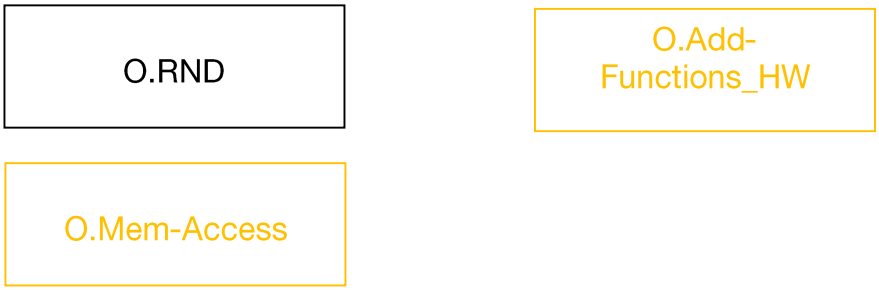
4.1 Security Objectives for the TOE

Standard security objectives for the TOE are defined in section 4.1 of [BSI-PP-0084]:



In addition to security objective for the TOE defined above, the following additional security objective for the TOE are identified

- In orange font, addition from Addition #1 & #4 of [AUG]



The TOE shall provide "Additional Specific Security Functionality (O.Add-Functions_HW)" as specified below.

O.Add-Functions_HW Hardware additional Specific Security Functionality

The TOE must provide the following specific security functionality to the Smartcard Embedded Software:

- Data Encryption Standard (DES) & (3DES with 112 & 168 bits key sizes), FIPS PUB 46-3, Data encryption standard (DES), National Institute of Standards and Technology, U.S. Department of Commerce, 1999
- Advanced Encryption Standard (AES with 128, 192 & 256 bits key sizes), FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001

The TOE shall provide "Area based Memory Access Control (O.Mem-Access)" as specified below.

O.Mem-Access Area based Memory Access Control

The TOE must provide the Smartcard Embedded Software with the capability to define restricted access memory areas. The TOE must then enforce the partitioning of such memory areas so that access of software to memory areas is controlled as required, for example, in a multi-application environment.

4.2 Security Objectives for the Operational Environment

Security objectives for the Operational Environment are defined in section 4.2 & 4.3 of [BSI-PP-0084].

4.3 Security Objectives rationale

Security objective rationale is given in chapter 4.4 of [BSI-PP-0084].

Rationale for [AUG] Addition #1 is given in the following table, detailed justifications in following chapter:

Assumption, Threat or Organisational Security Policy Security Objective Note	Security Objective	Note
P.Add-Functions_HW	O.Add-Functions_HW	
A.Key-Function	OE.Resp-Appl	Related to Phase 1

The justification related to the security objective "Additional Specific Security Functionality (O.Add-Functions_HW)" is as follows: Since O.Add-Functions_HW requires the TOE to implement exactly the same specific security functionality as required by P.Add-Functions_HW, the organisational security policy is covered by the objective. Nevertheless the security objectives O.Leak-Inherent, O.Phys-Probing, O.Malfunction, O.Phys-Manipulation and O.Leak-Forced define how to implement the specific security functionality required by P.Add-Functions_HW. (Note that these objectives support that the specific security functionality is provided in a secure way as expected from P.Add-Functions_HW.) Especially O.Leak-Inherent and 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 P.Add-Functions_HW.

OE.Resp-Appl actually upholds A.Key-Function. The Smartcard 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.

Moreover, the Smartcard 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 A.Resp-Appl is still covered by the security objective OE.Resp-Appl although additional functions are being supported according to P.Add-Functions_HW. The justification of the additional policy and the additional assumption show that they do not contradict to the rationale already given in the Protection Profile for the assumptions, policy and threats defined there.

Rationale for [AUG] Addition #4 is given in the following table, detailed justifications in following chapter:

Assumption, Threat or Organisational Security Policy Security Objective Note	Security Objective	Note
T.Mem-Access	O.Mem-Access	

According to O.Mem-Access the TOE must enforce the partitioning of memory areas so that access of software to memory areas is controlled. Any restrictions are to be defined by the Smartcard Embedded Software. Thereby security violations caused by accidental or deliberate access to restricted data can be prevented (refer to T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

It is up to the Smartcard Embedded Software to implement the memory management scheme by appropriately administrating the TSF. This is also expressed both in T.Mem-Access and O.Mem-Access. The TOE shall provide access control functions as a means to be used by the Smartcard Embedded Software. This is further emphasized by the clarification of “Treatment of User Data (OE.Resp-Appl)” which reminds that the Smartcard Embedded Software must not undermine the restrictions it defines. Therefore, the clarifications contribute to the coverage of the threat T.Mem-Access.

