REF:	2004-3-INF-71 v2	Created by:	TECNICO
Difussion:	Público	Reviewed by:	CERT3
Date:	08.05.2006	Approved by:	JEFEAREA

CERTIFICATION REPORT

Dossier: 2004-3 TARJETA ELECTRONICA MINISTERIO DE DEFENSA

References:

EXT-2	Solicitud de Certificación de la TEMD v1.0, 19/07/04
EXT-131	TMD/TRE/2042/001/INTA/05, ed. 1.0, 24/11/05
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, mayo 2000.
DIRF	Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Certification report of TARJETA ELECTRÓNICA DEL MININISTERIO DE DEFENSA (TEMD), version1.0, as requested by [EXT-2], dated 19-7-2004, and evaluated by the laboratory CESTI-INTA, as detailed in the Evaluation Technical Report [EXT-131], received on the 24th of November, 2005, and in compliance with [CCRA].

This is a courtesy translation of the Scheme documentation for the purposes of its shadow certification.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

INDEX

EXECUTIVE SUMMARY **3**
TOE SUMMARY 4
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
Requirements expressed as of [CC_P2]: *5*
Requirements augmented by [CWA14169]: *5*
IDENTIFICATION **6**
SECURITY POLICY **6**
ASSUMPTIONS AND CLARIFICATION OF SCOPE **7**
USAGE ASSUMPTIONS 7
ENVIRONMENTAL ASSUMPTIONS 8
CLARIFICATION OF SCOPE 8
SECURITY FUNCTIONAL REQUIREMENTS FOR THE TOE ENVIRONMENT 10
ARCHITECTURAL INFORMATION **12**
DOCUMENTATION **13**
IT PRODUCT TESTING **14**
EVALUATED CONFIGURATION **14**
RESULTS OF THE EVALUATION **15**
EVALUATOR COMMENTS/RECOMMENDATIONS **15**
CERTIFIER RECOMMENDATIONS **16**
GLOSSARY **16**
BIBLIOGRAPHY **16**
SECURITY TARGET **16**

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Executive Summary

This document constitutes the Certification Report for the product ELECTRONIC CARD FOR THE MINISTRY OF DEFENSE (TEMD v1.0) developed on the integrated circuit IC for smart card SLE66CX322P, manufactured by INFINEON TECHNOLOGIES AG.

Developer: MICROELECTRÓNICA ESPAÑOLA CORP.

Sponsor: MICROELECTRÓNICA ESPAÑOLA CORP.

Certification Body: National Cryptological Centre (CCN)

ITSEF: IT Security Evaluation Centre (CESTI), of the Technical Aerospace National Institute “Esteban Terradas”(INTA).

PP claims: CWA 14169: SECURE SIGNATURE-CREATION DEVICES " EAL4+ " LEVEL 3 14169:2002 E MARCH 2002

Evaluation Level: EAL4+ (AVA-MSU.3, AVA-VLA.4)

Strength of Function: High

ETR date: 2005-11-24.

All the assurance components required by the level EAL4+ (augmented with AVA_VLA.4, AVA_MSU.3, SOF high) have been assigned a “PASS” verdict. Consequently, the laboratory (CESTI /INTA) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the TEMD version 1.0 product on the integrated circuit for intelligent card SLE66CX322P, a positive resolution is proposed.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TOE Summary

The Target of Evaluation (TOE) is the Electronic Card of the Department of Defense (M.MAR TEMDv1.0), developed on the integrated circuit for smart card SLE66CX322P, manufactured by INFINEON TECHNOLOGIES AG, with an Operative System for smart card developed by Microelectrónica Española which use is focus on environments and applications with special security requirements. The TOE includes functionality for the generation of the Signature Creation Data, the creation of qualified electronic signatures, and to encipher data.

This integrated circuit belongs together with the version 'm1484b14 Release GDS-file-ID: m1484b14 with production line indicator: 2 (Dresden)' and it uses the libraries: RMS V1.3 AND RSA2048 V0.44. The operative system of the TOE includes code that will be stored in the EEPROM memory of the IC. This code is provided in the file INI_TEMD_V1_0.TST.

