



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



REF: 2009-9-INF-510 v3  
Distrib: Expediente  
Date: 27.10.2010

Created: TECNICO  
Reviewed: TECNICO  
Approved: JEFEAREA

---

**CERTIFICATION REPORT FOR KONA26CC v1.1**

---

Dossier: 2009-9  
Applicant data: KEBTechnology (KEBT)

---

References:

- EXT-750 Certification Request of KONA26CC. 14/05/09.  
KEBTechnology.
  - EXT-1013 Evaluation Report for KONA26CC v1.1.  
ETR-KEBT001 M0 23/06/10. LGAI-APPLUS.
  - CCRA Arrangement on the Recognition of Common Criteria  
Certificates in the field of Information Technology Security,  
May 2000.
  - SOGIS European Mutual Recognition Agreement of  
IT Security Evaluation Certificates v3.0, January 2010.
- 

Certification report of KONA26CC v1.1, as requested by KEBT in [EXT-750] dated 14-5-2009, and evaluated by the laboratory LGAI-APPLUS, as detailed in the Evaluation Technical Report [EXT-1013] received on June 23<sup>rd</sup> 2010, and in compliance with [CCRA] and [SOGIS] for components up to EAL4.



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



## Table Of Contents

<b>EXECUTIVE SUMMARY</b>	<b>3</b>
TOE SUMMARY	4
SECURITY ASSURANCE REQUIREMENTS	5
SECURITY FUNCTIONAL REQUIREMENTS	6
<b>IDENTIFICATION</b>	<b>10</b>
<b>SECURITY POLICIES</b>	<b>11</b>
<b>ASSUMPTIONS AND OPERATIONAL ENVIRONMENT</b>	<b>13</b>
THREATS	13
OPERATIONAL ENVIRONMENT OBJECTIVES	16
<b>TOE ARCHITECTURE</b>	<b>18</b>
<b>DOCUMENTS</b>	<b>20</b>
<b>TOE TESTING</b>	<b>21</b>
PENETRATION TESTING	22
<b>EVALUATED CONFIGURATION</b>	<b>23</b>
<b>EVALUATION RESULTS</b>	<b>24</b>
<b>COMMENTS &amp; RECOMMENDATIONS FROM THE EVALUATION TEAM</b>	<b>25</b>
<b>CERTIFIER RECOMMENDATIONS</b>	<b>26</b>
<b>GLOSSARY</b>	<b>27</b>
<b>ACRONYMS</b>	<b>28</b>
<b>BIBLIOGRAPHY</b>	<b>29</b>
<b>SECURITY TARGET</b>	<b>30</b>



## Executive Summary

This document constitutes the Certification Report for the composite product KONA26CC v1.1 developed by KEBT on the integrated circuit IC for smart card S3CC91C revision 0, manufactured by Samsung.

Developer/manufacturer: KEBTechnology.

**Sponsor:** KEBTechnology.

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

**ITSEF:** LGAI Technological Center. APPLUS.

**Protection Profile:** demonstrable conformance with Java Card System - Standard 2.2 Configuration Protection Profile version 1.0b, August 2003.

**Evaluation Level:** EAL4+ (AVA\_VAN.5, ALC\_DVS.2).

Evaluation end date: 23/06/2010.

All the assurance components required by the level EAL4+ (augmented with AVA\_VAN.5, ALC\_DVS.2) have been assigned a "PASS" verdict. Consequently, the laboratory (LGA-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as defined by the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the KONA26CC v1.1 product on the integrated circuit for intelligent card S3CC91C revision 0, a positive resolution is proposed.

During the execution of this smartcard evaluation the laboratory, responding to the CB's demand, has used the additional requirements and guidance provided by the *JIL Working Group (JIWG)* in the form of *JIL papers* and *CC supporting documents* related to the IT domain of *Smartcards and similar devices*. The *Joint Interpretation Library (JIL)* supports the specific technical competence aspects required by the SOGIS MRA [SOGIS] in this field for several CC activities, specially beyond the EAL1-EAL4 levels covered by the CCRA.



