| | |
|---|---|
| REF: 2010-10-INF-1372 v2 | Created by: CERT8 |
| Target: Expediente | Revised by: CALIDAD |
| Date: 14.11.2014 | Approved by: TECNICO |

# CERTIFICATION REPORT

File: 2010-10 ExaCard smart card

Applicant: A08244287 Calmell S.A.

References:

[EXT-1014] Certification request of ExaCard smart card

[EXT-2570] Evaluation Technical Report of ExaCard smart card.

The product documentation referenced in the above documents.

Certification report of the product Idoneum Electronic Identity ExaCard smart card v1.0, as requested in [EXT-1014] dated 17-06-2010, and evaluated by the laboratory Applus LGAI Technological Center S.A, as detailed in the Evaluation Technical Report [EXT-2570] received on 23/07/2014.



C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

**TABLE OF CONTENTS**





C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Idoneum Electronic Identity ExaCard smart card v1.0.

The ExaCard smart card v 1.0 is a secure signature-creation device intended to be used in a Public Key Infrastructure (PKI) system. Its main feature it's the combination of RSA and ECC algorithms for a greater resistance to breakage of some of these signature algorithms.

It addition to signature generation, it allows RSA key generation and export of 2048, 3072 and 4096 bits, ECC key generation of 192, 224, 256, 384 and 521 bits, TDES symmetric key generation, encipher/decipher operations either symmetric or asymmetric, generation of SHA-1, SHA-224 and SHA-256 message digests, generation of pseudo random numbers with the ANSI X9.17 Random Number Generator and it implements the main functionality of the ISO/IEC 7816- 3/4/8/ and CWA 14890-1 specifications.

All the above operations are managed by a complete smart card operating system highly configurable and with protection against accidental data corruption. This feature is provided by the file system which implements a powerful transaction system.

Its support for several logical channels allows for a secure multi-application environment while protecting the privacy of each application user's data.

**Developer/manufacturer**: Calmell, S.A.

**Sponsor**: Calmell, S.A.

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

**ITSEF**: Applus LGAI Technological Center S.A.

**Protection Profile**: Protection Profile Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002.

**Evaluation Level**: Common Criteria v3.1 R3 - EAL4 + AVA_VAN.5.

**Evaluation end date**: 23/07/2014.

All the assurance components required by the evaluation level EAL4 (augmented with AVA_VAN.5: Advanced methodical vulnerability analysis) 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 + AVA_VAN.5, as defined by the Common Criteria v3.1 R3 and the CEM v3.1 R3.



C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Considering the obtained evidences during the instruction of the certification request of the product Idoneum Electronic Identity ExaCard smart card v1.0, a positive resolution is proposed.

## TOE SUMMARY

The TOE is a secure signature-creation device (SSCD type 3) as defined in the CWA 14169:2004 CEN standard. The CWA 14169:2004 defines security requirements for Secure Signature- Creation Devices (SSCD) according to European Directive 1999/93/EC on a Community framework for electronic signatures.

It's main purpose is to be used as secure signature creation device in a PKI system, providing signature operation, key generation, key export, and confidentiality, integrity and protection of user's data.

The TOE is a composite TOE, and it consists of a complete smart card operating system designed by Idoneum Electronic Identity S.A. (a Calmell Group company) built on the certified NXP P5CC081 secure contact PKI smart card controller [ICST]. The cryptographic operations relies upon the certified “Secured Crypto Library on the P5CD016/021/041/081 and P5CC081” cryptographic subroutine library by NXP Semiconductors [LIBST], in the following NXP Crypto Library.

## SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component AVA_VAN.5: Advanced methodical vulnerability analysis, 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.1 Identification of security measures |
| | ALC_LCD.1 Developer defined life-cycle model |
| | ALC_TAT.1 Well-defined development tools |
| ASE: Security Target evaluation | ASE_CCL.1 Conformance claims |
| | ASE_ECD.1 Extended components definition |
| | ASE_INT.1 ST introduction |
| | ASE_OBJ.2 Security objectives |



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

| Assurance Class | Assurance components |
|---|---|
| | 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 the following functional requirements, according to the Common Criteria v3.1 R3 Part 2 extended with the additional component FPT_EMSEC.1:TOE Emanation.

