Certification Report

EAL 4+ (AVA_VAN.5) Evaluation of

ID&Trust Ltd.
HTCNS Applet v1.03

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.01/TSE-CCCS-29

TABLE OF CONTENTS

Document Information

Date of Issue	14.07.2015
Version of Report	1.1
Author	İbrahim Halil KIRMIZI
Technical Responsible	Zümrüt MÜFTÜOĞLU
Approved	Mariye UMAY AKKAYA
Date Approved	20.07.2015
Certification Report Number	21.0.01/15-038
Developer	ID&Trust Ltd.
Sponsor	TUV Rheinland InterCert Kft.
Evaluation Lab	TÜBİTAK BİLGEM OKTEM
TOE	ID&Trust CNS Card: NXP JCOP 2.4.2 R3 Smart Card with ID&Trust HTCNS v1.03
Pages	21

Document Change Log

Release	***Page***	***Pages Affected***	***Remarks/Change Reference***
V1.0	21	All	First Released
V1.1	23	All	Company Name Changed

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the STCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for HTCNS Applet v1.03 whose evaluation was completed on 07.07.2015 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 36 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the STCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org/

1 – EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: HTCNS Applet
IT Product version: v1.03
Developer's Name: ID&Trust Ltd.
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL4+ (AVA_VAN.5)
Completion date of evaluation: 07.07.2015 (DTR 34 TR 03)

1.1 Brief Description

The TOE is the Smart Card Integrated Circuit with Embedded Software serving as an SSCD (Secure Signature Creation Device) in accordance to its functional specification. The smart card chip module can be embedded in a plastic card or other device (ex. An USB token) providing a physical interface between the terminal and the chip. The TOE consists of;

- Integrated Circuit (Smart Card Platform),
  - o NXP Secure Smart Card Controllers 5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)
    - - Evaluation Level for the Smart Card Controller: EAL 5 augmented by ASE_TSS.2, AVA_VAN.5 and ALC_DVS.2, claiming conformance to the Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-CC-PP-0035-2007. Certification number: BSI-DSZ-CC-0857
  - o Crypto Library V2.7/V2.9 on SmartMX P5CD016/021/041/051 and P5Cx081 V1A/ V1A(s)

    - Evaluation Level for the hardware Platform including the cryptographic library: CC EAL 5+ augmented with ALC_DVS.2 and AVA_VAN.5, claiming conformance to the Protection Profile “Bundesamt für Sicherheit in der Informationstechnik (BSI): Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035”. Certification number: BSI-DSZ-CC-0633-2010

- Embedded Software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager) and Native MIFARE application,
    - OS Name: JCOP 2.4.2 R3
    - Product Identification: J3E081_M64, J3E081_M66 and J2E081_M64
    - Evaluation Level CC EAL 5+ with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 according to Java Card System – Open Configuration Protection Profile, version 2.6, certified by ANSSI, 19.04.2010. Certification number: C13-37761
- Secure Signature Creation Device applet, accomplishing the SSCD application and other applications
    - o Applet Name: HTCNS
    - o Applet Version: 1.03
- Secure Signature Creation Device application

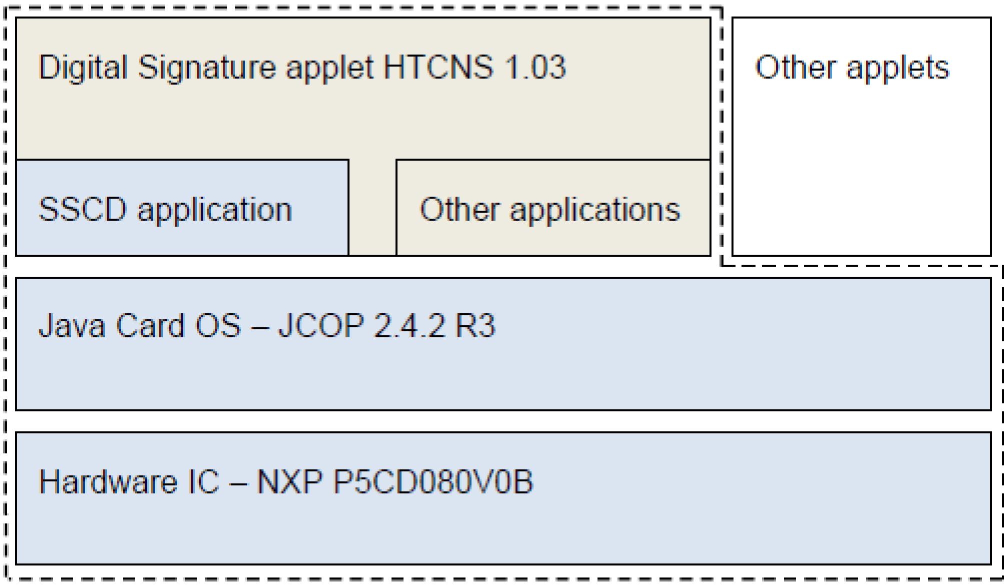
Digital Signature applet HTCNS 1.03
SSCD application
Other applications
Other applets
Java Card OS – JCOP 2.4.2 R3
Hardware IC – NXP P5CD080V0B

