Public

Common Criteria Information Technology Security Evaluation

STRONGV4P00 of S5E9945 with Specific IC Dedicated Software

Version 2.2

27th November 2024

ST Lite(Security Target Lite)

Important Notice

Samsung Electronics Co. Ltd. (“Samsung”) reserves the right to make changes to the information in this publication at any time without prior notice. All information provided is for reference purpose only. Samsung assumes no responsibility for possible errors or omissions, or for any consequences resulting from the use of the information contained herein.

This publication on its own does not convey any license, either express or implied, relating to any Samsung and/or third-party products, under the intellectual property rights of Samsung and/or any third parties.

Samsung makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Samsung assume any liability arising out of the application or use of any product or circuit and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

Customers are responsible for their own products and applications. "Typical" parameters can and do vary in different applications. All operating parameters, including "Typicals" must be validated for each customer application by the customer's technical experts.

Samsung products are not designed, intended, or authorized for use in applications intended to support or sustain life, or for any other application in which the failure of the Samsung product could reasonably be expected to create a situation where personal injury or death may occur. Customers acknowledge and agree that they are solely responsible to meet all other legal and regulatory requirements regarding their applications using Samsung products notwithstanding any information provided in this publication. Customer shall indemnify and hold Samsung and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim (including but not limited to personal injury or death) that may be associated with such unintended, unauthorized and/or illegal use.

Samsung Electronics Co., Ltd.
DSR, 1-1 SamsungJeonja-Ro, Hwaseong-Si, Gyeonggi-Do, Republic of Korea

Home Page: *http://www.samsungsemi.com*

Revision History

Revision No.	Date	Description
0.0	7th March 2024	Creation for initial version
0.1	12th March 2024	- The chapter 1.2.5 is updated. - Table 1-1 is updated.
2.0	23th October 2024	- The chapter 7.3, 8.1 and 9.1 are updated. - Table 1-1 is updated.
2.0	23th October 2024	- The chapter 7.3, 8.1 and 9.1 are updated. - Table 1-1 is updated.
2.1	22nd November 2024	- The chapter 7.3.4 is updated. - Table 1-1 is updated.
2.2	27th November 2024	- Table 1-1 is updated.

Edited:

Written by	Title
SungGeun Park	Staff Engineer
JungHyun Kim	Principal Engineer

Table of Contents

List of Figures

List of Tables

List of Terms

List of Acronyms

Acronyms	Descriptions
CC	Common Criteria
3S	Secure Sub-System
EAL	Evaluation Assurance Level
FPGA	Field Programmable Gate Array
IC	Integrated Circuit
PP	Protection Profile
RNG	Random Number Generator
SOC	System-On-a-Chip
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Feature
TSFI	TSF Interface
TSP	TOE Security Policy
BL	Bootloader
STRONG	Secure Tamper Resistance On Next Generation
PP_AN	Application Note in PP0117

1 ST INTRODUCTION

1 This introductory chapter1 contains the following sections:

1.1 Security Target and TOE Reference

1.2 TOE Overview and TOE Description

1.3 Functional Packages

1.4 Interfaces of the TOE

1.1 Security Target and TOE Reference

2 The Security Target Lite version is 2.2 and dated 27th November 2024.
The Security Target Lite is strictly conformance to:

3 [5]Secure Sub-System in System-on-Chip (3S in SoC), Version 1.5, BSI-CC-PP-0117

4 The Protection Profile and the Security Target are built on *Common Criteria version 3.1*.

- Title: Security Target Lite of STRONGV4P00 of S5E9945 with Specific IC Dedicated Software
- TOE: Revision 1.2
- Target of Evaluation: STRONGV4P00 of S5E9945 with Specific IC Dedicated Software
- Provided by: Samsung Electronics Co., Ltd.
- Common Criteria version:

5 [1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

6 [2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation,Part2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

7 [3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

8 [4]Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-004

1.2 TOE Overview and TOE Description

1.2.1 TOE Type

9 The Target of Evaluation (TOE), the STRONGV4P00 featuring the TORNADO™-H cryptographic coprocessor, is integrated as a Secure Sub System (3S) within an SOC. The TOE is composed of a processing unit, security components, hardware circuits for testing purposes during the manufacturing process and volatile and non-volatile memories (hardware). The TOE also includes IC Designer/Manufacturer proprietary IC Dedicated Software STRONGV4P00 after being delivered by the IC Manufacturer. Such software is used for providing additional services to facilitate the usage of the hardware, such as a random number generation library for the hardware random number generator. All other software is called STRONGV4P00 Embedded Software and is not part of the TOE. The SoC S5E9945 is necessary to operate the STRONGV4P00 but it is not TOE hardware.

10 Regarding the AH3 Secure RSA/ECC/SHA library, the user has the possibility to select IC Dedicated Software part of the TOE during the delivery process by choosing thier own public key cryptographic library. Hence, the TOE can be delivered with or without the functionality of the AH3 Secure RSA/ECC/SHA library, which results in two TOE configurations. This is considered in this Security Target and corresponding notes (indicated by “optional”) are added where applicable. If the user decides not to use the AH3 Secure RSA/ECC/SHA library, the library is not delivered to the user and the accompanying Rivest-Shamir-Adleman (O.RSA) and Elliptic Curve Cryptography (O.ECDSA, O.ECDH) is not provided by the TOE. Deselecting public key cryptographic libraries means excluding the code that the user decided not to use. Excluding the code of the deselected functionality has no impact on any other security policy of the TOE, it is exactly equivalent to the situation where the user decides just not to use the functionality.

1.2.2 TOE Definition

11 The TOE is a Secure Sub-System with defined physical boundaries, implemented in a SoC that is designed and packaged specifically for mobile applications.

12 The CORTEX-M35P CPU architecture of STRONGV4P00 follows the Harvard architecture, that is, it has separate program and data memories. Using those separate memory access paths, both instruction and data can be fetched simultaneously without causing a stall.

13 The main security features of the **TOE** are:

- Security sensors or detectors including High and Low Temperature detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detector and Laser detectors
- Active Shields against physical intrusive attacks
- Dedicated hardware mechanisms against side-channel attacks
- Dedicated hardware mechanisms against Fault Injection attacks, such as redundancy
- Secure TDES and AES Symmetric Cryptography support
- TORNADO™-H cryptographic coprocessor
- Key Manager: KDF (block KEYMGR in the Security Controller)
- ECC/ Parity/ CRC-32 calculators
- One True Random Number Generator (TRNG HS_MRO9) that meets PTG.2 class of BSI-AIS-20/31 [6] (German scheme)
- SHA-2/ SHA-3/ HMAC hardware engines in the Security Controller
- Direct Memory Access (SC_DMA)
- Secure AXI Bridge

- Memory Management Unit (MMU)
- The IC Dedicated Software includes:
  - AH3 Secure RSA/ECC/SHA library for the support of RSA, ECC and SHA cryptographic operations (optional)
  - AH3 Secure ML-DSA library for the support ML-DSA cryptographic operations (optional)
  - TRNG HS_MRO9 library built around a hardware TRNG HS_MRO9, together with corresponding TRNG HS_MRO9 application notes. This library meets PTG.2 class of BSI-AIS-20/31 [6] (German scheme)
  - Secure Boot Loader is a loader for copying the firmware from an external FLASH storage into the internal SRAM

14 The above main security features are part of the evaluation scope.

15 The main hardware blocks of the STRONGV4P00 Secure Sub-System are described in Figure 1-1 below:

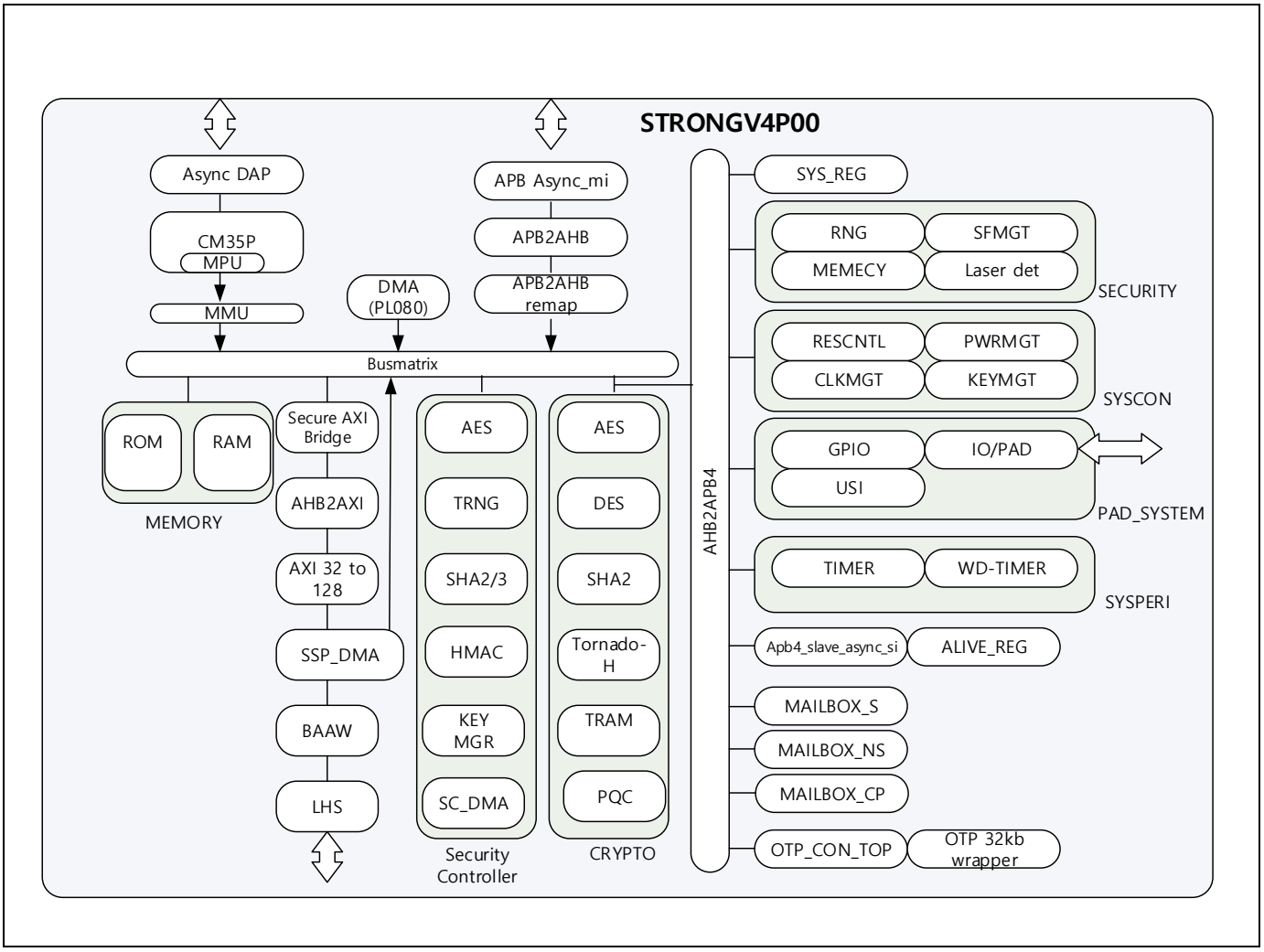


Figure 1-1 TOE (STRONGV4P00) Block Diagram

NOTE 1:No security functionality is claimed **for t**he following hardware blocks in this TOE or use cases:

- SHA2 in the CRYPTO block
- DMA (PL080)
- SSP_DMA

- Key manager KEYMGT in SYSCON
- Code execution through the Secure AXI bridge (eXecute In Place, XIP)

NOTE 2: Secure functionality is claimed for the AES in the Security Controller and the AES in the CRYPTO block.

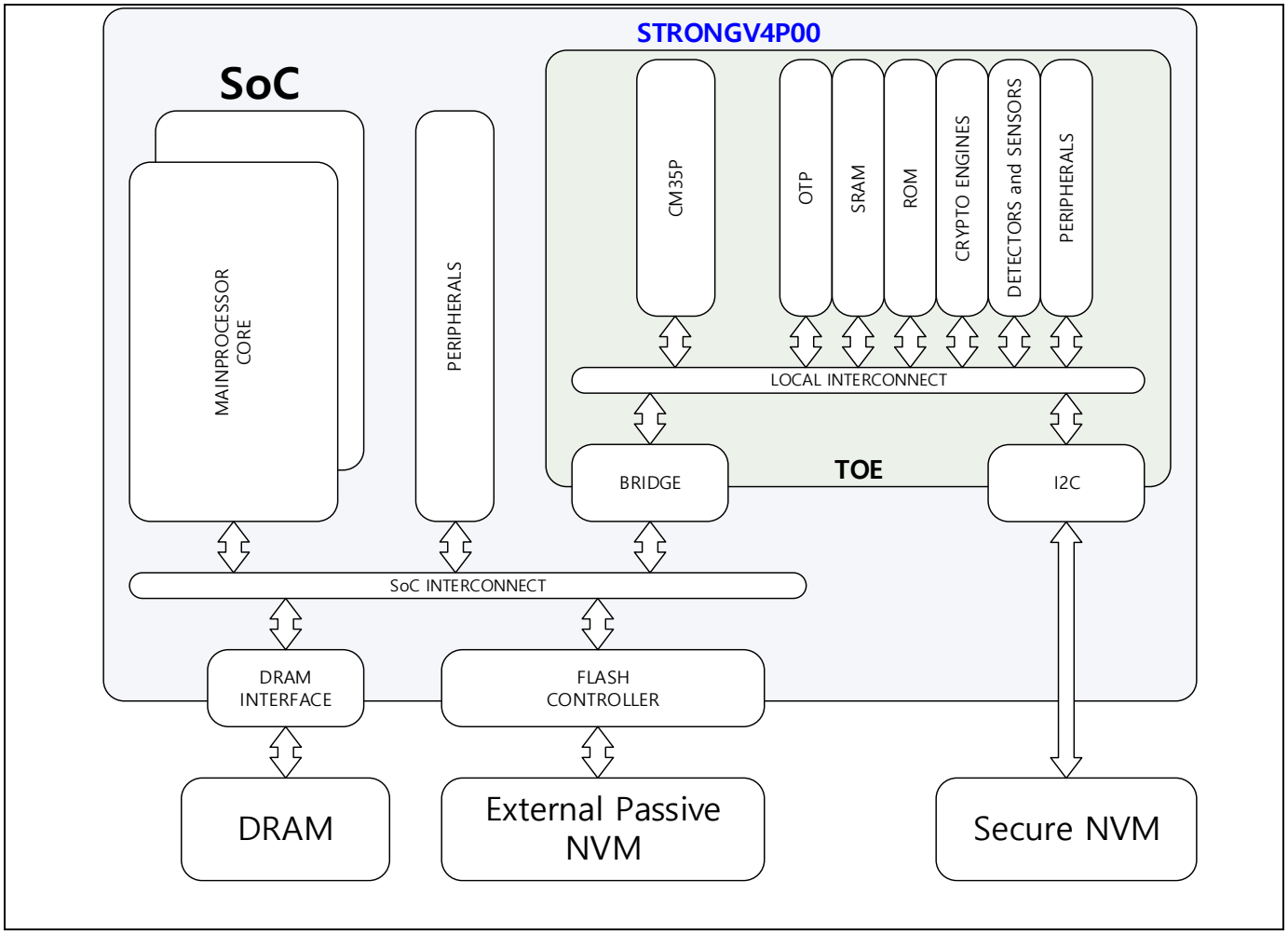


Figure **1-2. Overall Block Diagram of the SoC that includes TOE**

NOTE: The "Package for Secure External Memory", external Secure NVM, is not claimed as a secure functions of this TOE. Additional functionality is required by e.g. an Operating System that implements confidentiality, integrity and rollback protection for the information stored in the external memories.

16 Figure 1-2 shows the overall SoC block diagram.

17 The TOE consists of the following Hardware and Software:

TOE Hardware

- OTP storage/RAM/CryptoRAM (TRAM)/ROM
- 32-bit Central Processing Unit (CPU)
- Memory Protection Unit (MPU) with address space up to 4 GB
- Memory Management Unit (MMU)
- Internal Voltage Regulator (IVR)

- Power on Reset circuitry
- One Internal Clock generators
- Detectors & Security Logic
- Bilateral Pseudo Random Number Generator (BPRNG)
- True Random Number Generator (TRNG HS_MRO9) that meets PTG.2 class of BSI-AIS-20/31 (German scheme).
- PQC(Post-Quantum Cryptography) engine(CRYSTALS)
- Triple DES cryptographic coprocessor with 112- or 168-bit key size
- Two AES cryptographic coprocessors with 128 bits, 192 bits and 256 bits key size in the Security Controller and CRYPTO block
- Key Manager KDF (block KEYMGR inside the Security Controller)
- TORNADO-H coprocessor, supporting Montgomery multiplication, modular addition/subtraction and a computation for the square of a Montgomery constant up to 4,128-bit operand sizes.
- SHA-2, SHA-3, HMAC hardware engines
- ECC/ Parity/ CRC-32 calculators
- Direct Memory Access (SC_DMA)
- Secure AXI Bridge
- Timers
- Mailboxes to communicate with the SoC main core

TOE Software

18 The TOE software comprises the following components:

- The AH3 Secure RSA/ECC/SHA library (optional)
  TORNADO™-H is a hardware coprocessor for high speed modular multiplications, modular additions and modular subtractions. The AH3 Secure RSA/ECC/SHA library is a software library that is built on the TORNADO™-H coprocessor that provides high level interface for RSA, ECC and SHA cryptographic algorithms.
  The RSA functions of the library included in the TOE are:
    - RSA_KeyGen_Secure (RSA public/private key pair generation)
    - TND_RSA_SigSTD_Secure (RSA signature generation with the standard method)
    - TND_RSA_SigCRT_Secure (RSA signature generation with the CRT method)
    - TND_RSA_Verify (RSA signature verification)
    - RSA_R2modM_precompute_sec (R^2 value precomputation for the standard RSA)
    - RSA_R2modPandQ_precompute_sec (R^2 value precomputation for the CRT RSA)

  The library supports RSA operations with key sizes from 32-bits to 4,096-bits, in 2-bit steps. However, only the key size range from 1,900-bit up to 4,096-bit is within the scope of this evaluation.

  The functions TND_RSA_SigSTD_Secure and TND_RSA_SigCRT_Secure implement countermeasures against SPA, DPA and DFA attacks. The RSA_KeyGen_Secure function implements countermeasures against SPA and DFA attacks. Finally, the RSA_R2modM_precompute_sec and RSA_R2modPandQ_precompute_sec functions implement countermeasures against Fault Injection attacks.

  The AH3 Secure RSA/ECC/SHA library provides a set of functions to implement ECC cryptographic

algorithms. In particular, it provides functions to implement the ECDSA signing/verifying and the ECDH key exchange protocol. The library implements ECC for general curves over prime fields of sizes from 224-bit to 512-bit. Only curves whose security has been proven are in scope of this evaluation (see Note 1 below). The ECC functions of the library included in the TOE are:

- ECDSA_keygen (Ephemeral or static key pair generation for ECDSA signing/verifying)
- ECDSA_sign_digest (ECDSA signature generation for a message digest)
- ECDSA_verify_digest (ECDSA signature verification for a message digest)
- ECDH_generate (ECDH secret key derivation)

The functions ECDSA_keygen, ECDSA_sign_digest and ECDH_generate implement countermeasures against SPA, DPA and DFA for protection of the private key. The function ECDSA_verify_digest implements countermeasures against DFA. The base point is assumed to be public.

Note1) The AH3 Secure RSA/ECC/SHA library supports any valid elliptic curves over prime fields of sizes from 224-bit to 512-bit. However, only the proven standard curves listed below are in the scope of this evaluation.

1) *[NIST curves]*: Curves P-224, P-256, P-384, P-521
2) *[Brainpool curves]*: brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1
3) *[SEC-recommended curves]*: secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1
4) *[RFC7748]:* Curve25519

The AH3 Secure RSA/ECC/SHA library provides functions for calculating hash (digest) values using the SHA1, SHA256, SHA384 and SHA512 algorithms as specified in [FIPS PUB 180-3]. This library implements the following functions for the algorithms SHA256, SHA384 and SHA512:

- SHA_init, SHA_update, SHA_final

These functions which is in AH3 Secure RSA/ECC/SHA library do claim protection against Fault attacks, but do not claim protection against side channel analysis attacks.(i.e. these functions shall not be used to hash confidential information, such as keys etc.) These functions shall be only used for message digest of ECDSA and RSA digital signature. These functions shall not be used for other purposes.

- AH3 Secure ML-DSA library(optional)

  PQC (CRYSTALs) is a hardware coprocessor for high-speed Lattice operations. AH3 Secure ML-DSA library is a software library that is built on the PQC coprocessor that provides high-level interface for ML-DSA
  The ML-DSA functions of the library included in the TOE are

  - Dilithium_library_version_info
  - Key_destruction_mldsa_sec
  - crypto_sign
  - crypto_sign_open
  - crypto_sign_keypair
  - secure_get_parity_from_secret_key_packed_key

- A True Random Number Generator library (TRNG HS_MRO9 library) that fulfills the requirements of Class PTG.2 of BSI-AIS-20/31 (German Scheme).
- The Secure Boot Loader is a loader for copying, authenticating and decrypting firmware from an external FLASH storage into the internal SRAM.

19 The TOE configuration is summarized in Table1-1 below:

Table 1-1 TOE Configuration

Item type	Item	Version	Format	Form of delivery
Hardware	STRONGV4P00 Secure Sub-System on the SoC-related hardware	1.0	-	Hardware Secure Sub System as part of a SoC in a Package-on-Package (PoP)
Hardware	SoC Package	1730-FOWLP-14.0X16.3	-	PoP with DRAM
Hardware	SoC S5E9945, embedding the TOE	1.2	-	SOC in a PoP
Software	Secure Boot loader	1.1	-	Stored in ROM of the STRONGV4P00
Software	AH3 Secure RSA/ECC/SHA Library (optional)	3.10	-	Software Library. This library is delivered as object file and is optionally integrated into user code.
Software	AH3 Secure ML-DSA library (optional)	1.05	-	Software Library. This library is delivered as object file and is optionally integrated into user code.
Software	TRNG HS_MRO9 library	2.4	-	Software Library. This library is delivered as object file and is optionally integrated into user code.
Document	STRONGV4P00 HW TRNG HS_MRO9 and TRNG HS_MRO9 Library Application Note	1.3	PDF	Softcopy
Document	AH3 Secure RSA /ECC/SHA Library API Manual	3.13	PDF	Softcopy
Document	ACT3 MLDSA Library API Manual	1.09	PDF	Softcopy
Document	Hardware User's manual (STRONGV4P00 of S5E9945, 32-bit RISC Microcontroller for Secure Element Platform)	0.5	PDF	Softcopy
Document	Security Application Note for STRONGV4P00	0.6	PDF	Softcopy
Document	S5E9945 Chip Delivery Specification	1.0	PDF	Softcopy
Document	STRONGV4P00 Secure Bootloader Manual for S5E9945	0.1	PDF	Softcopy
Document	CORTEX-M35P Reference manual	0.0	PDF	Softcopy

Table 1-2 Method of Delivery

Item	Method of delivery
Hardware	Secure carrier

Item	Method of delivery
Software	Libraries are encrypted by PGP encryption and then delivered by email.
Documents	Documents are encrypted by PGP encryption and then delivered by e-mail.