| TOE Security Functional Requirements | Description |
|---|---|
| FCS_CKM.1/RSA | Cryptographic key generation |
| FCS_CKM.1/ECC | Cryptographic key generation |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1/CORRESP/RSA | Cryptographic operation |
| FCS_COP.1/CORRESP/ECC | Cryptographic operation |
| FCS_COP.1/SIGNING/RSA | Cryptographic operation |
| FCS_COP.1/SIGNING/ECC | Cryptographic operation |
| FDP_ACC.1/SVD TRANSFER SFP | Subset access control |
| FDP_ACC.1/INITIALISATION SFP | Subset access control |
| FDP_ACC.1/PERSONALISATION SFP | Subset access control |
| FDP_ACC.1/SIGNATURE-CREATION SFP | Subset access control |
| FDP_ACF.1/INITIALISATION SFP | Security attribute based access control |
| FDP_ACF.1/SVD TRANSFER SFP | Security attribute based access control |
| FDP_ACF.1/PERSONALISATION SFP | Security attribute based access control |
| FDP_ACF.1/SIGNATURE-CREATION SFP | Security attribute based access control |
| FDP_ETC.1/SVD TRANSFER | Export of user data without security attributes |
| FDP_ITC.1/DTBS | Import of user data without security attributes |
| FDP_RIP.1 | Subset residual information protection |
| FDP_SDI.2/Persistent | Stored data integrity monitoring and action |
| FDP_SDI.2/DTBS | Stored data integrity monitoring and action |
| FDP_UIT.1/SVD TRANSFER | Data exchange integrity |
| FDP_UIT.1/TOE DTBS | Data exchange integrity |
| FIA_AFL.1 | Authentication failure handling |
| FIA_ATD.1 | User attribute definition |
| FIA_UAU.1 | Timing of authentication |
| FIA_UID.1 | Timing of identification |
| FMT_MOF.1 | Management of security functions behaviour |
| FMT_MSA.1/ADMINISTRATOR | Management of security attributes |
| FMT_MSA.1/SIGNATORY | Management of security attributes |
| FMT_MSA.2 | Secure security attributes |
| FMT_MSA.3 | Static attribute initialisation |
| FMT_MTD.1 | Management of TSF data |



C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

| TOE Security Functional Requirements | Description |
|---|---|
| FMT_SMR.1 | Security roles |
| **FPT_EMSEC.1** | **TOE Emanation** |
| FPT_FLS.1 | Failure with preservation of secure state |
| FPT_PHP.1 | Passive detection of physical attack |
| FPT_PHP.3 | Resistance to physical attack |
| FPT_TST.1 | TSF testing |
| FTP_ITC.1/SVD TRANSFER | Inter-TSF trusted channel |
| FTP_ITC.1/DTBS IMPORT | Inter-TSF trusted channel |

# IDENTIFICATION

**Product**: Idoneum Electronic Identity ExaCard smart card v1.0.

**Security Target:** ExaCard smart card v 1.0 ST, version 1.05, Idoneum Electronic Identity, 04 June 2014.

**Protection Profile**: Protection Profile – Secure Signature-Creation Device Type 3, Version 1.05, BSI-PP-0006-2002.

**Evaluation Level**: Common Criteria v3.1 R3 EAL4 + AVA_VAN.5.

# SECURITY POLICIES

The use of the product Idoneum Electronic Identity ExaCard smart card v1.0 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

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

## Policy 01: P.CSP_QCert Qualified certificate

The CSP uses a trustworthy CGA to generate the qualified certificate for the SVD generated by the SSCD. The qualified certificates contains at least the elements defined in Annex I of the Directive, i.e., inter alia the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE is evident with signatures through the certificate or other publicly available information.

## Policy 02: P.QSign Qualified electronic signatures

The signatory uses a signature-creation system to sign data with qualified electronic signatures. The DTBS are presented to the signatory by the SCA. The qualified electronic signature is based on a qualified certificate (according to directive Annex 1) and is created by a SSCD.



C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

### Policy 03: P.Sigy_SSCD TOE as secure signature-creation device

The TOE implements the SCD used for signature creation under sole control of the signatory . The SCD used for signature generation can practically occur only once.

## 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.CGA - Trustworthy certification-generation application

The CGA protects the authenticity of the signatory's name and the SVD in the qualified certificate by an advanced signature of the CSP.