Figure 1 – TOE Boundaries

The applet provides the following services:

- a highly secure and configurable framework to store sensitive and user data, based on ISO/IEC 7816-4, ISO/IEC 7816-8 and ISO/IEC 7816-9,
- trusted channel, based on CNS specification,
- dynamic management of access control rules,
- onboard RSA key pair generation (up to 2048 bits), compliant with ISO/IEC 7816-8,
- all mandatory card services defined by CNS specification,
- command interface is compliant with ISO/IEC 7816-4, and CNS specification,
- symmetric device authentication based on CNS specification,
- asymmetric device authentication based on CNS,
- Card Holder verification based on PIN authentication,
- RSA digital signature, compliant with ISO/IEC 7816-8

1.2 TOE Security Functions

TOE Security functions are;

- **TSF.AccessControl** provides the access controls to data in the file system, initialization, personalization and pre-personalization data. During earlier life phases, when the applet may not be present yet, the Platform TSFs, SF.AccessControl and SF.I&A are responsible for managing the accesses correctly. It allows the maintenance of Signatory and Administrator users, and they access rights depending on the identification and authentication.
- **TSF.IdentificationandAuthentication** manages the identification and authentication of the Signatory and Administrator and enforces role separation. It has two parts, Administrator and User Authentication;
    - Administrator Authentication: the Manufacturer and Personalization Agent are identified through the relevant access rights during the initialization and personalization of the TOE. During these phases the storage area affected is a write-only-once area, and the access right is granted to the Manufacturer and Personalization Agent, while the applet may not be present yet, the Platform TSFs, SF.AccessControl and SF.I&A are responsible for managing the accesses correctly. The management of data in the write-only-once storage area is based on the Platform security functionality SF.SecureManagement. The audit functions are provided by the Platform security function SF.Audit. Access during operational phase is only read-only.
    - The User authentication part provides authentication of the users during Operational Phase

- **TSF.TrustedChannel** is responsible for the command and response exchanges between the TOE and the external devices. Various data and processes such as DTBSs, signatures, public keys, identification and authentication data, SVD Transfer or other user data are embedded in command and response frames. The TSF. TrustedChannel function is capable of providing a secure communication channel between legitimate end points both of the TOE and the external device. The secure communication channels are supported with cryptographic functions and provide assured identification of its end points and protection of the channel data from modification or disclosure. This function is responsible for confidentiality, data integrity and data authenticity
- **TSF.Crypto** is responsible for providing cryptographic support to all the other Security Functions including secure key generation, secure random generator, and data hashing. The TSF makes use of the Platform TSF SF.CryptoKey
- **TSF.Platform** contains functionalities based on the security functionalities of the certified cryptographic library and the certified IC platform, not mentioned in the other security functions. This Security Function is responsible for protection of the TSF data, user data, and TSF functionality. The TSF.Platform function is composed of software implementations of test and security functions. The platform provides the following security functions;
  - SF.AccessControl – enforces the Access Control
  - SF.Audit – Audit functionality
  - SF.CryptoKey – Cryptographic key management
  - SF.CryptoOperation – Cryptographic operation
  - SF.I&A – Identification and authentication
  - SF.SecureManagement – Secure management of TOE resources
  - SF.PIN – PIN management
  - SF.LoadIntegrity – Package integrity check
  - SF.Transaction – Transaction management
  - SF.Hardware – TSF of the underlying IC
  - SF.CryptoLib – TSF of the crypto library

1.3 Threats

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

An attacker stores or copies the SCD outside the TOE. An attacker can obtain 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 publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

