REF: 2012-2-INF-1240 v1	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 19.09.2013	Approved by: TECNICO

CERTIFICATION REPORT

File: 2012-2 TimeCOS JavaCard Platform and EasyCard

Applicant: 200004799LW Watchdata Technologies Pte. Ltd.

References:

[EXT-1569] Certification request of TimeCOS JavaCard Platform and EasyCard

[EXT-2252] ETR of TimeCOS JavaCard Platform and EasyCard.

The product documentation referenced in the above documents.

Certification report of the product TimeCOS JavaCard Platform and EasyCard, as requested in [EXT-1569] dated 2012-03-08, and evaluated by the laboratory APPLUS-LGAI, as detailed in the Evaluation Technical Report [EXT-2252] received on 2013-07-26.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product TimeCOS Java Card Platform and EasyCard version 1.1.

The TOE is designed and used as a multi-application platform, which provides the capabilities to the issuer for performing the installation, updating and deletion of various Java Card applets. The post-issued Java Card applets are outside of the scope of the current certificate.

Additionally, the TOE includes a native application, named as EasyCard, which provides payment functionalities, such as the electronic purse used for transactions in public transportations and parking. The EasyCard application is masked in the TOE and cannot be deleted. The EasyCard application is inside of the scope of the current evaluation.

The TOE provides dual interfaces for a maximum flexibility in using different communication protocols: ISO 7816 and ISO 14443 (including Type A and Type B).

Developer/manufacturer: Watchdata System Co, Ltd..

Sponsor: Watchdata System Co, Ltd..

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

ITSEF: Applus LGAI Technological Center S.A.

Protection Profile: Java CardTM System Protection Profile, Open Configuration, Version 2.6, April 19th, 2010. Sun Microsystems, Inc.

Evaluation Level: Common Criteria v3.1 r3 EAL4 + ALC_DVS.2 + AVA_VAN.5.

Evaluation end date: 27/07/2013.

All the assurance components required by the evaluation level EAL4 (augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_DVS.2 (Sufficiency of security measures)) have been assigned a “PASS” verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria v3.1 r3 and the CEM v3.1 r3.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Considering the obtained evidences during the instruction of the certification request of the product TimeCOS Java Card Platform and EasyCard version 1.1, a positive resolution is proposed.

TOE SUMMARY

The TOE is the Smart Card Platform that is composed of:

- **SLE78CLFX**: The IC underlying platform [ICST], SLE78CLFX4000PM and SLE78CLFX2400PM, with the following libraries: RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013
- **TimeCOS Java Card Platform**: The dedicated COS, composed of
  - **Chip Driver**: The driver for access to the security chip of SLE78CLFX4000PM and SLE78CLFX2400PM
  - **Watchdata OS**: The underlying OS, providing the access to the functionalities of SLE78CLFX
  - **JCS**: The Java Card System, fulfilling the specification of Java Card RTE (including VM, RE and API) version 3.0.1 Classic Edition
  - **GP**: The GlobalPlatform, fulfilling the specification of GlobalPlatform (including OPEN, ISD, SD and API) version 2.1.1
- **EasyCard:** The native application, relaying on the Watchdata OS

The EasyCard is a native application included in the TOE, which fulfils the EasyCard Specification [CPU_FS_ECC] and [KMS_ECC] with the following functionalities:

- Supporting the following payment functions:
  - Read purse data
  - Debit transaction
  - Extended Debit transaction
  - Partial Refund transaction
  - Credit transaction
  - Auto-Load transaction
  - Cancel debit transaction
  - Cancel credit transaction
  - Read debit transaction Log
- Supporting the CPU functions.

To support the above mentioned functionalities of the EasyCard, the Watchdata private OS “Watchdata OS” implements the following functionalities:

- File System: according to ISO 7816-4,
- Access control for the file system and the cryptographic services,
- Secure messaging for external communication via a trusted channel (TC),
- Selection and management of security environments;
- User authentication with passwords,

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- Component authentication with symmetric and asymmetric cryptographic keys.

The TimeCOS Java Card Platform fulfils the followings specifications:

- The Java Card System (including VM, RE and API) version 3.0.1
- The GlobalPlatform (including OPEN, ISD, SSD and API) version 2.1.1

The Java Card System fulfills the following specifications:

- Java Card Runtime Environment (JCRE), see [JCRE30]
- Java Card Virtual Machine (JCVM), see [JCVM30]
- Java Card Application Programming Interface (JCAPI), see [JCAPI30]

The GlobalPlatform fulfils the GlobalPlatform v2.1.1 specification [GPCS], but is compatible with the Visa GlobalPlatform v2.1.1 specification [VGPCIR].