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



These additional JIL references are mainly related to the evaluation of composite TOEs, and they are the documents listed below:

- [AAP] Application of Attack Potential to Smartcards v2.7
- [CPE] Composite product evaluation for Smart Cards and similar devices v1.0
- [SCG] Smartcard evaluation guidance v2.0
- [ARC] Security Architecture requirements (ADV\_ARC) for Smart Cards and similar devices v1.0
- [CDE] Collection of Developer Evidence v1.1
- [AMS] Attack Methods for Smartcards and Similar Devices v1.5
- [RIC] Requirements to perform Integrated Circuit Evaluations v1.0

The CB was updating to the ITSEF with the last versions of these documents during the whole evaluation process.

### ***TOE Summary***

This TOE is a smartcard composed of operative system KONA26CC version 1.1 and the IC Samsung S3CC91C revision 0.

As described in its Security Target, it provides the security level of EAL4+ augmented with ALC\_DVS.2 and AVA\_VAN.5 and allows loading and deleting applications, which are developed by the customers. Thus, it allows for multiple applications to run on a single TOE and provides security features to ensure secure interoperability of applications.

The examples of the application that can be loaded in the TOE are:

- Government applications - National Identification Card, Driver License, Health Card
- Banking applications - Credit/Debit cards, ePurse
- Security Token applications - Public Key Infrastructure(PKI)
- Telecom applications - 3G USIM, JavaSIM



The TOE requires the following components in order to operate:

- Card Acceptance Device(CAD) or Smartcard Reader complies with ISO/IEC 7816-3 communication
- Dedicated software that runs over the CAD to allow logical communication with the TOE

The TOE is been designed in order to provide functionality according to Java Card 2.2.1, and GlobalPlatform.1.1 (GP).

### **Security Assurance Requirements**

The product was evaluated with all the evidence required to fulfil EAL4, augmented with the components related to the vulnerability analysis AVA\_VAN.5 and also for ALC\_DVS.2, according to CC Part 3 [CC-P3].

Also the additional activities for composite product evaluation defined by JIL in the document [CPE] were performed by the laboratory and validated by the CB. They are described in the table below as “XXX\_COMP.n” components.

<b>Assurance Class</b>	<b>Assurance Components</b>
Security Target	ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, ASE_ECD.1, ASE_REQ.2, ASE_TSS.1 and ASE_COMP.1
Development	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3 and ADV_COMP.1
Guidance	AGD_OPE.1 and AGD_PRE.1
Life Cycle	ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1 and ALC_COMP.1
Tests	ATE_COV.2, ATE_DPT.2, ATE_FUN.1, ATE_IND.2 and ATE_COMP.1
Vulnerability Analysis	AVA_VAN.5 and AVA_COMP.1



## ***Security Functional Requirements***

The product security functionality satisfies several requirements as stated by its Security Target, and according to CC Part 2 [CC-P2]. They are requirements for security functions such as information flow control, identification and authentication.

These functional requirements satisfied by the product are:

### **→ TOE Core:**

**FDP\_ACC.2/FIREWALL COMPLETE ACCESS CONTROL**  
**FDP\_ACF.1/FIREWALL SECURITY ATTRIBUTE BASED ACCESS CONTROL**  
**FDP\_IFC.1/JCVM SUBSET INFORMATION FLOW CONTROL**  
**FDP\_IFF.1/JCVM SIMPLE SECURITY ATTRIBUTES**  
**FDP\_RIP.1/OBJECTS SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_RIP.1/APDU SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_RIP.1/bArray SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_RIP.1/TRANSIENT SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_RIP.1/ABORT SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_RIP.1/KEYS SUBSET RESIDUAL INFORMATION PROTECTION**  
**FDP\_ROL.1/FIREWALL BASIC ROLLBACK**  
**FDP\_SDI.2 STORED DATA INTEGRITY MONITORING AND ACTION**

