REF: 2015-24-INF-1537 v1	Created by: CERT11
Target: Público	Revised by: CALIDAD
Date: 01.02.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-24 Samsung Arikara 2

Applicant: 124-81-00998 SAMSUNG Electronics Co., Ltd

References:

[EXT 2810] Certification request of Samsung Arikara 2

[EXT 2955] Evaluation Technical Report of Samsung Arikara 2.

The product documentation referenced in the above documents.

Certification report of the product Samsung S3FW9FV/FT/F9/F8 Revision 0, as requested in [EXT 2810] dated 31/08/2015, and evaluated by the laboratory Applus Laboratories, as detailed in the Evaluation Technical Report [EXT 2955] received on 23/12/2015.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Samsung S3FW9FV/FT/F9/F8 Revision 0.

The Target of Evaluation (TOE), Samsung S3FW9FV/FT/F9/F8 Revision 0 is a smartcard integrated circuit which is composed of a processing unit, security components, contact based I/O ports, hardware circuit for testing purpose during the manufacturing process and volatile and non-volatile memories (hardware).

Developer/manufacturer: Samsung Electronics Co., Ltd.

Sponsor: Samsung Electronics Co., Ltd.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria version 3.1 revision 4

EAL4 + AVA_VAN.4 + ALC_DVS.2

Evaluation end date: 23/12/2015.

All the assurance components required by the evaluation level EAL4 augmented with *AVA_VAN.4 - Methodical vulnerability analysis and ALC_DVS.2 - Sufficiency of security measures* have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + AVA_VAN.4 + ALC_DVS.2, as defined by the Common Criteria version 3.1 revision 4 and the Common Evaluation Methodology version 3.1 revision 4.

Considering the obtained evidences during the instruction of the certification request of the product Samsung S3FW9FV/FT/F9/F8 Revision 0, a positive resolution is proposed.

TOE SUMMARY

The Samsung S3FW9FV/FT/F9/F8 Revision 0 Secure 32-bit RISC Microcontroller single-chip CMOS micro-controller is designed and packaged specifically for "Smart Card" applications.

The SC000 CPU architecture of the TOE follows the Harvard style, that is, it has separate program memory and data memory. Both instruction and data can be fetched simultaneously without causing a stall, using separate paths for memory access.

The main security features of the Samsung S3FW9FV/FT/F9/F8 Revision 0 integrated circuit are:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Security sensors or detectors including High and Low Temperature detectors, High and Low Frequency detectors, High and Low Supply Voltage detectors, Supply Voltage Glitch detector
- Active Shields against physical intrusive attacks
- Filters (High Frequency and Reset Noise) for preventing noise, glitches and extremely high frequency in the external reset or clock pad from causing undefined or unpredictable behavior of the chip.
- Dedicated tamper-resistant design based on synthesizable glue logic and secure topology
- Dedicated hardware mechanisms against side-channel attacks such as Internal Variable Clock and RAM and FLASH encryption mechanisms

The TOE is dedicated to applications such as:

- Network based transaction processing such a mobile phones (GSM SIM cards)

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional components *AVA_VAN.4 - Methodical vulnerability analysis* and *ALC_DVS.2 - Sufficiency of security measures*, according to Common Criteria version 3.1 revision 4.

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.4 Methodical vulnerability analysis**

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria version 3.1 revision 4:

TOE Security Functional Requirements	Description
FRU_FLT.2	Limited fault tolerance
FPT_FLS.1	Failure with preservation of secure state
FMT_LIM.1	Limited capabilities
FMT_LIM.2	Limited availability
FAU_SAS.1	Audit storage
FDP_SDC.1	Stored data confidentiality
FDP_SDI.2	Stored data integrity monitoring and action
FPT_PHP.3	Resistance to physical attack
FDP_ITT.1	Basic internal transfer protection
FPT_ITT.1	Basic internal TSF data transfer protection
FDP_IFC.1	Subset information flow control
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FMT_MSA.3	Static attribute initialisation
FMT_MSA.1	Management of security attributes
FMT_SMF.1	Specification of management functions

IDENTIFICATION

Product: Samsung S3FW9FV/FT/F9/F8 Revision 0

Security Target: Security Target of Samsung S3FW9FV/FT/F9/F8 Revision 0 Secure 32-Bit RISC Microcontroller for Smart Card, version 1.1. 23/12/2015.

Protection Profile: None.