- CARDS TEMD V1.0 with INI_TEMD_V1_0.tst 140705, MicroElectrónica Española, S.A.

- M.MAR TEMD v1.0 SOFTWARE CD 19/01/05, MicroElectrónica Española, S.A.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfill EAL4, augmented with the components related to the vulnerability analysis required by CWA 14169, AVA_MSU.3 and AVA_VLA.4.

Assurance Class	**Assurance Component**
Configuration Management	ACM AUT.1, ACM CAP.4, ACM SCP.2
Delivery and Operation	ADO DEL.2, ADO IGS.1
Development	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
Guidance	AGD ADM.1, AGD USR.1
Life Cycle	ALC DVS.1, ALC LCD.1, ALC TAT.1
Tests	ATE COV.2, ATE FUN.1, ATE IND.2, ATE DPT.1
Vulnerability Analysis	AVA SOF.1, AVA VLA.4, AVA MSU.3

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Security Functional Requirements

The product security functionality satisfies, with the support from the environment, the CWA 14169: Secure Signature-Creation Devices "EAL4+" Level 3 14169:2002 E March 2002, protection profile. In addition, It also offers cipher services, which are covered by the appropriate security functional requirements.

The functional requirements satisfied by the product are:

Requirements expressed as of [CC_P2]:

- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key destruction
- FCS_COP.1 Cryptographic operation
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_ETC.1 Export of user data without security attributes
- FDP_ITC.1 Import of user data without security attributes
- FDP_RIP.1 Subset residual information protection
- FDP_SDI.2 Stored data integrity monitoring and action
- FDP_UIT.1 Data exchange integrity
- FIA_AFL.1 Authentication failure handling
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_MTD.1 Management of TSF data
- FMT_SMF.1 Specification of Management Functions
- FPT_AMT.1 Abstract machine testing
- FPT_FLS.1 Failure with preservation of secure state
- FPT_PHP.3 Resistance to physical attack
- FPT_TST.1 TSF testing
- FTP_ITC.1 Inter-TSF trusted channel
- FTP_TRP.1 Trusted path

Requirements augmented by [CWA14169]:

- FPT_EMSEC.1 TOE emissions

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Identification

Product: TARJETA ELECTRÓNICA PARA EL MINISTERIO DE DEFENSA (TEMD v1.0)

Security Target: 'Declaración de Seguridad TEMD v1.0', Versión 1.01.

PP claims: CWA 14169: Secure Signature-Creation Devices "EAL4+" Level 3 14169:2002 E March 2002.

Evaluation level: EAL4+ (AVA-MSU.3, AVA-VLA.4)

Strength of Function: High

Security Policy

The usage of the product TEMD 1.0 as crypto smartcard compliant with the secure signature creation device requirements implies to implement a series of organizational policies that assure the commitment of the different standards and demands of security.

The applicable organizational policies are distinguished to the usage of the product in their facet as crypto device and in the facet of signature device. The details about them are included in the Security Target. In synthesis, the necessity settles down to implement organizational policies relative to:

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

a) CRYPTO: (see security target)

P.CSD the TOE as secure crypto device

The TOE implements the CCD use to create ciphering (with asymmetrical or symmetrical key) under the sole control of the signatory.

P.Cipher Secure ciphering

The signatory uses the crypto system in order to cipher/decipher data implementing symmetric or asymmetric algorithms. The DTBC are presented to the signatory by the CCA. The ciphering is based on robust crypto algorithms generated by a SCCD.

b) SIGNATURE: (see PP CWA14169)

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 [DIRF], 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.

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 [DIRF] Annex 1) and is created by a SSCD.

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 Clarification of Scope

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

Usage assumptions

No specific usage assumptions have been declared .

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Environmental assumptions

They are built around the crypto facet and signature facet in a separate way:

a) CRYPTO: (see security target)

A.CCA Trustworthy cipher/decipher creation application

The signatory uses a trustworthy CCA . The CCA generates and sends the data to be ciphered/deciphered under the appropriate conditions in order to allow the TOE to work with them.

b) SIGNATURE: (see PP CWA14169)

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.

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.