20 PRIVILEGE mode and USER mode:

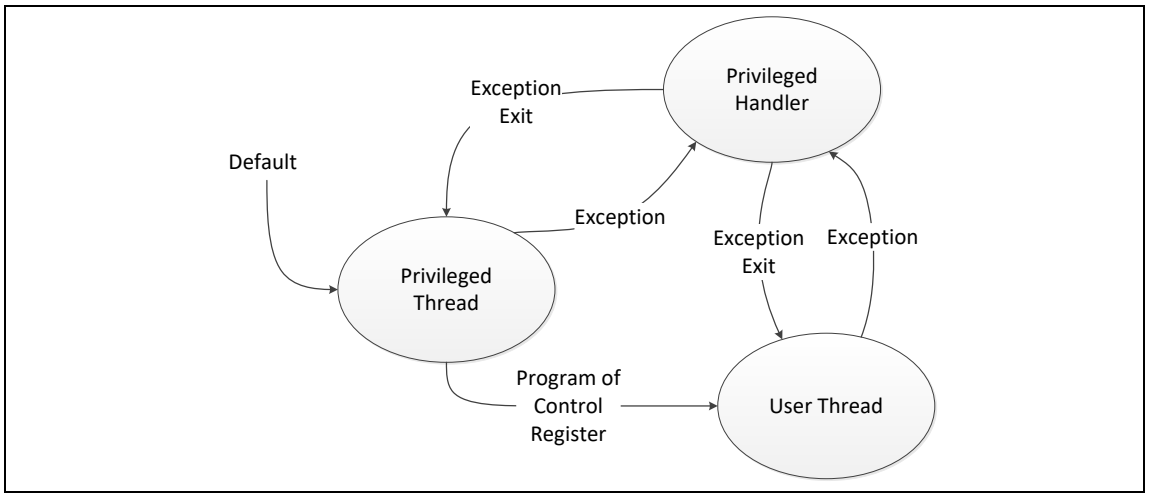


Figure 1-3 Privilege and User Modes

21 Code can execute as privileged or unprivileged (user). Unprivileged execution limits or excludes access to some resources. Privileged execution has access to all resources. Handler mode is always privileged. Thread mode can be privileged or unprivileged.

1.2.3 Usage and Major Security Features of a TOE

22 The TOE can be used for multiple application areas that require a high level of security, including:

- user authentication and password storage
- content protection
- payment
- Subscriber Identity Module (SIM)
- storage and management of digital identities
- secure key storage
- Root of Trust (RoT)
- storage of sensitive user data (e.g., healthcare records).

23 The TOE provides a security service to identify each instance of the 3S and to demonstrate the authenticity of HW and FW.

24 The Security Target defines a basic set of security services and security features that shall be provided by the TOE. The security services and security functionality may be extended to support the additional needs of specific configurations.

25 This Security Target supports the following types of memory:

- memory integrated in 3S inside the TOE perimeter named internal memory (IM)
- external memory outside the TOE perimeter named passive external memory (PM)

26 The details of the configurations with external memories are described in the related sections defining the associated package. The Security Target comprises the configuration with internal memory (IM) and passive external memory (PM). This configuration of the TOE includes all memory resources required for the operation of the TOE. The FW and SW are stored outside the memories of the TOE. Optionally a FW/SW image can be downloaded and verified in the TOE during a FW/SW update operation.

27 The features of the **TOE** are:

28 CPU

- Cortex-M35P 32-bit core (MPU extension up to 4GB)

29 Memory

- ROM, SRAM, Crypto RAM, OTP

30 DES

- Built-in hardware DES accelerator
- Circuits for resistance against side channel and Fault Injection attacks
- ECB mode

* Only Triple DES allowed.

31 AES in "CRYPTO" block and "Security Controller" block

- Built-in hardware AES accelerators
- Circuits for resistance against side channel and Fault Injection attacks
- ECB mode
- CBC mode
- CTR mode
- GCM mode

32 TORNADO-H

- TORNADO-H coprocessor, supporting Montgomery multiplication, modular addition/subtraction and a computation for the square of a Montgomery constant up to 4,128-bit operand sizes

33 Abnormal Condition Detectors

- Environmental & Life Time Detector

34 Interrupts

- Nested Vector Interrupt Controller

35 Reset and Power Down Mode

- Power-on reset and reset sequencer
- Power can be turned off by an external power management unit (Power Down Mode)

36 Random Number Generator

- A True Random Number Generator (TRNG HS_MRO9): PTG.2 class, compliant to BSI-AIS-20/31 (German Scheme)
- A Bilateral Pseudo Random Number Generator (BPRNG): no compliance to any specific metric, but BPRNG is used by the chip internally and for security software countermeasures. It is to be seeded by the TRNG HS_MRO9.

37 Memory Protection Unit

- Memory Protection Unit (MPU)

38 Memory Management Unit

- MMU performs address translation to map physical addresses (PA) to virtual addresses (VA) without setting individual protection attributes for each partition.

39 Memory Encryption and Bus Scrambling

40 Timers

- Timer programmable interval timers
- Watchdog Timer

41 CRC

- CRC32

42 Clock Sources

- Internal clock and external clocks

43 HASH engine

- SHA256/384/512 based on HASH standard-NIST FIPS 180-4
- SHA3 / SHAKE based on HASH standard-NIST FIPS PUB 202

- SHA1-based / SHA2-based / SHA3-based HMAC

44 Operating Voltage Range

45 Operating Temperature

46 Power inputs physically isolated from the SoC power supplies

47 Mailboxes to communicate with external components (application processor, external memories)

48 Secure DMA, inside the Security Controller block (SC_DMA)

49 Secure AXI Bridge

50 Package on Package

- DRAM packaged on top of the SoC package

1.2.4 Required Non-TOE hardware/software/firmware

51 The TOE relies on external memories located outside of the SOC to store contents. Besides that, the TOE makes use of a SoC clock used for TOE-internal counters.

1.2.5 TOE Life cycle

52 The TOE follows the life cycle of the TOE in the Figure 1-4.

53 The role of the TOE Manufacturer during phase 2 (3S hardware development and integration into SoC) is split into activities performed by the 3S Hard Macro Developer and activities performed by the SoC developer.

54 In 3S in SoC Packaging step, the package type of Soc is PoP.

55 In 3S Wafer Testing step, Initialization and Pre-personalization are performed.

Table 1-3 Sites of the TOE life cycle

Site / Building	Phase
Hwasung Plant/ DSR Building	Phase 1
Hwasung Plant/ DSR Building	Phase 2a, Phase 2b
Giheung Plant/ SR3 Building	Phase 3
Hwasung Plant/ Line S3	Phase 3

Giheung Plant/ SR1 Building	Phase 3
Hwasung Plant/ MR2 (NRD) Building	Phase 3
Giheung Plant/ Line 5	Phase 3
Giheung Plant/ Line 3	Phase 3
Giheung Plant/ Line 2	Phase 3
TESNA Plant	Phase 3
Onyang Plant/ Warehouse	Phase 4
Onyang Plant/ Line 2	Phase 3+4

56 The hardware of the 3S needs to be integrated into a hosting SoC. The integration process is applicable if the developers of the 3S and the hosting SoC belong to the same company, or if the 3S developer provides the 3S to an external company.

57 The integration process needs to ensure the integrity and confidentiality of the hard macro delivered by the 3S developer. All interfaces between the TOE and the SoC shall be used as described in the integration guidance. The hosting SoC may provide power supply and control signals as part of the operational environment for the 3S.

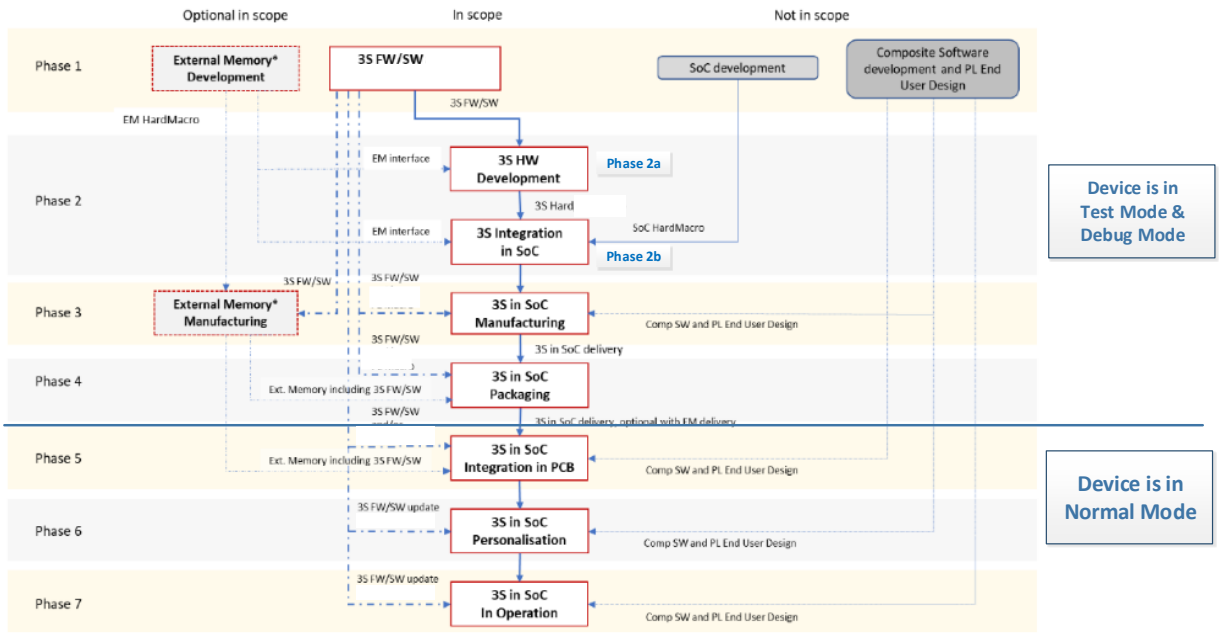
58 The complex hardware and software development process of System on Chips including a 3S can be split into seven generic phases. The form factor and the integration of the SoC are not standardised. Therefore, the life cycle can depend on the intended usage of the Composite Product. This can comprise the SoC packaging but also the download of the software and Composite Software.

59 The development of the hard macro is part of Phase 2, as shown in Figure 1-4. The development of the hosting SoC is also part of Phase 2, because both these developments need to be delivered as one complete product to the wafer fab as part of Phase 3. The development of hardware specific firmware including boot software and drivers are also part of the development in Phase 2, because this software is integrated in the hardware design.

60 The evaluation of the 3S development environment shall include all life-cycle phases that are required to trim, configure and personalise the 3S. After these steps the self-protection of the 3S shall be enabled and ensure the protection of the TOE. If the trimming, configuration and personalisation is done as part of the wafer test at the end of Phase 3, the delivery can be applied at the end of Phase 3. If the trimming, configuration and personalisation is performed after the IC packaging, Phase 4 needs to be in the scope of the evaluation. The external memory is manufactured in Phase 3. After manufacturing, the firmware and software, as well as composite software, might be loaded to the external memory. In the case firmware, software and/or composite software are stored in the external memory, they should be protected.

61 The secure external memory can be evaluated as part of the TOE or may have been evaluated separately, with evaluation results re-used during the evaluation of the TOE, based on the composition approach.

62 The following figure describes the life cycle of the TOE:



Note: Secure External Memory is not in the evaluation scope.

Figure 1-4 Life Cycle of TOE

63 Figure 1-4 describes a typical life cycle with different options of the initial loading and update of FW and SW. All items in dashed lines are optional according to the selected use case. In most cases, the delivery type of the SoC including the 3S is performed at the end of Phase 3 or Phase 4. The SoC development and the development of the Composite Application (Comp APP) are out of evaluation scope.

1.2.5.1 Phase 1: 3S Firmware and Software Development

64 The TOE SW can be stored either in the 3S or in external non-volatile memory.

65 Phase 1 also includes the design and development of the Composite Software for the 3S. Depending on the configuration, the Composite Software is stored on the 3S or is stored in the external non-volatile memory. If the Composite Software is remotely loaded using a secure loader, this loader shall be in the scope of the evaluation. Based on the use of a secure loader, life-cycle phase or the site where the download is applied are not security relevant.

1.2.5.2 Phase 2: 3S hardware development and integration into SoC

66 There are following two parts in Phase 2

- Phase 2a: where the 3S is developed
- Phase 2b: where the 3S is integrated into the SoC by the SoC developer.
  Note: In this ST, TOE(STRONGV4P00 3S) is only integrated in the S5E9945 SoC. This ST does not cover the case in which the TOE is integrated into a different SoC.

67 TOE, STRONGV4P00 Secure Sub-System, is delivered at the end of Phase 2a for SoC integration, which would happen in Phase 2b.

68 Comprises the development of the 3S hard macro and associated firmware. Phase 2 also comprises the development of the SoC hardware with the interfaces to the 3S. The development of the SoC is not in the scope

of the evaluation. The scope of the evaluation for Phase 2 is determined by the transfer of the 3S hard macro to the developer of the hosting SoC.

69 The deliverables of the 3S development comprise a hard macro and/or a Programmable Logic macro, associated guidance for the integration of the 3S as well as preparation of FW/SW code that is integrated in the ROM of the 3S. The protection of the 3S design has to be ensured by the development environment. The integration of 3S hard macro on the SoC is performed in this life-cycle step. In addition, the 3S can run on a SoC simulation.

70 The integration of the 3S on the SoC needs to be completed before the complete SoC is delivered to the mask shop or wafer fab that belongs to life-cycle Phase 3. The delivery needs to include all components that are required for production of the SoC including the 3S. This comprises the hardware design of the SoC including the 3S, the FW and the SW. Components of the Security Anchor, as well as credentials for production/preparation required for production, also need to be part of the delivery. The 3S design is protected by limiting the 3S design block to the information required for the integration and by protecting the integration environment of the SoC with the 3S. The transfer of the SoC including the 3S to the production shall protect the confidentiality and integrity of the complete design.

1.2.5.3 Phase 3: 3S in SoC Manufacturing

71 The manufacturing of external memory can be included as option.

72 The manufacturing comprises the production and the functional testing of the SoC, including the 3S. The tests of the 3S can be mainly independent of the SoC or they may be integral part of the test applied for the SoC. The testing in this phase can also include the initialisation and personalisation of the TOE.

73 The scope of the evaluation shall include the complete trimming, initialisation and pre-personalisation of the 3S. The scope of the evaluation can be limited to Phase 3, if these steps are all performed in Phase 3 and the self-protection of the 3S is active at the end of Phase 3.

74 At the end of Phase 3 also parts of the FW/SW for the 3S can be loaded into internal memories of the 3S. For secure external memory, FW/SW can be stored in the secure external memory at the end of Phase 3.

75 The exchange of software and scripts between the 3S developer and the test centre required for the testing, initialisation and personalisation needs to be described and considered during the evaluation.

76 The SoC including the 3S can be delivered to the customer at the end of this life-cycle phase. The 3S integrated in the SoC, as well as FW and SW can be delivered together, but this is not mandatory because the external memory may not be integrated in this life-cycle phase.

1.2.5.4 Phase 4: 3S in SoC Packaging

77 TOE, STRONGV4P00 3S on the S5E9945 SoC, is delivered at the end of Phase 4.

78 The packaging comprises the assembly of the SoC in a package. This may include the stacking of the SoC with memory in the same package. The packaged devices are subsequently tested. These tests also can comprise additional trimming, initialisation and personalisation of the 3S, if this is not completed in Phase 3. In addition, loading of SW or Composite Software can be performed in this life-cycle phase if the trimming, initialisation and personalisation are completed and the required non-volatile memory is already available.

79 At the end of this life-cycle phase the SoC including the 3S is packaged. This package is ready for the integration on a PCB.

80 The packaged SoC can be considered as delivery item in the scope of the evaluation, if the self-protection is enabled at the end of Phase 4 and the additional loading of SW or Composite Software on the 3S or in the memory does not require a secure environment.

1.2.5.5 Phase 5: 3S in SoC Integration in PCB

81 The SoC integration in PCB comprises further integration step, as soldering in the PCB. If the self-protection of the 3S is already enabled in preceding life-cycle phases, this phase does not need to be part of the evaluation.

82 The non-volatile memory may be integrated in this phase, so the SW stored in the external non-volatile memory might initially be downloaded in this life-cycle phase. It depends on the security mechanisms implemented in the loader of the 3S and security policy of the software, if the loading of the SW requires a trusted environment.

1.2.5.6 Phase 6: 3S in SoC Personalisation

83 Phase 6 is the personalisation phase that may also include customer specific configuration of the 3S. The 3S developer may leave configuration tasks to the personaliser. Such tasks are considered to be part of the preparative guidance for the 3S. In this personalisation phase an authorised user can perform an optional update of the 3S FW or SW. The user may be the administrator of this life-cycle phase.

1.2.5.7 Phase 7: 3S in SoC in Operation

84 Phase 7 is the operational phase, where the administrator operates the 3S in SoC and the end-user uses the device including the 3S in SoC.

1.3 Functional Packages

This Security Target includes several optional packages to extend the security functionality of the base Protection Profile [5] including the use of external memory. For details, see Chapter 7.

Each package defines a specific security problem, a set of security objectives and the corresponding Security Functional Requirements (SFRs).

The following figure illustrates the packages defined in this ST:

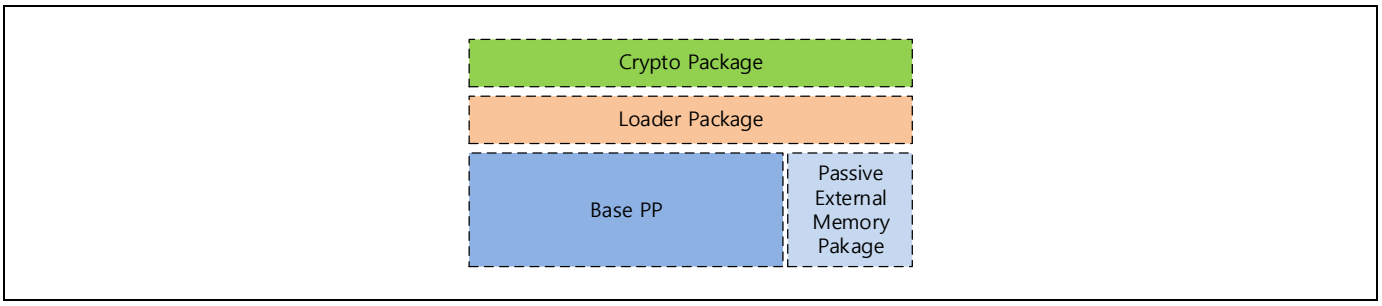


Figure 1-5 Package structure of this Security Target

Table 1-5 Overview of the functional packages

Package Name	Package Purpose	Reference
Base PP	-	Sections 3 to 6
Passive External Memory Package	The 3S is connected to a passive external memory. Neither the passive external memory nor the connection between the passive external memory and the 3S provide protection for software and data. The 3S shall protect software and data before it is transferred from or to the passive external memory.	Section 7.1
Loader Package	Loading of 3S SW or Composite Software from external memory. The package defines rigorous security functionality to restrict the loading of authenticated images with integrity protection prior to the execution by the TOE.	Section 7.2
Crypto Package	The package provides a framework for the integration of various cryptographic algorithms supported by the TOE.	Section 7.3

1.4 Interfaces of the TOE

85 TOE has the following interfaces:

- The physical interface of the TOE with the external environment is the entire surface of the STRONGV4P00
- The electrical interfaces of the TOE with the external environment are AVDD12_LDO_STR, AVDD18_LDO_STR, VDD_ALIVE, AVSS_LDO_STRONG.

- The data interfaces of the TOE consists of Mailboxes, Secure DMA (SC_DMA), I2C to Secure Flash and the Secure AXI Bridge (BAAW, Long Hop (LHS))
- The software interfaces of the TOE with the hardware consist of Special Function Registers (SFR) and CPU instructions
- The TRNG HS_MRO9 interface of the TOE is defined by the TRNG HS_MRO9 libraries interface
- The PKA interface of the TOE is defined by the AH3 Secure RSA/ECC/SHA library interface (optional).
- The Secure Boot Loader interface

2 CONFORMANCE CLAIMS

2.1 CC Conformance Claim

86 This Security target claims to be conformant to the Common Criteria version 3.1 R5.

87 Conformance of this Security Target with respect to CC Part 1 (Introduction and general model), see [1].

88 Conformance of this Security Target with respect to CC Part 2 (security functional components) is CC Part 2 extended, see [2].

89 Conformance of this Security Target with respect to CC Part 3 (security assurance components) is CC Part 3 conformant, see [3].

2.2 PP Claim

90 This Security Target is strictly compliant to the Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [5]. The Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile is registered and certified by the Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0117, Version 1.5, dated 28 Feb.2022

91 This ST does not claim conformance to any other PP.

2.3 Package Claim

92 The assurance level for this Security Target is EAL5 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.2.

93 This Security Target is strictly compliant to the Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile[5] with additional packages:

- Package “Passive External Memory”
- Package “Loader Functionality”
- Package “Cryptographic Services”

2.4 Conformance Claim Rationale

94 This security target claims strict conformance only to one PP, the Security IC Platform Protection Profile [5].

95 The minimum Evaluation Assurance Level (EAL) of the PP[5] is EAL 4, augmented with the assurance components ATE_DPT.2, ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2. However, the Assurance Requirements of the TOE obtain the Evaluation Assurance Level 5, augmented with the assurance components ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2.

96 The Target of Evaluation (TOE) is a complete solution, implementing a secure integrated circuit (secure IC) as defined in the PP[5], section 1.2.2, so the TOE is consistent with the TOE type in the PP[5].

97 The security problem definition of this security target is consistent with the statement of the security problem definition in the PP[5], as the security target claims strict conformance to the PP[5]. Additional threats, organizational security policies and assumptions are introduced in chapter 3 of this ST. A rationale is given in chapter 4.

98 The security objectives of this security target are consistent with the statement of the security objectives in the PP[5], as the security target claims strict conformance to the PP[5]. Additional security objectives are added in chapter 4.1 of this ST. A rationale is given in chapter 4.3.

99 The security requirements of this security target are consistent with the statement of the security requirements in the PP[5] as the security target claims strict conformance to the PP[5]. Additional security requirements are added in chapter 6.1 of this ST. A rationale is given in chapter 6.3. All assignments and selections of the security functional requirements are done in the PP[5] and in section 6 of this security target.

2.5 Conformance Statement

100 This security target claims strict conformance only to one PP, the Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile [5].

3 SECURITY PROBLEM DEFINITION

3.1 Description of Assets

101 The assets of the TOE are:

- user data of the TOE and the user data of the Composite Software[1]
- TSF data, including root keys and keys derived from root keys, as well as the unique identification of the TOE instances
- firmware/software that is part of the TOE and the Composite Software, stored and in operation
- security services provided by the TOE for the Composite Software

102 The end-user of the TOE places value upon the assets related to high-level security concerns:

SC1: integrity and authenticity of user data,

SC2: confidentiality of user data of the TOE and the Composite TOE being stored in the TOE's protected memory areas,

SC3: correct operation of the security services including the root of trust provided by the TOE for the Composite Software.

103 The Composite Software is user data and shall be protected while being executed/processed and while being stored in the TOE's protected memories.

104 The TOE may not distinguish between user data which is publicly known or kept confidential. Therefore, the TOE supports the protection of the user data in integrity, authenticity and confidentiality if stored in protected memory areas, unless the Composite Software chooses to disclose or modify it.

105 The integrity and authenticity of the software including Composite Software means that it is correctly being executed. This includes especially the correct operation of the TOE's security services including the root of trust. Parts of the FW, SW and Composite Software that do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the FW, SW and Composite Software may need to be kept confidential, because specific implementation details may assist an attacker.

106 The TOE Manufacturer shall apply protection to support the security of the TOE. This applies to the TOE and to all information and material exchanged with the developer of the Composite Software. This covers the Composite Software itself or any authentication data required to enable the installation of software in the TOE, including in phases after TOE Delivery.

107 The TSF processes user data objects (code and/or data) as well as TSF data objects. User data objects are imported, used in cryptographic operation, temporarily stored, exported and may be destroyed after use. They may contain cryptographic keys with or without security attributes, certificates and authentication data

[1] The Composite Software as well as the User Data of the Composite Software are both considered as part of the User Data of the TOE. The TOE, however, may allow different protection mechanisms for code and data. Therefore, they are mentioned separately in the assets.

of a device/user. Cryptographic keys are objects of the key management.

108 As stated in section 1.2.2, this Security Target requires the TOE to provide generation of random numbers security service by means of a physical Random Number Generator. Section 7.3 provides a general optional package for cryptographic services.

109 According to this Security Target, there is the following high-level security concern related to Random Number Generator security service:

SC4: deficiency of random numbers.

3.2 Threats

110 The threats described in this section are applicable to the base Protection Profile [5]. For threats related to functional extensions see Chapter 7.

111 The following figure describes the attacks that are applicable to the TOE. The interactions related to the attacks are marked with red arrows.