5 Extended Component Definition

Extended components are defined in [BSI-PP-0084]:

Definition of the Family FCS_RNG is made in chapter 5.1 of [BSI-PP-0084]

Definition of the Family FMT_LIM is made in chapter 5.2 of [BSI-PP-0084]

Definition of the Family FAU_SAS is made in chapter 5.3 of [BSI-PP-0084]

Definition of the Family FDP_SDC is made in chapter 5.4 of [BSI-PP-0084]

6 IT Security requirements

6.1 Security Functional Requirements

6.1.1 Security Functional Requirements from BSI-PP-0084

The following chapters details Security functional requirements taken from [BSI-PP-0084]. Application notes are not copied in this document, please refer to [BSI-PP-0084] for details.

FRU_FLT.2	Limited fault tolerance
Hierarchical to:	FRU_FLT.1
FRU_FLT.2.1	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).***
Dependencies:	FPT_FLS.1
Refinement:	***The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.***

FPT_FLS.1	Failure with preservation of secure state
Hierarchical to:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur.
Dependencies:	No dependencies.
Refinement:	***The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.***

FMT_LIM.1	Limited capabilities
Hierarchical to:	No other components.
FMT_LIM.1.1	The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced: ***Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks.***
Dependencies:	FMT_LIM.2

FMT_LIM.2	Limited availability
Hierarchical to:	No other components.
FMT_LIM.2.1	The TSF shall be designed and implemented in a manner that limits its availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced: ***Deploying Test Features after TOE Delivery does not allow user data of the Composite TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks***.
Dependencies:	FMT_LIM.1
FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
FAU_SAS.1.1	The TSF shall provide ***the test process before TOE Delivery*** with the capability to store ***Initialization Data and/or Pre-personalization Data and/or supplements of the Security IC Embedded Software in the NVM (non-volatile Flash memory).***
Dependencies:	No dependencies.
FDP_SDC.1	Stored data confidentiality
Hierarchical to:	No other components.
FDP_SDC.1.1	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the **Non Volatile Memory (Flash memory)**.
Dependencies:	No dependencies.
FDP_SDI.2	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1
FDP_SDI.2.1	The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors detectable by ECC and/or EDC** on all objects, based on the following attributes: **EDC or ECC value corresponding to the protected user data.**
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall correct the error (if possible and if requested by the embedded software) or trig a reset.
Dependencies:	No dependencies.

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components.
FPT_PHP.3.1	The TSF shall resist ***physical manipulation and physical probing*** to the ***TSF*** by responding automatically such that the SFRs are always enforced.
Refinement:	***The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.***
Dependencies:	No dependencies.

FDP_ITT.1	Basic internal transfer protection
Hierarchical to:	No other components.
FDP_ITT.1.1	The TSF shall enforce the ***Data Processing Policy*** to prevent the ***disclosure*** of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies:	FDP_ACC.1 OR_FDP_IFC.1
Refinement:	***The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.***

FPT_ITT.1	Basic internal TSF data transfer protection
Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from ***disclosure*** when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
Refinement:	***The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.***

FDP_IFC.1	Subset information flow control
Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the ***Data Processing Policy*** on **all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software.**
Dependencies:	FDP_IFF.1

Data processing policy is defined in § 162 of [BSI-PP-0084].

FCS_RNG.1	Cryptographic operation
Hierarchical to:	No other components.
FCS_RNG.1.1	The TSF shall provide a ***physical*** random number generator that implements***: the rule RègleArchiGVA-1 of [RGS_B1], the recommendation RecomArchiGVA-1 of [RGS_B1], total failure tests and online tests.***
FCS_RNG.1.2	The TSF shall provide ***numbers in 16 bit words*** that meet: ***the rule RègleArchiGVA-2 of [RGS_B1].***
Dependencies:	No dependencies.
Application Note:	The composite product's RNG will comply with [RGS_B1] only when all the rules of §2.4 "Génération d'aléa cryptographique" of [RGS_B1] are addressed. In particular, a cryptographic post-processing must be implemented by the composite developer.