Clarification of scope

The following treats are not exploitable for the TEMD 1.0 product, although the agents performing attacks have a high attack potential, and considering that the usage assumptions are true and implementing the security policies.

For any other treat not included in this list, there is no guarantee that the product can successfully resist to them.

Treats covered:

a) CRYPTO: (see security target)

T.Cipher_Divulg Crypto key disclosure

An attacker can get out and know the cipher key during the generation, storage or management of the key.

T.CCA_Deduce Deriving the cipher/decipher key

An attacker can derive the cipher/decipher key (symmetric or asymmetrical) just using the cipher processes executed previously.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

T.CCA_Misuse Misusing the cipher/decipher functions of the TOE

An attacker can misuse the cipher-decipher function of the TOE to create CDO that the signatory has not decided to cipher. The TOE is subject to deliberate attacks performed by experts with a high attack capability or potential, with an in deep knowledge of the principles and concepts of security implied by the TOE.

T.DTBC_Forgery Faking the DTBC

An attacker modifies the DTBC sent by the CCA. Thus, the DTBC used by the TOE to cipher are not the same as the DTBC that the signatory is believing to sign.

T.Key_Cipher_Forgery Faking the cipher keys

An attacker modifies the Cipher keys exported to the CCA. As a result the cipher key integrity is lost.

T.Cipher_Forgery Faking the ciphering

An attacker modifies the ciphered data and the integrity of them is not detected by the signatory or third people. The ciphering generated by the TOE are subject to deliberate attacks performed by experts with a high attack capability or potential, with an in deep knowledge of the principles and concepts of security implied by the TOE.

b) SIGNATURE: (see PP CWA14169)

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.

T.SCD_Divulg Storing, copying, and releasing of the signature-creation data

An attacker 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.

T.SCD_Derive Derive the signature-creation data

An attacker derives the SCD from public 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.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

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.

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.

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.

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.

Security functional requirements for the TOE environment

The product requires the cooperation from its operational environment to fulfill the CWA 14169: Secure Signature-Creation Devices "EAL4+" Level 3 14169:2002 E March 2002 protection profile.

The security functional requirements that must be fulfilled by the TOE environment are the following:

Certificate generation application (CGA)

- FCS_CKM.2 Cryptographic key distribution
- FCS_CKM.3 Cryptographic key access
- FTP_ITC.1 Inter-TSF trusted channel

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Signature creation application (SCA)

- FCS_COP.1 Cryptographic operation
- FTP_TRP.1 Trusted path

Ciphering application (CCA)

- FDP_UIT.1 Data exchange integrity
- FTP_ITC.1 Inter-TSF trusted channel

For further details on the security environment definition or on the security requirements, please refer to the Security Target of the TOE.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Architectural Information

The operating system of the TOE is constituted of several layers that manage specific aspects of the IC as shown by the figure 1.