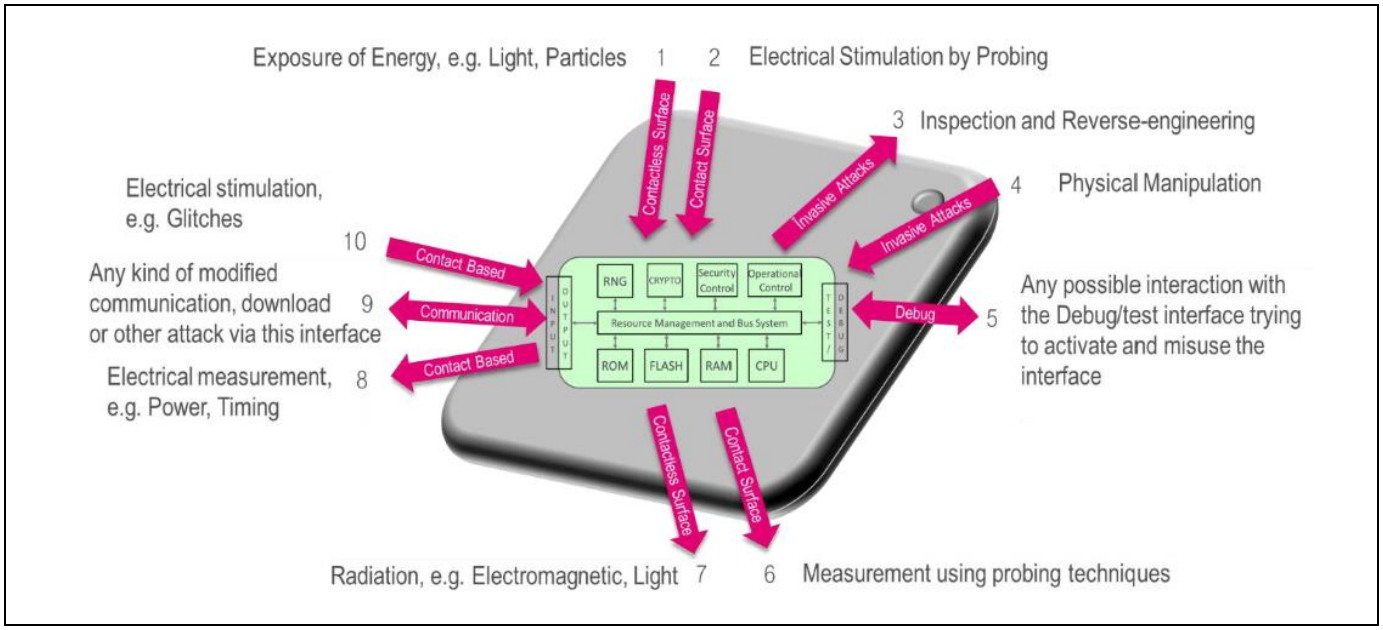


Figure 3-1 Attacks against the TOE

112 The Grey box represents the SoC and the green box represents the 3S. The 3S comprises various interfaces (see Figure 3-1), the dedicated interfaces are named in the threat description. Attacks may be applied on the internal interface between the 3S and the SoC or attacks may be applied from outside the SoC if an interface of the SoC is directly connected to the 3S. This depends on the implementation of the 3S. E.g., exposure to light is directly applicable to the 3S because it is part of the SoC substrate, while direct probing is possible only if the 3S uses all metal layers of the design. For the communication interface it depends whether remote connections are directly routed to the 3S or whether parts of the protocol stack are included in an application running on the SoC.

113 The surface of the 3S does not provide an interface from a functional point of view, but it is considered to be an interface for an attacker.

114 The TOE shall avert the threat "Inherent Information Leakage (T.Leak-Inherent)" as specified below.

T.Leak-Inherent	Inherent Information Leakage

An attacker may exploit information , as user data or TSF data, which is leaked from the TOE and/or the SoC interfaces while being stored and/or processed by the TOE.

115 Leakage may occur through emanations, variations in power consumption, response times, clock frequency, or similar variations in the behaviour, based on the data processed by the TOE. This leakage is related to measurement of operating parameters, which may be derived either from measurements of internal and/or external supply signals and/or measurement of emanations and/or IO signal. These operating parameters can then be matched to the specific operations inside the TOE. Examples of such attacks are Differential Power Analysis and Timing Attacks (8 in Figure 3-1 or analysis of emanation (7 in Figure 3-1)

116 The leakage may also be generated by the hosting SoC. It may not be possible to split between the power analysis of the TOE and of the SoC. This may make an attack more difficult but does not prevent attacks. Inherent emanation leakage may be identifiable also outside the TOE boundaries on the surface of the SoC and does not require direct contact with TOE internal signals.

117 The TOE shall avert the threat "Physical Probing (T.Phys-Probing)" as specified below.

T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE. The probing is performed (i) to disclose user data or TSF data while stored in protected memory areas, (ii) to disclose/reconstruct user data or TSF data while processed or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating user data of the composite TOE or the Composite Software.

118 Physical probing requires direct interaction with the hardware of the TOE inside the TOE boundary or at the border of the TOE. Physical probing done at the SoC level may also be used, however, to gain knowledge of the TOE.

119 Techniques and tools commonly employed in failure analysis and reverse engineering may be used for such attacks (2 and 6 in Figure 3-1). Before hardware security mechanisms and layout characteristics can be attacked, they need to be identified by reverse engineering. The analysis of software behaviour or processing of user data or TSF data may also be a prerequisite for the attack.

120 The TOE shall avert the threat "Malfunction due to Environmental Stress (T.Malfunction)" as specified below.

T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of security services provided by the platform by applying environmental stress to the SoC or the 3S, to (i) modify security services of the TOE or (ii) modify Composite Software including composite user data while being processed by security services of the platform, or (iii) deactivate or affect the TSF to enable disclosure or manipulation of user data. An attacker may also cause malfunction by (iv) modifying data or messages, or by (v) misuse of architectural and micro architectural weaknesses via control and communication interfaces.

121 The environmental stress can either directly be applied to the TOE or introduced via the interfaces of the SoC that integrates the 3S. The attacker may apply the environmental stress to the SoC without knowledge of details regarding the location and interaction between the TOE and the SoC hosting the 3S. Beside the environmental stress also logical attacks can cause malfunctions and impact the security features and security services.

122 The modification of security services of the TOE may affect the quality of random numbers provided by the random number generator, the malfunction of cryptographic coprocessors or the manipulation of TSF data or user data stored in the volatile memory. An attacker needs information about the functional operation. Based on this information the attacker can introduce a temporary failure by exposing energy to the 3S (1 in Figure 3-

1) or (10 in Figure 3-1). This may be achieved by operating the TOE outside the normal operating conditions. The same attack techniques applied at SoC interfaces level could also provoke malfunction of the TOE.

123 Modification of security services, circumvention of access control or forced leakage may also be achieved by exploiting physical, architectural or micro architectural weaknesses at the interfaces of the 3S, or disturbing or modifying the communication (9 in Figure 3-1) between the SoC and the 3S, or exposure of energy (1 in Figure 3-1) or glitches on the interfaces (10 in Figure 3-1) causing errors that lead to an exploitation of these weaknesses.

124 The TOE shall avert the threat "Physical Manipulation (T.Phys-Manipulation)" as specified below.

T.Phys-Manipulation	Physical Manipulation An attacker may physically modify the TOE or the SoC, to (i) modify user data of the Composite Product, (ii) modify the Composite Software, (iii) modify or deactivate security services of the TOE, or (iv) modify TSF of the TOE to enable attacks disclosing or manipulating TSF data, user data or the Composite Software.

125 The modification may be achieved through techniques commonly employed in failure analysis and reverse engineering efforts (numbers 3 and 4 in Figure 3-1). The modification may result in the deactivation of a security features. To apply this attack, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of user data of the Composite Product may also be a prerequisite. Changes of circuitry or data can be permanent or temporary. Some physical manipulations done at the SoC level could be used to gain knowledge of the TOE.

126 The TOE shall avert the threat "Forced Information Leakage (T.Leak-Forced)" as specified below:

T.Leak-Forced	Forced Information Leakage An attacker may disclose user data or TSF data, which is leaked from the TOE when such data is processed or stored by the TOE even if the information leakage is not inherent but caused by the attacker by influencing the TOE or the hosting SoC.

127 This threat pertains to attacks where environmental stress or physical manipulation is applied to the TOE or the hosting SoC to cause leakage from signals which do not compromise user data or TSF data during normal operation. This threat pertains to attacks where methods described in "Malfunction due to Environmental Stress" (see T.Malfunction) and/or "Physical Manipulation" (see T.Phys-Manipulation) are used to cause leakage from signals (Numbers 5, 6, 7, 8 or 9 in Figure 3-1) that normally do not contain significant information about secrets.

128 The threat also covers any influence of the SoC (e.g., by modification of the power management causing environmental stress without glitching or physical manipulation). Such threats may also force leakage of significant information about assets processed by the TOE. The same attack techniques applied at SoC interfaces level could also result in disclosure of sensitive data.

129 The TOE shall avert the threat "Abuse of Functionality (T.Abuse-Func)" as specified below.

T.Abuse-Func	Abuse of Functionality An attacker may misuse functions of the TOE which are disabled before the TOE is delivered. The misuse is applied, to (i) disclose or manipulate TSF data or user data, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE or (iii) manipulate (explore, bypass, deactivate or change) functions of the TOE FW/SW and of the Composite Software, or (iv) enable an attack disclosing or manipulating user data or the Composite Software.

130 This threat comprises the misuse of test and debug functionality provided by the TOE (5 in Figure 3-1). Further on an attacker may misuse or manipulate functions intended for the configuration and life-cycle

control of the TOE. This can comprise one or more interfaces either between the TOE and the SoC or interfaces providing external access to the TOE. Conducting attacks through SoC debug or tests interfaces could also have an impact on the TOE protection.

131 The TOE shall avert the threat "Deficiency of Random Numbers (T.RND)" as specified below.

T.RND	Deficiency of Random Numbers An attacker manipulates or influences the random number generator to reduce the entropy, to predict or obtain information about random numbers generated by the TOE. An attacker may also predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

132 This threat addresses the analysis of random numbers generated by the TOE security services under the various conditions under the control of an attacker. Unpredictability is the main property of random numbers, so this may be a problem if they are used to generate cryptographic keys or blinding parameters, for example. The entropy provided by the random numbers shall be appropriate for the strength of the cryptographic algorithm, the key, the cryptographic variable (e.g., masking) they are used for. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers. The attack applies to random numbers used by the TOE or provided by the TOE as security services.

133 The TOE shall avert the threat "Insecure State of the TOE (T.Insecure-State)" as specified below. An insecure boot process can occur during attacks, such as error manipulation of the TOE or hosting SoC manipulation that impacts the boot process. The attack may lead to a wrong initialisation of security services or security features, or the acceptance, import and execution of hostile software.

T.Insecure-State	Insecure State of the TOE An attacker disturbs the boot process of the TOE by interrupting the boot process or introducing faults using T.Malfunction or T.Phys-Manipulation during start-up, which may force malicious code execution or TSF data manipulation. In this way, an attacker may (i) force invalid settings of the TOE hardware (e.g., life-cycle state, trimming, etc.), (ii) load and execute unauthenticated firmware and/or software, (iii) masquerade the unique identity, or (iv) archive an inconsistent initialisation of the Root of Trust in order to compromise secrets or enable other threats.

134 This threat attacks the secure operation of the TOE and the TOE specific initialisation and configuration during start-up. The initialisation of Root of Trust during the boot process also may be violated by an attacker (see T.Malfunction and T.Phys-Manipulation for applicable attack technics).

135 The TOE shall avert the additional threat "Memory Access Violation (T.Mem-Access)" as specified below.

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 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 T.Abuse-Func but for functions available after TOE delivery), (ii) introduce flaws by forcing operational conditions (refer to T.Malfunction) and/or by physical manipulation (refer to T.Phys-Manipulation). This attacker is expected to have a high level potential of attack.

3.3 Organizational Security Policies

136 This section describes the policies applied in this Security Target.

137 The following organisational security policies need to be applied.

138 Either the 3S Developer or the 3S Integrator shall apply the policy "Identification of each TOE instance (P.Gen-Unique-ID)" as specified below.

P.Gen-Unique-ID: Identification of each TOE instance

An accurate identification shall be established for the TOE. The policy requires that each instantiation of the TOE stores its own unique identification.

139 A unique identification shall be stored on each instance of the TOE. The testing, trimming and configuration of the TOE after production shall include the download of the unique identification. These processes are in the evaluation scope of the life cycle and performed before the TOE is delivered. The unique identification also considers that the TOE may be delivered to different 3S integrators performing their own configuration and trimming of the TOE.

3.4 Assumptions

140 The following section describes the assumptions applied in this Security Target.

141 Appropriate "Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)" shall be ensured after TOE Delivery up to the end of Phase 5, as well as during the delivery to Phase 6 as specified below.

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

It is assumed that security procedures are in place after delivery of the TOE (3S included in the SoC) up to delivery of the device to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (including the prevention of any possible copy, modification, retention, theft or unauthorised use).

142 The protection of the TOE is required until the delivery of the product (including the TOE) to the end-user. The assembly and integration processes are part of the evaluated life-cycle scope until the initialisation and pre-personalisation is completed. The TOE needs to be controlled and protected, however, until it is delivered to the end-user.

143 The Composite Software shall ensure the appropriate "Treatment of user data of the Composite Product (A.Resp-Appl)" as specified below.

A.Resp-Appl Treatment of user data of the Composite Product

It is assumed that user data of the Composite Product is owned by the Composite Software and treated as required for the specific application context if processed by the Composite Software. Therefore, the Composite Software shall fulfil the guidance of the 3S when security relevant code of the Composite Software is executed and/or security relevant user data of the Composite Product is processed by the Composite Software (especially cryptographic keys).

144 The application context specifies how the user data of the Composite Product shall be handled and protected. The evaluation of the 3S HW, FW and SW according to this Security Target is conducted on generalised application context. The concrete requirements for the Composite Software shall be defined in the Protection Profile [respective Security Target] of the Composite Product. The 3S cannot prevent any compromising or modification of user data of the Composite Product by malicious Composite Software.

4 SECURITY OBJECTIVES

145 This chapter describes the security objectives.

4.1 Security Objectives for the TOE

146 The user has the following high-level security goals related to the assets:

SG.1 maintain the integrity of user data (when being executed/processed and when being stored in the TOE's memories)

SG.2 maintain the confidentiality of user data (when being processed and when being stored in the TOE's protected memories).

SG.3 maintain the correct operation of the security services provided by the TOE for the Composite Software.

SG.4 maintain the authenticity of the boot sequence and the setup of the root of trust.

SG.5 maintain the confidentiality, integrity and authenticity of the keys belonging to the Root of Trust.

147 The integrity of TSF data as well as FW and SW as described in SG.1 are inherently covered because they are part of the TOE. Confidentiality is required for User Data. TSF data require confidentiality, in case the TSF data can be used to extract sensitive User Data without further information. The provisioning of random numbers is a security service covered by SG.3. The random numbers may also be used by the 3S, however, for internal purposes.

148 Note that the 3S does not distinguish between user data that are publicly known or kept confidential. Therefore, the 3S shall protect the user data in integrity and in confidentiality if stored in protected memory areas, unless the Composite Software chooses to disclose or modify this user data. Parts of the Composite Software which do not contain secret data or security critical source code, may not require protection from being disclosed. Other parts of the Composite Software may need to be kept confidential because specific implementation details can assist an attacker.

149 These standard high-level security goals in the context of the security problem definition build the starting point for the definition of security objectives as required by the Common Criteria. Note that the integrity of the TOE is a means to reach these objectives.

150 The TOE shall provide "Protection against Inherent Information Leakage (O.Leak-Inherent)" as specified below.

O.Leak-Inherent	Protection against Inherent Information Leakage The TOE shall provide protection against disclosure of confidential TSF data and user data stored and/or processed in the 3S (i) by measurement and analysis of the shape and amplitude of any signal at the interfaces of the 3S (e.g., on the power, clock, or I/O lines) and/or (ii) by measurement and analysis of the time between events found by measuring signals (e.g., on the power, clock, or I/O lines).

151 This objective pertains to measurements with subsequent complex signal processing whereas O.Phys-Probing is about direct measurements on elements on the chip surface. Details correspond to an analysis of attack

scenarios, which are not given here.

152 The TOE shall provide "Protection against Physical Probing (O.Phys-Probing)" as specified below.

O.Phys-Probing	Protection against Physical Probing The TOE shall provide protection against disclosure and reconstruction of user data or TSF data while stored in protected memory areas and processed by the TOE. This comprises also disclosure of other critical information about the operation of the TOE. This protection comprises (i) measuring through contacts which is direct physical probing on the chip surface except on pads being bonded (using standard tools for measuring voltage and current) or (ii) measuring not using direct contacts but other types of physical interaction between charges (using tools used in solid-state physics research and IC failure analysis) with a prior reverse-engineering to understand the design and its properties and functions.

153 The TOE shall be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

154 The TOE shall provide "Protection against Malfunctions (O.Malfunction)" as specified below.

O.Malfunction	Protection against Malfunctions The TOE shall ensure its correct operation. The TOE shall indicate or prevent its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested to prevent malfunctions. Examples of environmental conditions are voltage, clock frequency, temperature, or external energy fields. Further on, the TOE detects abnormal interface behaviour and/or protocol parameters or protocol sequences that do not meet the specified behaviour.

Remark: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (see O.Phys-Manipulation) provided that detailed knowledge about the TOE´s internal construction is required and the attack is performed in a controlled manner.

155 The TOE shall provide "Protection against Physical Manipulation (O.Phys-Manipulation)" as specified below.

O.Phys-Manipulation	Protection against Physical Manipulation The TOE shall provide protection against manipulation of the TOE hardware, software and data including FW, SW, TSF data, the Composite Software and the user data of the Composite Product. This comprises protection against (i) reverse-engineering (understanding the design and its properties and functions), (ii) manipulation of the hardware, security services and any sensitive data, as well as (iii) undetected manipulation of TOE memory content.

156 The TOE shall be designed and fabricated so that it requires a high combination of complex equipment, knowledge, skill, and time to be able to derive detailed design information or other information which could be used to compromise security through such a physical attack.

157 The TOE shall provide "Protection against Forced Information Leakage (O.Leak-Forced)" as specified below:

O.Leak-Forced	Protection against Forced Information Leakage

The 3S shall be protected against disclosure of confidential user data or TSF data processed or stored in the 3S (using methods as described under O.Leak-Inherent) even if the information leakage is not inherent but caused by the attacker (i) by forcing a malfunction (see "Protection against Malfunction due to Environmental Stress (O.Malfunction)" and/or (ii) by a physical manipulation (see "Protection against Physical Manipulation (O.Phys-Manipulation)".

158 If the protection against forced information leakage is not effective, signals that normally do not contain significant information about secrets could become an information channel for a leakage attack.

159 The TOE shall provide "Protection against Abuse of Functionality (O.Abuse-Func)" as specified below.

O.Abuse-Func	Protection against Abuse of Functionality The TOE shall prevent functions of the TOE that may not be used after TOE Delivery from being abused and forced to (i) disclose critical TSF data or user data of the Composite Product, (ii) manipulate critical TSF data or user data of the Composite Product, (iii) manipulate Composite Software, or (iv) bypass, deactivate, change or explore security features or security services of the TOE. This also comprises the protection of Test features and/or Debug features provided by the HW, FW and SW of the 3S, which support the development and production of the TOE.

160 The TOE shall provide "Random Numbers (O.RND)" as specified below.

O.RND	Random Numbers The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have a sufficient entropy. The TOE will ensure that no information about the generated random numbers is available to an attacker since they might be used for instance to generate cryptographic keys. The TOE shall detect and/or prevent manipulation or influence of the entropy source to ensure cryptographic quality of random number generation.

Application Note 4-1(PP_AN 24)	The TOE adds the Security Objective O.Mem-Access to counter the threat T.Mem-Access.

161 The TOE shall provide "Secure start-up and re-start (O.Secure-State)" as specified below.

O.Secure-State	The TOE shall be started through a secure initialisation process that ensures (i) integrity and authenticity of code executed during start-up, (ii) integrity and authenticity of the hardware settings and the initialisation during start-up including the secure start-up of the Root of Trust functionality.

162 The TOE shall provide "TOE Identification (O.Identification)" as specified below:

O.Identification	TOE Identification The TOE shall provide means to store a unique identifier that allows the unique identification of the TOE. Further on, the TOE shall be able to store further initialisation data and pre-personalisation data in non-volatile memory. The unique

identifier, the initialization data and the pre-personalisation data are protected against modification.

163 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 Security IC 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 Environment

164 The Security Objectives for the Environment are split according to the different life-cycle phases.

4.2.1 Security Objectives for the Composite SW (Phase 1)

165 The development of the Composite Software is outside the development and manufacturing of the TOE. The Composite Software defines the operational use of the TOE. This section describes the security objective for the Composite Software.

166 Note that, to ensure that the TOE is used in a secure manner, the Composite 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 Firmware (FW), Software (SW) of the TOE, and (iii) TOE application notes and other guidance documents that are included in the evaluation of the TOE.

167 Note that findings of the TOE evaluation need to be addressed in the guidance for the development of Composite Software.

168 The Composite Software shall provide "Treatment of user data of the Composite Product (OE.Resp-Appl)", as specified below.

OE.Resp-Appl	Treatment of user data of the Composite Product
	Security relevant user data of the Composite Product (especially cryptographic keys) are treated by the Composite Software as required by the security needs of the specific application context.

169 E.g., the Composite Software will not disclose security relevant user data of the Composite Product to unauthorised users or processes when communicating with the remaining SoC or SoC external entities.

4.2.2 Security Objectives for Test and Pre-Personalisation of the 3S (Phases 3 to 5)

170 The pre-personalisation environment shall ensure "Uniqueness and authenticity of the device individual identifier" (OE.Secure-Initialisation).

OE.Secure-Initialisation	Uniqueness and authenticity of the device individual identifier
	Security procedures shall be applied during the initialisation of the TOE, to ensure that each device is loaded with an individual identifier. The identifier shall allow the unique identification of each device in later life cycle phases.

171 Phases after the initialisation can use the individual identifier for tracking and further provisioning. Depending on the application context, the tracking may not be possible in the operational phase of the 3S.

4.2.3 Security Objectives for the Operational Environment after TOE Delivery

172 Appropriate "Protection during Packaging, Finishing and Personalisation (OE.Process-Sec-IC)" shall be ensured after TOE Delivery up to the end of Phase 5, as well as during the delivery to Phase 6 as specified below.

OE.Process-Sec-IC	Protection during Composite Product manufacturing Security procedures shall be applied after TOE Delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft, or unauthorised use).

173 This means that phases after TOE Delivery up to the end of Phase 5 shall protect the TOE appropriately.

4.3 Security Objectives Rationale

	O.Leak-Inherent	O.Phys-Probing	O.Malfunction	O.Phys-Manipulation	O.Leak-Forced	O.Abuse-Func	O.RND	O.Secure-State	O.Mem-Access	O.Identification	OE.Resp-Appl	OE.Secure-Initialisation	OE.Process-Sec-IC
T.Leak-Inherent	X												
T.Phys-Probing		X											
T.Malfunction			X										
T.Phys-Mani-pulation				X									
T.Leak-Forced			X	X	X								
T.Abuse-Func						X							
T.RND							X						
T.Insecure-State								X					
T.Mem-Access									X				
P.Gen-Unique- ID:										X		X	
A.Resp-Appl											X		
A.Process-Sec-IC													X

Table 4-1 Security Objectives versus Assumptions, Threats and Policies

174 T.Leak-Inherent is countered by O.Leak-Inherent, because the objective requires the protection of confidential TSF data and user data against leakage while being processed and/or stored by the TOE.

175 T.Phys-Probing is countered by O.Phys-Probing, because the objective requires protection against disclosure and reconstruction of user data or TSF data while stored in protected memory areas and processed by the TOE. In addition, protection is required for disclosure of other critical information about the operation of the TOE.

176 T.Malfunction is countered by O.Malfunction, because the objective requires indication of operation outside reliable and secure operating conditions or prevent the operation outside the normal operating conditions. Further on, the objective requires the detection of abnormal interface behaviour and protocol parameters or protocol sequences that do not meet the specified behaviour.

177 T.Phys-Manipulation is countered by O.Phys-Manipulation, because the objective requires protection against manipulation of the TOE comprising TOE hardware, software including FW, SW, TSF data, the Composite Software and TSF data as well as user data of the Composite Product. The protection covers reverse engineering, manipulation of hardware and security services as well as undetected modification of TOE memory content.

