KECS-CR-12-63

Ucard UBJ31-G11 V1.1

Certification Report

Certification No.: KECS-ISIS-0419-2012

2012. 10. 31

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2012.10.31	-	Certification report for Ucard UBJ31-G11 V1.1 - First documentation

This document is the certification report for Ucard UBJ21-G11 V1.1 of UBIVELOX.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Telecommunications Technology Association. (TTA)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL4+ evaluation of Ucard UBJ31-G11 V1.1 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is the composite product which is consisting of the certified contact/contactless integrated circuit chip, and embedded software(IC chip operating system(COS), Java Card Virtual Machine (JCVM), Java Card Runtime Environment (JCRE), Java Card API (JCAPI), Card Manager & GP API) in accordance with the Sun’s Java Card 2.2.2 [7], [8], [9], the Global Platform Card Specification [10], the Visa Global Platform Card Specification [11], and the Korean Finance IC Card Standard [12]. The TOE provides Java Card Platforms for multiple applications by allowing them to be loaded and deleted, cryptographic services to be used by applications installed on the Java Card Platform.

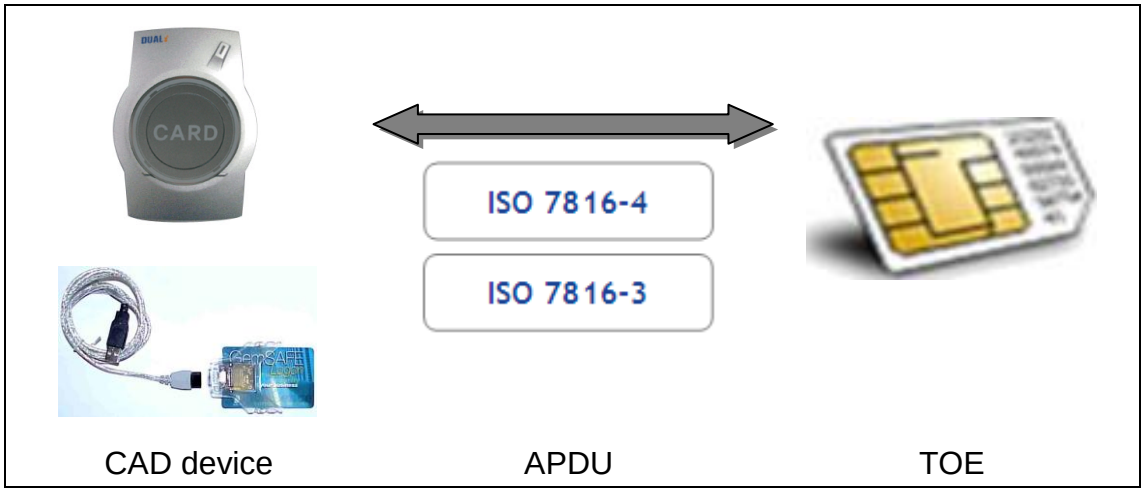
The TOE Ucard UBJ31-G11 V1.1 is composed of the following components:

- IC chip SB23YR80B provided by STMicroelectronics, see ANSSI-CC-2010/02 [13] and ANSSI-2010/02-M01 [14], and
- Embedded software UBJ31-G11_DEL provided by UBIVELOX.

The evaluation of the TOE has been carried out by Telecommunications Technology Association (TTA) and completed on Oct 5, 2012. This report grounds on the evaluation technical report (ETR) TTA had submitted [16] and the Security Target (ST) [17].

The ST is based on the certified Protection Profile (PP) Java Card™ System Protection Profile Open Configuration, Version 2.6, 19 April 2010 [19]. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL4 augmented by ALC_DVS.2 and AVA_VAN.5. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE.



[Figure 1]Operational environment of the TOE

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is composite product consisting of the following components and related guidance documents.