**FMT\_MSA.1/JCRE MANAGEMENT OF SECURITY ATTRIBUTES**  
**FMT\_MSA.2/JCRE SECURE SECURITY ATTRIBUTES**  
**FMT\_MSA.3/FIREWALL STATIC ATTRIBUTE INITIALIZATION**  
**FMT\_SMR.1/JCRE SECURITY ROLES**  
**FMT\_SMF.1/JCRE SPECIFICATION OF MANAGEMENT FUNCTIONS**  
**FMT\_MTD.1/JCRE MANAGEMENT OF TSF DATA**  
**FMT\_MTD.3 SECURE TSF DATA**

**FCS\_CKM.1/RSA CRYPTOGRAPHIC KEY GENERATION**  
**FCS\_CKM.1/TRIPLE-DES CRYPTOGRAPHIC KEY GENERATION**  
**FCS\_CKM.2/RSA CRYPTOGRAPHIC KEY DISTRIBUTION**  
**FCS\_CKM.2/TRIPLE-DES CRYPTOGRAPHIC KEY DISTRIBUTION**  
**FCS\_CKM.3/TRIPLE-DES CRYPTOGRAPHIC KEY ACCESS**  
**FCS\_CKM.3/RSA CRYPTOGRAPHIC KEY ACCESS**  
**FCS\_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION**  
**FCS\_COP.1/TRIPLE-DES CRYPTOGRAPHIC OPERATION**  
**FCS\_COP.1/RSA CRYPTOGRAPHIC OPERATION**  
**FCS\_COP.1/DESMAC CRYPTOGRAPHIC OPERATION**



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



**FCS\_COP.1/RSA SIGNATURE** CRYPTOGRAPHIC OPERATION  
**FCS\_COP.1/SHA-1** CRYPTOGRAPHIC OPERATION  
**FCS\_COP.1/MD5** CRYPTOGRAPHIC OPERATION

**FAU\_ARP.1/JCS** SECURITY ALARMS

**FPR\_UNO.1** UNOBSERVABILITY

**FPT\_TDC.1** INTER-TSF BASIC TSF DATA CONSISTENCY  
**FPT\_FLS.1/JCS** FAILURE WITH PRESERVATION OF SECURE STATE  
**FPT\_TST.1** TSF TESTING

**FIA\_ATD.1/AID** USER ATTRIBUTE DEFINITION  
**FIA\_UID.2/AID** USER IDENTIFICATION BEFORE ANY ACTION  
**FIA\_USB.1** USER-SUBJECT BINDING

**→ Installation of Applets SFRs:**

**FDP\_ITC.2/INSTALLER** IMPORT OF USER DATA WITH SECURITY ATTRIBUTES

**FMT\_SMR.1/INSTALLER** SECURITY ROLES

**FPT\_FLS.1/INSTALLER** FAILURE WITH PRESERVATION OF SECURE STATE  
**FPT\_RCV.3/INSTALLER** AUTOMATED RECOVERY WITHOUT UNDUE LOSS

**FRU\_RSA.1/INSTALLER** MAXIMUM QUOTAS

**→ Deletion of Applets SFRs:**

**FDP\_ACC.2/ADEL** COMPLETE ACCESS CONTROL  
**FDP\_ACF.1/ADEL** SECURITY ATTRIBUTE BASED ACCESS CONTROL  
**FDP\_RIP.1/ADEL** SUBSET RESIDUAL INFORMATION PROTECTION

**FMT\_MSA.1/ADEL** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.3/ADEL** STATIC ATTRIBUTE INITIALIZATION  
**FMT\_SMR.1/ADEL** SECURITY ROLES  
**FMT\_SMF.1/ADEL** SPECIFICATION OF MANAGEMENT FUNCTIONS

**FPT\_FLS.1/ADEL** FAILURE WITH PRESERVATION OF SECURE STATE

**→ RMI SFRs:**



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



**FDP\_ACC.2/JCRMI** COMPLETE ACCESS CONTROL  
**FDP\_ACF.1/JCRMI** SECURITY ATTRIBUTE BASED ACCESS CONTROL  
**FDP\_IFC.1/JCRMI** SUBSET INFORMATION FLOW CONTROL  
**FDP\_IFF.1/JCRMI** SIMPLE SECURITY ATTRIBUTES