6.1.2 Security functional requirements from Addition #1

The following chapters details Security functional requirements taken from [AUG] Addition #1. These SFRs are related to TDES and AES crypto services. Operations are performed by the TSF, keys are imported from the ES and managed by the ES using TSF interfaces.

NB: PKI accelerator is present in the TOE but not formalized trough SFRs. Security, related to services provided by the TOE for PKI acceleration are described in ADV_ARC documentation.

FCS_COP.1 / A	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform ***encryption & decryption*** in accordance with a specified cryptographic algorithm that meet the following: ***Triple Data Encryption Standard (3DES) and cryptographic key sizes of 112 bits & 168 bits that meet the following standards:*** ***U.S. Department of Commerce / National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46-3, 1999 October 25, keying options 1, 2, 3***
Dependencies:	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1], FCS_CKM.4

FCS_COP.1 / B	Cryptographic operation
Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform ***encryption & decryption*** in accordance with a specified cryptographic algorithm that meet the following: ***Advanced Encryption Standard (AES) and cryptographic key sizes of 128, 192, and 256 bits that meet the following standards:*** ***Federal Information Processing Standards (FIPS) Publication draft available at the AES home page: http://www.nist.gov/aes/.*** ***FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001***
Dependencies:	[FDP_ITC.1 OR FDP_ITC.2 OR FCS_CKM.1], FCS_CKM.4

6.1.3 Security functional requirements from Addition #4

The following chapters details Security functional requirements taken from [AUG] Addition #4. These SFRs are related to TOE MPU features and configuration.

FDP_ACC.1	Subset access control
Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the ***Memories access control policy*** on ***Subjects:*** – ***(CPU)*** – ***(MDMA)*** – ***(UCP)-PKI*** ***Objects:*** – ***(NVM) regions*** – ***(RAM) regions*** – ***Peripherals regions*** ***Operations:*** – ***read operation to regions.*** – ***write operation to regions.*** – ***execution operation for regions.***
Dependencies:	FDP_ACF.1

FDP_ACF.1	Security attribute based access control
Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the ***Memories access control policy*** to objects based on the following: ***Subjects security attributes (Permission control information)*** – ***(CPU) "run" mode*** – ***(CPU) "runperso" mode*** ***Object security attributes (Permission control information)*** – ***(NVM) region base (NVM) region limit*** – ***(RAM) region base (RAM) region limit*** – ***Peripherals selection OTP start*** – ***Read access to (NVM) regions*** – ***Write access to (NVM) regions*** – ***Lock of (NVM) regions Read access to (RAM) regions*** – ***Write access to (RAM) regions Lock of (RAM) regions*** – ***Freeze area size*** – ***NVM No-exec region base*** – ***NVM No-exec region limit***
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: – ***The TSF shall allow memory read on regions if the related attributes authorize it for (NVM), for (RAM).*** – ***The TSF shall allow memory write on regions if the related attributes authorize it for (NVM), for (RAM).*** – ***The TSF shall allow NVM execution only outside No-exec region.***

- ***The TSF shall allow access (read/write) to peripherals if the related attributes authorize it.***
- ***The TSF shall allow memory base & limit address update only if the related attributes authorize it.***

Permission control information checks are achieved before the operation

FDP_ACF.1.3	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: – ***The TSF shall allow memory write of Freeze area only if the related attributes authorize it*** – ***The TSF shall allow access to mpu peripheral lock only if the related attributes authorize it.***
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: – ***Execution is forbidden for Peripherals regions, (RAM) regions.*** – ***An access (read or write) to a memory area which is not covered by a (MPU) region is unauthorized.*** – ***Once Freeze area size is set, the Freeze area cannot be modified anymore, even after reset (except in (CPU) "runperso" mode).***
Dependencies:	FDP_ACC.1, FMT_MSA.3

FMT_MSA.3	Static attribute initialization
Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the ***Memories access control policy*** to provide **permissive** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow ***any subject (provided that the Memory Access Control Policy is enforced and the necessary access is therefore allowed)*** to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1, FMT_SMR.1

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the ***Memories access control policy*** to restrict the ability to **modify** the security attributes ***permission control information*** to ***CPU.***
Dependencies:	[FDP_ACC.1 OR FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

6.2 Security Assurance Requirements

The following table details assurance requirements for this security target regarding those defined in the protection profile [BSI-PP-0084].