178 T.Leak-Forced is countered by O.Leak-Forced, because the objective requires the protection against leakage even if the leakage is caused by an attacker trying to force malfunction and/or physical manipulation. Physical manipulation or environmental stress may be used to force leakage, so the protection against physical manipulation provided by O.Phys-Manipulation and the protection against malfunctions provided by O.Malfunction support the resistance against the threat T.Leak-Forced.

179 T.Abuse-Func is countered by O.Abuse-Func, because the objective requires to prevent the abuse of TOE functions which are disabled before TOE Delivery. The considered abuse covers disclosure or manipulation of critical TSF data or user data of the Composite Product as well as manipulation of Composite Software and bypass, deactivation, change or exploitation of security features or security services of the TOE, including test and debug functionality.

180 T.RND is countered by O.RND, because the objective requires detection and/or prevent manipulation or influence of the entropy source to ensure cryptographic quality of random number generation.

181 T.Insecure-State is countered by O.Secure-State, because the objective requires a secure initialisation process that ensures integrity and authenticity of code executed during start-up as well as integrity and authenticity of the hardware configuration including the Root of Trust after start-up.

182 The assumption related to the organisational security policy “Identification of each TOE instance (P.Gen-Unique-ID)” is as follows:

183 O.Identification requires that the TOE supports the possibility of a unique identification. The unique identification can be stored in the TOE. The unique identification is generated by the production environment, so the production environment shall support the integrity and initialisation of the generated unique identification as required by OE.Secure-Initialisation. The technical and organisational security measures that ensure the security of the testing and initialisation environment are evaluated, based on the assurance measures that are part of the evaluation. Therefore, the organisational security policy P.Gen-Unique-ID is covered by this objective, as far as organisational measures are concerned.

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

185 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 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 T.Mem-Access). The threat T.Mem-Access is therefore removed if the objective is met.

186 The clarification of O.Mem-Access makes clear that it is up to the Security IC Embedded Software to implement the memory management scheme by appropriately administrating the TSF. 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 of the Composite TOE(OE.Resp-Appl) 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 T.Mem-Access.

187 The justification related to the assumption “Treatment of user data of the Composite TOE (A.Resp- Appl)” is as follows:

188 OE.Resp-Appl requires the Composite Software to implement measures as assumed in A.Resp-Appl, so the assumption is covered by the objective.

189 The justification related to the assumption “Protection during Packaging, Finishing and Personalisation (A.Process-Sec-IC)” is as follows:

190 OE.Process-Sec-IC requires the Composite Product Manufacturer to implement those measures assumed in A.Process-Sec-IC, so the assumption is covered by this objective.

5 EXTENDED COMPONENTS DEFINITION

191 The definition of the IT security functionality of the 3S requires additional SFRs that are not defined in Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components.

5.1 Definition of the Family FCS_RNG

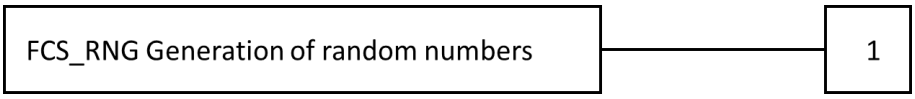
192 An additional family (FCS_RNG) of the Class FCS (cryptographic support) is defined for the random number generator. This family describes the functional requirements for random number generation used for cryptographic purposes.

FCS_RNG Generation of random numbers

Family behaviour:

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component levelling:



FCS_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

Application Note 5-1(PP_AN 27) A physical random number generator (RNG) produces the random number by a noise source, based on physical random processes.

5.2 Definition of the Family FMT_LIM

193 The additional family (FMT_LIM) of the Class FMT (Security Management) describes the functional requirements for Test and/or Debug Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The TOE implements technical mechanisms to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability. The functional requirement allows a combination of technical mechanisms to limit the capabilities and the availability. Therefore, the definition includes a dependency between the two components.

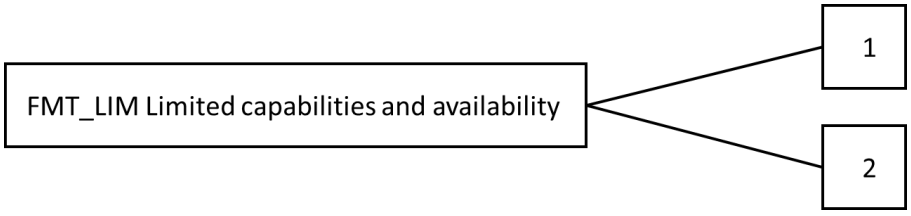
194 The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour:

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that the family FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



195 FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

196 FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (see Limited Capabilities (FMT_LIM.1)). This can be achieved by removing or by disabling functions in a specific phase of the TOE's life-cycle, for example.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

197 The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows:

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

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 [assignment: *Limited capability policy*].

198 The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited capabilities.

FMT_LIM.2.1 The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited availability policy].

Application Note 5-2(PP_AN 28) The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limitation of capabilities and limitation of availability) which together shall provide protection in order to enforce the same policy or two mutual supportive policies related to the same functionality. E.g., this enables the following:

(i) The TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced.
Or, conversely:

(ii) The TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

5.3 Definition of the Family FAU_SAS

199 The additional family (FAU_SAS) of the Class FAU (Security Audit) is defined to describe the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

200 The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour:

This family defines functional requirements for the storage of audit data.

Component levelling:

FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory].

5.4 Definition of the Family FDP_SDC

201 The Protection Profile defines the additional family (FDP_SDC.1) of the Class FDP (User data protection) to address confidentiality requirements for user data while stored under control of the TSF. The existing SFR on user data is limited to integrity protection.

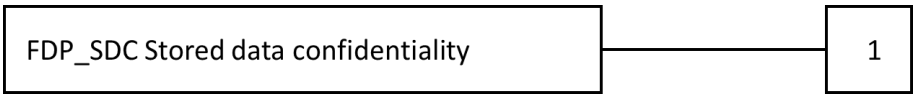
202 The family "Stored data confidentiality (FDP_SDC)" is specified as follows.

FDP_SDC Stored data confidentiality

Family behaviour:

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromising their information bypassing these interfaces. It complements the family "Stored data integrity (FDP_SDI)" which protects the user data from integrity errors while being stored in the memory.

Component levelling



FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: There are no management activities foreseen.

Audit: There are no actions defined to be auditable.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area].

5.5 Definition of the Family FPT_INI

203 The additional family (FPT_INI) of the Class FPT (Protection of the TSF) is defined to describe the functional requirements for the secure initialisation of the TSF. This family describes the functional requirements for the initialisation of the TSF by a dedicated security functionality of the TOE that ensures the initialisation in a correct and secure operational state.

204 The family "TSF Initialisation (FPT_INI)" is specified as follows.

FPT_INI TSF Initialisation

Family behaviour:

This family defines functional requirements for the secure initialisation of the TSF.

Component levelling:

FPT_INI.1 Requires the TOE to enforce a secure initialisation of the TSF.

Management: FPT_INI.1

There are no management activities foreseen.

Audit: FPT_INI.1

There are no actions defined to be auditable.

FPT_INI.1 TSF Initialisation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_INI.1.1 The TOE initialization function shall verify [assignment: list of verifications] prior to establishing the TSF in a secure initial state.

FPT_INI.1.2 The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE either successfully completes initialization or is halted.

FPT_INI.1.3 The TOE initialization function shall not be able to arbitrarily interact with the TSF after TOE initialization completes.

6 IT Security Requirements

6.1 Security Functional Requirements for the TOE

205 In order to define the Security Functional Requirements the Part 2 of Common Criteria and the Protection Profile[5] was used.

206 However, some Security Functional Requirements have been refined. The refinements are described by the associated SFRs below.

207 Please note that the following conventions are used to state each Security Functional Requirement:

- Refinement operations are explicitly identified at the end of the SFR definition.
- Assignment operations are identified *italic*.
- Selection operations are identified by underline.
- Iteration is denoted by showing a slash "/".

6.1.1 Protection against Malfunction

208 The TOE shall either tolerate disturbance (e.g., from external operating conditions) or, if malfunctions cannot be prevented, stop the operations. The TOE shall be protected from misconfiguration and by-passing by means of the Composite Software. These aspects are addressed by the security assurance requirements Architectural design (ADV_ARC.1).

209 The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2/Env)" as specified below.

FRU_FLT.2/Env	Limited fault tolerance
Hierarchical to:	FRU_FLT.1 Degraded fault tolerance
Dependencies:	FPT_FLS.1 Failure with preservation of secure state.
FRU_FLT.2.1/Env	The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *exposure to operating conditions or usage conditions out of range, which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1/Env)*
Refinement:	The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.
Application Note 6-1(PP_AN 29)	Environmental conditions include but are not limited to power supply, clock, and other external signals (e.g., a reset signal) necessary for the TOE operation.

210 The TOE shall meet the requirement "Limited fault tolerance (FRU_FLT.2/Log)" as specified below.

FRU_FLT.2/Log	Limited fault tolerance
Hierarchical to:	FRU_FLT.1 Degraded fault tolerance

Dependencies:	FPT_FLS.1 Failure with preservation of secure state.
FRU_FLT.2.1/Log	The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: *abnormal interface behaviour and/or protocol parameters or protocol sequences that can be tolerated and that are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1/Log).*
Refinement:	The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

211 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1/Env)" as specified below.

FPT_FLS.1/Env	Failure with preservation of secure state
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1/Env	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/Env) and where, therefore, a malfunction could occur.*
Refinement:	The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

Application Note 6-2(PP_AN 30) The secure state is maintained by TOE's detectors.

212 The TOE shall meet the requirement "Failure with preservation of secure state (FPT_FLS.1/Log)" as specified below.

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

Application Note 6-3(PP_AN 31, 32) The secure state is maintained by TOE's detectors.

6.1.2 Protection against Abuse of Functionality

213 The 3S may implement test functions to support the functional testing after the production. The TOE shall prevent abuse of such functionality after the test phase. The protection can be achieved either by limiting the capability of the implemented functions or limiting the availability. Limited capability prevents misuse or compromise of TSF data or user data, or the characterization of security functions and security services, even if the function can be reactivated, while limited availability prevents access to the functionality after testing. In most cases, both types of limitations are implemented to ensure the required protection.

214 The 3S may provide debugging services based on specific configuration of the TOE. The TOE prevents the use of this debugging functionality to prevent misuse or compromise of TSF data or user data, or perform characterization of security functions and security services. The debugging functionality may be limited, however, in terms of its capabilities and availability.

215 Test functionality and debug functionality may be limited by independent security mechanisms, so the SFRs defining the associated protection are iterated.

216 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1/Test)" to prevent the misuse of test functionality, as follows:

FMT_LIM.1/Test	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1/Test	The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: *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*.

217 The TOE shall meet the requirement "Limited availability (FMT_LIM.2/Test)" as specified below to prevent the misuse of test functionality.

FMT_LIM.2/Test	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1/Test	The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *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*.

218 The TOE shall meet the requirement "Limited capabilities (FMT_LIM.1/Debug)" as specified to prevent the misuse of debug functionality.

FMT_LIM.1/Debug	Limited capabilities
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.2 Limited availability.
FMT_LIM.1.1/Debug	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: *Deploying Debug 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.*

219 The TOE shall meet the requirement "Limited availability (FMT_LIM.2/Debug)" as specified below to prevent the misuse of debug functionality.

FMT_LIM.2/Debug	Limited availability
Hierarchical to:	No other components.
Dependencies:	FMT_LIM.1 Limited capabilities.
FMT_LIM.2.1/Debug	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: *Deploying Debug 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.*

6.1.3 Protection against Physical Manipulation and Probing

220 The TOE shall meet the requirement "Stored data confidentiality (FDP_SDC.1/3S)" as specified below.

FDP_SDC.1/3S	Stored data confidentiality
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1/3S	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *RAM or ROM.*

221 The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2/3S)" as specified below.

FDP_SDI.2/3S	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1/3S	The TSF shall monitor user data stored in containers controlled by the TSF for *ECC error or Parity error* on all objects, based on the following attributes: *RAM or ROM read operation*.
FDP_SDI.2.2/3S	Upon detection of a data integrity error, the TSF shall *enforce a device an interrupt (IRQ)*.
Refinement:	This SFR applies for internal memory of the 3S.

222 The TOE shall meet the requirement "Resistance to physical attack (FPT_PHP.3)" as specified below.

FPT_PHP.3	Resistance to physical attack
Hierarchical to:	No other components.
Dependencies:	No dependencies.
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, to ensure that SFRs are enforced. Therefore, in this case, "automatic response" means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

Application Note 6-5(PP_AN 34) This requirement is achieved by physical security feature.

6.1.4 Protection against Leakage

223 The security functional requirements "Basic internal transfer protection (FDP_ITT.1)" and "Basic internal TSF data transfer protection (FPT_ITT.1)" have been selected to ensure that the TOE must resist leakage attacks (both for user data and TSF data). The corresponding security policy is defined in the security functional requirement "Subset information flow control (FDP_IFC.1)".

224 The TOE shall meet the requirement "Basic internal transfer protection (FDP_ITT.1/3S)" as specified below.

FDP_ITT.1/3S	Basic internal transfer protection
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_ITT.1.1/3S	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.
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.

225 The TOE shall meet the requirement "Basic internal TSF data transfer protection (FPT_ITT.1/3S)" as specified below.

FPT_ITT.1/3S	Basic internal TSF data transfer protection
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_ITT.1.1/3S	The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.
Refinement:	The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

226 This requirement is equivalent to FDP_ITT.1/3S 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.1/3S below.

227 The TOE shall meet the requirement " Subset information flow control (FDP_IFC.1/3S)" as specified below:

FDP_IFC.1/3S	Subset information flow control
Hierarchical to:	No other components.
Dependencies:	FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/3S	The TSF shall enforce the *Data Processing Policy* on *all confidential data when they are processed or transferred by the TOE or by the Composite Software*.

228 The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "Subset information flow control (FDP_IFC.1/3S)":

229 "User data and TSF data shall not be accessible from the TOE except when the firmware, software or Composite Software decides to communicate the user data of the Composite TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by the firmware, software and Composite Software."

6.1.5 TOE Identification and Root of Trust

230 The TOE shall meet the requirement "Audit storage (FAU_SAS.1)" as specified below (Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components extended).

FAU_SAS.1	Audit storage
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FAU_SAS.1.1	The TSF shall provide the test process before TOE Delivery with the capability to store the Initialisation Data and/or Prepersonalisation Data in the *OTP*.
FPT_INI.1	TSF Initialization
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_INI.1.1	The TOE initialization function shall verify *correct configuration of configurable and/or trimmable security mechanisms and the unique identification, integrity of start-up software, correct initialisation of internal keys, correct configuration of life cycle state such as security detectors and Integrity checkers and bootloader secure sequence* prior to establishing the TSF in a secure initial state.
FPT_INI.1.2	The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE either successfully completes initialization or is halted.
FPT_INI.1.3	The TOE initialization function shall not be able to arbitrarily interact with the TSF after TOE initialization completes.

6.1.6 Generation of Random Numbers

231 The TOE shall meet the requirement "Quality metric for random numbers (FCS_RNG.1)" as specified below (Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components extended).

FCS_RNG.1/PTG.2	**Random number generation - PTG.2**
Hierarchical to:	No other components.
FCS_RNG.1.1/PTG.2	The TSF shall provide a physical true random number generator that implements:
(PTG.2.1)	*A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.*

(PTG.2.2) *If a total failure of the entropy source occurs while the RNG is being operated, the RNG* prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.

(PTG.2.3) *The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.*

(PTG.2.4) *The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.*

(PTG.2.5) *The online test procedure checks the quality of the raw random number sequence. It is triggered,* applied upon specified internal events (i.e., crypto key generation). *The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.*

FCS_RNG.1.2/PTG.2 The TSF shall provide numbers, *32-bit per number* that meet:

(PTG.2.6) *Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.*

(PTG.2.7) *The average Shannon entropy per internal random bit exceeds 0.997.*

Application Note 6-7(PP_AN 37): The TRNG HS_MRO9 library comprises some functions that perform statistical tests on the TRNG HS_MRO9.

Dependencies: No dependencies

6.1.7 Memory Access Control

232 Usage of multiple applications in one Security IC often requires separating code and data in order to prevent that one application can access code and/or data of another application. To support the TOE provides Area based Memory Access Control.

233 The security service being provided is described in the Security Function Policy (SFP) Memory Access Control Policy. The security functional requirement “Subset access control (FDP_ACC.1)” requires that this policy is in place and defines the scope were it applies. The security functional requirement “Security attribute based access control (FDP_ACF.1)” defines addresses security attribute usage and characteristics of policies. It describes the rules for the function that implements the Security Function Policy (SFP) as identified in FDP_ACC.1. The decision whether an access is permitted or not is taken based upon attributes allocated to the software. The user software defines the attributes and memory areas. The corresponding permission control information is evaluated “on-the-fly” by the hardware so that access is granted/effective or denied/inoperable.

234 The security functional requirement “Static attribute initialization (FMT_MSA.3)” ensures that the default values of security attributes are appropriately either permissive or restrictive in nature. Alternative values can be specified by any subject provided that the Memory Access Control Policy allows that. This is described by the security functional requirement “Management of security attributes (FMT_MSA.1)”. The attributes are determined during TOE manufacturing (FMT_MSA.3) or set at run-time (FMT_MSA.1).

235 From TOE´s point of view the different roles in the user software can be distinguished according to the memory based access control. However the definition of the roles belongs to the user software.

236 The following Security Function Policy (SFP) Memory Access Control Policy is defined for the requirement “Security attribute based access control (FDP_ACF.1)”:

Memory Access Control Policy

The TOE shall control read, write, delete, and execute accesses of software running at between two different modes (privilege and user mode) on data including code stored in memory areas.

The TOE shall restrict the ability to define, to change or at least to finally accept the applied rules (as mentioned in FDP_ACF.1) to software with privilege mode).

237 The TOE shall meet the requirement "Subset access control (FDP_ACC.1/3S)" as specified below:

FDP_ACC.1/3S	Subset access control
Hierarchical to:	No other components.
FDP_ACC.1.1/3S	The TSF shall enforce *the Memory Access Control Policy* on *all subjects (software with privilege mode and user mode), all objects (data including code stored in memories) and all the operations defined in the Memory Access Control Policy.* *Subjects are software codes in Privilege and User mode.* *Objects are data stored in ROM, RAM and OTP memories.*
Dependencies:	FDP_ACF.1 Security attribute based access control

238 The TOE shall meet the requirement "Security attribute based access control (FDP_ACF.1/3S)" as specified below:

FDP_ACF.1/3S	Security attribute based access control The attributes are all the operations related to the data stored in memories, which are *the read, write* and *execute* operations.
Hierarchical to:	No other components.
FDP_ACF.1.1/3S	The TSF shall enforce the *Memory Access Control Policy* to objects based on the following: *memory area where the software is executed from and/or the memory area where the access is performed to and/or the operation to be performed*.
FDP_ACF.1.2/3S	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *evaluate the corresponding permission control information before the access so that accesses to be denied cannot be utilised by the subject attempting to perform the operation*.
FDP_ACF.1.3/3S	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/3S	The TSF shall explicitly deny access of subjects to objects based on the following additional rules*: none*.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

239 The TOE shall meet the requirement "Static attribute initialisation (FMT_MSA.3)" as specified below:

FMT_MSA.3	Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the *Memory Access Control Policy* to provide *well defined* 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 Management of security attributes FMT_SMR.1 Security roles

240 The TOE shall meet the requirement "Management of security attributes (FMT_MSA.1)" as specified below:

FMT_MSA.1	Management of security attributes
Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the *Memory Access Control Policy* to restrict the ability to change default, modify or delete the security attributes *permission control information* to *running at privilege mode.*
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles

241 The TOE shall meet the requirement "Specification of management functions (FMT_SMF.1)" as specified below:

FMT_SMF.1	Specification of management functions
Hierarchical to:	No other components
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: *access the control registers of the MPU*.
Dependencies:	No dependencies

6.2 Security Assurance Requirements for the TOE

242 The Security Target will be evaluated according to

Security Target evaluation (Class ASE)

243 The Security Assurance Requirements for the evaluation of the TOE are those taken from the

- Evaluation Assurance Level 5 (EAL5)

244 and augmented by taking the following components:

- ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2.

245 corresponding to level "EAL5+".

246 The assurance requirements are:

Class ADV: Development		
	Architectural design	(ADV_ARC.1)
	Functional Specification	(ADV_FSP.5)
	Implementation Representation	(ADV_IMP.1)
	TSF Internals	(ADV_INT.2)
	TOE Design	(ADV_TDS.4)
Class AGD: Guidance documents activities		
	Operational User Guidance	(AGD_OPE.1)
	Preparative procedures	(AGD_PRE.1)
Class ALC: Life-cycle support		
	CM Capabilities	(ALC_CMC.4)
	CM Scope	(ALC_CMS.5)
	Delivery	(ALC_DEL.1)
	Development Security	***(ALC_DVS.2)***
	Flaw reporting procedures	***(ALC_FLR.2)***
	Life Cycle Definition	(ALC_LCD.1)
	Tools and Techniques	(ALC_TAT.2)
Class ASE: Security Target evaluation		
	Conformance claims	(ASE_CCL.1)
	Extended components definition	(ASE_ECD.1)
	ST introduction	(ASE_INT.1)
	Security objectives	(ASE_OBJ.2)
	Derived security requirements	(ASE_REQ.2)
	Security problem definition	(ASE_SPD.1)
	TOE summary specification	(ASE_TSS.1)
Class ATE: Tests		
	Coverage	(ATE_COV.2)
	Depth	(ATE_DPT.3)
	Functional Tests	(ATE_FUN.1)
	Independent Testing	(ATE_IND.2)
Class AVA: Vulnerability assessment		
	Vulnerability Analysis	***(AVA_VAN.5)***

Application Note 6-8(PP_AN 38): As required by this application note of the PP, this section defines the claimed SARs. The ST claims an augmented set of SARs to provide additional assurance to users of the TOE.

6.2.1 Refinements of the TOE Assurance Requirements

247 The CCDB, the JILWG and the certification bodies publish supporting documents and guidance documents for evaluation and certification of smartcards and similar devices mandatory under CCRA and SOG-IS or the national certification schemes, cf. . [10], [18], [19], [20], [21] and [22]. These documents are updated regularly and are valid for the ongoing evaluation in their actual versions.

248 The following refinements shall support the comparability of evaluations according to this Security Target. Where refinements are not needed, some background information based on such documents is provided. In all cases the background information is informative only. The mandatory documents themselves shall be consulted for exact details and overrule the refinements in case of any inconsistency (e.g., due to updates).

Refinements regarding Delivery procedure (ALC_DEL)

Refinement regarding CM scope (ALC_CMS)

Refinement regarding CM capabilities (ALC_CMC)

Refinement regarding Test Coverage (ATE_COV)

Refinement regarding User Guidance (AGD_OPE)

Refinement regarding Preparative User Guidance (AGD_PRE)

249 The Refinement operations are explicitly identified at the end of the elements definition.

Application Note 6-9(PP_AN 39): As required by this application note of the PP, this section defines the claimed SARs. The ST claims an augmented set of SARs to provide additional assurance to users of the TOE.

6.2.1.1 Refinements regarding Delivery procedure (ALC_DEL) Introduction

250 The Common Criteria assurance component of the family ALC_DEL (delivery procedure) refers to the delivery of (i) the TOE or parts of it (ii) to the user or user's site (Developer of the Composite Software or the Composite TOE Manufacturer). The Common Criteria assurance component ALC_DEL.1 requires procedures and technical measures to detect modifications and prevent any compromise of the Initialization Data and/or Pre-personalization Data and/or assigned other data.

251 In the particular case of a 3S " material and information" than the TOE itself (which by definition includes the necessary guidance) is exchanged with "users". Therefore, considering the definition of the Common Criteria the following refinement is made regarding the items "TOE" and "to the user or user's site":

252 The following text reflects the requirements of the selected component ALC_DEL.1:

Developer action elements:

ALC_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.

253 Content and presentation elements:

ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

254 Evaluator action elements:

ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement

For delivery of the TOE to the "Composite Product Manufacturer" or "integrated SoC manufacturer " as consumer, all the external interfaces of the TOE Manufacturer have to be taken into account. These are:

The interface with the 3S Software Developer (Phase 1) where information about the 3S, development software and/or tools for software development and possible information about mask options are exchanged and the interface with the Phase after TOE Delivery (Phase 4 or 5) where pre-personalization data, information about tests, and the product in the form of wafers, sawn wafers (dice) or packaged products are exchanged.