Type	Identifier	Release	Delivery Form
HW/SW	SB23YR80B Secure Microcontrollers	Revision B (dedicated software ANC, K2M0BFB mask set)	- (Note: The SW is contained in ROM and EEPROM. The delivery of smart card product is not covered by the evaluation.)
	Cryptographic library NesLib 3.0 SB	V3.0	
SW	UBJ31-G11_DEL	V2.0	
DOC	Ucard UBJ31-G11 V1.1	V1.3	Softcopy

Type	Identifier	Release	Delivery Form
	Operation User Guidance		
	Ucard UBJ31-G11 V1.1 Preparative procedure	V1.3	

[Table 1] TOE identification

The TOE is finalized at Phase 3 (Security IC manufacturing) in accordance with the Java Card™ System PP [19], and the delivery of JCS is in phase 3. After the TOE finalization, the IC Packaging Manufacturer and the Composite Product Manufacturer are responsible for IC packaging, smart card product finishing process and testing. The smart card product delivery is in phase 7.

For details on the IC chip and the crypto library, see the documentation under ANSSI-CC-2010/02 [13] and ANSSI-2010/02-M01 [14].

The certified IC chip which is a component of the TOE provides SHA-224, it is not used by the TOE. Thus it is out of TOE scope.

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009) Korea Evaluation and Certification Regulation for IT Security (February 1, 2012)
TOE	Ucard UBJ31-G11 V1.1
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
EAL	EAL4+ (augmented by ALC_DVS.2 and AVA_VAN.5)
Developer	UBIVELOX
Sponsor	UBIVELOX
Evaluation Facility	Telecommunications Technology Association. (TTA)
Completion Date of Evaluation	October 5, 2012
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [17] for the TOE claims demonstrable conformance to the Java Card™ System PP [19], and the TOE complies security policies defined in the Java Card™ System PP [19] by security objectives and security requirements based on the Sun's Java Card 2.2.2 [7], [8], [9]. Thus the TOE provides security features defined in the Java Card™ System PP [19] as follows.

- Core with logical channels, ensures the runtime environment of the Java Card System implementing logical channels. This includes the firewall policy and the requirements related to the Java Card API.
- Installation, ensures the installation of post-issuance applications. It does not address card management issues in the broad sense, but only those security aspects of the installation procedure that are related to applet execution.
- Applet deletion, ensures erasure of installed applets from the card.
- Remote method invocation, ensures the remote method invocation feature, which provides a new protocol of communication between the terminal and the applets.
- Object deletion, ensures the object deletion capability. This provides a safe memory recovering mechanism.
- Secure carrier, ensures secure downloading of applications on the card. This provides security features for preventing, in those configurations that do not support on-card static or dynamic bytecode verification, the installation of a package that has not been bytecode verified, or that has been modified after bytecode verification.
- Card manager, ensures security policies for controlling access to card content management operations and for expressing card issuer security concerns. Also, this group contains the security requirements to fulfill GP specific objectives.
- Smart card platform, ensures smart card platform, that is, operating system and chip that the Java Card System is implemented upon.

Furthermore, the TOE is composite product based on the certified IC chip, the TOE utilizes and therefore provides some security features covered by the IC chip certification such as security monitoring and control register, clock random jitter, active Shields against physical attacks, memory scrambling and encryption, glue logic, secure cryptographic services, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation. For more details refer to the Security Target

Lite for the IC chip [15].

4. Assumptions and Clarification of Scope

The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used:

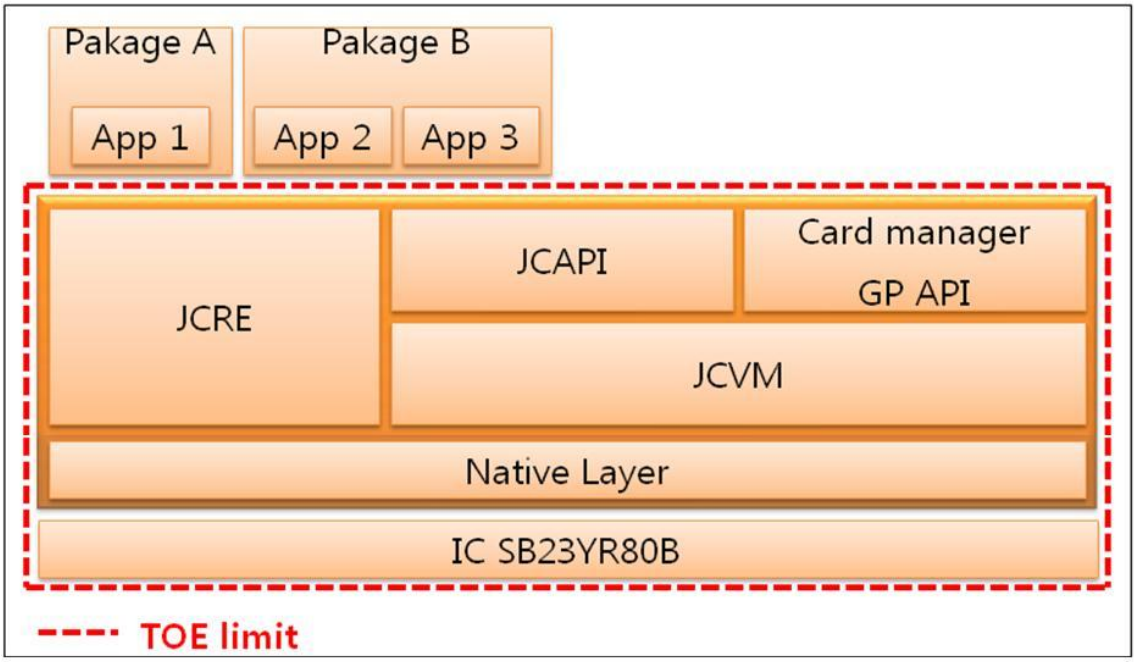
- Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly "does not include support for native methods" ([JCVM22], §3.3) outside the API.
- All the bytecodes are verified at least once, before the loading, before the installation or before the execution, depending on the card capabilities, in order to ensure that each bytecode is valid at execution time.
- 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.
- It is assumed that the CVM values are generated maintained and used off card in a secure manner during personalization phases. It is assumed that the Card Holder keeps his personal code secret.
- It is assumed that the Card Administrator is the sole Application Provider and also plays the roles of Application Loader and Verification Authority.

Furthermore, some aspects of threats and organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment.

- 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.
- Appropriate functionality testing of the TOE shall be used in during initialization, personalization and other operations before Issuance. During these operations, security procedures shall be used to maintain confidentiality and integrity of the TOE manufacturing and test data.

5. Architectural Information

[Figure 2] show the physical scope of the TOE. The TOE is the composite product which is consisting of the certified contact/contactless IC chip and the embedded software (i.e., COS and JCS).



[Figure 2]Physical boundary of the TOE

- The JCRE consists of the Java Card virtual machine (JCVM), the Java Card API (JCAPI), and its associated native methods. This concerns all those dynamic features that are specific to the execution of a Java program in a smart card, like applet lifetime, applet isolation and object sharing, transient objects, the transaction mechanism, and so on. The basic runtime security feature imposed by the JCRE enforces isolation of applets using an applet firewall. It prevents objects created by one applet from being used by another applet without explicit sharing. This prevents unauthorized access to the fields and methods of class instances, as well as the length and contents of arrays.
- The JCVM provides the embedded interpreter of bytecodes. The JCVM is the component that enforces separation between applications (firewall) and enables secure data sharing.

- The card manager and GP API are responsible for the management of applets in the card.
- The native layer including COS and NesLib provided by the IC chip, which processes commands and manages files according to ISO/IEC 7816-3, 4 [20], provides the basic functionalities (memory management, I/O management and cryptographic libraries) with native interface with the dedicated IC. The cryptographic library provides high-level routines to perform RSA, SHA, AES and ECC operation using NESCRYPT for highly secure IC.
- The IC chip provides security features such as security monitoring and controlling register, clock random jitter, active Shields against physical attacks, memory scrambling and encryption, glue logic, secure cryptographic services, and a True Random Number Generator (TRNG) for AIS31-compliant Random Number Generation.

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Release	Date
Ucard UBJ31-G11 V1.1 Operation User Guidance	V1.3	September 20, 2012
Ucard UBJ31-G11 V1.1 Preparative procedure	V1.3	September 20, 2012

[Table 3] Documentation

7. TOE Testing

The developer took a testing approach based on the component of the TOE and the respective specification of each component. Physically, the embedded software is not separated, but logically, it can be divided into Java card system in accordance with Sun's Java Card 2.2.2 [7], [8], [9], card manager in accordance with Visa Global Platform Card Specification [11], and other API in accordance with the Korean Finance IC Card Standard [12].