- **T.Hack_Phys** – Physical attacks through the TOE interfaces

  An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

- **T.SVD_Forgery** – Forgery of the signature verification data

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

- **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

- **T.DTBS_Forgery –** Forgery of the DTBS/R

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

- **T.Sig_Forgery –** Forgery of the electronic signature

  An attacker forges a signed data object, maybe using an electronic signature which has been 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 created 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

2 – CERTIFICATION RESULTS

2.1 Identification of TOE

The TOE is Secure Signature Creation Device (SSCD) for the generation of signature-creation data (SCD) and the creation of qualified electronic signatures. It fulfils requirements of directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a community framework for electronic signatures. The Security Target refers to the SSCD compliant configurations of the HTCNS applet. The HTCNS applet is a Java Card Application used exclusively on the NXP JCOP 2.4.2. R3 Platform, which is a CC EAL5+ certified product.

The TOE comprises:

- JCOP 2.4.2 R3 (J3E081_M64, J3E081_M66, J2E081_M64 Secure Smart Card Controller Revision 3) Underlying Platform of the TOE, which is evaluated by Brightsight and certified by TÜV Rheinland Nederland b.V. at assurance level EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 under the certificate number C13-37761
  It consists of:
    - Smart Card Platform (SCP), which consists of:
        - Hardware Abstraction Layer with the Crypto Library,
        - Hardware Platform
    - Embedded software (Java Card Virtual Machine, Runtime Environment, Java Card API, Card Manager)
    - Native MIFARE application
- The Application Part of the TOE:
  HTCNS Applet version 1.03
- HTCNS Admin Guide v1.03.11
- HTCNS User Guide v1.03.13

Certificate Number	21.0.01/TSE-CCCS-29
TOE Name and Version	ID&Trust CNS Card: NXP JCOP 2.4.2 R3 Smart Card with HTCNS v1.03
Security Target Title	Security Target for ID&Trust SSCD Application
Security Target Version	0.37
Security Target Date	02.06.2015
Assurance Level	EAL4+ (AVA_VAN.5)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	Protection Profile for Secure signature creation device – Part 2: Device with key generation, BSI-CC-PP-0059 version 2.01

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012, conformant
Sponsor	TUV Rheinland InterCert Kft.
Developer	ID&Trust Ltd.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE-CCCS

2.2 Security Policy

The Security Target for the TOE claims strict conformance to the Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation, BSI-CC-PP-0059 version 2.01

Organizational Security Policies are;

- **P.CSP_Qcert –** Qualified certificate

  The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. [7], article 2, clause 9, Annex I) for the SVD generated by the SSCD. The certificates contain at least 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 as SSCD 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 an advanced electronic signature (cf. [7], article 1, clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate ([7] Annex I). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable

- **P.Sigy_SSCD** – TOE as secure signature creation device
  The TOE meets the requirements for an SSCD laid down in Annex III of [7]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once

- **P.Sig_Non-Repud** – Non-repudiation of signatures
  The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.CGA –** Trustworthy certification generation application
  The CGA protects the authenticity of the signatory’s name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP

- **A.SCA –** Trustworthy signature creation application
  The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE

  There is one more Assumption not in defined in the PP, justified by the fact that one part of TOE is platform and is developed by NXP at the NXP sites, which are already certified at the EAL5+ assurance level.

- **A.Sec_Manufac –** Protection during ROM-coding, Packaging and JCOP Personalization

It is assumed that security procedures are used correctly by the TOE Manufacturer up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use)

2.4 Architectural Information

The TOE is the ID&Trust CNS Card 1.03: NXP JCOP 2.4.2 R3 Smart Card with HTCNS Applet Version 1.03. The JCOP 2.4.2 R3 is the Platform, which already has a valid Certification, EAL5+.

The Card Manager contains in itself a Security Domain, which is the Issuer Security Domain [8], the Issuer Security Domain (ISD), as the mandatory on-card representative of the Card Issuer, has the capability of loading, installing, and deleting applications that belong either to the Card Issuer or to other Application Providers.

Because of the JCOP 2.4.2 R3 Java Card firewall, on the ID&Trust CNS card, other Applets can be loaded too, this is allowed according to the JCOP 2.4.2 R3 certification. The Secure Box technology allows to run none certified third party native code and ensures that this code cannot harm, influence or manipulate the JCOP 2.4.2 R3 operating system or any of the applets executed by the operating system. The separation of the native code in the Secure Box from other code and/or data residing on the hardware is ensured by the Hardware Memory management unit which has been certified in the hardware evaluation.