Assurance components in [BSI-PP-0084]. EAL 4 augmented with: ALC_DVS.2 & AVA_VAN.5	**Assurance components in this ST EAL 5 augmented with: ALC_DVS.2 & AVA_VAN.5**	**Refined in [BSI-PP-0084]**
ADV_ARC.1 Security architecture description	ADV_ARC.1 Security architecture description	yes
ADV_FSP.4 Complete functional specification	ADV_FSP.5 Complete semi-formal functional	yes
ADV_IMP.1 Implementation representation of the TSF	ADV_IMP.1 Implementation representation of the TSF	yes
	ADV_INT.2 Well-structured internals	no
ADV_TDS.3 Basic modular design	ADV_TDS.4 Semiformal modular design	no
AGD_OPE.1 Operational user guidance	AGD_OPE.1 Operational user guidance	yes
AGD_PRE.1 Preparative procedures	AGD_PRE.1 Preparative procedures	yes
ALC_CMC.4 Production support, acceptance procedures and automation	ALC_CMC.4 Production support, acceptance procedures and automation	yes
ALC_CMS.4 Problem tracking CM coverage	ALC_CMS.5 Development tools CM coverage	yes
ALC_DEL.1 Delivery procedures	ALC_DEL.1 Delivery procedures	yes
ALC_DVS.2 Sufficiency of security measures	ALC_DVS.2 Sufficiency of security measures	yes
ALC_LCD.1 Developer defined life-cycle model	ALC_LCD.1 Developer defined life-cycle model	no
ALC_TAT.1 Well-defined development tools	ALC_TAT.2 Compliance with implementation standards	no
ASE_CCL.1 Conformance claims	ASE_CCL.1 Conformance claims	no
ASE_ECD.1 Extended components definition	ASE_ECD.1 Extended components definition	no
ASE_INT.1 ST introduction	ASE_INT.1 ST introduction	no
ASE_OBJ.2 Security objectives	ASE_OBJ.2 Security objectives	no
ASE_REQ.2 Derived security requirements	ASE_REQ.2 Derived security requirements	no
ASE_SPD.1 Security problem definition	ASE_SPD.1 Security problem definition	no
ASE_TSS.1 TOE summary specification	ASE_TSS.1 TOE summary specification	no
ATE_COV.2 Analysis of coverage	ATE_COV.2 Analysis of coverage	yes
ATE_DPT.1 Testing: basic design	ATE_DPT.3 Testing: modular design	no
ATE_FUN.1 Functional testing	ATE_FUN.1 Functional testing	no
ATE_IND.2 Independent testing - sample	ATE_IND.2 Independent testing - sample	no
AVA_VAN.5 Advanced methodical vulnerability analysis	AVA_VAN.5 Advanced methodical vulnerability analysis	yes

NB: Refinements on Assurance Requirements are detailed in chapter 6.2.1 of [BSI-PP-0084]. They are also applicable to all augmented components in this ST

6.3 Security Requirements Rationale

6.3.1 Rationale for BSI-PP-0084 Security Functional Requirements

Rationale for security functional requirements is given in chapter 6.3.1 of [BSI-PP-0084].

Dependencies analysis is given in chapter 6.3.2 of [BSI-PP-0084].

6.3.2 Rationale for Augmentation #1 Security Functional Requirements

Security Objective	Security Functional Requirement
O.Add-Functions_HW	- FCS_COP.1 „Cryptographic operation“

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

The security functional requirement(s) “Cryptographic operation (FCS_COP.1)” exactly requires those functions to be implemented which are demanded by O.Add-Functions_HW. Therefore, FCS_COP.1 is suitable to meet the security objective. Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional functions are used as specified and that the User Data processed by these functions are protected as defined for the application context.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, fulfilled by the ES and evaluated during composite TOE evaluation. These requirements are also considered as being related to OE.Resp-Appl. They are covered by guidance documentation evaluation.