Tests for Java card system were conducted for compliance to those specifications and

security mechanisms for self-protection and domain separation:

- 771 functional tests for API,
- 120 functional tests for JCRE, and
- 759 functional tests for JCVM.

Tests for card manager were conducted for compliance the the specification and security mechanism for non-bypassability:

- 607 functional tests for APDU,
- 618 functional tests for API, and
- 433 functional tests for SD.

Tests for other API were conducted for compliance to the specification:

- 17 functional tests for API used for SEED cryptographic operation and FICCS API for digital signature generation.

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.2. This means that the developer tested all the TSFI defined for each life cycle state of the TOE, and demonstrated that the TSF behaves as described in the functional specification.

The developer tested subsystems (including their interactions), and analyzed testing results according to the assurance component ATE_DPT.1.

The evaluator performed all the developer's tests listed in this report chapter 7.1, and conducted independent testing based upon test cases devised by the evaluator.

Also, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These test cases cover testing APDU commands, perturbation attacks, observation attacks such as SPA/DPA and SEMA/DEMA, fault injection attacks, and so on. No exploitable vulnerabilities by attackers possessing high attack potential were found from penetration testing.

The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [16].

8. Evaluated Configuration

The TOE is Ucard UBJ31-G11 V1.1. The TOE is composite product consisting of the following components:

- IC chips: SB23YR80B Secure Microcontrollers with cryptographic library

NesLib 3.0 SB

- Embedded software: UBJ31-G11_DEL V2.0

The TOE is identified by the name and version number. The TOE identification information is provided by the command-response APDU following:

- Command APDU: 00CA9F7F
- Response APDU: **5342 5942 5542** 2007 **8011** 1225 53009A00 81D4 55422100 5542 00000000000000000000000000000000000009000
  - '5342': SB (Chip Manufacture/Chip Manufacture NesLib)
  - '5942': YB (Chip Type/Revision)
  - '5542': UBIVELOX (Operating system identifier)
  - '80': EEPROM Size
  - '11': TOE final version

And the guidance documents listed in this report chapter 6, [Table 3] were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [16] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2], and CCRA supporting documents for the Smartcard and similar device [22], [23], [24], [25]. Also the evaluation facility utilized German scheme's Evaluation Methodology for CC Assurance Class for EAL5+ and EAL6 [27] under confirmation of the CB.
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL4 augmented by ALC_DVS.2 and AVA_VAN.5.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Also, the evaluator confirmed that the ST of the composite TOE does not contradict the ST of the IC chip according to the CCRA supporting document Composite Product Evaluation [15].

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has used a documented model of the TOE life-cycle. Therefore the verdict PASS is assigned to ALC_LCD.1.

The developer has used well-defined development tools (e.g. programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results. Therefore the verdict PASS is assigned to ALC_TAT.1.

The developer has clearly identified the TOE and its associated configuration items, and the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence. Therefore the verdict PASS is assigned to ALC_CMC.4.

The configuration list includes the TOE, the parts that comprise the TOE, the TOE implementation representation, security flaws, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.4.

The developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Additionally, sufficiency of the measures as applied is intended be justified. Therefore the verdict PASS is assigned to ALC_DVS.2.
The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.
Also, the evaluator confirmed that the correct version of the embedded software is installed onto/into the correct version of the underlying IC chip, and the delivery procedures of IC chip and embedded software developers are compatible with the acceptance procedure of the composite product integrator according to the CCRA supporting document Composite Product Evaluation [15].
Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the life-cycle model used by the developer, the configuration management, the security measures used throughout TOE development, the tools used by the developer throughout the life-cycle of the TOE, the handling of security flaws, and the delivery activity.
The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.
The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.
Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.
The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR-supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented; as such, the TOE design provides an explanation of the implementation representation.Therefore the verdict PASS is assigned to ADV_TDS.3.

The developer has completely described all of the TSFI in a manner such that the evaluator was able to determine whether the TSFI are completely and accurately described, and appears to implement the security functional requirements of the ST.Therefore the verdict PASS is assigned to ADV_FSP.4.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other.Therefore the verdict PASS is assigned to ADV_ARC.1.

The implementation representation made available by the developer is suitable for use in other analysis activities (analyzing the TOE design). Therefore the verdict PASS is assigned to ADV_IMP.1.