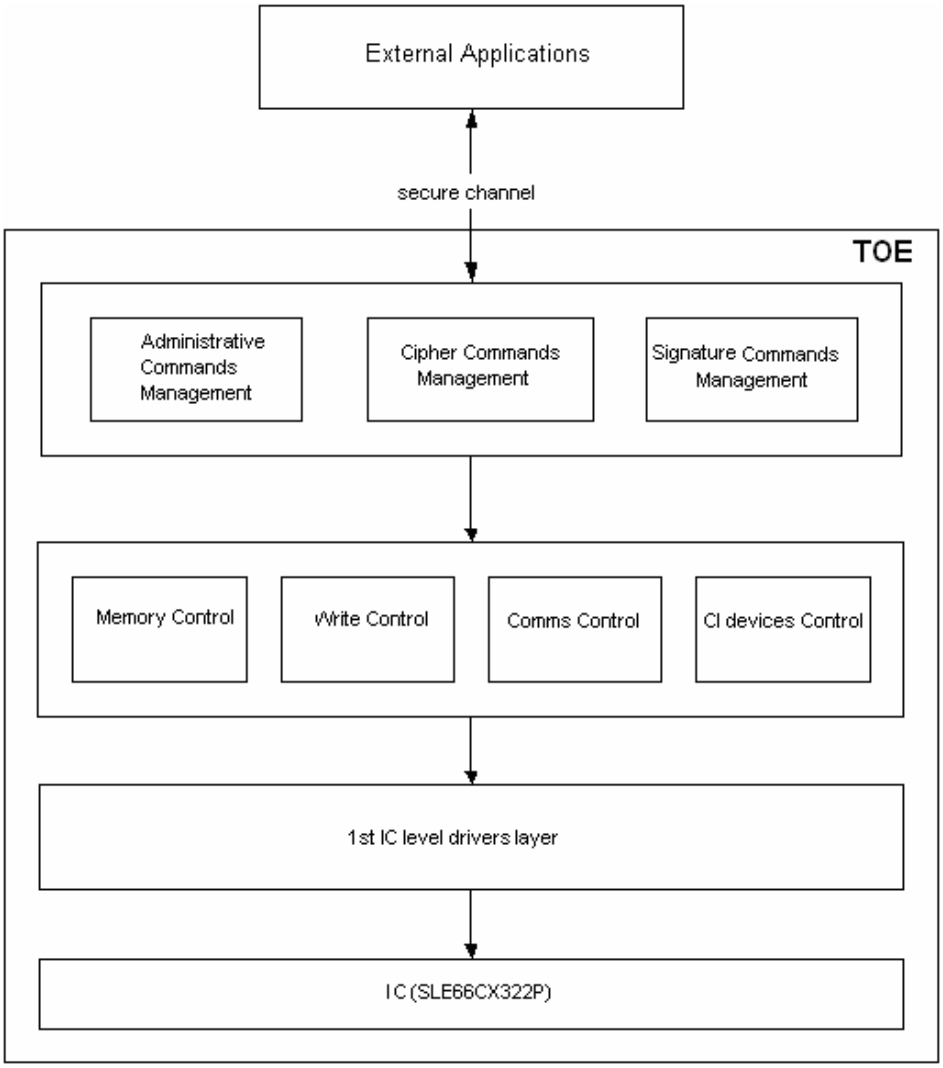

Figure 1. O.S. Layers

The first IC level drivers management layer is composed by functions that access directly with the IC creating an interface with the upper layers. These drivers control the following devices of the IC: ROM, EEPROM, RAM, MMU, RMS, PLL, TIMER, STS, Random Number Generator, DES Coprocessor y Advanced Crypto Engine.

The memory control manages the permanent memory including the structures related to the applications as file structures handled by the O.S.

The control of the writing operations manages all the actions to write that are executed on the permanent memory generating another interface that can be only

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

used by the upper layers or the layers located at the same level. The functions that create this interface are mainly based on in the driver that performs the writing into the EEPROM and RAM of the layer below.

The communications control manages the comm. protocol T=0 creating an interface of communication for the upper layers. The functions that create this interface are based on the drivers that control the UART in layer below.

The IC devices control generates the interface that is going to be used by the layers at the same level and upper, in order to do operations with specific devices of the IC as the RNG, the DES accelerator or the crypto processor. The functions that are created in this interface are based on the drivers of the level below.

Into the higher level layer it is possible to see:

- The management of the administrative commands, this is the layer that is related to the administrative aspects of the operative system.
- The management of the signature commands which main objective is to be a basis for the crypto operations of signing.
- The management of the cipher commands which main objective is to be a basis for the cipher-decipher operations of data.

Documentation

The product includes the documents listed below, and they have to be distributed and be available as a set for the user of the evaluated version.

- Infineon:

SLE66CX322P with RSA2048/m1484 Security Target 1.0.5 Infineon Technologies AG

Certification Report for Infineon Smart Card IC SLE66CX322P with RSA 2048 / m1484b14 BSIDSZ-CC-0223-2003 Bundesamt für Sicherheit in der Informationstechnik (BSI)

- MicroElectrónica Española, S.A.:

Declaración de Seguridad 1.01, 11/07/05	(security target)
Manual de Usuario 1.01, 11/07/05	(user manual)
Manual de Administrador 1.01, 11/07/05	(admin manual)
Distribución del Producto 1.0, 13/06/05	(product delivery)

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

IT Product Testing

The manufacturer has developed testing for each security function. All this tests have been performed by the manufacturer in their location and facilities with success.