The Application layer is a System. To this System, one or more Applet(s) can be Loaded, Selected and Configured. In this case, where the TOE meets the requirements of Common Criteria Certification, there is only one Applet which is Loaded, Selected and Configured and this is HTCNS Applet Version 1.03.

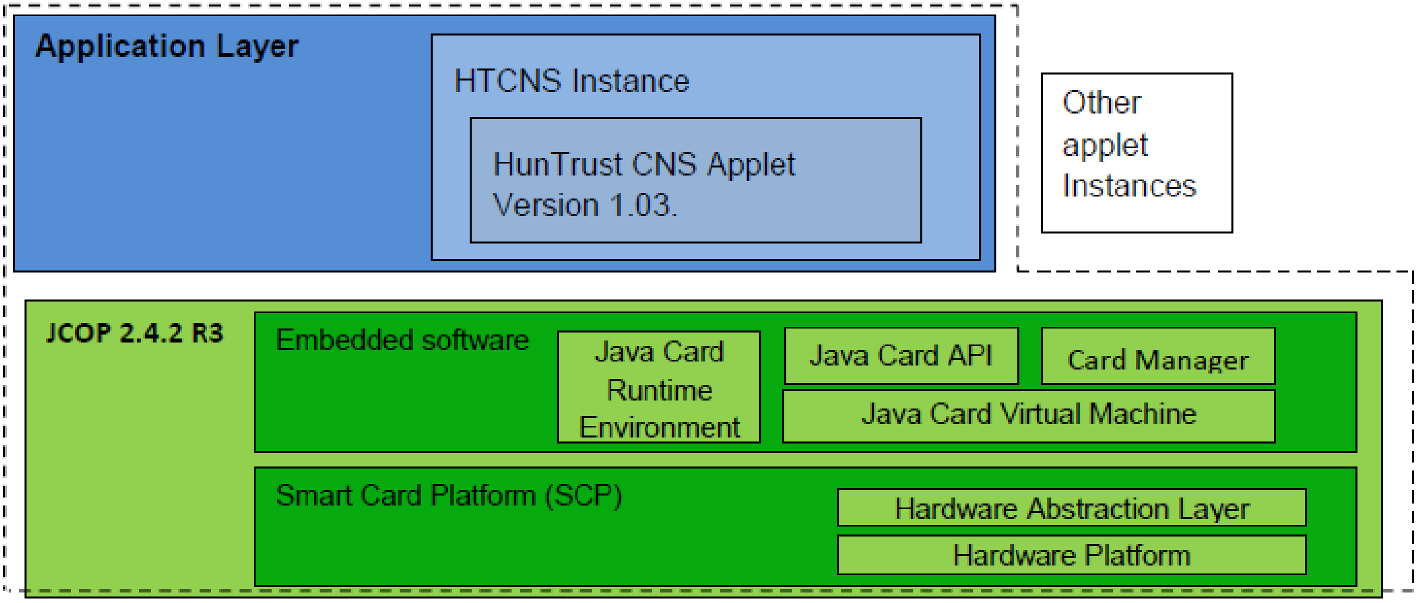
Application Layer
HTCNS Instance
HunTrust CNS Applet Version 1.03.
Other applet Instances
JCOP 2.4.2 R3
Embedded software
Java Card Runtime Environment
Java Card API
Card Manager
Java Card Virtual Machine
Smart Card Platform (SCP)
Hardware Abstraction Layer
Hardware Platform

Figure 2 – The TOE and its subsystems

This Subsystems behaviour and interactions can be easily reviewed. The Platform Subsystem provides the environment and operating system for the Application layer, and even some functions, which are at operating-system level. The Applet uses the resources of the Platform, and provides additional functionality.