### Assumption 02: A.SCA Trustworthy signature-creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS-representation of data the signatory wishes to sign in a form appropriate for signing by the TOE.

## CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Idoneum Electronic Identity ExaCard smart card v1.0, although the agents implementing attacks have a high attack potential according to the assurance level EAL4 + AVA_VAN.5 and always fulfilling the usage assumptions and the proper security policies satisfaction.

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

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

### Threat 01: T.Hack_Phys Physical attacks through the TOE interfaces

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. This threat addresses all the assets.



C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

### Threat 02: T.SCD_Divulg Storing, copying, and releasing of the signature-creation data

An atacker can store, copy, the SCD outside the TOE. An attacker can release the SCD during generation, storage and use for signature-creation in the TOE.

### Threat 03: T.SCD_Derive Derive the signature-creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data communicated outside the TOE, which is a threat against the secrecy of the SCD.

### Threat 04: T.Sig_Forgery Forgery of the electronic signature

An attacker forges the signed data object maybe together with its electronic signature created by the TOE and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

### Threat 05: T.Sig_Repud Repudiation of signatures

If an attacker can successfully threaten any of the assets, then the non-repudiation of the electronic signature is compromised. This results in the signatory is able to deny having signed data using the SCD in the TOE under his control even if the signature is successfully verified with the SVD contained in his un-revoked certificate.

### Threat 06: T.SVD_Forgery Forgery of the signature-verification data

An attacker forges the SVD presented by the TOE to the CGA. This result in loss of SVD integrity in the certificate of the signatory.

### Threat 07: T.DTBS_Forgery Forgery of the DTBS-representation

An attacker modifies the DTBS-representation sent by the SCA. Thus the DTBS-representation used by the TOE for signing does not match the DTBS the signatory intended to sign.

### Threat 08: T.SigF_Misuse Misuse of the signature-creation function of the TOE

An attacker misuses the signature-creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

## OPERATIONAL ENVIRONMENT FUNCTIONALITY

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



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

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

### Environment objective 01: OE.CGA_QCert Generation of qualified certificates

The CGA generates qualified certificates which include inter alia

(a) the name of the signatory controlling the TOE,

(b) the SVD matching the SCD implemented in the TOE under sole control of the signatory,

(c) the advanced signature of the CSP.

### Environment objective 02: OE.SVD_Auth_CGA CGA verifies the authenticity of the SVD

The CGA verifies that the SSCD is the sender of the received SVD and the integrity of the received SVD. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

### Environment objective 03: OE.HI_VAD Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed.

### Environment objective 04: OE.SCA_Data_Intend Data intended to be signed

The SCA

(a) generates the DTBS-representation of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,

(b) sends the DTBS-representation to the TOE and enables verification of the integrity of the DTBS-representation by the TOE

(c) attaches the signature produced by the TOE to the data or provides it separately.

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



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

# ARCHITECTURE

## LOGICAL ARCHITECTURE

The TOE provides the following functions necessary for devices involved in creating qualified electronic signatures:

(1) to generate the SCD and the correspondent signature-verification data (SVD) and
(2) to create qualified electronic signatures
  (a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function may either be provided by the TOE itself or by appropriate environment
  (b) using appropriate hash functions that are agreed as suitable for qualified electronic signatures
  (c) after appropriate authentication of the signatory by the TOE.
  (d) using appropriate cryptographic signature function that employ appropriate cryptographic parameters agreed as suitable.

The TOE implements all IT security functionality which are necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control.

The [ST] assumes that the Signature Creation Application (SCA) is part of the environment of the TOE.

The SSCD protects the SCD during the whole life cycle of the card as to be solely used in the signature creation process by the legitimate signatory. The TOE will be initialised for the signatory's use by:

1. Generating a SCD/SVD pair
2. Personalisation for the signatory by means of the signatory's verification authentication data (SVAD).

The SVD corresponding to the signatory's SCD will be included in the certificate of the signatory by the certificate-service-provider (CSP). The TOE will destroy the SCD if it is no longer used for signature generation.

The TOE allows user authentication by means of a trusted human interface (HI) device connected via a trusted channel with the TOE. The HI device is used for the input of verification authentication data (VAD) for authentication by knowledge. The TOE holds reference authentication data (RAD) to check the provided VAD.