The process has verified each unit test, checking that the security function that covers is been identified and also that the kind of test is appropriate to the security function that is intended to test.

All the tests have been developed using the same testing scenario, appropriate to the established architecture in the security target.

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

In order to verify the results of the manufacturer testing, the ITSEF has repeated these functional testing in the manufacturer facilities. Similarly, the ITSEF also has selected and repeated a 25% of the functional testing defined by the manufacturer, in the testing platform built by the ITSEF, selecting one test for each more relevant functional class: audit generation functions, crypto functions, user data protection functions.

In addition to this, the ITSEF has developed one test for each of the security functions of the product, verifying that the results that they get are consistent with the results that the manufacturer obtained.

It is been checked also that the results obtained in the tests correspond to the previously expected ones, and also that those cases where a deviation was observed in relationship to the expected result, that deviation is not a problem for the security of the product, and also they were not a decrease in the product functionality.

Evaluated Configuration

The TEMD product can be used in a variety of platforms and smartcard readers, which must comply with the security assumptions and requirements already stated. In particular, during the evaluation, PHOENIX and PC/SC readers, and other measurement devices and software has been used, but not configured as a trusted CGA. The identification of a particular environment that could be considered a trusted CGA, as defined by the PP CWA 14169, is out of the scope of this evaluation.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Results of the Evaluation

The product TEMD 1.0 on the integrated circuit for intelligent card SLE66CX322P has been evaluated in front of the “Security Target TEMD 1.0”, dated 11/07/05 and version 1.01.

All the assurance components required by the level EAL4+ (augmented with AVA_VLA.4, AVA_MSU.3, SOF high) present the verdict “PASS”. Consequently, the laboratory (CESTI /INTA) assigns the VERDICT “PASS” to the whole evaluation due all the evaluator actions are satisfied for the EAL4 methodology, as define by the third part of the Common Criteria.

Evaluator Comments/Recommendations

For a secure usage of the TOE, the EAU parameter, required for the establishment of a secure communication channel, and set by the administrator during the application creation phase, must only be known by the proper administrator and end users. The EAU must be provided maintaining its confidentiality. The administrator must not choose simple values for this parameter.

For a secure usage of the TOE, it is recommended to store imported data so that their confidentiality is kept, for example using ciphering mechanisms.

For a secure usage of the TOE, it is recommended to store all the confidential data within applications that require mutual authentication and ciphering, to avoid unauthorized users to have access to proprietary data.

For a secure usage of the TOE, it is recommended that applications be created requiring secure communication channels.

For a secure usage of the TOE, it is recommended to transmit the PIN always through a secured channel, thus avoiding the capture of its value.

For a secure usage of the TOE, it is recommended that the private key be marked as non exportable, for the Ciphering Application.
For a secure usage of the TOE, it is recommended that the user checks, on reception of the TOE, that the card is in life cycle phase 3, by issuing the command "Get data" 00 CA 02 00 01, and the proper response should be 03 90 00.

For a secure usage of the TOE, it is recommended that keys be stored protected by PIN.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the TEMD version 1.0 product on the integrated circuit for intelligent card SLE66CX322P, a positive resolution is proposed.

Glossary

APDU - Application Protocol Data Unit
CCA - Cipher Creation Application
CGA - Certificate Generation Application
DTBS - Data To Be Signed
EAL - Evaluation assurance level
IC - Integrated Circuit
SCA - Signature Creation Application
SCD - Signature Creation Device
SSCD - Secure Signature Creation Device
SVD - Signature Verification Data

Bibliography

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

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 2.2, rev 256, January 2004.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, rev 256, January 2004.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, rev 256, January 2004.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.2, rev 256, January 2004.

[AIS-34] AIS-34, Evaluation Methodology for CC Assurance classes for EAL5+ v1.0 1-june-2004 BSI

[CWA14169] Annex C CWA 14169:2002. Protection Profile – Secure Signature-Creation Device, Type 3, version 1.05.

Security Target

It is published jointly with this certification report the security target, “Declaración de Seguridad TEMD 1.0”, version 1.01, dated 11/07/05.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es