6.2.1.2 Refinement regarding CM scope (ALC_CMS)

Introduction

255 The Common Criteria assurance component of the family ALC_CMS (CM scope) refers to the tracking of specific configuration items within the developers configuration management system.

256 In the particular case of a 3s it is helpful to clarify the scope of the configuration item "TOE implementation representation":

257 The following text reflects the requirements of the selected component ALC_CMS.5: Developer action elements:

ALC_CMS.5.1D	The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.5.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; the implementation representation; security flaw reports and resolution status; and development tools and
ALC_CMS.5.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.5.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.5.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement

258 The "TOE Software" is as user data not part of the TOE but the whole "TOE Software" or part of it may be delivered together with the TOE (as implemented in the ROM or written by the TOE manufacturer in persistent memory). Therefore, the items "TOE SW" or "authentication data" are only relevant for the configuration list as far as the TOE manufacturer can control these items. Since the TOE Software may be

developed by another company it is only available in a specific form and is not part of the TOE though delivered together with it. Authentication data may be required for products implementing programmable non-volatile memory to enable the download of software.

259 CM list should include 3S deliveries from other than the developer, as IP developers.

Background information

260 Depending on the product type with programmable non-volatile memory and/or ROM the TOE SW and/or authentication data for a secure loader of the programmable non-volatile memory may be considered as part of the TOE implementation representation.

The "TOE implementation representation" within the scope of the CM will include at least:

- logical design data,
- physical design data,
- IC Dedicated Software,
- final physical design data necessary to produce the photomasks, and
- photomasks.

6.2.1.3 Refinement regarding CM capabilities (ALC_CMC)

Introduction

261 The Common Criteria assurance component of the family ALC_CMC (CM capabilities) refers to the capabilities of a CM system. The component ALC_CMC.4 "Production support, acceptance procedures and automation" refers to "configuration items" and "configuration list" and uses the term "TOE" in addition.

262 In the particular case of a 3S the scope of "configuration items" and the meaning of "TOE" in this context need to be clarified:

263 The following text reflects the requirements of the selected component ALC_CMC.4:

Developer action elements:

ALC_CMC.4.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.4.2D	The developer shall provide the CM documentation.
ALC_CMC.4.3D	The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.4.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.4.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.4.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.4.4C	The CM system shall provide automated measures such that only authorised changes are made to the configuration items.
ALC_CMC.4.5C	The CM system shall support the production of the TOE by automated means.
ALC_CMC.4.6C	The CM documentation shall include a CM plan.

ALC_CMC.4.7C	The CM plan shall describe how the CM system is used for the development of the TOE.
ALC_CMC.4.8C	The CM plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.
ALC_CMC.4.9C	The evidence shall demonstrate that all configuration items are being maintained under the CM system.
ALC_CMC.4.10C	The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

Evaluator action elements:

ALC_CMC.4.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement

"Configuration items" comprise all items defined and refined under ALC_CMS (see above) to betracked under CM.

A production control system has to be applied to guarantee the traceability and completeness of different production charges or lots. The number of wafers, dies and chips must be tracked by this system. Appropriate administration procedures have to be provided for managing wafers, dies or complete chips, which are being removed from the production-process in order to verify and to control predefined quality standards and production parameters. It has to be controlled that these wafers, dies or assembled devices are returned to the same production stage from which they are taken or they have to be securely stored or destroyed otherwise.

6.2.1.4 Refinement regarding Test Coverage (ATE_COV)

Introduction

264 The Common Criteria assurance component of the family ATE_COV (test coverage) "addresses the extent to which the TSF is tested, and whether the testing is sufficiently extensive to demonstrate that the TSF operates as specified.

265 The following text reflects the requirements of the selected comp4onent ATE_COV.2:

Developer action elements:

ATE_COV.2.1D	The developer shall provide an analysis of the test coverage.

Content and presentation elements:

ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

Evaluator action elements:

ATE_COV.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Refinement

The TOE must be 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)" must be proven for the complete TSF. The tests must also cover functions which may be affected by "ageing".

The existence and effectiveness of mechanisms against physical attacks (as specified by the functional requirement FPT_PHP.3) cannot be tested in a straightforward way. Instead, the TOE Manufacturer shall provide evidence that the TOE has the particular physical characteristics (especially layout design principles). This can be 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 they are obvious).

Background information

The 3S Dedicated Test Software is seen as a "test tool" delivered as part of the TOE. The Test Features, however, do not provide security functionality. Therefore, Test Features need not be covered by the Test Coverage Analysis, but all functions and mechanisms that limit the capability of the functions (cf. FMT_LIM.1) and control access to the functions (cf. FMT_LIM.2) provided by the 3S Dedicated Test Software must be part of the Test Coverage Analysis.

6.2.1.5 Refinement regarding User Guidance (AGD_OPE)

Introduction

266 The Common Criteria assurance components of the families AGD_OPE (Operational user guidance) and AGD_PRE (Preparative user guidance) "describe all relevant aspects for the secure application of the TOE".

267 The Operational User Guidance documents should provide only the information which is necessary for using the TOE. Depending on the recipient of that guidance documentation Operational and Preparative User Guidance can be given in the same document.

268 After production the TOE is tested where communication is performed by directly contacting the pads that mostly become part of the interface during packaging. Here no guidance document according to Common Criteria class AGD is required (provided that the tests are performed by the TOE Manufacturer). Note that test procedures are described under the Common Criteria assurance component of the family ATE_FUN.

269 The following text reflects the requirements of the selected component AGD_OPE.1:

Developer action elements:

AGD_OPE.1.1D	The developer shall provide the operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges thatshould be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user

role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role,

clearly present each type of security-relevant event relative to the user- accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible

modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role,

describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided

meets all requirements for content and presentation of evidence.

Refinement

The TOE serves as a platform for the 3S Software. Therefore, the role of the developer of the 3S Software is the main focus of the guidance, see also section 6.2.1.1.

If the TOE provides security functionality which can or need to be administrated (i) by the 3S Software or (ii) if the 3S Software provides additional services (see section 1.2.2), these aspects must be described in Guidance. This may also comprise specific functionality that must be provided by the 3S Software to support the security of the platform and configuration options of the TOE.

Guidance documents must not contain security relevant details which are not necessary for the usage or administration of the security functionality of the TOE.

Background information

Most of the security functionality will already be effective before TOE Delivery. However, guidance to determine the behaviour of security functionality, to disable, to enable or to modify the behaviour of security functionality must be given if a configuration is possible after TOE Delivery (that means either by the Developer of the 3S Software or by the Composite Product Manufacturer). This guidance is delivered by the TOE Manufacturer.

6.2.1.6 Refinement regarding Preparative User Guidance (AGD_PRE)

Introduction

270 Preparative user guidance is intended to be used by those persons responsible for secure acceptance and installation of the TOE as well as the secure preparation of the operational environment in a correct manner for maximum security.

271 The following text reflects the requirements of the selected component AGD_PRE.1:

Developer action elements:

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Refinement

The Family AGD_PRE addresses the activities of the delivery acceptance procedures. For the hardware platform this comprises procedures that can be applied to identify the TOE and eventually to verify the authenticity of that part of the TOE using e.g. the security functionality provided according to FAU_SAS.1.

The TOE may be configured after production before the Composite Product is delivered to the consumer. In this case, these configuration aspects have to be considered. Differences between the TOE before first use (normally done during wafer test) and Phase 7 must be summarized. Guidance to change that behaviour must exist.

The preparation may include the download of 3S Software if parts of the 3S Software are stored in the programmable non-volatile memory. If the TOE includes software that is delivered separately the preparation includes integration of the 3S Software. The preparation also includes the configuration of the TOE according to the options described in the ST that can be changed after TOE delivery. The guidance documentation shall describe all relevant procedures.

6.2.2 Refinements of the TOE Integration Assurance Requirements

272 The 3S integration process needs to ensure the integrity and confidentiality of the hard macro delivered by the 3S developer. All interfaces between the TOE and the SoC should be described in the integration guidance.

273 The refinements ensure that the integration process will be evaluated as part of the TOE evaluation.

274 The following refinements shall support the comparability of evaluations according to this Security Target:

ADV_ARC.1 Architectural design

Refinements related to the integration guidance:

- ADV_ARC.1.4D: The developer shall provide a rationale for the correct integration of the 3S in the SoC as part of the TSF security architecture description.
- ADV_ARC.1.6C: The rationale shall be at the level of detail of the TOE design and the integration guidance requirements.
- ADV_ARC.1.2E in CEM: The evaluator shall examine the security architecture description to determine that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design document. TOE integration guidance should be examine as well.

AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative user guidance

Refinements related to the integration guidance:

The SoC integrator should be identified as a User. Therefore, integration guidance shall be evaluated as part of the AGD class.

6.3 Security Requirements Rationale

6.3.1 Rationale for the SFRs

275 Table 6-1 provides an overview, how the SFRs are combined to meet the security objectives. The justification for each objective is detailed after the table.

Objective	TOE Security Functional and Assurance Requirements
O.Leak-Inherent	FDP_ITT.1/3S Basic internal transfer protection FPT_ITT.1/3S Basic internal TSF data transfer protection FDP_IFC.1/3S Subset information flow control
O.Phys-Probing	FDP_SDC.1/3S Stored data confidentiality FPT_PHP.3 Resistance to physical attack
O.Malfunction	FRU_FLT.2/Env Limited fault tolerance FPT_FLS.1/Env Failure with preservation of secure state FRU_FLT.2/Log Limited fault tolerance FPT_FLS.1/Log Failure with preservation of secure state Supported by: FPT_INI.1 TSF Initialisation
O.Phys-Manipulation	FDP_SDI.2/3S Stored data integrity monitoring and action FPT_PHP.3 Resistance to physical attack
O.Leak-Forced	FDP_ITT.1/3S Basic internal transfer protection FPT_ITT.1/3S Basic internal TSF data transfer protection FDP_IFC.1/3S Subset information flow control FRU_FLT.2/Env Limited fault tolerance FPT_FLS.1/Env Failure with preservation of secure state FRU_FLT.2/Log Limited fault tolerance FPT_FLS.1/Log Failure with preservation of secure state FPT_PHP.3 Resistance to physical attack
O.Abuse-Func	FMT_LIM.1/Test Limited capabilities FMT_LIM.2/Test Limited availability FMT_LIM.1/Debug Test Limited capabilities

	FMT_LIM.2/Debug Limited availability Supported by: FAU_SAS.1 Audit storage FRU_FLT.2/Env Limited fault tolerance FPT_FLS.1/Env Failure with preservation of secure state RU_FLT.2/Log Limited fault tolerance FPT_FLS.1/Log Failure with preservation of secure state FDP_SDI.2/3S Stored data integrity monitoring and action FPT_PHP.3 Resistance to physical attack
O.RND	FCS_RNG.1 Random number generation Supported by: FRU_FLT.2/Env Limited fault tolerance FPT_FLS.1/Env Failure with preservation of secure state FDP_ITT.1/3S Basic internal transfer protection FPT_ITT.1/3S Basic internal TSF data transfer protection FDP_IFC.1/3S Subset information flow control FPT_PHP.3 Resistance to physical attack
O.Secure-State	FPT_INI.1 TSF Initialisation Supported by: FRU_FLT.2/Env Limited fault tolerance FPT_FLS.1/Env Failure with preservation of secure state FRU_FLT.2/Log Limited fault tolerance FPT_FLS.1/Log Failure with preservation of secure state FDP_SDI.2/3S Stored data integrity monitoring and action FPT_PHP.3 Resistance to physical attack
O.Identification	FAU_SAS.1 Audit storage Supported by: FPT_INI.1 TSF Initialisation
O.Mem-Access	FDP_ACC.1/3S “Subset access control” FDP_ACF.1/3S “Security attribute based access control”

	FMT_MSA.3 “Static attribute initialisation” FMT_MSA.1 “Management of security attributes” FMT_SMF.1 “Specification of Management Functions”

Table 6-1 Security Requirements versus Security Objectives

276 The justification related to the security objective “Protection against Inherent Information Leakage (O.Leak-Inherent)” is as follows:

277 The SFRs FPT_ITT.1/3S and FDP_ITT.1/3S together with the policy statement in FDP_IFC.1/3S explicitly requires the prevention of emission that enables access to secret data (TSF data as well as user data) over the TOE attack surface. According to the already performed assignment, this covers power, emanation and timing. The attack surface comprises the chip surface as well as all interfaces of the 3S.

278 It is possible that the TOE needs additional support by the FW, SW and/or Composite Software (e.g., timing attacks are possible if the processing time of algorithms implemented in the software depends on the content of secret). This support shall be addressed in the Guidance Documentation. FPT_ITT.1/3S and FDP_ITT.1/3S together with the policy statement in FDP_IFC.1/3S in conjunction with the guidance are suitable to meet the objective

279 The justification related to the security objective “Protection against Physical Probing (O.Phys-Probing)” is as follows:

280 The SFR FDP_SDC.1/3S requires the TSF to protect the confidentiality of the information of user data and TSF data stored in specified memory areas and prevent their compromising by physical attacks bypassing the specified interfaces for memory access. The scenario of physical probing as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, this SFR supports the objective.

281 It is possible that the TOE needs additional support by the FW, SW and/or Composite Software (e.g., to send data over certain buses only with appropriate precautions). This support shall be addressed in the Guidance Documentation. Together with this, FPT_PHP.3 is suitable to meet the objective.

282 The justification related to the security objective “Protection against Malfunctions (O.Malfunction)” is s follows:

283 The definition of this objective covers situations where malfunction of the TOE might be caused by the operating conditions of the TOE or abnormal usage of TOE interfaces (while direct manipulation of the TOE is covered by O.Phys-Manipulation). For the operating conditions the security objective covers the following two circumstances: either all operating conditions are inside the tolerated range or at least one of them is outside this range. The second case is covered by FPT_FLS.1/Env, because it states that a secure state is preserved in this case. The first case is covered by FRU_FLT.2/Env, because it states that the TOE operates correctly under normal (tolerated) conditions. For the abnormal interface behaviour and/or protocol parameters or protocol sequences also two circumstances are covered: Either the interface behaviour can be tolerated as described by FRU_FLT.2/Log or the interface behaviour may cause a mal function and, therefore, shall stop the operation and change to a secure state covered by FPT_FLS.1/Log. The TOE may enter the same a secure state for both iterations of FPT_FLS.1 or defines a secure state for each instance FPT_FLS.1/Env and FPT_FLS.1/Log.

284 The objective is supported by FPT_INI.1 that ensures the correct initialisation and configuration of the 3S during start-up.

285 The functions implementing FRU_FLT.2/Env and FPT_FLS.1/Env shall work independently from

the Composite Software so that their operation cannot be affected by the Composite Software. The functions implementing FRU_FLT.2/Log and FPT_FLS.1/Log shall apply for the interfacing between the TOE and the Composite Software as well as for the external interfaces provided by the TOE so that the different interfaces cannot be affected by the Security Services of the TOE. Therefore, there is no possible instance of conditions under O.Malfunction, which is not covered.

286 The justification related to the security objective "Protection against Physical Manipulation (O.Phys-Manipulation)" is as follows:

287 The SFR FDP_SDI.2/3S defines a security mechanism to detect integrity errors of the stored user data and TSF data and react to detected errors. The scenario of physical manipulation as described for this objective is explicitly included in the assignment chosen for the physical tampering scenarios in FPT_PHP.3. Therefore, it is clear that this SFR supports the objective.

288 It is possible that the TOE needs additional support by the FW, SW and Composite Software (e.g., by implementing FDP_SDI.2) to check data integrity with the help of appropriate checksums. This support shall be addressed in the Guidance Documentation. Together with FPT_PHP.3, this is suitable to meet the objective.

289 The justification related to the security objective "Protection against Forced Information Leakage O.Leak-Forced)" is as follows:

290 This objective is directed against attacks where an attacker wants to force an information leakage, which would not occur under normal conditions. In order to achieve this, the attacker has to combine a first attack step, which modifies the behaviour of the TOE (either by exposing it to extreme operating conditions or by modifying the interface behaviour or by directly manipulating it) with a second attack step measuring and analysing some output generated by the TOE. The first step is prevented by the SFR FRU_FLT.2/Env, FRU_FLT.1/Log, FPT_FLS.1/Env and FPT_FLS.1/Log for the control of the operating conditions and FPT_PHP.3 that prevent physical modification. Furthermore, the protection against leakage defined by FPT_ITT.1/3S and FDP_ITT.1/3S together with the policy statement in FDP_IFC.1/3S supports O.Leak-Forced, because it prevents the attacker from being successful if he tries the second step directly (e.g., with operating conditions at their limits that are not detected).

291 The justification related to the security objective "Protection against Abuse of Functionality (O.Abuse- Func)" is as follows:

292 This objective states that abuse of test functions (especially provided by the firmware components that are used for product test, for example, to read data from memories) shall not be possible in Phase 7 of the life-cycle. There are two possibilities to achieve this: (i) they cannot be used by an attacker (i.e., their availabilities are limited), or (ii) using them would not provide an exploitable response for an attacker (i.e., their capabilities are limited) because the functions are designed in a specific way. The limited availability is specified by FMT_LIM.2/Test and the limited capability is specified by FMT_LIM.1/Test. These requirements are combined to support the policy, which is suitable to fulfil O.Abuse-Func, so both SFRs together are suitable to meet the objective.

293 The two SFRs FMT_LIM.1/Debug and FMT_LIM.2/Debug are iterated, because debug functionality also needs to be disabled in Phase 7 of the life-cycle to prevent disclosure or modification of user data or TSF data using debug functionality. Debug functionality may be implemented with different security mechanisms to limit the capabilities and the availability of this functionality.

294 The SFR FAU_SAS.1 allows a unique identification of each TOE instance and thereby supports the protection against abuse. FRU_FLT.2/Env and FPT_FLS.1/Env control the operating conditions and prevent malfunctions that may allow to circumvent the control implemented by FMT_LIM.1 and FMT_LIM.2. FRU_FLT.1/Log and FPT_FLS.1/Log control the interface behaviour and prevent malfunctions that may allow to circumvent the control implemented by FMT_LIM.1 and FMT_LIM.2.

The SFR FDP_SDI.2/3S ensures the integrity of configuration data to ensure secure life-cycle control. The protection against manipulation as defined by FPT_PHP.3 prevents attackers from manipulation of the hardware. The supporting SFR overview is included in Table 6-1.

295 FMT_LIM.1 and FMT_LIM.2 are explicitly (not using Part 2 of the Common Criteria) defined for the following reason: though taking components from the Common Criteria catalogue makes it easier to recognise functions, any selection from Part 2 of the Common Criteria would have made it harder for the reader to understand the special situation meant here. As a consequence, the statement of explicit SFRs was chosen to provide more clarity.

296 The justification related to the security objective "Random Numbers (O.RND)" is as follows:

297 FCS_RNG.1 requires the TOE to provide random numbers of good quality. The specification of the exact metric is left to the individual Security Target for a specific TOE.

298 The SFRs FPT_FLS.1/Env and FPT_FLT.2/Env prevent malfunction of the TOE, based on malicious operating conditions. FPT_PHP.3 prevents physical manipulation and FPT_ITT.1/3S and FDP_ITT.1/3S together with the policy statement in FDP_IFC.1/3S prevent leakage that may disclose data generated by the random number generator.

299 Random numbers are mainly used by the Composite Software to generate cryptographic keys for internal use. Therefore, the TOE shall prevent the unauthorised disclosure of random numbers. Other SFRs, which support the prevention of inherent leakage attacks, probing and forced leakage attacks, ensure the confidentiality of the random numbers provided by the TOE.

300 The FW, SW or the Composite Software have to support the objective by providing runtime-tests of the random number generator, depending on the implementation of the random number generator and the associated protection in a specific TOE. Together, these requirements allow the TOE to provide random numbers with high entropy and to ensure that no information about the generated random numbers is available to an attacker.

301 It was chosen to define FCS_RNG.1 explicitly, because Part 2 of the Common Criteria does not contain generic SFRs for Random Number generation.

302 The justification related to the security objective "Secure start-up and re-start (O.Secure-State)" is as follows:

303 The SFR FPT_INI.1 implements security mechanisms to verify the correct configuration of the required parameter (e.g., trimming and life-cycle control) and the unique identification during the start-up. Further on, the SFR requires an integrity protection of the software executed during start-up and the correct initialisation of internal keys as required by the objective. Therefore, FPT_INI.1 is suitable to meet the objective.

304 The security objective O.Secure-State is supported by FRU_FLT.2/Env and FPT_FLS.1/Env controlling the operating conditions and FRU_FLT.1/Log and FPT_FLS.1/Log controlling the interface behaviour prevent malfunctions that may allow to manipulate the secure initialisation. The SFR FDP_SDI.2/3S ensures the integrity of configuration data. The protection against manipulation as defined by FPT_PHP.3 prevents attackers from manipulation of the hardware to circumvent the secure initialisation. The supporting SFR overview is included in Table 6-1.

305 The justification related to the security objective "TOE Identification (O.Identification)" is as follows:

306 This objective states that the TOE shall be able to provide a unique identification of the TOE instance. The SFR defines the capability to store audit information provided by a subject in a persistent memory of the TOE. Therefore, the SFRs are suitable to meet the objective.

307 O.Secure-State requires the correct initialisation and configuration of the TOE. This includes the integrity check of the unique identifier of the TOE. Therefore, this objective supports O.Identification.

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

309 The security functional requirement "Subset access control (FDP_ACC.1/3S)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly require the implementation of an area based memory access control, which is a requirement from O.Mem-Access. Therefore, FDP_ACC.1/3S with its SFP is suitable to meet the security objective.

310 The security functional requirement "Security attribute based access control (FDP_ACF.1/3S)" with the related Security Function Policy (SFP) "Memory Access Control Policy" exactly requires the implementation of an area based memory access control, which is a requirement from O.Mem-Access. Therefore, FDP_ACF.1/3S with its SFP is suitable to meet the security objective.

311 The security functional requirement "Static attribute initialisation (FMT_MSA.3)" requires that the TOE provides default values for the security attributes. Since the TOE is a hardware platform these default values are generated by the reset procedure. Therefore FMT_MSA.3 is suitable to meet the security objective O.Mem-Access.

312 The security functional requirement "Management of security attributes (FMT_MSA.1)" requires that the ability to change the security attributes is restricted to privileged subject(s). It ensures that the access control required by O.Mem-Access can be realised using the functions provided by the TOE. Therefore FMT_MSA.1 is suitable to meet the security objective O.Mem_Access.

313 Finally, the security functional requirement "Specification of Management Functions (FMT_SMF.1)" is used for the specification of the management functions to be provided by the TOE as required by O.MEM_ACCESS. Therefore, FMT_SMF.1 is suitable to meet the security objective O.Mem_Access.

6.3.2 Dependencies of SFRs

314 Table 6-2 lists the SFRs defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases

Requirement	Dependency	Satisfied Dependency
FDP_ITT.1/3S	FDP_ACC.1 or FDP_IFC.1	Yes by FDP_IFC.1/3S
FDP_IFC.1/3S	FDP_IFF.1	See discussion below
FPT_ITT.1/3S	None	No dependency
FPT_PHP.3	None	No dependency
FDP_SDC.1/3S	None	No dependency
FRU_FLT.2/Env	FPT_FLS.1/Env	Satisfied by FPT_FLS.1/Env
FPT_FLS.1/Env	No dependency	No dependency
FRU_FLT.2/Log	FPT_FLS.1/Log	Satisfied by FPT_FLS.1/Log

FPT_FLS.1/Log	No dependency	No dependency
FDP_SDI.2/3S	No dependency	No dependency
FMT_LIM.1/Test	FMT_LIM.2	Satisfied by FMT_LIM.2/Test
FMT_LIM.2/Test	FMT_LIM.1	Satisfied by FMT_LIM.1/Test
FMT_LIM.1/Debug	FMT_LIM.2	Satisfied by FMT_LIM.2/Debug
FMT_LIM.2/ Debug	FMT_LIM.1	Satisfied by FMT_LIM.1/Debug
FCS_RNG.1	None	No dependency
FPT_INI.1	None	No dependency
FAU_SAS.1	None	No dependency
FDP_ACC.1/3S	FDP_ACF.1	Yes
FDP_ACF.1/3S	FDP_ACC.1 FMT_MSA.3	Yes Yes
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Yes See discussion below
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Yes See discussion below Yes
FMT_SMF.1	None	No dependency

Table 6-2 Overview of SFR dependencies

315 Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1/3S there are no attributes necessary. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1/3S and its Data Processing Policy (FDP_IFC.1/3S).