The TOE life cycle is shown in Figure 1. Basically, it consists of a development phase and the operational phase. In the initialisation phase the basic structures of the system are built. The operational phase starts with personalisation, including loading of the structures generated during initialisation and generation of the first key pair SCD/SVD. The main functionality in the usage phase is signature-creation including all supporting functionality (e.g., SCD storage and SCD use).

The life cycle ends with the destruction of the SSCD.



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

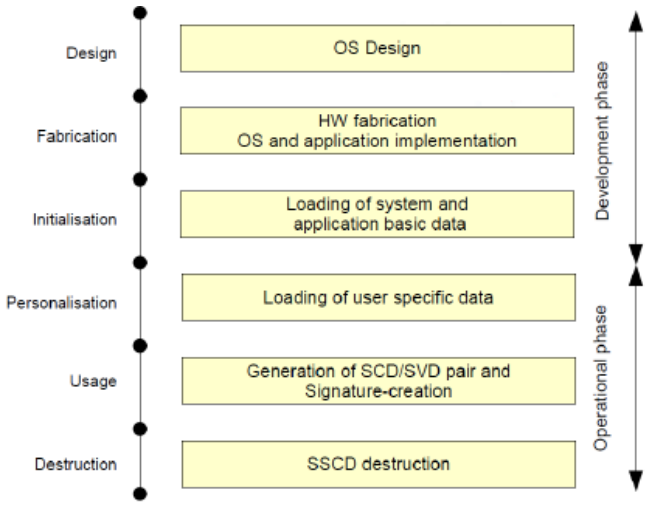


Figure 1

## PHYSICAL ARCHITECTURE

The figure 1 shows the different components of the TOE and its relationships. A more emphasis is given to the operating system.

The TOE communicates via trusted channel with the external applications:

- Certification-generation Application (CGA)
- Signature-creation Application (SCA)

The main OS subsystems are depicted in the figure below. All of them are interrelated to a greater or lesser degree.

- The configuration subsystem manages the customizable parameters of the operating system and its external functionality.
- The command subsystem is the functional high level for the signature creation, key generation and other smart card user operations.
- The authorization and authentication subsystem controls the access to the resources based on an Access Control List (ACL) system. An ACL is basically a list of permissions attached to a resource. Each entry of the ACL indicates an access mode to the resource and the conditions to be met in order to allow that access. Also it performs the device authentication protocol operations which allows the communication with authorised applications only.
- The crypto and key management subsystem contains the functions that implements the cryptographic operations needed mainly for the signature-creation operation.
- The volatile and non-volatile memory subsystem manages the volatile (RAM) and non-volatile (EEPROM) memory from a low level.
- The security subsystem ensures that the execution flow and the function calls inside the operating system run as expected. Also it manages the unexpected errors from some critical operations and performs the necessary actions.



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

- The file subsystem manages all the user's data in a secure way, relying on the authorization and authentication subsystem and the crypto and key management subsystem.
- The utilities subsystem offers functionality to be used by the other subsystems. There are functionality for: BER-TLV or simple-TLV structures, CRC, big numbers and memory.
- The I/O subsystem is the responsible of the external communication via the ISO/IEC 7816- 3 T=0 protocol.

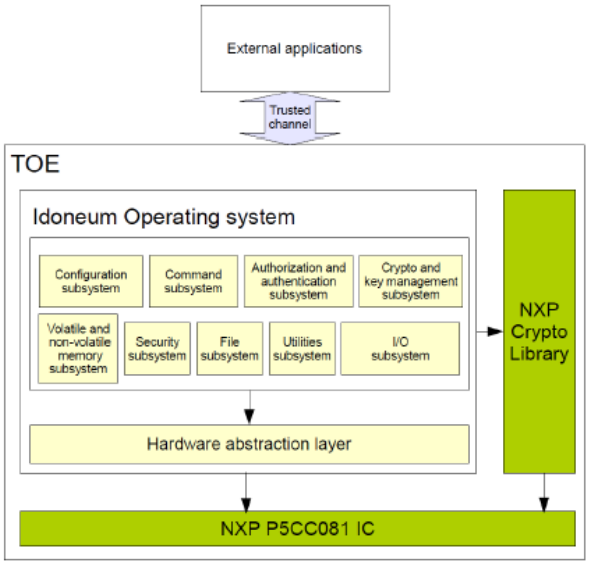


Figure 2

In a lower level is located the hardware abstraction layer (HAL) which is made up of functions that access the hardware directly, creating an interface for the upper subsystems. The HAL controls the following components of the P5CC081: UART, timers, interruptions, EEPROM, FameXE, Random Number Generator, CPU & coprocessors clock and security hardware.