Evaluation Level: Common Criteria version 3.1 revision 4 EAL4 + AVA_VAN.4 + ALC_DVS.2.

SECURITY POLICIES

The use of the product Samsung S3FW9FV/FT/F9/F8 Revision 0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organizational policies related to the following aspects.

Policy 01: P.Process-TOE Protection during TOE Development and Production

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumption 01: A.Process-Sec-IC Protection during Packaging, Finishing and Personalisation

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the consumer 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).

Assumption 02: A.Resp-Appl Treatment of User Data

All User Data are owned by Security IC Embedded Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Samsung S3FW9FV/FT/F9/F8 Revision 0, although the agents implementing attacks have the attack potential Moderate according to the assurance of EAL4 + AVA_VAN.4 + ALC_DVS.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: T.Leak-Inherent Inherent Information Leakage

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential data as part of the assets.

Threat 02: T.Phys-Probing Physical Probing

An attacker may perform physical probing of the TOE in order (i) to disclose User Data, (ii) to disclose/reconstruct the Security IC Embedded Software or (iii) to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

Threat 03: T.Malfunction Malfunction due to Environmental Stress

An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to (i) modify security services of the TOE or (ii) modify functions of the Security IC Embedded Software (iii) deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions (Numbers 1, 2 and 9 in Figure 5).

Threat 04: T.Phys-Manipulation Physical Manipulation

An attacker may physically modify the Security IC in order to (i) modify User Data, (ii) modify the Security IC Embedded Software, (iii) modify or deactivate security services of the TOE, or (iv) modify security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software.

Threat 05: T.Leak-Forced Forced Information Leakage

An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential data as part of the assets even if the information leakage is not inherent but caused by the attacker.

Threat 06: T.Abuse-Func Abuse of Functionality

An attacker may use functions of the TOE which may not be used after TOE Delivery in order to (i) disclose or manipulate 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 Security IC Embedded Software or (iv) enable an attack disclosing or manipulating the User Data or the Security IC Embedded Software.

Threat 07: T.Mem-Access Memory Access Violation

Parts of the IC Smartcard 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 Smartcard IC Embedded Software.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Environment objective 01: OE.Resp-Appl Treatment of user data of the Composite TOE

Security relevant user data of the Composite TOE (especially cryptographic keys) are treated by the Security IC Embedded Software as required by the security needs of the specific application context.

Environment objective 02: OE.Process-Sec-IC Protection during composite product manufacturing

Security procedures shall be used after TOE Delivery up to delivery to the "consumer" 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).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The main TOE features are:

CPU

- 32-bit SC000 core

Memory

- 480Kbytes (S3FW9FV), 440Kbytes (S3FW9FT), 408Kbytes (S3FW9F9) and 376Kbytes (S3FW9F8) for Data and Program Memory (FLASH)
- 13K-byte Data Memory (RAM)

FLASH Write Operations

- Program with 4bytes unit
- Page(256B) / Sector(4kB) / Mat (168kB, 172kB) erase operation
- Minimum 100,000 write/erase cycles at 25°C
- Data retention for minimum 10 years at 25°C

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Abnormal Condition Detectors

- Abnormal Voltage
- Frequency
- Temperature detectors
- Power glitch detector
- Active shield removal detector

Filters

- High Frequency Filter
- Reset Noise Filter

Interrupts

- Sources for IRQ: I/O1 buffer available
- Source for IRQ: Timer0, IO1 falling edge, Flash erase/write time end interrupts, security
- Software Interrupts

Serial I/O Interface

- T=0 and 1 (ISO 7816-3)

Reset and Power Down Mode

- Power-on reset and external reset
- Stop mode

Memory Encryption and Bus Scrambling

- Static bus scrambling
- Automatic RAM encryption
- FLASH encryption

Timers

- 16-Bit Timer with 8 Bit prescaler

Clock Sources

- External clock: 1 MHz–10 MHz(Class A,B) 1MHz-7.5MHz(Class C)
- Internal clock: up to 28MHz

Operating Voltage Range

- 1.62 V - 5.5 V

Operating Temperature

- - 25°C to 85°C

Package

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Wafer

TOE Life cycle

The complex development and manufacturing processes of a Composite Product can be separated into seven distinct phases. The phases 2 and 3 of the Composite Product life cycle cover the IC development and production:

Site / Building	Purpose	Phase
Hwasung Plant/ DSR Building	Development	Phase 2
Giheung Plant/ Line 6,S1	Production(Wafer Fab)	Phase 3
Onyang Plant	Production(Warehouse/Delivery)	Phase 4
PKL Plant	Production (Mask House)	Phase 3

Table 1

The following phases according to [ICPP] are covered in the scope of the certificate.