316 The dependency FMT_SMR.1 introduced by the two components FMT_MSA.1 and FMT_MSA.3 is considered to be satisfied because the access control specified for the intended TOE is not role-based but enforced for each subject. Therefore, there is no need to identify roles in form of a security functional requirement FMT_SMR.1.

6.3.3 Rationale for the Assurance Requirements

317 The assurance level EAL5 and the augmentation with the requirements ALC_DVS.2, AVA_VAN.5 and ALC_FLR.2 were chosen in order to meet assurance expectations explained in the following paragraphs.

318 An assurance level of EAL5 with the augmentations AVA_VAN.5 ALC_DVS.2 and ALC_FLR.2 is required for this type of TOE, because it is intended to defend against sophisticated attacks. This evaluation assurance package was selected to permit a developer to gain maximum assurance from positive security engineering, based on good commercial practices. In order to provide a meaningful level of assurance that the TOE provides an adequate level of defence against such attacks, the evaluators should have access to a sufficiently detailed TOE Design Specification and the source

code. In addition the developer needs to implements security flaw reporting procedures for TOE users in order to act appropriately upon reported security flaw and provide corrective fixes.

6.3.3.1 ALC_DVS.2 Sufficiency of security measures

319 Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

320 In the particular case of a 3S hardware design block, the TOE is developed and produced within a complex and distributed industrial process which shall be protected in particular. 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 hardware design block, maintaining the confidentiality of the design is very important. ALC_DVS.2 includes requirements to continuously assess the security measures and verify the applicability and sufficiency for all sensitive configurations items that are part of the TOE.

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

6.3.3.2 AVA_VAN.5 Advanced methodical vulnerability analysis

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

323 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.

324 AVA_VAN.5 has dependencies to ADV_ARC.1 “Security architecture description”, ADV_FSP.4 “Complete 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”.

325 All these dependencies are satisfied by EAL5.

326 It has to be assumed that attackers with high attack potential try to attack 3Ss, such as the TOE used for payment systems, Subscriber Identity Module (SIM), storage and management of digital identities. Therefore, AVA_VAN.5 was chosen specifically to assure that even these attackers cannot successfully attack the TOE.

6.3.3.3 ALC_FLR.2 Flaw reporting procedures

327 The augmentation with ALC_FLR.2 has been chosen to achieve a secure continuous operation of the TOE.

328 The flaw remediation process includes the possibility for users to report identify failures, flaws and abnormal behaviour to the developer. The developer needs an internal tracking and assessment of these issues. Furthermore the developer needs to implement corrective actions and deliver information on the flaw, corrections and guidance on corrective actions to TOE users. This provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE.

329 ALC_FLR.2 has no dependencies.

330 ALC_FLR.2 is not included in the defined assurance level.

331 During the operation of the TOE in the field users may identify failures, flaws or abnormal

behaviour. An analysis of such events can only be performed by the developer. Therefore, secure continuous operation is supported by a security flaw remediation process implemented by the developer.

7 Definition of Packages

332 The following packages are added. Each package defines an extension of the TOE functionality.

Application Note 7-1(PP_AN 43) All functional packages have been used in the ST only once, i.e. all iterations are reused from the PP without change.

333 Some of the packages have dependencies that need to be considered; for details, see section 1.3.

7.1 Package for Passive External Memory

334 This package describes the extension of the security problem definition and the SFRs, if the 3S is connected to passive external memory. The passive external memory does not provide any security functionality and is outside the boundary of the TOE. The usage of passive memory outside the TOE has the following effects:

- The TOE implements an interface to the internal SoC bus to access the passive external memory. The SoC implements the interface to the external memory that is shared by the SoC and the 3S. The passive external memory does not implement any security service or security functionality, so the external memory is named passive external memory.
- The passive external memory can store an encrypted and authenticated software image that can either be loaded in the TOE during start-up or during runtime. In this case the TOE implements a security service to authenticate, verify the integrity and decrypt the content of the software image before it is executed in the TOE. Further on, the security service prevents rollback to older versions of the software image. When TOE FW/SW is activated, the TOE can load Composite Software to be executed by the TOE as user data.
- The passive external memory can also store a firmware image to enable updates of the firmware. Loading Firmware images require a similar security service than the loading of software images.
- Further on, the TOE can store TSF data and User Data in the passive external memory as protected data container. The security functionality for TSF data and User Data shall enforce confidentiality, integrity, freshness and replay protection.

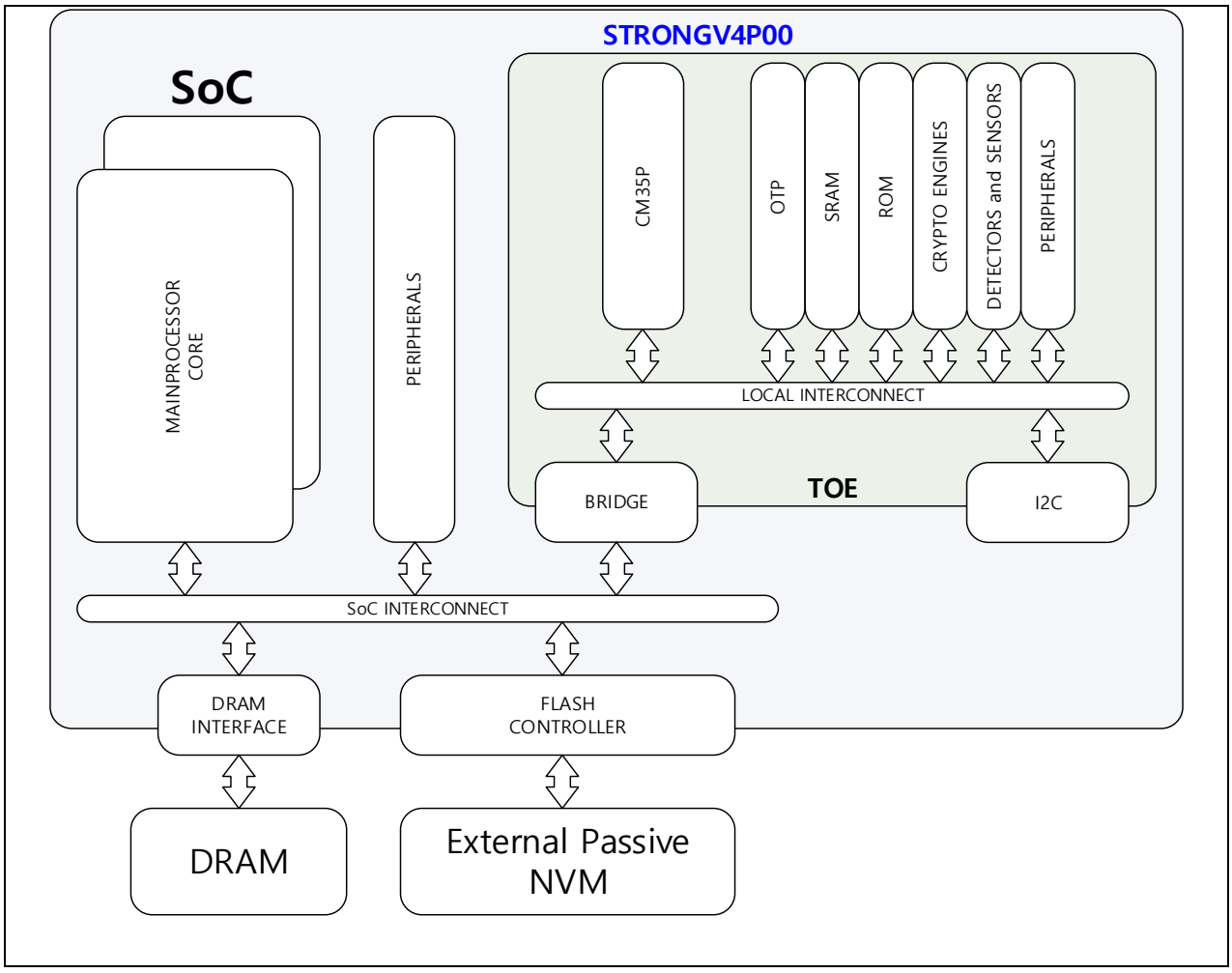


Figure 7-1: 3S with passive external memory (PM)

335 Attacks on data stored in passive external memory shall be detected to protect the TOE against the consequences of such attacks outside the TOE boundary, because the passive external memory is shared with the remaining components of the SoC. Therefore, additional threats shall be included in the Security Target.

7.1.1 Security Problem Definition

7.1.1.1 Description of Assets

Application Note 7-2(PP_AN 44) There are no additional assets defined in this package.

7.1.1.2 Threats

336 The following figure describes the attacks on the TOE with passive external memory. The threats described in this section shall be added in the Security Target together with the threats against the TOE described for the base configuration (see section 3.2).

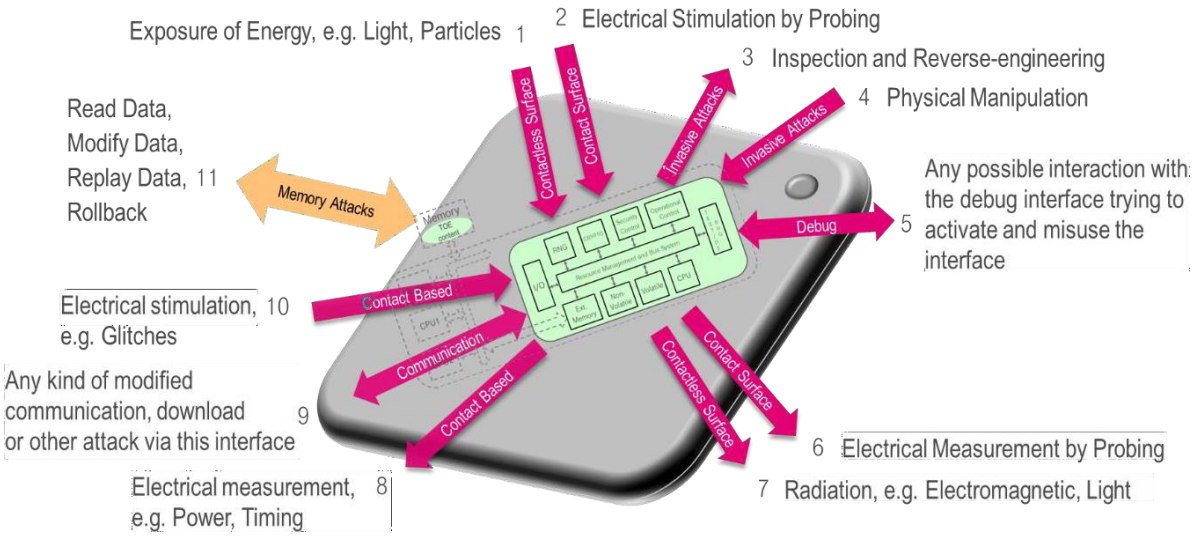


Figure 7-2: Attacks against passive external memory

337 In Figure 7-2, the grey box represents the SoC with the TOE (green box) and its interaction channels. The external memory may store a protected software image and data that both belong to the TOE.

338 The TOE shall protect against the threat "Cloning the TOE with a copy of the passive external memory (T.Pas-Mem-Clone-Replace)" as specified below.

T.Pas-Mem-Clone-Replace	Cloning or replacement of passive external memory An attacker may attempt to clone the full content of the external memory or a specific memory area storing User Data of the 3S and write it to the external memory used by a different unit; alternatively, an attacker may physically replace the external memory used by a 3S with a different memory that may come from a different unit.

339 This threat refers to the case where partial or full content of the external memory is cloned to a different device. It can also cover the replacement of the physical external memory used by the 3S with the memory of a different unit. The second case might not be viable on some architectures or memory when the physical design or assembly procedures impede it.

340 The effect of this threat is in replacing the data and/or image of a TOE with a different one and to obtain a valid but unauthorised instance of the TOE.

341 This threat involves using two different TOE units or instances. One TOE unit is used as a source for the external memory content. This content is used to replace the genuine content of the external memory of the second TOE unit.

342 Another possible scenario for this threat can be contemplated for passive external non-volatile memory: the external non-volatile memory is replaced with an empty or virgin non-volatile memory, removing the user and TSF data used by the TOE, and possibly forcing the TSF to generate new user and TSF data, potentially affecting the TSF behaviour.

343 The TOE shall protect against the threat "Abuse of passive external memory content (T.Pas-Mem- Content-Abuse)" as specified below.

T.Pas-Mem-Content-Abuse	Abuse of passive external memory content An attacker may attempt to access for disclosing or modifying the content of the external memory used by the 3S. Thereby an attacker may compromise confidentiality and/or integrity of TSF data and/or user data that shall be protected by the TOE.

344 An attacker may obtain unauthorised access to the external memory and attempt to read, disclose, modify or replace the content of the external memory. This threat addresses also the authenticity of the data stored in the external memory.

345 Note that the access to the external memory or the transfer of data between the TOE and the external memory may also support an attack.

346 The TOE shall avert the threat "Replay of commands between the 3S and the passive external memory (T.Pas-Mem-Cmd-Replay)" as specified below.

T.Pas-Mem-Cmd-Replay	Replay of commands between the 3S and the passive external memory An attacker may attempt to replay the write and erase commands or responses to the read commands between the 3S and the passive external memory, to affect the freshness of the content read from or written to the external memory.

347 The read, write and erase commands issued by the 3S to exercise the storage functionality of the external memory, and their payloads, can be intercepted by an attacker (e.g., eavesdrop the commands on the link between the 3S and the external memory). Such an attacker may use copies of these commands to try to misuse the TOE or compromise data. The command replay attack can take the following forms:

- The attacker reacts to a read command and replies with a previously recorded answer (e.g., to a previous read request). In this way, the 3S gets an old version of such content.
- The attacker issues a previous write command, trying to overwrite the external memory with the previous content, and leading to the 3S obtaining old versions of such content in later read operations.
- The attacker issues a previous erase command, trying to overwrite status information or other data that may lead to misuse of the TOE.

348 The TOE shall avert the threat "Unauthorised rollback of content in the passive external memory (T.Pas-Mem-Unauth-Rollback)" as specified below.

349 T.Pas-Mem-Unauth-Rollback	Unauthorised rollback of content in the passive external memory An attacker may attempt to read the content of the external memory, record it, and later write it back to the external memory after the original content were updated by the TOE.

350 This threat takes advantage of the fact that the external memory is not integrated into the 3S. Hence, physical protections for preventing the replacement of content may not cover the external memory. This situation enables an attacker to read and write the content of the external memory. Even if the

confidentiality and integrity of the external memory content is protected, the replacement with an old copy may also be valid, because it is retrieved from the external memory.

351 If the TOE image is stored in an external memory, this threat may lead to an unauthorised rollback of the TOE image to an older version. Even when the TOE stores data and not code in the external memory, this data rollback might affect the behaviour of the TSF.

352 The replacement of content stored in the external memory with previous versions of it may refer to the full content of the external memory or partial content of it, depending on the organization and protection of the data stored in the external memory.

7.1.1.3 Organisational Security Policies

Application Note 7-3(PP_AN 45). There are no additional Organisational Security Policies defined in this package.

7.1.1.4 Assumption

Application Note 7-4(PP_AN 46). This package does not define an additional assumption.

7.1.2 Security Objectives

7.1.2.1 Security Objectives for the TOE

353 The TOE shall provide "Protection against disclosure and undetected modification of passive external memory content (O.Pas-Mem-Content-Prot)" as specified below.

O.Pas-Mem-Content-Prot: Protection against disclosure and undetected modification of passive external memory content.

The content in the external memory shall be protected against disclosure and undetected modification, because an attacker can directly access the external memory.

354 This security objective requires protection of the content stored in external memory by the TOE. The protection prevents disclosure and identifies modifications of stored code and data that is not performed by the TOE.

355 The TOE shall provide "Protection against replay of commands to store or modify data in passive external memory to the 3S (O.Pas-Mem-Cmd-Replay-Prot)" as specified below.

O.Pas-Mem-Cmd-Replay-Prot: Protection against replay of commands to store or modify data in passive external memory to the 3S.

The TOE shall protect against replay of content during write, read and erase operations to the external memory by the 3S.

356 This security objective requires protection against replay of read, write and erase operations. This covers simple replay of previously recorded commands or memory content but also the replay of modified commands or memory content. The TOE shall be able to detect such attacks violating the TOE.

357 The TOE shall provide "Protection against an unauthorised rollback of external memory content (O.Pas-Mem-Unauth-Rollback-Prot)" as specified below.

O.Pas-Mem-Unauth-Rollback-Prot:	Protection against an unauthorised rollback of external memory content. The TOE shall protect against replacement of the external memory content with a previous version, even if it was valid in the past.

358 The security objective requires protection against the simulation of outdated memory content. Replacement of memory content with a previous version of the same content or the manipulations of write operations violate the freshness of the external memory content and shall be detected by the TOE.

359 The TOE shall provide "Passive external memory content Irreversibility Anchor (O.Pas-Mem- Irreversible-Anchor)" as specified below.

O.Pas-Mem-Irreversible-Anchor	Passive external memory content Irreversibility Anchor The TOE shall implement a reference inside the 3S that represents the current content of the external memory. This reference shall be updated, based on each authorised modification of the external memory to ensure freshness of the data.

360 The security objective requires the verification of freshness for data read from the external memory. Therefore, the 3S shall maintain a reference that represents the current content of the external memory. This reference needs to be updated with each authorised read and write operation to detect a violation of the data freshness. It should be maintained in any TOE operational state, including the standby and sleep states. In the case of non-volatile memory, the Irreversibility Anchor needs to be persistently saved between two boots.

361 The TOE shall provide "Protection against passive external memory cloning or replacement (O.Pas- Mem-Clone-Replace-Prot)" as specified below.

O.Pas-Mem-Clone-Replace-Prot:	Protection against passive external memory cloning or replacement. The TOE shall protect against cloning or replacement of user data with user data stored in the memory of another instance of the TOE and against replacement of the external memory with the one from another instance of the TOE.

362 The security objective requires protection against replacement of its external memory content with the external memory content of another instance of the TOE. The external memory content shall only be valid for the 3S that is initially linked to this external memory. The replacement of the external memory or the transfer of the content from a memory that is linked to another instance of the TOE shall be detected.

7.1.2.2 Security Objectives for the TOE Environment

Application Note 7-5(PP_AN 47)	This package does not include additional Security Objectives for the TOE Environment.

7.1.2.3 Security Objectives Rationale

	O.Pas-Mem-Content-Prot	O.Pas-Mem-Cmd-Replay-Prot	O.Pas-Mem-Irreversible- Anchor	O.Pas-Mem-Unauth-Rollback- Prot	O.Pas-Mem-Clone-Replace- Prot
T.Pas-Mem-Content-Abuse	X				
T.Pas-Mem-Cmd-Replay		X	X		
T.Pas-Mem-Unauth-Rollback			X	X	
T.Pas-Mem-Clone-Replace					X

Table 7-1 Mapping between objectives and threats

363 In the following, the justification of the coverage of the threats by the security objectives is given.

364 T.Pas-Mem-Content-Abuse is countered by O.Pas-Mem-Content-Prot, which requires the TOE to prevent disclosure and undetected modification of the content stored in external memory.

365 T.Pas-Mem-Cmd-Replay is countered by O.Pas-Mem-Cmd-Replay-Prot and O.Pas-Mem-Irreversible-Anchor as follows:

- O.Pas-Mem-Cmd-Replay-Prot requires protection against replay of commands exported from the 3S in the external memory mitigating T.Pas-Mem-Cmd-Replay.
- O.Pas-Mem-Irreversible-Anchor requires the implementation of a reference inside the 3S representing the current content of the external memory. The reference inside the 3S is updated associated with each change issued by the 3S on the external memory. This reference allows verification of the freshness of the data when they are loaded from the external memory.

366 T.Pas-Mem-Unauth-Rollback is countered by O.Pas-Mem-Unauth-Rollback-Prot and O.Pas-Mem-Irreversible-Anchor as follows:

- O.Pas-Mem-Unauth-Rollback-Prot requires that the TOE protects against replacement of external memory content with older content of the same external memory, where the data freshness property is not met, thereby mitigating this threat.
- O.Pas-Mem-Irreversible-Anchor requires that the TOE implements a reference inside the 3S representing the current content of the external memory. The reference inside the 3S is updated associated with each change issued by the 3S on the external memory. This reference allows verification of the freshness of the data when they are loaded from the external memory.

367 T.Pas-Mem-Clone-Replace is countered by O.Pas-Mem-Clone-Replace-Prot, which requires the TOE to

detect the replacement of the external memory content with one of a different TOE's memory, or physical replacement of the external memory with the external memory of a different instance of the TOE.

7.1.3 Extended Component Definition

7.1.3.1 Definition of the Family FDP_URC

368 The Protection Profile [5] defines the additional family (FDP_URC) of the Class FDP (User data protection) to verify the freshness of data stored in a physically separated memory. This family defines mechanisms to determine whether the content read from a physically separated memory meets the property of data freshness, by verifying that they are those resulting from the latest authorised operation (write or erase) of the TSF that modifies the content in the physically separated memory. If the content read from the physically separated memory cannot be uniquely linked to the latest authorised write or erase operation executed by the TSF, the data freshness property is not met, and the read data is rejected.

FDP_URC: Protection against an unauthorised rollback of memory content

Family behaviour:

This family defines functional requirements for the detection of an unauthorised rollback of content stored in the external memory.

Component Levelling

FDP_URC Protection against an unauthorized rollback of memory content	1

FDP_URC.1 Requires the TOE to protect against an unauthorised rollback of the content stored in the external memory.

Management FDP_URC.1

There are no management activities foreseen.

Audit FDP_URC.1

There are no actions defined to be auditable.

FDP_URC.1 Protection against an unauthorised rollback of memory content

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 or FDP_IRA.1

FDP_URC.1.1 The TOE shall detect an unauthorised replacement of the content stored in [assignment: physically separated memory] before the content is used. The detection shall be effective in any case where modification or read operation depends on the current content of this external memory.

FDP_URC.1.2 Upon detection of unauthorised rollback of the content stored in a physically separated memory, the TOE shall [selection: *stop TOE operation, [assignment: other actions]*].

7.1.3.2 Definition of the Family FDP_IRA

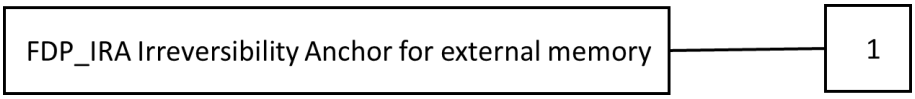
369 The family "Irreversibility Anchor of external memory content (FDP_IRA)" is specified as follows.

FDP_IRA **Irreversibility Anchor for external memory**

Family behaviour:

This family provides requirements for the implementation of a mechanism that verifies that read operations from this physically separated memory always represent the latest authorised modification of this memory. The TSF provides an Irreversibility Anchor that maintains a link between a transaction counter associated write or erase operation and the data transferred to a physically separated memory. Thereby, the Irreversibility Anchor allows to determine, whether a data read operation from the physically separated memory represents the data, based on the latest write or erase operation. The anchor is implemented in an irreversible way representing unique states (i.e., without the possibility of reverting to previous states). The pattern maintained by the Irreversibility Anchor value allows verification of the data freshness provided by subsequent read operations to the physically separated memory. If the physically separated memory is a non-volatile memory, the Irreversibility Anchor shall be maintained in any operational state of the TOE.

Component levelling



FDP_IRA.1 Requires the TOE to verify that read operations from a physically separated memory represent always the latest authorised modification of this memory.

Management: FDP_IRA.1

There are no management activities foreseen.

Audit: FDP_IRA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Any violation of the data freshness detected upon a read operation from the physically separated memory.

FDP_IRA.1 **Irreversibility Anchor for external memory**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_IRA.1.1 The TOE shall implement an Irreversibility Anchor mechanism to verify the freshness of data stored in [assignment: physically separated memory].

FDP_IRA.1.2 The Irreversibility Anchor shall provide a reference for [selection: write, erase, [assignment: other operation that changes the content of the physically separated memory]] transactions, such that that each transaction of this type shall be associated with a different value of the Irreversibility Anchor.