**FMT\_MSA.1/JCRMI** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.1/EXPORT** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.1/REM\_REFS** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.3/JCRMI** STATIC ATTRIBUTE INITIALIZATION  
**FMT\_REV.1/JCRMI** REVOCATION  
**FMT\_SMR.1/JCRMI** SECURITY ROLES  
**FMT\_SMF.1/JCRMI** SPECIFICATION OF MANAGEMENT FUNCTIONS

**→ Deletion of Objects SFRs:**

**FDP\_RIP.1/ODEL** SUBSET RESIDUAL INFORMATION PROTECTION  
**FPT\_FLS.1/ODEL** FAILURE WITH PRESERVATION OF SECURE STATE

**→ Card SFRs:**

**FCO\_NRO.2/CM** ENFORCED PROOF OF ORIGIN  
**FIA\_UID.1/CM** TIMING OF IDENTIFICATION  
**FDP\_IFC.2/CM** COMPLETE INFORMATION FLOW CONTROL  
**FDP\_IFF.1/CM** SIMPLE SECURITY ATTRIBUTES  
**FDP\_UIT.1/CM** DATA EXCHANGE INTEGRITY  
**FMT\_MSA.1/CM** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.3/CM** STATIC ATTRIBUTE INITIALIZATION  
**FMT\_SMR.1/CM** SECURITY ROLES  
**FMT\_SMF.1/CM** SPECIFICATION OF MANAGEMENT FUNCTIONS  
**FTP\_ITC.1/CM** INTER-TSF TRUSTED CHANNEL

**→ Smart card platform SFRs:**

**FRU\_FLT.2/SCP** LIMITED FAULT TOLERANCE  
**FPT\_FLS.1/SCP** FAILURE WITH PRESERVATION OF SECURE  
**FPT\_PHP.3/SCP** RESISTANCE TO PHYSICAL ATTACK  
**FPT\_RCV.3/SCP** AUTOMATED RECOVERY WITHOUT UNDUE LOSS



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



**FPT\_RCV.4/SCP** FUNCTION RECOVERY  
**FPT\_ITT.1/SCP** BASIC INTERNAL TSF DATA TRANSFER PROTECTION

**FDP\_ITT.1/SCP** BASIC INTERNAL TRANSFER PROTECTION  
**FDP\_IFC.1/SCP** SUBSET INFORMATION FLOW CONTROL

**FCS\_RND.1/SCP** QUALITY METRIC FOR RANDOM NUMBERS

**→ Card Manager SFRs:**

**FDP\_ACC.1/CMGR** SUBSET ACCESS CONTROL  
**FDP\_ACF.1/CMGR** SECURITY ATTRIBUTE BASED ACCESS CONTROL

**FMT\_MSA.1/CMGR** MANAGEMENT OF SECURITY ATTRIBUTES  
**FMT\_MSA.3/CMGR** STATIC ATTRIBUTE INITIALIZATION  
**FMT\_SMR.1/CMGR** SECURITY ROLES  
**FMT\_SMF.1/CMGR** SPECIFICATION OF MANAGEMENT FUNCTIONS

**FIA\_UID.1/CMGR** TIMING OF IDENTIFICATION

**→ General Global Platform related SFRs:**

**FDP\_DAU.1/GP** BASIC DATA AUTHENTICATION

**FIA\_AFL.1/GP** BASIC AUTHENTICATION FAILURE HANDLING  
**FIA\_ATD.1/GP** USER ATTRIBUTE DEFINITION  
**FIA\_UAU.1/GP** TIMING OF AUTHENTICATION  
**FIA\_UAU.4/GP** SINGLE-USE AUTHENTICATION MECHANISMS  
**FIA\_USB.1/GP** USER-SUBJECT BINDING

**FMT\_MOF.1/GP** MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR  
**FMT\_MSA.2/GP** SECURE SECURITY ATTRIBUTES  
**FMT\_MTD.1/GP** MANAGEMENT OF TSF DATA  
**FMT\_SMF.1/GP** SPECIFICATION OF MANAGEMENT FUNCTION



## Identification

**Product:** KONA26CC v1.1.

**Security Target:** SP-01-07 KONA26CC Security Target v1.6, 2010/06/07.

**Protection Profile:** demonstrable conformance with Java Card System - Standard 2.2 Configuration Protection Profile version 1.0b, August 2003.