The Card Manager is implemented by the GlobalPlatform, which provides the Issuer Security Domain (ISD), Supplementary Security Domains (SSD), GlobalPlatform Registry, Open GlobalPlatform Environment (OPEN), GlobalPlatform API, Cardholder Verification Method (CVM) and DAP.

Java Card Applets are outside of the TOE scope, so they are not covered by this certificate in any way.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfill the evaluation level EAL4 and the evidences required by the additional components AVA_VAN.5 (Advanced methodical vulnerability analysis) and ALC_DVS.2 (Sufficiency of security measures), according to Common Criteria v3.1 r3.

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

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	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
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.5 Advanced methodical vulnerability analysis**

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies functional requirements according to the Common Criteria v3.1 r3. The TOE specific security functional requirements can be found on section *"6. Security functional requirements"* of the ST. The reference of the ST is explicitly identified in section "SECURITY TARGET" in this Certification Report.

IDENTIFICATION

Product: TimeCOS Java Card Platform and EasyCard version 1.1

Security Target: TimeCOS Java Card Platform and EasyCard Security Target version 1.8.

Protection Profile: Java CardTM System Protection Profile, Open Configuration, Version 2.6, April 19th, 2010. Sun Microsystems, Inc.

Evaluation Level: Common Criteria v3.1 r3 EAL4 + ALC_DVS.2 + AVA_VAN.5.

SECURITY POLICIES

The use of the product TimeCOS Java Card Platform and EasyCard version 1.1 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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

Policy 01: OSP.VERIFICATION

This policy shall ensure the adequacy between the export files used in the verification and those used for installing the verified file. The policy must also ensure that no modification of the file is performed between its verification and the signing by the verification authority.

Policy 02: OSP.MNG_SECRETS

Management of secret performed outside the product on behalf of the S.ISSUER shall comply with security organizational policies that enforce integrity and confidentiality of these data.

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.APPLET

Applets loaded post-issuance do not contain native methods. The Java Card specification explicitly “does not include support for native methods” ([JCVM30], §3.3) outside the API.

Assumption 02: A.VERIFICATION

All the bytecodes are verified at least once, before the loading, before the installation or before the execution, in order to ensure each bytecode is valid at execution time.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product TimeCOS Java Card Platform and EasyCard version 1.1, although the agents implementing attacks have a high attack potential according to the assurance level of EAL5 + AVA_VAN.5 + 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.

Confidentiality

Threat 01: T.CONFID-APPLI-DATA

The attacker executes an application to disclose data belonging to another application. See #.CONFID-APPLI-DATA for details. Directly threatened asset(s): D.APP_C_DATA, D.PIN and D.APP_KEYs.

Threat 02: T.CONFID-JCS-CODE

The attacker executes an application to disclose the Java Card System code. See #.CONFID-JCS-CODE for details. Directly threatened asset(s): D.JCS_CODE.

Threat 03: T.CONFID-JCS-DATA

The attacker executes an application to disclose data belonging to the Java Card System. See #.CONFID-JCS-DATA for details. Directly threatened asset(s): D.API_DATA, D.SEC_DATA, D.JCS_DATA and D.CRYPTO.

Threat 04: T.CONFID-EASY-DATA

The attacker tries to get the confidential data of D.APP_EASY_KEYS, and D.APP_APPLICATION_DATA through the communication interface of the TOE by sending commands or by listening to the communication between a terminal and the TOE.

Integrity

Threat 05: T.INTEG-APPLI-CODE

The attacker executes an application to alter (part of) its own code or another application's code. See #.INTEG-APPLI-CODE for details. Directly threatened asset(s): D.APP_CODE.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Threat 06: T.INTEG-APPLI-CODE.LOAD

The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation. See #.INTEG-APPLI-CODE for details. Directly threatened asset(s): D.APP_CODE.

Threat 07: T.INTEG-APPLI-DATA

The attacker executes an application to alter (part of) another application's data. See #.INTEG-APPLI-DATA for details. Directly threatened asset(s): D.APP_I_DATA, D.PIN and D.APP_KEYs.

Threat 08: T.INTEG-APPLI-DATA.LOAD

The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation. See #.INTEG-APPLI-DATA for details. Directly threatened asset(s): D.APP_I_DATA and D_APP_KEY.

Threat 09: T.INTEG-JCS-CODE

The attacker executes an application to alter (part of) the Java Card System code. See #.INTEG-JCS-CODE for details. Directly threatened asset(s): D.JCS_CODE.