FDP_IRA.1.3 The state of the Irreversibility Anchor implemented by the TSF shall be maintained

during [selection: operation, power off, power saving, any operation mode].

7.1.4 IT Security Requirements

Application Note 7-6(PP_AN 48) All SFR comprise an iteration identifier to support the integration in this Security Target.

7.1.4.1 SFRs for the TOE

370 The TOE shall meet the requirement "Data Authentication with Identity of Guarantor (FDP_DAU.2)", as specified below.

FDP_DAU.2/PM	Data Authentication with Identity of Guarantor
Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/PM	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of *data objects and containers stored in the passive external memory*.
FDP_DAU.2.2/PM	The TSF shall provide *the 3S* with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.
Refinement:	The TSF generates the evidence that the data objects and containers stored in the external memory are generated by the dedicated 3S instance, based on FDP_IRA.1/PM, FDP_SDC.1/PM and FDP_SDI.2/PM.

The TOE shall meet the requirement "Timing of identification (FIA_UID.1)", as specified below.

FIA_UID.1/PM	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/PM	The TSF shall allow *any TSF-mediated actions that do not access data objects and/or containers stored in the external memory* on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PM	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Refinement:	The user is the 3S itself. The data objects and containers stored in the passive external memory need to be identified before any further action.

371 The TOE shall meet the requirement "Replay detection (FPT_RPL.1)", as specified below.

FPT_RPL.1/PM	Replay detection
Hierarchical to:	No other components
Dependencies:	No dependencies

FPT_RPL.1.1/PM	The TSF shall detect replay for the following entities: *commands issued by the 3S to the passive external memory for the read, write and erase operations.*
FPT_RPL.1.2/PM	TSF shall perform *1) halt the boot procedure* *2) return an error status* when a replay is detected.

Application Note 7-7(PP_AN 49) The TSF stops the boot procedure and returns an error message in case replay is detected.

372 The TOE shall meet the requirement "Protection against an unauthorised rollback of content (FDP_URC.1)", as specified below.

FDP_URC.1/PM	Protection against an unauthorised rollback of memory content
Hierarchical to:	No other components.

373

Dependencies:	FIA_UAU.1 or FDP_IRA.1
FDP_URC.1.1/PM	The TOE shall detect an unauthorised replacement of the content stored in *passive external memory* before the content is used. The detection shall be effective in any case where modification or read operation depends on the current content of this external memory.
FDP_URC.1.2/PM	Upon detection of unauthorised rollback of the content stored in a physically separated memory, the TOE shall stop TOE operation*, and return an error status*.

374 The TOE shall meet the requirement "Irreversibility Anchor for external memory (FDP_IRA.1)", as specified below.

FDP_IRA.1/PM	Irreversibility Anchor for external memory
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_IRA.1.1/PM	The TSF shall verify the freshness of data for each read operation from *the passive external memory*.
FDP_IRA.1.2/PM	The Irreversibility Anchor shall maintain a distinct transaction reference for each *write, erase* operation and that is unambiguously linked with the current content of the transaction with the associated physically separated memory.
FDP_IRA.1.3/PM	The state of the Irreversibility Anchor implemented by the TSF shall be maintained during any operation mode.
Refinement:	The passive external memory is considered outside the TOE, even though it may be packaged together with the SoC including the 3S.

375 The TOE shall meet the requirement "Stored data confidentiality (FDP_SDC.1/PM)" as specified below.

FDP_SDC.1/PM	Stored data confidentiality
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_SDC.1.1/PM	The TSF shall ensure the confidentiality of the information of the user data while it is stored in the *external memory*.

The TOE shall meet the requirement "Stored data integrity monitoring and action (FDP_SDI.2/PM)" as specified below.

FDP_SDI.2/PM	Stored data integrity monitoring and action
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
FDP_SDI.2.1/PM	The TSF shall monitor user data stored in containers controlled by the TSF for *cryptographic integrity errors* on all objects, based on the following attributes: *digital signature or authentication tag.*
FDP_SDI.2.2/PM	Upon detection of a data integrity error, the TSF shall *stop TOE operation and return an error status.*
Refinement:	This SFR applies for passive external memory.

7.1.4.2 Rationale for the SFRs

376 Table 7-2 below provides an overview, how the SFRs are combined to meet the security objectives. The justification for each objective is detailed after the table.

Objective	TOE Security Functional and Assurance Requirements
O.Pas-Mem-Content-Prot	FDP_SDC.1/PM for confidentialityprotection FDP_SDI.2/PM for integrity protection
O.Pas-Mem-Cmd-Replay-Prot	FPT_RPL.1/PM for Replay detection
O.Pas-Mem-Irreversible-Anchor	FDP_IRA.1/PM for Irreversibility Anchor of external memory content
O.Pas-Mem-Unauth- Rollback-Prot	FDP_URC.1/PM for Protection against an unauthorised rollback of content Supported by: FDP_IRA.1/PM for Irreversibility Anchor of external memory content
O.Pas-Mem-Clone-Replace-Prot	FDP_DAU.2/PM for Data Authentication with Identity of Guarantor FIA_UID.1/PM for Timing of identification

Table 7-2 Mapping between Objectives and SFRs for passive external memory

377 The justification related to the security objective "Protection against unauthorised disclosure and undetected modification of external memory content (O.Pas-Mem-Content-Prot)" is as follows:

378 The SFR FDP_SDC.1/PM ensures protection of confidentiality of the content stored in the external memory, while the SFR FDP_SDI.2/PM ensures protection of the integrity of the content stored in the external memory. The protection is under full control inside the 3S, so the transfer between the 3S and the external memory is also protected. Therefore, these SFRs support the objective.

379 The justification related to the security objective "Protection against replay of commands between the 3S and the external memory (O.Pas-Mem-Cmd-Replay-Prot)" is as follows:

380 The SFR FPT_RPL.1/PM requires the TSF to detect replayed transactions (read, write and erase operations) to the external memory. This requirement is considered in the assignment of FPT_RPL.1.1/PM. Therefore, this SFR supports the objective.

381 The justification related to the security objective "Protection against content (O.Pas-Mem-Unauth- Rollback-Prot)" is as follows:

382 The SFR FDP_URC.1/PM requires that the TSF detects the case when the content of the external memory has been replaced by previous versions of them. In this way, this SFR supports the objective. The SFR FDP_IRA.1/PM unambiguously links the current content of the transaction with the associated physically separated memory to a distinct transaction references and thereby ensures that an unauthorised replacement of the memory content is detected.

383 The justification related to the security objective "External memory content Irreversibility Anchor (O.Pas-Mem-Irreversible-Anchor)" is as follows:

384 The SFR FDP_IRA.1/PM requires the TOE to implement distinct transaction references for each write and erase operation that is unambiguously linked with the current content of the transaction with the external memory. Thereby, the data freshness can be verified during a read operation, based on the data maintained by the irreversible anchor. If the external memory is non-volatile, the Irreversibility Anchor needs to be maintained in any operation mode. By providing the mechanism required by this SFR, the security objective O.Pas-Mem-Irreversible-Anchor is directly supported.

385 The justification related to the security objective "Protection against external memory cloning or replacement (O.Pas-Mem-Clone-Replace-Prot)" is as follows:

386 The SFR FDP_DAU.2/PM requires the TOE to be able to generate evidence that guarantees the validity of data objects and containers stored in the external memory. The cloning or replacement of the external memory is detected, based on FIA_UID.1/PM, which requires the user identification before any data objects or containers stored in the external memory are accessed. By providing the mechanism required by these two SFRs, the security objective O.Pas-Mem-Clone-Replace-Prot is directly supported.

7.1.4.3 Dependencies of SFRs

Requirement	No dependency	Satisfied Dependencies
FDP_SDC.1/PM	No dependency	-
FDP_SDI.2/PM	No dependency	-
FPT_RPL.1/PM	No dependency	-

FDP_IRA.1/PM	No dependency	-
FDP_URC.1/PM	FIA_UAU.1 or FDP_IRA	Satisfied by FDP_IRA.1/PM
FDP_DAU.2/PM	FIA_UID.1	Satisfied by FIA_UID.1/PM
FIA_UID.1/PM	No dependency	-

Table 7-3 Overview of SFR dependencies for passive external memory

387 All dependencies are satisfied.

7.2 Package for Loader Functionality

7.2.1 Security Problem Definition

7.2.1.1 Description of Assets

Application Note 7-8(PP_AN 59) There are no additional assets defined in this package.

7.2.1.2 Threat

Application Note 7-9(PP_AN 60) No new threat is defined in this package while all threats of the base Protection Profile [5] are applicable to the loader package.

7.2.1.3 Organisational Security Policies

388 The Loader Package defines a secure loading process.

389 This package supports access control on usage of the Loader, mutual authentication of the TOE and the authorised user as end-points of a trusted channel and protection of integrity and confidentiality of the data downloaded to the TOE.

P.Access-Ctlr-Loader	Loader Functionality with User Authorisation Authorised user controls the usage of the Loader functionality in order to protect user data stored and loaded to the TOE from disclosure and manipulation.

7.2.1.4 Assumption

Application Note 7-10(PP_AN 61) This package does not define an additional assumption.

7.2.2 Security Objectives

7.2.2.1 Security Objectives for the TOE

390 The TOE shall provide "Access control and authenticity for the Loader (O.Ctrl-Auth-Loader)" as specified below.

O.Ctrl-Auth-Loader	Access control and authenticity for the Loader The TSF provides trusted communication channel with authorised user, supports confidentiality protection and authentication of the user data to be loaded and access control for usage of the Loader functionality.

7.2.2.2 Security Objectives for the Environment

391 The operational environment of the TOE shall provide "Secure communication and usage of the Loader (OE.Loader-Usage)" as specified below.

OE.Loader-Usage	Secure communication and usage of the Loader The authorised user shall support a trusted communication channel with the TOE which protects confidentiality and proofs authenticity of data to be loaded and fulfilling the access conditions required by the Loader.

7.2.2.3 Security Objectives Rationale

	O.Ctrl-Auth-Loader	OE.Loader-Usage
P.Access-Ctlr-Loader	X	X

Table 7-4 Mapping overview between objectives and threats respectively policies

392 The organisational security policy "Controlled usage to Loader Functionality (P.Access-Ctlr-Loader) is directly implemented by the security objective for the TOE "Access control and authenticity for the Loader (O.Ctrl-Auth-Loader)" and the security objective for the TOE environment "Secure communication and usage of the Loader (OE.Loader-Usage)".

7.2.3 Extended Component Definition

Application Note 7-11(PP_AN 62) This package does not define additional extended components.

7.2.4 IT Security Requirements

7.2.4.1 SFRs for the TOE

393 The TOE shall meet the requirement "Inter-TSF trusted channel (FTP_ITC.1)" is specified as follows.

FTP_ITC.1/Load	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/Load	The TSF shall provide a communication channel between itself and *the authorized user for using the Bootloader* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/Load	The TSF shall permit another trusted IT product to initiate communication via the trusted channel.
FTP_ITC.1.3/Load	The TSF shall initiate communication via the trusted channel for deploying Loader *Authentication sequence*.

394 The TOE shall meet the requirement "Basic data exchange confidentiality (FDP_UCT.1)" is specified as follows.

FDP_UCT.1/Load	**Basic data exchange confidentiality**
Hierarchical to:	No other components.

Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/Load	The TSF shall enforce the Loader SFP to receive user data in a manner protected from unauthorised disclosure.

395 The TOE Functional Requirement "Data exchange integrity (FDP_UIT.1)" is specified as follows.

FDP_UIT.1/Load	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FDP_UIT.1.1/Load	The TSF shall enforce the Loader SFP to receive user data in a manner protected from modification, deletion, insertion errors.
FDP_UIT.1.2/Load	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion has occurred.

396 The TOE shall meet the requirement "Subset access control - Loader (FDP_ACC.1/Load)" is specified as follows.

FDP_ACC.1/Load	Subset access control - Loader
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1/Load	The TSF shall enforce the Loader SFP on (1) the subjects *Authentication Sequence*, (2) the objects user data in *external FLASH memory*, (3) the operation deployment of Loader.

Application Note 7-12(PP_AN 63) The TOE enforces the Loader SFP by FTP_ITC.1, FDP_UCT.1 and FDP_UIT.1 and FDP_ACF.1 to describe additional access control rules.

397 The TOE shall meet the requirement "Security attribute based access control - Load (FDP_ACF.1/Load)" is specified as follows.

FDP_ACF.1/Load	Security attribute based access control - Load
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1/Load	The TSF shall enforce the *Loader SFP* to objects, based on the following: (1) the subjects *Bootloader* with security attributes *SRAM loading* (2) the objects *user data in external DRAM memory* with security attributes *SRAM*

loading

FDP_ACF.1.2/Load	The TSF shall enforce the following rules to determine whether an operation among controlled subjects and controlled objects is allowed: *Bootloader can do loading operation in SRAM after succession of Authentication*.
FDP_ACF.1.3/Load	The TSF shall explicitly authorise access of subjects to objects, based on the following additional rules: *SRAM can be controlled based on security attributes ,which can be limited by Bootloader sequence.*
FDP_ACF.1.4/Load	The TSF shall explicitly deny access of subjects to objects, based on the following additional rules: *Bootloader can't loading the SRAM without succession of Authentication*.

Application Note 7-13(PP_AN 64) Bootloader is only allowed in ROM Booting mode.

7.2.4.2 Rationale for the SFRs

Objective	TOE Security Functional and Assurance Requirements
O.Ctrl-Auth-Loader	FTP_ITC.1/Load Inter-TSF trusted channel FDP_UCT.1/Load Basic data exchange confidentiality FDP_UIT.1/Load Data exchange integrity FDP_ACC.1/Load Subset access control – Load FDP_ACF.1/Load Security attribute based access control - Load

Table 7-5 Mapping between Objectives and SFRs for the Loader

398 The security objective Access control and authenticity for the Loader (O.Ctrl-Auth-Loader) is covered by the SFR as follows:

399 The SFR FDP_ACF.1/Load and FDP_ACC.1/Load require the TSF to implement access control for the Loader functionality.

400 The SFR FTP_ITC.1/Load, FDP_UCT.1/Load and FDP_UIT.1/Load require the TSF to establish a trusted channel with assured identification of its end points, encryption and protection of the channel data from modification or disclosure.

7.2.4.3 Dependencies of the SFRs

Requirement	No dependency	Satisfied Dependencies
FTP_ITC.1/Load	No dependency	

Requirement	No dependency	Satisfied Dependencies

FDP_UCT.1/Load	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FTP_ITC.1/Load and FDP_ACC.1/Load
FDP_UIT.1/Load	[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FTP_ITC.1/Load and FDP_ACC.1/Load
FDP_ACC.1/Load	FDP_ACF.1	FDP_ACF.1/Load
FDP_ACF.1/Load	FMT_MSA. FMT_SM1	The dependencies FMT_MSA.3 is not satisfied, see the rationale below the table

Table 7-6 Overview of SFR dependencies for the Loader package

401 The SFR FMT_MSA.3 and its dependencies FMT_MSA.1 and FMT_SMR.1 are not defined, because the security attributes shall not be changed. Each software image loaded in the TOE shall be checked and verified in the same way. Therefore, no functionality and no role are required to manage the security attributes.

7.3 Package for Cryptographic Services

402 This section defines a general optional package for cryptographic services that may be provided by a TOE.

7.3.1 Security Problem Definition

7.3.1.1 Description of Assets

403 The assets are covered by the asset description in the base PP.

7.3.1.2 Threats

404 No new threats are included in this package while all threats of the base Protection Profile [5] are applicable to these cryptographic services.

7.3.1.3 Organisational Security Policies

405 The cryptographic security services described in this package implement the organizational security policy comprising a list with the implemented cryptographic services. The use of this services by the Composite Software is optional.

406 The TOE shall implement the policy "Cryptographic service of the TOE (P.Crypto-Service)" as specified below.

P.Crypto-Service Cryptographic service of the TOE

The TOE provides secure platform based cryptographic services that can be used by the Composite Software.

Application Note 7-14(PP_AN 65) The organizational security policy P.Crypto-Service shall be implemented by separate security objectives for each cryptographic service. Each security objective can be directly implemented by specific SFR of the class "Cryptographic Support". This is a hardware implementation of the cryptographic algorithm. The cryptographic services is provided as library functions that need to be compiled together with the Composite Software.

7.3.1.4 Assumption

407 This package does not define an additional assumption.

7.3.2 Security Objectives

7.3.2.1 Security Objectives for the TOE

408 The TOE shall provide the "Cryptographic service (O.Crypto-Service)" as specified below.

O.Crypto-Service Cryptographic Algorithm

The TOE provides the cryptographic algorithm for the selected cryptographic operations and the selected modes of operation for the following Triple-DES, AES, RSA, ECC, SHA, HMAC, KDF and ML-DSA.

409 The security objectives listed under "Cryptographic service (O.Crypto-Service)" enforces the organizational security policy P.Crypto-Service.

7.3.2.2 Security Objectives for the TOE Environment

410 This package does not include additional Security Objectives for the TOE Environment.

7.3.2.3 Security Objectives Rationale

	O.Crypto-Services
P.Crypto-Service	X

Table 7-7 Mapping between OSP and objectives

411 The organisational security policy "Cryptographic services of the TOE (P.Crypto-Service) is directly implemented by the security objective(s) for the TOE "Cryptographic Algorithm (O.Crypto-Service)".

7.3.3 Extended Component Definition

412 This package does not define additional extended components.

7.3.4 IT Security Requirements

Application Note 7-15(PP_AN 67) As described in this application note of the PP, the SFR "FCS_COP.1/iteration" is replaced by the FCS_COP.1 iterations given in this Security Target.

Application Note 7-16(PP_AN 68) The set of cryptographic algorithms supported by the TOE is based on well established standards.

Application Note 7-17(PP_AN 69) As described in this application note of the PP, the SFR "FCS_CKM.4/iteration" is replaced by the FCS_CKM.4 iterations given in this Security Target.

7.3.4.1 SFRs for the TOE

Triple-DES Operation

413 The Triple DES (TDES) operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/TDES	Cryptographic operation – TDES
Hierarchical to:	No other components.
FCS_COP.1.1/TDES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Triple Data Encryption Standard (TDES) – ECB mode* and cryptographic key sizes *112 bit or 168 bit key size* that meet the following: *[FIPS SP800-67], chapter 2 and 3. TOE implements TDES with key option 1 and 2 with ECB mode.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

414 The TOE shall meet the requirement "Cryptographic key destruction – TDES FCS_CKM.4/TDES)" as specified below.

FCS_CKM.4/TDES	Cryptographic Key destruction – TDES
Hierarchical to:	No other components.
FCS_CKM.4.1/TDES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-18	The cryptographic key destruction can be done by overwriting the internal stored key

AES Operation

415 The AES operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/AES	Cryptographic operation – AES
Hierarchical to:	No other components.
FCS_COP.1.1/AES	The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *Advanced Encryption Standard (AES) – ECB, CTR, CBC*

	and GCM mode and cryptographic key sizes *128bit, 192bit or 256bit key size* that meet the following: *[FIPS197], chapter 5*.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

416 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/AES	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/AES	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *overwriting or setting key clear bit* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-19	The cryptographic key destruction can be done by security action overwriting the internal stored key.

Key Manager (KDF) Operation

417 The Key Manager (KDF) operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/KDF_KeyWrap	Cryptographic operation – KDF with Key Wrap
Hierarchical to:	No other components.
FCS_COP.1.1/KDF_KeyWrap	The TSF shall perform *key management of AES* in accordance with a specified key derivation function with *Key wrap (AES) and* cryptographic key sizes *128bit, 192bit or 256bit key size* that meet the following: *[SP800-38F].*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

418 The Key Manager (KDF) operation of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/KDF_KBKDF	Cryptographic operation – KDF with KBKDF

Hierarchical to:	No other components.
FCS_COP.1.1/KDF_KBKDF	The TSF shall perform *key management of HMAC* in accordance with a specified key derivation function with *KBKDF (HMAC) in Counter mode - SHA2-256/384/512, SHA3-224/256/384/512 and cryptographic key sizes 256bit, 512bit, 768bit, 1024bit, 1152bit* that meet the following: *[SP800-108]*.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

419 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/KDF	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/KDF	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *setting key clear bit* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-20	The cryptographic key destruction can be done by setting control register.

Secure Hash Algorithm (SHA_HW)

420 This SFR related to SHA-2/ SHA-3/ HMAC hardware engines in the Security Controller.

421 The Secure Hash Algorithm (SHA_HW) of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/SHA_HW	Cryptographic operation-SHA
Hierarchical to:	No other components.
FCS_COP.1.1/SHA_HW	The TSF shall perform *secure hash computation* in accordance with a specified cryptographic algorithm *SHA2-256/384/512, SHA3-224/256/384/512, SHAKE128/256* and cryptographic key sizes *none* that meet the following: *[FIPS PUB 180-3], [FIPS PUB 202]*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Hash-based Message Authentication Code (HMAC)

422 The Hash-based Message Authentication Code (HMAC) of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/HMAC	Cryptographic operation-HMAC
Hierarchical to:	No other components.
FCS_COP.1.1/HMAC	The TSF shall perform *keyed-Hash Message Authentication Code* in accordance with a specified cryptographic algorithm *HMAC* and cryptographic key sizes *SHA2-256/384/512, SHA3-224/256/384/512* that meet the following: *[FIPS PUB 198-1]*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

423 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/HMAC	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/HMAC	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *setting key clear bit* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-21	The cryptographic key destruction can be done by setting control register.

Rivest-Shamir-Adleman (RSA) Operation (optional)

424 The AH3 Secure RSA/ECC/SHA library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/RSA	Cryptographic operation – RSA
Hierarchical to:	No other components.
FCS_COP.1.1/RSA	The TSF shall perform *the modular exponentiation part of RSA signature generation and verification* in accordance with a specified cryptographic algorithm Rivest-Shamir-Adleman (RSA:standard RSA and RSA-CRT) and cryptographic key *sizes from 1900-bit up to 4096-bit with 2-bit granularity* that meet the following: *[ISO/IEC14888-2:2008] section 6.2 and 6.3.* Note 1: In context of signature generation only the modular exponentiation, i.e. only Step 2 of [ISO14888-2:2008], section 6.2 and in addition the check of the message's length are

implemented. Especially the proper use of a format mechanism (including the related hash algorithm) is in the responsibility of the embedded software developer.

Note 2: In context of signature verification only the modular exponentiation, i.e. only the part asking to compute G* = S^v mod n in Step 1 of [ISO/IEC14888-2:2008], section 6.3 is implemented. Especially the proper check of a signatures format (including the related hash algorithm) is in the responsibility of the embedded software developer.

Dependencies: [FDP_ITC.1 Import of user data without security attributes or
FDP_ITC.2 Import of user data with security attributes or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

Rivest-Shamir-Adleman (RSA) Key Generation (optional)

425 The RSA key generation for the AH3 Secure RSA/ECC/SHA library shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

FCS_CKM.1/RSA Cryptographic key generation – RSA

Hierarchical to: No other components.

FCS_CKM.1.1/RSA The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm *RSA* and specified cryptographic key sizes *from 1900-bit up to 4096-bit with 2-bit granularity* that meet the following: *[ETSI TS 102 176-1], section 6.2.2.1 Key and parameter generation algorithm rsagen1 and [ISO 18032], Incremental search.*

Dependencies: [FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

Note 1: The RSA cryptographic key generation of the TOE generates two primes P and Q with the equal bit length, while the standard recommends to generate two primes P and Q such that 0.1 < |log_2(P)-log_2(Q)| < 30. This inequality is not assured by the RSA cryptographic key generation routine of the TOE and must be implemented by the user.

Note 2: While the standard specifies that the private exponent D should be larger than the square root of the RSA modulus, i.e. D > sqrt(N), this verification is not performed by the RSA cryptographic key generation of the TOE. It must be implemented by the user.

Note 3: The RSA cryptographic key generation of the TOE performs a number of Miller-Rabin tests to ensure that the probability that the generated prime candidate is not a prime is below 2^(-100).

426 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/RSA	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/RSA	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroing that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-22	The key destruction FCS_CKM.4/ RSA applies only for the keys stored by the AH3 Secure RSA/ECC/SHA library in CryptoRAM and/or RAM. This internal key storage can be cleared either through a hardware reset or by using the key destruction function.