**Evaluation Level:** CC v3.1 r3 EAL4+ (AVA\_VAN.5, ALC\_DVS.2).



## Security Policies

The usage of KONA26CC v1.1 as a composite smartcard product implies to implement a series of organizational policies that assure the commitment of different demands of security.

The details about them are included in the Security Target. In synthesis, the necessity settles down to implement organizational policies relative to:

### • P.VERIFICATION

This policy is described in Java Card System - Standard 2.2 Configuration Protection Profile, it has been renamed from OSP.VERIFICATION to P.VERIFICATION.

### • P.ROLES-3

The TOE shall recognize the following roles associated with:

- Card Administrator,
- Application Provider

### • P.INITIAL\_LIFECYCLE\_STATE-2

Card shall be moved in OP\_READY state before any GP function or service is used. Card shall be issued to Cardholders with the card set to SECURED Life-Cycle state. A security domain shall be moved into the PERSONALIZED life cycle state before any security domain User or Application uses the services of that Security Domain.

### • P.CARD\_ADMINISTRATOR\_PRE-APPROVAL\_2b

The Card Administrator may allow privileged Application Providers to perform CCMFs.

The Card Administrator shall preauthorize every CCMF (except delete of the Application Provider's own Applications) performed by a privileged Application Provider.

The Card Administrator shall request a confirmation for each delegated CCMF that has taken place.

The Card Administrator shall always be allowed to perform any CCMF for any Application.



• **P.APPLICATION\_PROVIDER\_PRE-APPROVAL\_2b**

The Application Provider allows another (privileged) Application Provider to perform CCMFs for its own Applications as well as personalizing and managing some Application(s) specific data (or keys).

• **P.LOAD\_FILE\_VERIFICATION\_3**

Integrity and authenticity of the Load File shall be verified and shall always be carried out successfully prior to Application Load File installation. This shall take place on-card.

• **P.APPLICATION\_CODE\_VERIFICATION\_3**

Byte code verification and other forms of Application Code Verification is a requirement and shall always be carried out successfully prior to Application Load File on-card installation. This shall take place off card and shall be confirmed by using a Security Domain with Mandated DAP Verification privilege. Application Code Verification shall at least include the algorithms necessary to establish that the Application would pass all omitted runtime checks.

• **P.SECURE\_COMMUNICATION\_1**

Only the minimum security requirements for GP commands as defined by GPCS are required.

• **P.CRYPTO**

The TOE must provide the following cryptographic functionality to application providers:

- RSA public key asymmetric cryptography
- TRIPLE-DES symmetric cryptography
- RSA signatures.
- SHA-1 hashes
- MD5 hashes



## 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, and briefly described below. These same 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.

In this TOE ST there are only these assumptions to be considered:

- **A.VERIFICATION**

This assumption is described in Java Card System - Standard 2.2 Configuration Protection Profile.

- **A.APPLLET**

This policy is described in Java Card System - Standard 2.2 Configuration Protection Profile.

- **A.KEY\_MANAGEMENT**

It is assumed that cryptographic keys, which are stored outside the TOE and which are used for secure communication and authentication between Smart Card and terminals are protected in their own (off-card) storage environment.

## ***Threats***

This section describes the security threats to the TOE:

- **T.PHYSICAL**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

- **T.CONFID-JCS-CODE**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

- **T.CONFID-APPLI-DATA**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection



Profile.

•**T.CONFID-JCS-DATA**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-APPLI-CODE**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-JCS-CODE**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-APPLI-DATA**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-JCS-DATA**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.SID.1**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.SID.2**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.EXE-CODE.1**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.EXE-CODE.2**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.NATIVE**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.