Threat 10: T.INTEG-JCS-DATA

The attacker executes an application to alter (part of) Java Card System or API data. See #.INTEG-JCS-DATA for details. Directly threatened asset(s): D.API_DATA, D.SEC_DATA, D.JCS_DATA and D.CRYPTO.

Threat 11: T.INTEG-EASY-DATA

The attacker tries to compromise the D.APP_PURSE, D.APP_FCI, D.APP_EASY_KEYS, D.APP_ALC, D.APP_DT_LOGs, and D.APP_APPLICATION_DATA through the communication interface of the TOE by sending commands or by listening to the communication between a terminal and the TOE.

Identity Usurpation

Threat 12: T.SID.1

An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal. See #.SID for details. Directly threatened asset(s): D.SEC_DATA (other assets may be jeopardized should this attack succeed, for instance, if the identity of the JCRE is usurped), D.PIN and D.APP_KEYs.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Threat 13: T.SID.2

The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role. See #.SID for further details. Directly threatened asset(s): D.SEC_DATA (any other asset may be jeopardized should this attack succeed, depending on whose identity was forged).

Unauthorized Execution

Threat 14: T.EXE-CODE.1

An applet performs an unauthorized execution of a method. See #.EXE-JCS-CODE and #.EXE-APPLI-CODE for details. Directly threatened asset(s): D.APP_CODE.

Threat 15: T.EXE-CODE.2

An applet performs an execution of a method fragment or arbitrary data. See #.EXE-JCSCODE and #.EXE-APPLI-CODE for details. Directly threatened asset(s): D.APP_CODE.

Threat 16: T.EXE-CODE-REMOTE

The attacker performs an unauthorized remote execution of a method from the CAD. See #.EXE-APPLI-CODE for details. Directly threatened asset(s): D.APP_CODE.

Application note: This threat concerns version 2.2.x of the Java Card RMI, which allow external users (that is, other than on-card applets) to trigger the execution of code belonging to an on-card applet. On the contrary, T.EXE-CODE.1 is restricted to the applets under the TSF.

Threat 17: T.NATIVE

An applet executes a native method to bypass a TOE Security Function such as the firewall. See #.NATIVE for details. Directly threatened asset(s): D.JCS_DATA.

Threat 18: T.FORGE_TRANS

An attacker tries to force the EasyCard application into a non stable state by retrying a previous transaction, bypassing some code, stopping or disrupting the execution of the application instance in order to succeed an unauthorized transaction.

Denial of Service

Threat 19: T.RESOURCES

An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM. See #.RESOURCES for details. Directly threatened asset(s): D.JCS_DATA.

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Card Management

Threat 19: T.DELETION

The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to pave the way for further attacks (putting the TOE in an insecure state). See #.DELETION for details). Directly threatened asset(s): D.SEC_DATA and D.APP_CODE.

Threat 20: T.INSTALL

The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process. See #.INSTALL for details. Directly threatened asset(s): D.SEC_DATA (any other asset may be jeopardized should this attack succeed, depending on the virulence of the installed application).

Threat 21: T.DELETION.2

The attacker uses a bug in the card manager implementation to delete applets without authorization.

Services

Threat 22: T.OBJ-DELETION

The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application. See #.OBJ-DELETION for further details. Directly threatened asset(s): D.APP_C_DATA, D.APP_I_DATA and D.APP_KEYs.

Miscellaneous

Threat 22: T.PHYSICAL

The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing and unexpected tearing. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques.

Threat 23: T.ISOLATION

The attacker uses problems or bugs identified in the native application to access/modify/erase actives from the Java Card System implementation or vice

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

versa. And attacker uses the Mifare legacy application to access/modify/erase without authorization the EasyCard assets.

Threat 24: T.MISUSE

An attacker tries to use the TOE functions to gain access to the Easycard D.APP_PURSE, D.APP_FCI, D.APP_EASY_KEYS, D.APP_ALC, D.APP_DT_LOGs, D.APP_APPLICATION_DATA assets without knowledge of user authentication data or any implicit authorization.

Threat 25: T.LEAKAGE

An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential data (User Data or TSF data). The information leakage may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements.

Threat 26: T.RND

An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided.

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.APPLET

No applet loaded post-issuance shall contain native methods.

Environment objective 02: OE.VERIFICATION

All the bytecodes shall be 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. See #.VERIFICATION for details.