Elliptic Curve DSA Operation (optional)

427 The ECC library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/ECDSA	Cryptographic operation – ECDSA
Hierarchical to:	No other components.
FCS_COP.1.1/ECDSA	The TSF shall perform *the signature generation/verification* in accordance with the specified cryptographic algorithm *ECDSA* and cryptographic key *sizes from 224-bit up to 512-bit* that meet the following*: [ANS X9.62] , section 7.3 Signing Process and section 7.4 Verifying Process.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Note 1: The AH3 Secure RSA/ECC/SHA library supports any valid curves over prime fields of size from 224-bit to 512-bit. However standard curves listed below whose security has been proven are in the scope of this evaluation. 1) [NIST curves]: Curves P-224, P-256, P-384 2) [Brainpool curves]: brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, 3) [SEC-recommended curves]: secp224k1, secp224r1, secp256k1, secp256r1, secp384r1

Elliptic Curve DSA Key Generation (optional)

428 The key generation for the ECC library shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

FCS_CKM.1/ECDSA	Cryptographic key generation – ECDSA
Hierarchical to:	No other components.
FCS_CKM.1.1/ECDSA	The TSF shall generate cryptographic keys in accordance with the cryptographic key generation algorithm *ECC* and with the cryptographic key sizes *from 224-bit up to 512-bit* that meet the following: *[ANS X9.62] , section A.4.3 Elliptic Curve Key Generation*.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

Note 1: The AH3 Secure RSA/ECC/SHA library supports any valid curves over prime fields of size from 224-bit to 512-bit. However standard curves listed below whose security has been proven are in the scope of this evaluation. 1) [NIST curves]: Curves P-224, P-256, P-384, P-521 2) [Brainpool curves]: brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, 3) [SEC-recommended curves]: secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1

429 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/ECDSA	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/ECDSA	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroing* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-23	The key destruction FCS_CKM.4/ECDSA applies only for the keys stored by the AH3 Secure RSA/ECC/SHA library in CryptoRAM and/or RAM. This internal key storage can be cleared either through a hardware reset or by using the key destruction function.

Elliptic Curve Diffie-Hellman (ECDH) Key Agreement (optional)

430 The ECC library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/ECDH	Cryptographic operation – ECDH
Hierarchical to:	No other components.
FCS_COP.1.1/ECDH	The TSF shall perform *the key exchange* in accordance with the specified cryptographic algorithm *ECDH* and cryptographic key sizes *from 224-bit up to 512-bit* that meet the following: *[ANS X9.63], section 5.4.1 Standard Diffie-Hellman primitive*.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Note 1: The AH3 Secure RSA/ECC/SHA library supports any valid curves over prime fields of size from 224-bit to 512-bit. However standard curves listed below whose security has been proven are in the scope of this evaluation. 1) [NIST curves]: Curves P-224, P-256, P-384, P-521 2) [Brainpool curves]: brainpoolP224r1, brainpoolP224t1, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1, brainpoolP512t1, 3)[SEC-recommended curves]: secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1

Note 2: The implemented routines can be used with ephemeral or static private keys. The base point is assumed to be public.

Note 3: For full compatibility, the user is responsible to perform step 2 of [ANS X9.63], section 5.2.2.1, prior to using the ECDH_generate function.

431 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/ECDH	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/ECDH	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroing* that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-24	The key destruction FCS_CKM.4/ECDH applies only for the keys stored by the AH3 Secure RSA/ECC/SHA library in CryptoRAM and/or RAM. This internal key storage can be cleared either through a hardware reset or by using the key destruction function.

Secure Hash Algorithm (SHA_SW) (optional)

432 This SFR related to AH3 Secure RSA/ECC/SHA library for the support of RSA, ECC and SHA cryptographic operations (optional).

433 The Secure Hash Algorithm (SHA_SW) of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/SHA_SW	Cryptographic operation-SHA
Hierarchical to:	No other components.
FCS_COP.1.1/SHA_SW	The TSF shall perform *secure hash computation* in accordance with a specified cryptographic algorithm *SHA256, SHA384 and SHA512* and cryptographic key sizes *none* that meet the following: *[FIPS PUB 180-3].*

Note 1: The TOE offers the functionality of hash value computation using SHA-1, SHA-256, SHA-384 and SHA-512. However, only the functions related to SHA-256, SHA-384 and SHA-512 are in scope of this evaluation and are intended to be used only for signature generation and verification. Note that neither of the functions must be used to hash secret values. In addition, the user is responsible for the truncation or padding of the hash value as required by step e), section 7.3 and step c), section 7.4.1 of the standard cited above.

Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

Module-Lattice Based Digital Signature Algorithm (ML-DSA) Operation (optional)

434 The AH3 Secure ML-DSA library of the TOE shall meet the requirement "Cryptographic operation (FCS_COP.1)" as specified below.

FCS_COP.1/PQC	Cryptographic operation – ML-DSA
Hierarchical to:	No other components.
FCS_COP.1.1/PQC	The TSF shall perform *Lattice Operations of ML-DSA signature generation and verification* in accordance with a specified cryptographic algorithm *ML-DSA (ML-DSS: standard ML-DSA)* and cryptographic key sizes *ML-DSA-44 and ML-DSA-65* that meet the following: *[FIPS 204] section 6.2 ML-DSA Signing (Internal) and section 6.3 ML-DSA Verifying (Internal).*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Application Note 7-25	The AH3 Secure ML-DSA library of the TOE implements the signature and verification functionality as defined in sections *6.2 ML-DSA Signing (Internal)* and *6.3 ML-DSA Verifying (Internal)* of [FIPS 204]. It is the responsibility of the

embedded software developer to follow [FIPS 204] sections 5.2 and 5.3 to implement the External functions defined in the standard [FIPS 204].

Module-Lattice Based Digital Signature Algorithm (ML-DSA) key generation (optional)

435 The AH3 Secure ML-DSA library shall meet the requirement "Cryptographic key generation (FCS_CKM.1)" as specified below.

FCS_CKM.1/PQC	Cryptographic key generation – ML-DSA
Hierarchical to:	No other components.
FCS_CKM.1.1/PQC	The TSF shall generate cryptographic keys in accordance with the specified cryptographic key generation algorithm *ML-DSA* and specified cryptographic key sizes *ML-DSA-44, ML-DSA-65* that meet the following: *[FIPS 204] section 5.1 (ML-DSA Key Generation).*
Dependencies:	[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Application Note 7-26	The AH3 Secure ML-DSA library of the TOE implements the key generation function following section 5.1 ML-DSA Key Generation of [FIPS 204]. In this implementation, the 32-byte random seed ξ used by the ML-DSA Key Generation algorithm is generated using a PTG.2 class compliant TRNG (see FCS_RNG.1/PTG.2) with the SHAKE256 algorithm (see FCS_COP.1/SHA_HW) used as conditioning component. This construction meets the freshness and security strength requirements outlined in the [FIPS 204] standard. The internal function defined in section 6.1 ML-DSA Key Generation (Internal) of [FIPS 204] is not provided as a separate API.

436 The TOE shall meet the requirement "Cryptographic key destruction (FCS_CKM.4)" as specified below.

FCS_CKM.4/PQC	Cryptographic key destruction
Hierarchical to:	No other components.
FCS_CKM.4.1/PQC	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroing that meets the following: *none.*
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Application Note 7-27	The key destruction FCS_CKM.4/PQC applies only for the keys stored by the AH3 Secure ML-DSA library in CryptoRAM and/or RAM. This internal key storage can be cleared either through a hardware reset or by using the key destruction function.

7.3.4.2 Rationale for the SFRs

Objective	TOE Security Functional and Assurance Requirements
O.Crypto-Services	FCS_COP.1/TDES FCS_CKM.4/TDES FCS_COP.1/AES FCS_CKM.4/AES FCS_COP.1/SHA_HW (SHA2/3) FCS_COP.1/KDF_KeyWrap FCS_COP.1/KDF_KBKDF FCS_CKM.4/KDF FCS_COP.1/HMAC FCS_CKM.4/HMAC FCS_COP.1/RSA FCS_CKM.1/RSA FCS_CKM.4/RSA FCS_COP.1/ECDSA FCS_CKM.1/ECDSA FCS_CKM.4/ECDSA FCS_COP.1/ECDH FCS_CKM.4/ECDH FCS_COP.1/SHA_SW (SHA2) FCS_COP.1/PQC FCS_CKM.1/PQC FCS_CKM.4/PQC

Table 7-8 Mapping between Objectives and SFRs for the Cryptographic Services

437 The FCS_COP.1/TDES, FCS_CKM.4/TDES, FCS_COP.1/AES, FCS_CKM.4/AES, FCS_COP.1/SHA_HW (SHA2/3), FCS_COP.1/KDF_KeyWrap, FCS_COP.1/KDF_KBKDF, FCS_CKM.4/KDF, FCS_COP.1/HMAC, FCS_CKM.4/HMAC, FCS_COP.1/RSA, FCS_CKM.1/RSA, CS_CKM.4/RSA, FCS_COP.1/ECDSA, FCS_CKM.1/ECDSA, FCS_CKM.4/ECDSA, FCS_COP.1/ECDH, FCS_CKM.4/ECDH, FCS_COP.1/SHA_SW(SHA2), FCS_COP.1/PQC, FCS_CKM.1/PQC and FCS_CKM.4/PQC meet the security

objective “Cryptographic service (O.Crypto-Services)”.

7.3.4.3 Dependencies of the SFRs

438 Table 7-9 below lists the security functional requirements defined in this Security Target, their dependencies and whether they are satisfied by other security requirements defined in this Security Target. The text following the table discusses the remaining cases.

Security Functional Requirement	Dependencies	Fulfilled by security requirements
FCS_COP.1 /TDES	FCS_CKM.4	Yes (by environment, see discussion below)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.4/TDES	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1 /AES	FCS_CKM.4	Yes (by environment, see discussion below)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.4/AES	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1 /KDF	FCS_CKM.4	Yes (by environment, see discussion below)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.4/KDF	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1 /SHA_HW	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,FCS_CKM.4	See discussion below
FCS_COP.1 /HMAC	FCS_CKM.4	Yes (by environment, see discussion below)
	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.4/HMAC	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_CKM.1 /RSA	FCS_COP.1 or FCS_CKM.2	Yes

Security Functional Requirement	Dependencies	Fulfilled by security requirements
(optional)	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_COP.1/RSA (optional)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_CKM.4/RSA (optional)	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1/ECDSA (optional)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_CKM.1 /ECDSA (optional)	FCS_COP.1 or FCS_CKM.2	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_CKM.4/ECDSA (optional)	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1/ECDH (optional)	FDP_ITC.1 or FDP_ITC.2, or FCS_CKM.1	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_CKM.4/ECDH (optional)	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)
FCS_COP.1/SHA_SW (optional)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,FCS_CKM.4	See discussion below
	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
FCS_CKM.1/PQC (optional)	FCS_COP.1 or FCS_CKM.2	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_COP.1/PQC (optional)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Yes
	FCS_CKM.4	Yes (by environment, see discussion below)
FCS_CKM.4/PQC (optional)	FDP_ITC.1 or FDP_ITC.2 (if not FCS_CKM.1) or FCS_CKM.1	Yes (by environment, see discussion below)

Table 7-9 Overview of SFR dependencies for the Cryptographic Services

439 The functional requirements FCS_CKM.1 which are dependent to FCS_COP.1/TDES and FCS_COP.1/AES

are not included in this Security Target since the TOE only provides an engine for encryption and decryption. But the Security IC Embedded Software may fulfill these requirements related to the needs of the implemented application. The dependent requirements of FCS_COP.1/TDES and FCS_COP.1/AES concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

440 The functional requirements FCS_CKM.1 which are dependent to FCS_COP.1/HMAC is not included in this Security Target since the TOE only provides an engine for message digesting. But the Security IC Embedded Software may fulfill these requirements related to the needs of the implemented application. The dependent requirements of FCS_COP.1/HMAC concerning these functions shall be fulfilled by the environment (Security IC Embedded Software).

441 The TOE provides the cryptographic key generation for RSA and ECDSA by the TOE (FCS_CKM.1/RSA, FCS_CKM.1/ECDSA), but it is up to the Security IC Embedded Software's security policy to adopt the cryptographic key generation by the TOE or use the cryptographic key generation by the Secure Sub-System Embedded Software. The dependent requirements of FCS_COP.1/RSA and FCS_COP.1/ECDSA shall be fulfilled by the environment (Security IC Embedded Software).

442 The functional requirement FCS_CKM.1 which is dependent to FCS_COP.1/ECDH is not included in this Security Target. But the Security IC Embedded Software may fulfil this requirement related to the needs of the implemented application. The dependent requirements of FCS_COP.1/ECDH concerning this function shall be fulfilled by the environment (Security IC Embedded Software).

443 The TOE provides the cryptographic key generation for PQC by the TOE (FCS_CKM.1/PQC), but it is up to the Security IC Embedded Software's security policy to adopt the cryptographic key generation by the TOE or use the cryptographic key generation by the Secure Sub-System Embedded Software. The dependent requirements of FCS_COP.1/PQC shall be fulfilled by the environment (Security IC Embedded Software).

444 Since SHA is a keyless algorithm, there is no need for key import as required by dependency to FDP_ITC.1, FDP_ITC.2 or key generation as required by dependency to FCS_CKM.1 or destruction as required by dependency to FCS_CKM.4. So the dependencies to FDP_ITC.1, FDP_ITC.2, FCS_CKM.1 and FMT_CKM.4 are not required.

8 TOE SUMMARY SPECIFICATION

445 This chapter 8 TOE Summary Specification contains the following sections:

8.1 List of Security Functional Requirements

8.1 List of Security Functional Requirements

SFR1: Failure with preservation of secure state(FPT_FLS.1)

FPT_FLS.1/Env

446 The detection thresholds of TOE's detectors are inside the operating range of the TOE. Therefore, abnormal events/failures are detected before the secure state is compromised. This allows to take User-defined appropriate actions by software the TOE.

447 The secure state is maintained by TOE's detectors. The TOE's detectors are monitoring the failure occurs.

448 Security domains are maintained since accesses to the access-prohibited area are trapped by this access control function.

SFR2: Limited fault tolerance(FRU_FLT.2)

FRU_FLT.2/Env

449 These Integrity Checkers are used for preventing noise and laser from causing undefined or unpredictable behaviour of the chip.

FRU_FLT.2/Log

450 These Integrity Checkers are used for preventing noise and laser from causing abnormal interface behaviour and/or protocol parameters or protocol sequences.

SFR3: Resistance to physical attacks(FPT_PHP.3)

451 This requirement is achieved by security feature against a physical manipulation or physical probing attack.

SFR4: Subset access control(FDP_ACC.1/3S)

452 This requirement is achieved by security features for access control.

SFR5: Security attributes based access control(FDP_ACF.1/3S)

453 This is covered by the Privilege and User modes of the TOE.–

SFR6: Static attribute initialization(FMT_MSA.3)

454 All Special Function Registers including MPU have DEFAULT values after Power on Reset.

SFR7: Management of security attributes(FMT_MSA.1)

455 This is achieved with the MPU feature.

SFR8: Specification of management functions(FMT_SMF.1)

456 This is achieved via access to Special Function Registers of Memory Protection Unit (MPU).

SFR9: Audit Storage(FAU_SAS.1)

457 This is fulfilled by the traceability/identification data written once and for all during the TEST mode of the manufacturing process.

SFR10: Limited capabilities(FMT_LIM.1)

FMT_LIM.1/Test

458 TEST mode can be accessed only by the TEST administrator.

FMT_LIM.1/Debug

459 Debug mode can be accessed only by the Debugger in Debugging step.

SFR11: Limited availabilities(FMT_LIM.2)

FMT_LIM.2/Test

460 TEST mode can be accessed only by the TEST administrator.

FMT_LIM.2/Debug

461 Debug mode can be accessed only by the Debugger in Debugging step.

SFR12: Subset information flow control(FDP_IFC.1/3S)

462 This is achieved by security features for protecting memory data or detectors.

SFR13: Basic internal transfer protection(FDP_ITT.1/3S)

463 This requirement is achieved by the combination of the TOE security features which is unpractical to get access to internal signals and interpret them.

SFR14: Basic internal TSF data transfer protection(FPT_ITT.1/3S)

464 This requirement is achieved by the combination of the TOE security features which is unpractical to get access to internal signals and interpret them.

SFR15: Random number generation(FCS_RNG.1)

FCS_RNG.1/PTG.2

465 This requirement is ensured by the design of the random number generation algorithm that makes use of True Random Number Generator (TRNG HS_MRO9) and the associated TRNG HS_MRO9 library conforming to *BSI-AIS-20/31 Class PTG.2* requirements (German scheme).

※ A Bilateral Pseudo Random Number Generator (BPRNG): no compliance to any specific metric, but BPRNG is used by the chip for internal use and security S/W countermeasure.

SFR16: Cryptographic operation(FCS_COP.1)

466 This requirement is covered by the TOE.

Triple Data Encryption Standard Engine

467 This function is used for encrypting and decrypting data using the Triple DES symmetric algorithm with 112 bit or 168 bit key size. (FCS_COP.1/TDES)

AES (Advanced Encryption Standard)

468 This function supports the AES operation with ECB, CTR, CBC and GCM mode and cryptographic key sizes 128bit, 192bit or 256bit key size.

KDF (Key Derivation Function, Key Manager)

469 This function supports the Key derivation function of AES operation (FCS_COP.1/KeyWrap) and HMAC operation. (FCS_COP.1/KBKDF)

SHA2/3 (Secure Hash Algorithm)

470 This function supports to calculate hash (digest) values. (FCS_COP.1/SHA_HW)

HMAC (Keyed-Hash Message Authentication Code)

471 This function supports to calculate keyed-hash (digest) values. (FCS_COP.1/HMAC)

472 TORNADO-H RSA Cryptographic Library as part of AH3 Secure RSA/ECC/SHA library (optional)

473 This function assists in the acceleration of modulo exponentiations required in the RSA encryption/decryption algorithm. (FCS_COP.1/RSA)

474 TORNADO-H is a high speed modular multiplication coprocessor for the support of the RSA public key cryptosystem. The AH3 Secure RSA/ECC/SHA library is the software built on the TORNADO-H coprocessor that provides high level interface for RSA-based algorithms.

475 TORNADO-H ECC Cryptographic Library as part of AH3 Secure RSA/ECC/SHA library (optional)

476 This function assists in the acceleration of required for the ECC cryptographic operations including the ECDSA signature generation/verification and the ECDH secret key derivation. (FCS_COP.1/ECDSA, FCS_COP.1/ECDH)

477 AH3 Secure RSA/ECC/SHA library provides a set of functions to implement elliptic curve cryptographic algorithms. In particular, it provides some functions to implement the ECDSA signature generation/verification and the ECDH secret key derivation.

478 The AH3 Secure RSA/ECC/SHA library provides the functions to calculate hash (digest) values using the SHA1, SHA256, SHA384 and SHA 512 algorithm as specified in [FIPS PUB 180-3].

479 PQC (CRYSTALs) ML-DSA Cryptographic Library as part of AH3 Secure ML-DSA library (optional)

480 PQC (CRYSTALs) is a hardware coprocessor for high-speed Lattice operations. AH3 Secure ML-DSA library is a software library that is built on the PQC coprocessor that provides high-level interface for ML-DSA.

SFR17: Cryptographic key generation(FCS_CKM.1)

481 This requirement is covered by the TOE for the RSA/ECC key generation and ML-DSA public/private key pair. (optional)

SFR18: TSF Initialisation (FPT_INI.1)

482 This requirement is achieved by correct configuration of life cycle state.

SFR19: Reserved for future use

SFR20: Inter-TSF trusted channel (FTP_ITC.1/Load)

483 This requirement is achieved by processing the Authentication sequence.

SFR21: Basic data exchange confidentiality (FDP_UCT.1/Load)

484 This requirement is achieved by secure external FLASH loading.

SFR22: Data exchange integrity (FDP_UIT.1/Load)

485 This requirement is achieved by checking the checksum.

SFR23: Subset access control - Loader (FDP_ACC.1/Load)

486 This requirement is achieved by security feature for access attribute.

SFR24: Security attribute based access control - Load (FDP_ACF.1/Load)

This is covered by the Booting mode of the TOE.

SFR25: Stored data confidentiality (FDP_SDC.1/3S)

487 This requirement is achieved by the combination of the TOE security features which is unpractical to get access to internal signals and interpret them.

SFR26: Stored data integrity monitoring and action (FDP_SDI.2/3S)

488 This requirement is achieved by the security features for checking integrity.

SFR27: Reserved for future use

SFR28: Data Authentication with Identity of Guarantor (FDP_DAU.2/PM)

489 This requirement is achieved by the secure authentication process.

SFR29: Timing of identification (FIA_UID.1/PM)

490 This requirement is achieved by the security feature for timing of identification.

SFR30: Replay detection (FPT_RPL.1/PM)

491 This requirement is achieved by the security feature for reply detection.

SFR31: Protection against an unauthorized rollback of memory content (FDP_URC.1/PM)

492 This requirement is achieved by the security feature for the protection against an unauthorized rollback of memory content.

SFR32: Irreversibility Anchor for external memory (FDP_IRA.1/PM)

493 This requirement is achieved by the security feature for an irreversibility Anchor for external memory.

SFR33: Stored data confidentiality (FDP_SDC.1/PM)

494 This requirement is achieved by the security feature for confidentiality of the stored data..

SFR34: Stored data integrity monitoring and action (FDP_SDI.2/PM)

495 This requirement is achieved by the security feature for integrity monitoring and action of the stored data.

SFR35: FCS_CKM.4: Cryptographic key destruction

496 This requirement is covered by security features for cryptographic key destruction.

9 Annex

9.1 References

[1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[5] Secure Sub-System in System-on-Chip (3S in SoC), Version 1.5, BSI-CC-PP-0117

[6] A proposal for: Functionality classes for random number generators, Version 2.0, 18.09.2011, Bundesamt für Sicherheit in der Informationstechnik

[7] [FIPS SP800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revision 2

[8] [FIPS 197] Advanced Encryption Standard (AES), 2001-11-26

[9] [ISO/IEC14888-2:2008]- Information technology -- Security techniques-- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms.

[10] Supporting Document: Application of Attack Potential to Smartcards, Version 3.2.1, February 2024.

[11] [FIPS PUB 180-3] U.S. Department of Commerce / National Bureau of Standards, Secure Hash Algorithm, FIPS PUB 180-3, 2008-October

[12] [NIST curves] Federal Information Processing Standards Publication FIPS PUB 180-3, Digital Signature Standard; U.S. department of Commerce / National Institute of Standards and Technology (NIST), June 2009

[13] [ETSI TS 102 176-1] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, 2007-11, version 2.0.0

[14] [SCA on Prime Gen] T. Finke, M. Gebhardt and W. Schindler, A New Side-Channel Attack on RSA Prime Generation, CHES 2009, LNCS 5747, pp. 141-155, 2009.

[15] [FIPS PUB 202] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions / National Institute of Standards and Technology (NIST), August 2015

[16] [FIPS PUB 198-1] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION The Keyed-Hash Message Authentication Code (HMAC) / National Institute of Standards and Technology (NIST), July 2008

[17] [SEC-recommended curves] SEC2: Recommended Elliptic Curve Domain Parameters, Certicom Research, v1.0, September 20, 2000

[18] Supporting Document: The Application of CC to Integrated Circuits, for CC3.1, Version 3.0, February 2009

[19] Supporting Document: Guidance for smartcard evaluation, for CC3.1, Version 2.0, February 2010.

[20] Supporting Document: Security Architecture requirements (ADV_ARC) for smart cards, and similar devices extended to Secure Sub-Systems in SoC, Version 2.1, July 2021.

[21] Supporting Document: Composite product evaluation for Smart Cards and similar devices, for CC3.1, Version 1.5.1, May 2018.

[22] Supporting Document: Minimum Site Security Requirements, Version 3.1, December 2023.

[23] STRONGV4P00 Secure Bootloader Manual for S5E9945, Revision 0.1, 2023-07-10, Samsung Electronics Co., Ltd.

[24] [FIPS 204] Federal Information Processing Standards Publication. ``*Module-Lattice-Based Digital Signature Standard*", Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900, This publication is available free of charge from: https://doi.org/10.6028/NIST.FIPS.204 Published August 13, 2024

[25] [Brainpool curves] ECC Brainpool Standard Curves and Curve generation, M. Lochter, v1.0, www.ecc-brainpool.org

[26] [RFC7748] Elliptic Curves for Security, January 2016, RFC 7748 - Elliptic Curves for Security