6.3.3 Rationale for Augmentation #4 Security Functional Requirements

Security Objective	Security Functional Requirement
O.Mem-Access	- FDP_ACC.1 “Subset access control” - FDP_ACF.1 “Security attribute based access control” - FMT_MSA.3 “Static attribute initialisation” - FMT_MSA.1 “Management of security attributes”

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

The security functional requirements “Subset access control (FDP_ACC.1)” and “Security attribute based access control (FDP_ACF.1)” with the related Security Function Policy (SFP) “Memory Access Control Policy” exactly require to implement an area based memory access control as demanded by O.Mem-Access. Therefore, FDP_ACC.1 with its SFP is suitable to meet the security objective. Nevertheless, the developer of the Smartcard Embedded Software must ensure that the additional

functions are used as specified and that the User Data processed by these functions are protected as defined for the application context. These issues are addressed by the requirement RE.Phase-1.

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). These management functions ensure that the required access control can be realized using the functions provided by the TOE.

Dependencies:

Security Functional Requirement	Dependencies	Fulfilled by security requirements or justification
FDP_ACC.1	FDP_ACF.1	yes
FDP_ACF.1	FDP_ACC.1	yes
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1.	Yes, except for FMT_SMR.1 & FMT_SMF.1: the access control specified for the intended TOE is not role-based but enforced for subjects. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1. Because actions related to the policies are already defined in FDP_ACC.1 / FDP_ACF.1 and because these functions are not-role based, there is no need to identify these functions in form of a security functional requirement FMT_SMF.1.
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	

6.3.4 Rationale for the Security Assurance Requirements

An assurance level of EAL4 with the augmentations AVA_VAN.5 and ALC_DVS.2 are required for this type of TOE in [BSI-PP-0084] since it is intended to defend against sophisticated attacks. This security target claims an EAL5 with the augmentations AVA_VAN.5 and ALC_DVS.2. to permit the developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators must have access to the design and source code.

ALC_DVS.2 Sufficiency of security measures:

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. In the particular case of a Security IC the TOE is developed and produced within a complex and distributed industrial process which must especially be protected. Details about the implementation, (e.g. from design, test and development tools as well as Initialisation Data) may make such attacks easier. Therefore, in the case of a Security IC, maintaining the confidentiality of the design is very important.

This assurance component is a higher hierarchical component to EAL5 (which only requires ALC_DVS.1). ALC_DVS.2 has no dependencies.

AVA_VAN.5 Advanced methodical vulnerability analysis:

Due to the intended use of the TOE, it must be shown to be highly resistant to penetration attacks. This assurance requirement is achieved by the AVA_VAN.5 component.

Independent vulnerability analysis is based on highly detailed technical information. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing high attack potential.

AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.2 “Security enforcing functional specification”, ADV_TDS.3 “Basic modular design”, ADV_IMP.1 “Implementation representation of the TSF”, AGD_OPE.1 “Operational user guidance”, and AGD_PRE.1 “Preparative procedures”. All these dependencies are satisfied by EAL4 and therefore also by EAL5.

It has to be assumed that attackers with high attack potential try to attack Security ICs like smart cards used for digital signature applications or payment systems.

Therefore, specifically AVA_VAN.5 was chosen in order to assure that even these attackers cannot successfully attack the TOE.

Note that detailed refinements for assurance requirements are given in Section 6.2.1. of [BSI-PP-0084] .

7 TOE Summary Specification

7.1 Resistance to Faults:

Related SFRs:

FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state

Noise filters are embedded on SCR400L pads. This increases the resistance to transmission with noise.

SCR400L embeds environmental detectors to protect the code execution from an unexpected behavior due to high variation of running context.

Thus, several monitors are embedded to detect low/high voltages on Vcc, low and high frequencies on Clk.

Additional digital fault detectors are embedded in the product to cover light, EM injection and abnormal temperature operating.

Hardware Code Signature Unit (CSU) and Control Flow Unit (CFU) peripherals are designed to let sensitive software ensure the algorithms it runs are executed as expected. It provides the embedded application with tool to resist Fault Injection attacks.

All these monitors generate security alarms for the Security Manager.

The role of the Security Manager is to collect all the security alarms from the whole system and reacts according to global security policy partially configured by the software.

7.2 Test mode & Personalization security:

Related SFR(s):

FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FAU_SAS.1	Audit storage

SCR400L embeds a full test mode before the TOE is released (FTM). This full test mode is protected by strong authentication mechanisms (128 bit password). It is also a dedicated protocol with a proprietary set of commands.