•**T.RESOURCES**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-APPLI-CODE.2**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INTEG-APPLI-DATA.2**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.INSTALL**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.EXE-CODE-REMOTE**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.DELETION**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.OBJ-DELETION**

This threat is defined in Java Card System - Standard 2.2 Configuration Protection Profile.

•**T.RND**

Deficiency of Random Numbers.

An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided. An attacker may gather information about the produced random numbers which might be a problem because they may be used for instance to generate cryptographic keys. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. Malfunctions or premature aging are also considered which may assist in getting information about random numbers.

•**T.ACCESS**

Unauthorized access to sensitive information stored in memories in order to disclose or to corrupt the TOE data. This includes any consequences of bad or incorrect user



authentication by the TOE.

#### •T.OS\_OPERATE

An attacker modifies the correct Software behavior by unauthorized use of TOE or use of incorrect or unauthorized instructions or commands or sequence of commands, in order to obtain an unauthorized execution of the TOE code.

#### •T.LEAKAGE

An attacker may exploit information which is leaked from the TOE during usage of the Smart Card in order to disclose the Software behavior and Application Data handling (TSF data or User data).

No direct contact with the Smart Card Internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is the Differential Power Analysis (DPA)

#### •T.FAULT

An attacker may cause a malfunction of TSF by applying environmental stress in order to (1) deactivate or modify security features or functions of the TOE or (2) deactivate or modify security functions of the Smart Card. This may

### ***Operational environment objectives***

The product requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment.

With this purpose, the security objectives declared for the TOE environment are the following:

#### • OE.VERIFICATION

This objective is described in Java Card System - Standard 2.2 Configuration Protection Profile.

#### • OE.APPLLET

This objective is described in Java Card System – Standard 2.2 Configuration Protection Profile.

#### • OE.KEY\_MANAGEMENT

During the TOE usage, the terminal or system in interaction with the TOE, shall ensure



the protection of their own keys by operational means and/or procedures

- **OE.ACTORS\_3**

After Card manufacturing and initialization, the card administrator shall move the Card in the OP\_READY state before any GP function or service is used.

The card Issuer shall issue the card to the Cardholders with the card set to SECURED Life-Cycle state.

A security domain shall be moved into the PERSONALIZED life cycle state before any security domain User or Application uses the services of that Security Domain.

- **OE.APPLICATION**

Applications loaded during personalization phases (after the TOE is in OP-READY life cycle state) or Applications loaded after post issuance, are verified and tested off-card before loading.



## TOE Architecture

As previously described in this document, the TOE is a composite smartcard with:

- The Samsung S3CC91C IC, including the low level library that controls cryptographic operations (Secure Crypto Library v3.5S) and random number generation (DRNG v2.0).
- The Kona OS operative system software v1.2 , that runs on top of the IC and controls the operation of the whole card. The KONA OS allows customers to load and control their own applications while keeping them isolated from the rest of the card.

It is important to remark that user applications and bytecode-verifier are not included under the TOE scope and that no additional native applications are installed in the TOE.

The TOE enables the Java Card technology, which consists of the Java Card Virtual Machine (JCVM), the Java Card Runtime Environment (JCRE) and the Java Card Application Programming Interface (JCAPI).

Also, the TOE is designed to provide the features of GlobalPlatform Environment (OPEN), the Issuer Security Domain (ISD) and Cardholder Verification Method Services.

Therefore, the TOE allows loading of multiple applications, called applets, that interact securely, under the rules defined by TOE provider.

The TOE architecture provides functionality for:

- Java Card 2.2.1 Functionalities:
  - Remote Method Invocation  
Supports the remote methods that can be invoked remotely from CAD.
  - Multiple Logical Channel  
Supports Multiple logical channels which allow a terminal to open up to two channels with the smart card, one session per logical channel. (Logical channels functionality is described in detail in ISO 7816-4.)
  - Garbage Collector  
Reclaims deallocated data automatically during the execution of a program.
- Global Platform 2.1.1 Functionalities:
  - Issuer Security Domain  
Operates as the mandatory on-card representative of the Card Issuer which has capability of loading, installing, and deleting application that belong either to the Card Issuer or to other Application Provider.
  - Supplementary Security Domain



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



Operates as the on-card representative of an Application Provider or Controlling Authority.