Also, the evaluator confirmed that the requirements on the embedded software, imposed by the IC chip, are fulfilled in the composite product according to the CCRA supporting document Composite Product Evaluation [15].

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed), and an implementation description (a source code level description). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested all of the TSFIs, and that the developer’s test coverage evidence shows correspondence between the tests identified in the test documentation

and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.2.
The developer has tested all the TSF subsystems against the TOE design and the security architecture description. Therefore the verdict PASS is assigned to ATE_DPT.1.
The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.
By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.
Also, the evaluator confirmed that composite product as a whole exhibits the properties necessary to satisfy the functional requirements of its ST according to the CCRA supporting document Composite Product Evaluation [15].
Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).
The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing High attack potential in the operational environment of the TOE.Therefore the verdict PASS is assigned to AVA_VAN.5.
Also, the evaluator confirmed that there is no exploitability of flaws or weakness in the composite TOE as a whole in the intended environment according to the CCRA supporting document Composite Product Evaluation [15].
Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), don't allow attackers possessing High attack potential to violate the SFRs.
The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_LCD.1	ALC_LCD.1.1E	PASS	PASS	PASS
	ALC_TAT.1	ALC_TAT.1.1E	PASS	PASS	
	ALC_CMS.4	ALC_CMS.4.1E	PASS	PASS	
	ALC_CMC.4	ALC_CMC.4.1E	PASS	PASS	
	ALC_DVS.2	ALC_DVS.2.1E	PASS	PASS	
		ALC_DVS.2.2E	PASS		
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.3	ADV_TDS.3.1E	PASS	PASS	PASS
		ADV_TDS.3.2E	PASS	PASS	
	ADV_FSP.4	ADV_FSP.4.1E	PASS	PASS	
		ADV_FSP.4.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
	ADV_IMP.1	ADV_IMP.1.1E	PASS	PASS	
ATE	ATE_COV.2	ATE_COV.2.1E	PASS	PASS	PASS
	ATE_DPT.1	ATE_DPT.1.1E	PASS	PASS	
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.5	AVA_VAN.5.1E	PASS	PASS	PASS
		AVA_VAN.5.2E	PASS		
		AVA_VAN.5.3E	PASS		
		AVA_VAN.5.4E	PASS		

[Table 4] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE provides cryptographic algorithm DES and SHA-1 not used by the TOE itself but used by future applications. Application developers should be careful when they use these weak algorithms in unavoidable situations.
- The TOE is Java card platform with open configuration, users can load and install, therefore use Java applets on the TOE. The applet itself and applet data are stored in the EEPROM, users should consider additional security countermeasures (e.g., integrity check or encryption) to protect those data.
- The TOE complies Visa Global Platform Card Specification [11], thus the TOE should be operated in accordance with the life-cycle status defined in the Global Platform Card Specification [10] which is referenced by Visa Global Platform Card Specification [11].

11. Security Target

Ucard UBJ31-G11 V1.1 Security Target V1.2, September 20, 2012 [17] is included in

this report by reference. For the purpose of publication, it is provided as sanitized version [18] according to the CCRA supporting document ST sanitizing for publication [26].

12. Acronyms and Glossary

AID	Application Identifier
APDU	Application Protocol Data Unit
CC	Common Criteria
CVM	Cardholder Verification Method
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
GP	Global Platform
JCAPI	Java Card API
JCRE	Java Card Runtime Environment
JCVM	Java Card Virtual Machine
JCS	Java Card System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SD	Security Domain
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

Application Protocol Data Unit(APDU)	Standard communication messaging protocol between a card accepting device and a smart card
Application (Applet)	The name is given to a Java Card technology-based user application. An application is the basic piece of code that can be selected for execution from outside the card. Each application on the card is uniquely identified by its AID.
Cardholder	The end user of a card
Cardholder Verification Method (CVM)	A method to ensure that the person presenting the card is the person to whom the card was issued