## DOCUMENTS

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

- Exacard smart card v 1.0: AGD_OPE, guía de recomendaciones para el usuario, version 1.03.
- ExaCard smart card v 1.0 profile, version 1.00.
- Especificación Funcional ExaCard OS v1.03, 29 October 2013.



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
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 certificates BSI-DSZ-CC-0555 and BSI-DSZ-CC-0633.

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



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

# EVALUATED CONFIGURATION

The TOE is defined by its name and version number:

- Idoneum Electronic Identity ExaCard smart card v1.0

The TOE is composed of:

- Smart card operating system Idoneum Electronic Identity ExaCard smart card v1.0.
- NXP P5CC081 secure contact PKI smart card controller [ICST] certified by BSI with certificate identifier BSI-DSZ-CC-0555.
- Secured Crypto Library on the P5CD016/021/041/081 and P5CC081 cryptographic subroutine library by NXP Semiconductors [LIBST] certified by BSI with certificate identifier BSI-DSZ-CC-0633.

The TOE identification may be retrieved by following the procedure in section *"3 Adquisición, recepción y aceptación"* of [AGD_OPE].

The resumed identification procedure is based on the ATR TOE provides:

3B 7F 18 00 00 00 6A **49 45 49 01 01 01 00 00 00 00 07** 90 00

where:

| ***Description*** | ***Bytes*** |
|---|---|
| ROM mask versión | 49 45 49 01 01 01 |
| Personalization and patch profile | 00 00 00 00 |
| Life cycle: activation | 07 |

# EVALUATION RESULTS

The product Idoneum Electronic Identity ExaCard smart card v1.0 has been evaluated against the Security Target ExaCard smart card v 1.0 ST, version 1.05, Idoneum Electronic Identity, 04 June 2014.

All the assurance components required by the evaluation level EAL4 + 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 + AVA_VAN.5, as defined by the Common Criteria v3.1 R3 and the CEM v3.1 R3.

# COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

The Idoneum Electronic Identity ExaCard smart card v 1.0 fulfils the requirements of CC version 3.1 with an evaluation assurance level EAL4+AVA_VAN.5.

## CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Idoneum Electronic Identity ExaCard smart card v1.0, a positive resolution is proposed.

## GLOSSARY

| | |
|---|---|
| CC | Common Criteria |
| CCN | Centro Criptológico Nacional |
| CM | Configuration Management |
| CMS | Configuration Management System |
| CNI | Centro Nacional de Inteligencia |
| DTBS | Data to be signed |
| EAL | Evaluation Assurance Level |
| ECC | Elliptic Curve Cryptography |
| ETR | Evaluation Technical Report |
| IC | Integrated Circuit |
| OC | Organismo de Certificación |
| OSP | Organisational Security Policies |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |
| SPD | Security Problem Definition |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TOE Security Functionality Interface |

## BIBLIOGRAPHY

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



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

product:

[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.

[PP] Protection Profile Secure Signature-Creation Device Type 3, Version 1.05, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference EAL4+ BSI-PP-0006-2002.

[ICST] NXP Semiconductors. NXP Secure Smart Card Controllers P5CD016/021/041V1A and P5Cx081V1A Security Target Lite, Rev. 1.3, 21 September 2009.

[LIBST] NXP Semiconductors. Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A Security Target, Rev. 0.8, 28 April 2010.

[AGD_OPE] Exacard smart card v 1.0: AGD_OPE, guía de recomendaciones para el usuario, version 1.03.

[EC_P] ExaCard smart card v 1.0 profile, version 1.00.

[ADV_FSP] Especificación Funcional ExaCard OS v1.03, 29 October 2013

## SECURITY TARGET

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

- ExaCard smart card v 1.0 ST, version 1.05, Idoneum Electronic Identity, 04 June 2014.



ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es