- Public key DAP Verification

Supports verification of application code integrity and authenticity before the application code is loaded, installed and made available to the Cardholder on behalf of an Application Provider.

- Mandated DAP Verification

Supports verification of application code integrity and authenticity before the application code is loaded, installed and made available to the Cardholder on behalf of a Controlling Authority.

- Secure Channel Protocol 01 and Secure Channel Protocol 02

Provides a secure communication channel between a card and an off-card entity during an Application Session.

- CVM interface supporting Global PIN

Provides support for CVM management which is responsible for Cardholder verification, including velocity checking.

- Delegated Management

Provides authority to Supplementary Security Domain to manage Card Contents.

- Cryptographic Algorithms and Functionalities:

- DES with 64 bits key size

- Triple DES with 128 bits or 192 bits key size

- RSA with key length of multiple of 32 bits from 512 bits to 2048 bits

- RSA CRT with key length of multiple of 32 bits from 512 bits to 2048 bits

- Hash Algorithm - MD5 and SHA-1

- General Functionalities:

- Protection against Physical Probing and against malfunctions

- A non-deterministic random number generator (RNG)

- Storage data integrity

- Security alarms in case of detect a security violation

- Atomicity of critical operations

- Support for Communication Protocols T=0 and T=1

- Support various baud rate for Communication Protocols (9600, 19200, 38400, 76800 and 115200) bit/sec



## Documents

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

KONA26CC Proprietary Command Manual KEBT Only, version 1.4, 2010-03-03

KONA26CC Proprietary Command Manual, version 1.1, 2010-03-03

KONA26CC Delivery procedure, version 1.1, 2009-10-06

KONA26CC Technical Manual English, version 1.5



## TOE Testing

The manufacturer has developed testing for the TOE TSF. All these tests have been performed by the manufacturer in their location and facilities with success.

The process has 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 is been checked also that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality (low level design) are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The evaluator has repeated all the tests defined in the TOE test specification according to the different configurations defined the developer. All tests have been successfully performed.

The developer provides all the equipment necessary to perform independent testing, including 150 samples of the TOE.

Hardware equipment:

- Standard workstation with XP professional SP3
- GemPlus GemPC410 card reader for using with ICCSim
- Generic USB SmartCard reader
- MP-300, a specialized CAD with capability of customized power control

Software or firmware:

- Java2 SE runtime environment version 1.4.2.19
- CalmSHINE16 version 1.56h
- PBS3CC91C emulator
- Eclipse version 3.0

Testing tools:

- Konatester v1.5 - 2004 - KEBT Propietary.
- Java Card Technology Compatibility Kit 2.2.1 – October 2003.
- ICCSimCT v6.15 nonPCSC for GP.
- BSI AIS20 Test Tool, 01/02/2010.



The evaluator executed the tests and updated the test documentation with new devised tests. The evaluator verified that the obtained results were agreed with expected results.

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

### ***Penetration Testing***

The evaluator defined as research criterion to identify potential vulnerabilities the use of the JIL Attack Methods reference [AMS] and the Samsung IC ETR-lite for the composition, complemented with:

Specialist publication in terms of secure coding in C and assembler

Use of CHES proceedings

Use of Cryptoanalysis specialist proceedings

The evaluator devised a methodology to perform methodical vulnerability assessment analysis based in two phases:

- A bottom-up strategy analyses the source code to detect software bugs or flaws. To confirm the existence of bug or flaw the high level evidences must be used.
- A top-down strategy analyses the high level design taking into account the security architecture to formulate flaw hypothesis. To confirm the flaw hypothesis the low level evidences must be used.

To confirm the completeness of the methodology the whole source code, the whole top level (subsystem and modules) design and the security architecture should be analysed.