2.5 Documentation

During the evaluation; the configuration of evaluation evidences which are composed of Software source code, Common Criteria related documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Publication Date
Security Target for ID&Trust SSCD Application	0.37	02.06.2015
HTCNS Applet Administrator’s Guide	1.03	July 2015
HTCNS Applet User’s Guide	1.03	July 2015
HTCNS Applet Initialization and Configuration	1.03	July 2015
Profile FileSystemCNS_21112005_with_DS	1.02	

Table 1 – Evaluation Evidences

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of ID&Trust HTCNS Applet v1.03

It is concluded that the TOE supports EAL 4+ (AVA_VAN.5). There are 24 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

2.6.1 Developer Testing:

- TOE Test Coverage: Developer has prepared TOE System Test Document according to the TOE Functional Specification documentation.
- TOE Test Depth: Developer has prepared TOE System Test Document according to the TOE Design documentation which include TSF subsystems and its interactions.
- TOE Functional Testing: Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2.6.2 Evaluator Testing:

The tests were performed with the composite smart card product NXP JCOP 2.4.2 R3 Smart Card with HTCNS Applet Version 1.03.

- Independent Testing: Evaluator has done a total of 26 sample independent tests. 9 of them are selected from developer`s test plans. The other 17 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- Penetration Testing: Evaluator has done 3 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "TOE Security Functions Penetration Tests Scope" which is in Annex-D of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

During the evaluation; the configuration of evaluation evidences which are composed of Software source code, Common Criteria related documents, sustenance documents and guides are shown below;

Name of Document	Version Number	Publication Date
Security Target for ID&Trust SSCD Application	0.37	02.06.2015
HTD02 Security Architecture Description	0.10	17.06.2015
HTD03 The Functional Specification CNS	0.12	06.07.2015
HTD04 The TOE Design CNS	0.13	07.06.2015
HTD06 Configuration Management Documentation CNS	0.6	06.07.2015
HTD07 Configuration List CNS	0.4	06.07.2015
HTD08 The Delivery Documentation CNS	0.6	06.07.2015
HTD09 Development Security Document CNS	0.5	06.07.2015
HTD10 Life-Cycle Definition Documentation CNS	0.6	06.07.2015
HTD11 Development Tool Documentation CNS	0.8	06.07.2015
HTD13-14 Analysis of Test Coverage and Depth CNS	0.5	
HTD15 Test Documentation	0.8	06.07.2015
HTCNS Admin Guide	1.03.11	July 2015

HTCNS User Guide	1.03.13	July 2015
HTCNS Initialization and Configuration for SSCD	1.03.10	July 2015
CNS Applicative Test Specification CNS Test Suite	1.04.4	
CNS Standard File System Test Specification CNS Test Suite	1.02.2	
CNS Evaluation Test Specification CNS Test Suite	1.03.5	

Table 2 – Documentation

2.8 Results of the Evaluation

Table 2 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with AVA_VAN.5

Assurance Class	Component	Component Title
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
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
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
	ALC_TAT.1	Well-defined Development Tools
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
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.5	Advanced Methodological Vulnerability Analysis

Table 2 – Security Assurance Requirements of TOE

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE “HTCNS Applet v1.03” the results of the assessment of all evaluation tasks are “Pass”.

The result of AVA_VAN.5 evaluation is given below:
It is determined that TOE, in its operational environment, is resistant to an attacker possessing **“High”** attack potential.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “HTCNS Applet v1.03” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: ID&Trust Security Target for Secure Signature Creation Device

Version: 0.37

Date of Document: 02.06.2015

A public version has been created and verified according to ST-Santizing:

Title: ID&Trust HTCNS Security Target Lite for Secure Signature Creation Device

Version: 1.0

Date of Document: 29.04.2015

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory (OKTEM)

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

EAL : Evaluation Assurance Level

GR : Observation Report

OKTEM : Ortak Kriterler Test Merkezi

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

SSCD: Secure Signature Creation Device

ST : Security Target

STCD :Software Test and Certification Department

TOE : Target of Evaluation

TSF : TOE Secrity Functionality

TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] CC Supporting Document Guidance, Mandatory Technical Document Composife Product Evaluation for Smart Cards and Similar Devices,April,2012,CCDB-2012-04-001

[4] YTBD-01-01-TL-01 Certification Report Preparation Instructions, Rel.Date: July,30,2013

[5] CC Supporting Document Guidance, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.9 , May 2013, CCDB-2013-05-002

[6] CC Supporting Document Guidance, Mandatory Technical Document, The Application of CC to Integrated Circuits, Version 3.0 Revision 1, March 2009, CCDB-2009-03-002

[7] DIRECTIVE 1999/93/EC OF EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[8] GlobalPlatform Card Specification v2.2, March 2006

6 ANNEXES

There is no additional information which is inappropriate for reference in other sections