- IC Development (Phase 2):
  - IC design,
  - IC Dedicated Software development,
- the IC Manufacturing (Phase 3):
  - integration and photomask fabrication,
  - IC production,
  - IC testing,
  - preparation and - Pre-personalisation if necessary
- the IC Packaging (Phase 4):
  - Security IC packaging (and testing),
  - Pre-personalisation if necessary.

The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE is delivered in form of wafers. In this case, the development and production of the TOE not only pertain to Phase 2 and 3 but to Phase 4 in addition. The IC Embedded Software is downloaded at phase 3 and no loader software is included within the TOE in phase 3 or phase 4 since involved engineers download the embedded software with only testing tools.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

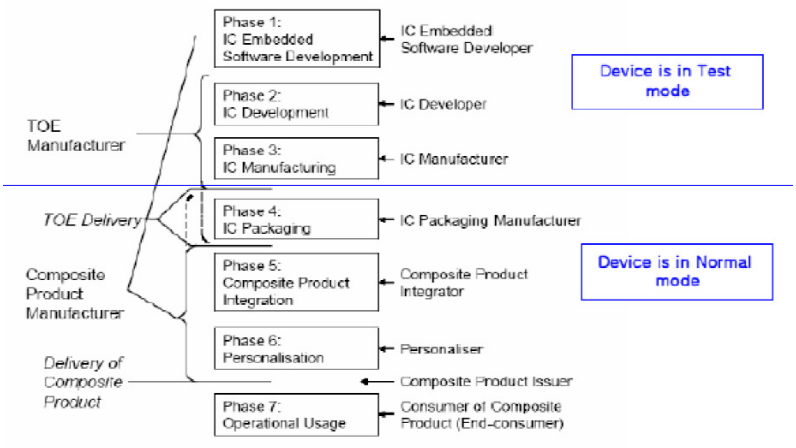

Figure 1

TEST mode	NORMAL mode
TEST mode of the TOE provides full access to all security registers and memory area available in TOE's specification to verify full functionalities.	In NORMAL mode of the TOE, TOE can no longer go back to TEST mode domain again since traceability data are written in the non-volatile memory of the TOE which cannot be altered after it has been written to. The NORMAL mode consists of PRIVILEGE mode and USER mode.

PHYSICAL ARCHITECTURE

The main hardware blocks of the TOE are described in Figure 1 below:

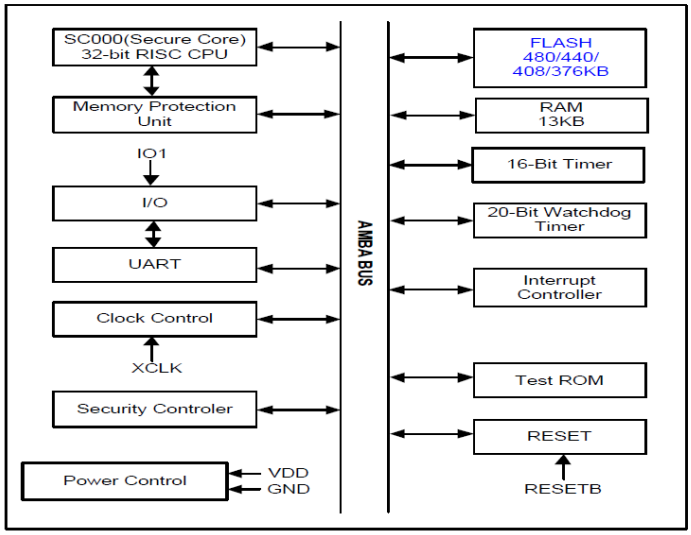

Figure 2

TOE Hardware

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- 480Kbytes (S3FW9FV), 440Kbytes (S3FW9FT), 408Kbytes (S3FW9F9) and 376Kbytes (S3FW9F8) of FLASH with 13K bytes RAM for all devices in the device family
- 32-bit Central Processing Unit (CPU)
- Internal Voltage Regulator (IVR)
- Detectors & Security Logic
- Filters
- Hardware UART for contact I/O modes
- Address & data buses
- Internal Clock
- Timers
- Power on Reset

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- S3FW9FX 32-bit CMOS Microcontroller for Smart Card User's Manual Revision 1.00 August 2015.
- S3FW9FG / FV Security Application Note Version 1.0. 24th October 2015.
- S3FW9FV/FT/F9/F8 Delivery Procedures Version 1.0. 6th November 2015.