After TOE is released, the FTM is not accessible anymore, a reduced test mode is nevertheless present (RTM). This test mode permits to analyze field returns but without any sensitive action possible. This reduced test mode is protected by strong authentication mechanisms (128 bit password). It is also a dedicated protocol with a proprietary set of commands.

Traceability data (unique identifier) is written in the NVM during test mode.

Any other personalization or initialization data can be written in the NVM depending on customer needs.

7.3 Resistance to physical attack:

Related SFR(s):

FPT_PHP.3	Resistance to physical attack
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored data integrity monitoring and action

SCR400L embeds an active shield. The active shield is a network of wires that uses dynamic values which are progressing on it.

Sensitive wire reverse is made difficult by a fully managed synthesis of the core. Data busses are encrypted and redounded, addresses are scrambled.

The Flash memory uses a 40-bit word including 8-bit reserved for an ECC function. This allows error detection & correction for security reasons but also for reliability reasons (endurance or retention). If one or few bits of the memory array have been physically modified, they will be detected.

7.4 Information leakage:

Related SFRs:

FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control

SCR400L embeds several mechanisms that guarantee that information leakage during transfers & processing is limited. SCR400L is also build in a way that stored information is protected.

Secured Memories & busses

- Data Encryption
- Address Bus Scrambling
- Digital power consumption & electromagnetic masking

Secured Core

- Synthesizable core with dedicated security
- Digital power consumption & electromagnetic masking

7.5 Cryptographic features

Related SFRs:

FCS_RNG.1	Cryptographic operation
FCS_COP.1 / A	Cryptographic operation (3DES)
FCS_COP.1 / B	Cryptographic operation (AES)

SCR400L embeds a true random number generator: In this mode, the Analog Noise Source is the only source of entropy (randomness). Due to the noise source baud rate, interrupts permit to get the complete 16-bit word as soon as it is generated. Moreover, Failure detector (chi2 test) verifies if the Analog block works correctly.

SCR400L embeds Triple Data Encryption Standard (3DES) and cryptographic key sizes of 112 bits & 168 bits with state of the art side channel protection (Digital power consumption & electromagnetic masking, fault protection).

SCR400L embeds Advanced Encryption Standard (AES) and cryptographic key sizes of 128, 192, and 256 bits with state of the art side channel protection (Digital power consumption & electromagnetic masking, fault protection).

7.6 Memory protection unit

Related SFRs:

FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MSA.3	Static attribute initialisation
FMT_MSA.1	Management of security attributes

The Memory Protection Unit Secure (MPU) is a security module, which checks that the software memory accesses are not done where there is no memory or peripheral (memory map hole). The MPU checks that software memory accesses and code execution are not done outside regions or inside regions with restrictive rules. The MPU checks that software peripheral accesses are not done if it's deactivated by the MPU.

8 Referenced documents

[CCpart1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, September 2012.

[CCpart2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 4, September 2012.

[CCpart3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 4, September 2012 has been taken into account.

[BSI-PP-0084] Security IC Platform Protection Profile Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014.

[AUG] Smartcard Integrated Circuit Platform Augmentations Version 1.00 March 8, 2002

[RGS_B1] Référentiel Général de Sécurité version 2.0 Annexe B1

[TEP045] Security Guidance & Recommendations Version 5

[TEP021] SCR400L Technical Datasheet Version 6

[TEP044] SCR400L Errata Sheet Version 11

9 Glossary & Abbreviations

DPA	Differential Power Analysis
SPA	Simple Power Analysis
EMA	Electro Magnetic Analysis
DEMA	Differential Electro Magnetic Analysis
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
ST	Security Target
TSS	TOE Security Specification
IC	Integrated Circuit
ES	Embedded Software
DS	Dedicated Software
RAM	Random Access Memory
ROM	Read Only Memory
NVM	Non-Volatile Memory
MPU	Memory Protection Unit
DES	Data Encryption Standard
AES	Advanced Encryption Standard
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman algorithm for public-key cryptography
ECC	Elliptic Curves Cryptography
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
EDC	Error Detection Code
TRNG	True Random Number Generator
DRNG	Deterministic Random Number Generator
RTL	Register Transfer Language
SCH	Schematic
CPU	Central Processing Unit
(MDMA)	Multi-Channel Direct Memory Access
(UCP)	Unified Crypto Processor
(UCP) - PKI	PKI accelerator sub module of UCP