The independent penetration testing devised several test cases covering the main types of attacks in [AMS] including physical attacks, probing, overcoming of sensors and filters, clock and voltage glitches, DFA, perturbation and light attacks (laser), SPA/DPA, EMA, EEPROM attacks, and software attacks.

The evaluator did not find neither exploitable vulnerabilities nor residual vulnerabilities in the operational environment as a result of independent penetration testing.



## Evaluated Configuration

The TOE is defined by its name and version number **KONA26CC v1.1**.

The composite TOE includes:

- The IC Samsung **S3CC91C revision 0**, including the low level library that control cryptographic operations (**Secure Crypto Library v3.5S**) and random number generation (**DRNG v2.0**).
- The **Kona OS v1.2**, that runs on top of the IC and controls the operation of the whole card.



## Evaluation Results

The composite product KONA26CC v1.1 on the integrated circuit for intelligent card S3CC91C has been evaluated in front of the “SP-01-07 KONA26CC Security Target v1.6”, 2010/06/07.

All the assurance components required by the level EAL4+ (augmented with AVA\_VAN.5, ALC\_DVS.2) have been assigned a “PASS” verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].



## Comments & Recommendations from the Evaluation Team

The developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product. Therefore the KONA26CC v1.1 fulfils the requirements of CC version 3.1 with an evaluation assurance level EAL4+ augmented with ALC\_DVS.2 and AVA\_VAN.5.

To identify the TOE version use the command manuals listed in the "Documents " section of this report, in order to see the command about how to get the information of the chip.



## Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the KONA26CC v1.1 composite product on the integrated circuit for intelligent card Samsung S3CC91C, a positive resolution is proposed.

Note that this composite TOE claim for CC v3.1 EAL4+ with ALC\_DVS.2 and AVA\_VAN.5, and the IC platform level of assurance is CC v2.3 EAL4+ with ADV\_IMP.2, ALC\_DVS.2, AVA\_MSU.3 and AVA\_VLA.4.

The certification body authorised the evaluation although the CC versions were different, based on:

EAL4 for v2.3 is equivalent to EAL4 for v3.1.

ALC\_DVS.2 is one assurance requirement of both.

AVA\_VAN.5 is considered equivalent to AVA\_MSU.3 and AVA\_VLA.4.

Therefore the EAL chosen for the composite evaluation does not exceed the EAL applied to the evaluation of the platform.

This certification is recognised under the terms of the Recognition Agreements [CCRA] and [SOGIS] for components up to EAL4 according to the mutual recognition levels of them and the accreditation status of the Spanish Scheme.



## Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

**Extension** - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Protection Profile** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.



## Acronyms

**APDU** Application Protocol Data Unit

**CB** Certification Body

**CC** Common Criteria

**EAL** Evaluation Assurance Level

**EEPROM** Electronically Erasable Programmable Read Only Memory

**EMA** ElectroMagnetic Analysis

**GP** Global Platform

**IT** Information Technology

**ITSEF** Information Technology Security Evaluation Facility

**ST** Security Target

**TOE** Target of Evaluation

**TSF** TOE Security Functionality

**PP** Protection Profile

**RNG** Random Number Generator

**SAR** Security Assurance Requirement

**SFR** Security Function Requirement

**SPA/DPA** Simple/Differential Power Analysis

**VM** Virtual Machine



## Bibliography

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

### Common Criteria

[CC\_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC\_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC\_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

### JIL papers

[AAP] Application of Attack Potential to Smartcards v2.7

[CPE] Composite product evaluation for Smart Cards and similar devices v1.0

[SCG] Smartcard evaluation guidance v2.0

[ARC] Security Architecture requirements (ADV\_ARC) for Smart Cards and similar devices v1.0 (trial)

[CDE] Collection of Developer Evidence v1.1

[AMS] Attack Methods for Smartcards and Similar Devices v1.5

[RIC] Requirements to perform Integrated Circuit Evaluations v1.0



## Security Target

It is published jointly with this certification report the security target,

“SP-01-07 KONA26CC Security Target v1.6”, 2010/06/07.

Public version: “SP-01-14 KONA26CC Security Target Lite v1.0”, 2010/08/03.