The evaluation evidences and references can be found on section 4 in the Evaluation Technical Report.

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result. During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluation team has applied a sampling strategy and has concluded that the information is complete and coherent enough to reproduce tests and identify the functionality tested. Moreover, the

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

evaluation team has planned and executed additional tests independently of those executed by the developer.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

PENETRATION TESTING

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment [JILAAPS], the evaluation team has devised vulnerability analysis and attack scenarios for penetration testing according to JIL supporting documents [JILAAPS] and [JILADVARC]. Within these activities all aspects of the security architecture which were not covered by functional testing have been considered.

EVALUATED CONFIGURATION

The TOE is defined by its commercial name and version Samsung S3FW9FV/FT/F9/F8 Revision 0.

The acceptance procedure for the evaluated configuration of the TOE is described in section 3.8 “CUSTOMER ACCEPTANCE PROCEDURE FOR DELIVERED GOODS” of the Security Application Note [SAN].

Here it is reminded that to fulfil the requirements in the security target, the TOE consumer must strictly follow the security recommendations that can be found on documents [SAN] and [UM] as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

The TOE also includes the documents identified in section DOCUMENTS of this certification report that shall be distributed and made available together to the users of the evaluated version.

EVALUATION RESULTS

The product Samsung S3FW9FV/FT/F9/F8 Revision 0 has been evaluated against the Security Target “Security Target of Samsung S3FW9FV/FT/F9/F8 Secure 32-Bit RISC Microcontroller for Smart Card, version 1.1”.

All the assurance components required by the evaluation level EAL4 + AVA_VAN.4 + ALC_DVS.2 have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “**PASS**” **VERDICT** to the whole evaluation due all

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

the evaluator actions are satisfied for the evaluation level EAL4 + AVA_VAN.4 + ALC_DVS.2, as defined by the Common Criteria version 3.1 revision 4 and the Common Evaluation Methodology version 3.1 revision 4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- There is not any evaluation team recommendation or comment.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Samsung S3FW9FV/FT/F9/F8 Revision 0, a positive resolution is proposed.

The **certifier strongly recommends** to the TOE consumer **to strictly follow the security recommendations that can be found on documents [SAN] and [UM]** as well as to observe the operational environment requirements and assumptions defined in the applicable security target.

Finally this certification body wants to remark that some ALC evaluation results of the evaluation with the BSI reference BSI-DSZ-CC-0882-2013 have been re-used for the evaluation of this TOE. Concretely, the results of the site audit are re-used. The BSI confirmed to this Certification Body that these results are applicable for this TOE and provided support to the evaluation team during the evaluation process to confirm the applicability of the results.

Taking into account the aforementioned facts, the current positive resolution is conditioned by the validity of certificate BSI-DSZ-CC-0882-2013, whose evaluation effort, including the audited sites, are summarized in Annex B of that document. A revocation of BSI-DSZ-CC-0882-2013 certificate may imply the revocation of the current certificate.

GLOSSARY

CC	Common Criteria
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

OC	Organismo de Certificación
PP	Protection Profile
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSFI	TSF Interface
TSP	TOE Security Policy

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1. Revision 4. Sept. 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Version 3.1. Revision 4. Sept. 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Version 3.1. Revision 4. Sept. 2012

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4. Sept. 2012.

[JILAAPS] Application of Attack Potential to Smartcards, version 2.9. Jan. 2013. Joint Interpretation Library.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices, version 2.0. Jan. 2012. Joint Interpretation Library.

[UM] S3FW9FX 32-bit CMOS Microcontroller for Smart Card User's Manual Revision 1.00. Samsung Electronics Co., Ltd. August 2015.

[SAN] S3FW9FG / FV Security Application Note Version 1.0. Samsung Electronics Co., Ltd. 24th October 2015.

[DEL] S3FW9FV/FT/F9/F8 Delivery Procedures Version 1.0. 6th November 2015.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

- Security Target of Samsung S3FW9FV/FT/F9/F8 Secure 32-Bit RISC Microcontroller for Smart Card version 1.1. Samsung Electronics Co., Ltd. 23rd December 2015.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es