Environment objective 03: OE.MNG_SECRETS

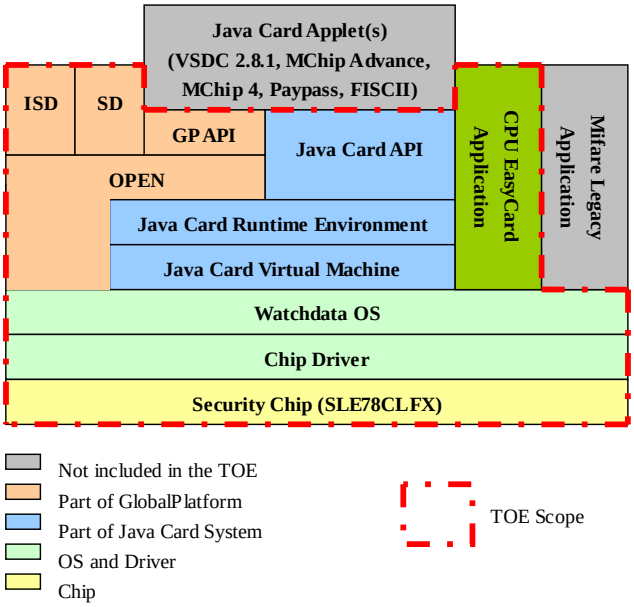
ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The secret User or TSF data managed outside the TOE shall be protected against unauthorized disclosure and modification.

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

ARCHITECTURE

The TOE includes several components: IC underlying platform, OS, Java Card System, GlobalPlatform (compatible with Visa GlobalPlatform specification), and a native application EasyCard. The following picture describes the TOE architecture.



DOCUMENTS

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

- [AGD_OPE] Operational User Guidance, version 1.2. 2013.06.24. Watchdata System Co., Ltd.
- [AGD_PRE] Preparative Procedures, version 1.0. 2013.06.23. Watchdata System Co., Ltd

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

PRODUCT TESTING

The evaluation has been performed according to the Composite Evaluation Scheme as defined in the guides [JILCOMP] and [JILADVARC] in order to assess that the combination of the TOE with the underlying platform did not lead to any exploitable vulnerability.

This evaluation has then taken into account the evaluation results and security recommendations for the platform which is part of the evaluated composite TOE, and was already certified with certificate BSI-DSZ-CC-0758.

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

The obtained results have been checked to be conformant to the expected results and in cases where a deviation relative to the expected results has been detected, 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, the evaluation team has devised attack scenarios for penetration tests 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.

The implementations of the requirements of the provided platform's ETR for Composition and guidance, as well as of the security mechanisms of the TOE in general have been verified by the evaluation team. An appropriate test set was devised to cover these potential vulnerabilities.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential **High** has been

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

successful in the TOE's operational environment as defined in the security target when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The TOE is defined by its name and version number: TimeCOS Java Card Platform and EasyCard version 1.1.

The TOE is composed of:

- **SLE78CLFX**: The IC underlying platform [ICST], SLE78CLFX4000PM and SLE78CLFX2400PM, with the following libraries: RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013
- **TimeCOS Java Card Platform**: The dedicated COS, composed of
  - **Chip Driver**: The driver for access to the security chip of SLE78CLFX4000PM and SLE78CLFX2400PM
  - **Watchdata OS**: The underlying OS, providing the access to the functionalities of SLE78CLFX
  - **JCS**: The Java Card System, fulfilling the specification of Java Card RTE (including VM, RE and API) version 3.0.1 Classic Edition
  - **GP**: The GlobalPlatform, fulfilling the specification of GlobalPlatform (including OPEN, ISD, SD and API) version 2.1.1
- **EasyCard:** The native application, relaying on the Watchdata OS

The commercial version and internal version of the applet may be retrieved by following the procedure in section *"3.1 Identification"* of [AGD_PRE].

The resumed identification procedure is as follows:

1. To identify the TOE, the APDU of GET DATA [CPLC] can be adopted. The format of GET DATA [CPLC] is as following:
   a. <80/00> CA 9F 7F 00
2. The bytes to identify the TOE are shown in the following table.

Data Element	***Length***	***Default Value***	***Remark***
IC fabricator	2	'40 90'	Infineon
IC type	2	'00 05' or '00 07'	'00 05': SLE78CLFX4000PM; '00 07': SLE78CLFX2400PM
Operating system identifier	2	'86 93'	Watchdata developed OS
Operating system release date[1]	2	'1A 10'	January 16th, 2013

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Operating system release level	2	'01 01'	OS version 1.1

EVALUATION RESULTS

The product TimeCOS Java Card Platform and EasyCard version 1.1 has been evaluated against the Security Target TimeCOS Java Card Platform and EasyCard Security Target version 1.8.