Card Manager	Generic term for the 3 card management entities of a GlobalPlatform card i.e. the OPEN, Issuer Security Domain and the Cardholder Verification Method Services provider
Global Platform (GP)	Global Platform, GP is an organization that has been established by leading companies from the payments and communications industries, the government sector and the vendor community, and is the first to promote a global infrastructure for smart card implementation across multiple industries. Its goal is to reduce barriers hindering the growth of cross-industry, multiple Application smart cards. The smart card issuers will continue to have the freedom to choose from a variety of cards, terminals and back-end systems.
JCRE	The Java Card runtime environment consists of the Java Card virtual machine, the Java Card API, and its associated native methods. This notion concerns all those dynamic features that are specific to the execution of a Java program in a smart card, like applet lifetime, applet isolation and object sharing, transient objects, the transaction mechanism, and so on.
JCVM	The embedded interpreter of bytecodes. The JCVM is the component that enforces separation between applications (firewall) and enables secure data sharing.
Logical channel	A logical link to an application on the card. A new feature of the Java Card System, version 2.2.2, that enables the opening of up to four simultaneous sessions with the card, one per logical channel. Commands issued to a specific logical channel are forwarded to the active applet on that logical channel.

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-001 ~ CCMB-2009-07-003, July 2009
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, CCMB-2009-07-004, July 2009

[3] Korea Evaluation and Certification Guidelines for IT Security (September 1, 2009)

[4] Korea Evaluation and Certification Scheme for IT Security (February 1, 2012)

[5] Java Card Platform, version 2.2 Runtime Environment (Java Card RE) Specification. June 2002. Published by Sun Microsystems, Inc.

[6] Java Card Platform, version 2.2 Virtual Machine (Java Card VM) Specification. June 2002. Published by Sun Microsystems, Inc.

[7] Java Card Platform, version 2.2.2 Runtime Environment (Java Card RE) Specification. March 2006. Published by Sun Microsystems, Inc.

[8] Java Card Platform, version 2.2.2 Virtual Machine (Java Card VM) Specification. Beta release, October 2005. Published by Sun Microsystems, Inc.

[9] Java Card Platform, version 2.2.2 Application Programming Interface, March 2006. Published by Sun Microsystems, Inc.

[10] GlobalPlatform Card Specification, Version 2.1.1, March 2003

[11] Visa GlobalPlatform 2.1.1 Card Implementation Requirements, Version 2.0, July 2007

[12] Finance IC card standard revision – Open platform – October 2010

[13] Certification Report ANSSI-CC-2010/02 – SA23YR48/80B and SB23YR48/80B Secure Microcontrollers, including the cryptographic library NesLib v2.0 or v3.0, in SA or SB configuration, February 1 2010, ANSSI

[14] Maintenance Report ANSSI-2010/02-M01 – Secured microcontrollers SA23YR48/80B and SB23YR48/80B, including the cryptographic libraries NesLib v2.0 or v3.0, in SA or SB configurations, March 19 2010, ANSSI

[15] STMicroelectronics SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B Security Target – Public Version, SMD_Sx23Yrxx_ST_09_002 Rev 02.01, November 2009

[16] TTA-CCE-11-027 Ucard UBJ31-G11 V1.1 Evaluation Technical Report V1.1, Oct 5, 2012

[17] Ucard UBJ31-G11 V1.1 Security Target V1.2, September 20, 2012 (Confidential Version)

[18] Ucard UBJ31-G11 V1.1 Security Target Lite V1.0, September 20, 2012 (Sanitized Version)

[19] Java Card™ System Protection Profile Open Configuration, Version 2.6, 19 April 2010

[20] ISO/IEC 7816 Identification cards – Integrated circuit(s) cards with contacts

[21] ISO/IEC 14443 Identification cards – Contactless ICCs - Proximity cards

[22] Composite product evaluation for Smartcards and similar devices Version 1.0 Revision 1, CCDB-2007-09-01, September 2007

[23] Application of Attack Potential to Smartcard Version 2.7 Revision 1, CCDB-2009-03-001, March 2009

[24] The Application of CC to Integrated Circuits Version 3.0 Revision 1, CCDB-2009-03-002, March 2009

[25] Requirements to perform Integrated Circuit Evaluations, Version 1.0 Revision 1, CCDB-2009-03-003, September 2009

[26] ST sanitising for publication, CCDB-2006-04-004, April 2006

[27] Application Notes and Interpretation of the Scheme (AIS), AIS 34, Version 3, BSI, March 9, 2009