All the assurance components required by the evaluation level EAL4 + ALC_DVS.2 + AVA_VAN.5 have been assigned a "PASS" verdict. Consequently, the laboratory Applus LGAI Technological Center S.A. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4 + ALC_DVS.2 + AVA_VAN.5, as defined by the Common Criteria v3.1 r3 and the CEM v3.1 r3.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

During the evaluation process the developer gave support to the evaluator answering to the observation reports as soon as they received.

The developer follows all the underlying platform security recommendations and contributes with additional countermeasures to enforce the security of the whole product.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product TimeCOS Java Card Platform and EasyCard version 1.1, a positive resolution is proposed.

Additionally, the Certification Body wants to remark to the TOE's consuming organizations the following aspects:

- Applet developers using this TOE as platform for Java Card applets, should carefully observe section *"15 Secure Recommendation for Applet Developers"* in the Operational User Guidance [AGD_OPE], in order to properly follow security properties and recommendations to develop applications for this TOE.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- The Mifare operating MODE of this product is explicitly out of the scope of this certificate.

GLOSSARY

AES	Advanced Encryption Standard
API	Application Program Interface
CC	Common Criteria
CCN	Centro Criptológico Nacional
CLK	Clock
CM	Configuration Management
CNI	Centro Nacional de Inteligencia
CPA	Correlation Power Analysis
CPU	Central Processing Unit
CVM	Cardholder Verification Method
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DPA	Differential Power Analysis
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
EMA	ElectroMagnetic Analysis
ETR	Evaluation Technical Report
ETR	Evaluation Technical Report
GND	Ground
GP	Global Platform
IC	Integrated Circuit
ISD	Issuer Security Domain

ENAC CERTIFICACIÓN Nº 45/C-PR110
C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

MED	Memory Encryption/Decryption Unit
OC	Organismo de Certificación
OS	Operating System
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PM	Project Manager
PP	Protection Profile
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman cryptosystem
SAR	Security Assurance Requirement
SEMA	Simple Electromagnetic Analysis
SFR	Security Functional Requirement
SPA	Simple Power Analysis
SPD	Security Problem Definition
SSD	Supplementary Security Domain
ST	Security Target
TOE	Target of Evaluation
TOE	Target Of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
USB	Universal Serial Bus

BIBLIOGRAPHY

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

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R3 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R3 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R3 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R3 Final, July 2009.

[JILCOMP] Composite product evaluation for Smart Cards and similar devices version 1.2. Jan. 2012.

[JILAAPS] Application of Attack Potential to Smartcards, Version 2.8. Jan. 2012.

[JILADVARC] Security Architecture requirements (ADV_ARC) for Smart Cards and similar devices. Version 2.0. Jan. 2012.

[CCDB-2006-04-004] ST sanitising for publication. CCMC. Apr. 2006.

[AGD_OPE] Operational User Guidance, version 1.2. 2013.06.24. Watchdata System Co., Ltd.

[AGD_PRE] Preparative Procedures, version 1.0. 2013.06.23. Watchdata System Co., Ltd

[ICST] Security Target (ST) M7892 A21 and comprises the Infineon Technologies Security Controller M7892 A21 with specific IC dedicated software and optional RSA v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries.

[CPU_FS_ECC] EasyCard Phoenix Project: Functional Specification – CPU CARD, Release A19, December 9th, 2010. Gemalto.

[KMS_ECC] EasyCard Phoenix Project: Key Management Specification, Release A19, December 9th, 2010. Gemalto.

[JCRE30] Java Card Platform Runtime Environment Specification, Version 3.0.1, Classic Edition, May 2009. Sun Microsystems, Inc.

[JCVM30] Java Card Platform Virtual Machine Specification, Version 3.0.1, Classic Edition, May 2009. Sun Microsystems, Inc.

[JCAPI30] Java Card Platform Application Programming Interface, Version 3.0.1, Classic Edition, May 2009. Sun Microsystems, Inc.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

[JCS-OP-PP] Java Card System Protection Profile Open Configuration, v2.6, April 19th 2010. ANSSI-CC-PP-2010/03. Sun Microsystems, Inc.

[GPCS] GlobalPlatform Card Specification, Version 2.1.1, March 2003. GlobalPlatform Inc.

[VGPCIR] Visa GlobalPlatform 2.1.1 Card Implementation Requirements, v2.0, July 2007. Visa International Service Association.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security. Common Criteria Management Comitee. 2000.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates. Version 3.0. SOG-IS Management Committee. 2010.

SECURITY TARGET

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

- Title: TimeCOS Java Card Platform and EasyCard Security Target
- Version: 1.8
- Issue Date: 2013.05.14
- Reference: SEC_20110121_963_ASE

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es