Certification Report

EAL 5+ (AVA_VAN.5) Evaluation of

TUBITAK BILGEM UEKAE YITAL

NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

TABLE OF CONTENTS

Table of contents **..............** ***2***
Document Information **..............** ***3***
Document Change Log **..............** ***3***
DISCLAIMER **..............** ***3***
FOREWORD **..............** ***4***
RECOGNITION OF THE CERTIFICATE **..............** ***5***
1 EXECUTIVE SUMMARY **..............** ***6***
2 CERTIFICATION RESULTS **..............** ***9***
2.1 Identification of Target of Evaluation **..............** ***9***
2.2 Security Policy **..............** ***10***
2.3 Assumptions and Clarification of Scope **..............** ***11***
2.4 Architectural Information **..............** ***14***
2.5 Documentation **..............** ***16***
2.6 IT Product Testing **..............** ***17***
2.7 Evaluated Configuration **..............** ***17***
2.8 Results of the Evaluation **..............** ***20***
2.9 Evaluator Comments / Recommendations **..............** ***22***
3 SECURITY TARGET **..............** ***22***
4 GLOSSARY **..............** ***22***
5 BIBLIOGRAPHY **..............** ***23***
6 ANNEXES **..............** ***24***

Document Information

Date of Issue	***03.09.2013***
Version of Report	***1.1***
Author	***Mehmet Kürşad ÜNAL&Zümrüt MÜFTÜOĞLU***
Technical Responsible	***Mustafa YILMAZ***
Approved	***Mariye Umay AKKAYA***
Date Approved	***05.09.2013***
Certification Report Number	***21.0.01/13-029***
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE YİTAL***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE	***NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE***
Pages	***24***

Document Change Log

Release	***Date***	***Pages Affected***	***Remarks/Change Reference***
V1.0	***02.09.2013***	***All***	***Initial***
V1.1	***03.09.2013***	***All***	***Final***

DISCLAIMER

This certification report and the IT product/PP 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 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3 This certification report and the associated Common Criteria document apply only to the identified version and release of the product/PP 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/PP 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 NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE whose evaluation was completed on 03.09.2013 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM *(as CCTL), and with the Security Target document with version no 06 (08.07.2013) 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

Description of TOE

TOE is a contact-based smartcard IC which is designed for security-based applications. TOE also includes IC Dedicated Software and DES-3DES v7.0, AES256 v7.0, RSA2048 v7.0 libraries. TOE is designed by Semiconductor Technology Research Laboratory (YİTAL) division under National Research Institute of Electronics and Cryptology (UEKAE) of TUBITAK-BILGEM and fabricated with HHNEC's 0.25µm eFlash technology process. It is aimed that this smartcard IC is utilised as Turkish national ID Card and national Health Card where secrecy and security is an issue.

National Smartcard IC, UKTÜM-H v7.0 consists of an 8052-type microprocessor with a 256 Byte internal memory, a 10K Test ROM, three 64K Flash memory, an 8K Static RAM, and a True

Random Number Generator. Furthermore, it is equipped with the hardware implementations of the RSA2048 , the DES-3DES and the AES ciphering algorithms.

An UKTÜM-H product can have three different flash memory usage configurations as follows: In the first configuration, user can load operating system into one 64K flash memory, and other two flash memories are used as user data area. In the second configuration, user can load operating system into two 64K flash memory, and he/she can use other one as user data area. In the third configuration, the user can use flash memories such as in the second configuration. The difference between second and third configuration is that the operating system loader software adds CheckSum values of operating system loaded to an 64K flash memory to the other 64K flash memory and vice versa. The entire configuration is done during the manufacturing and testing process of the TOE according to the choice of the user. All differences between the products of this TOE are realized by means of blocking without changing the hardware. Therefore, all products of this TOE are equal from hardware perspective. The flash memory usage configuration is done by setting the according value in the chip configuration page, which is not available to the user.

The Test ROM stores the IC Dedicated Software used to support testing of the TOE during production. The IC Dedicated Software also includes flash loader for downloading user software to NVM. The TOE includes hardware of UKTÜM-H v7.0 Smartcard IC, IC Dedicated Software, Flash memory access and user libraries of the DES-3DES, AES and RSA algorithms, and related documentation. The user or/and a subcontractor can download software to flash memory blocks.

UKTÜM-H v7.0 communicates with the outer environment through a smartcard reader in accordance with ISO/IEC 7816-3 protocol. Smartcard IC is designed to be resistant against power and fault attacks. In addition, it is equipped with security sensors which sense physical attacks and environmental operating conditions.

The smartcard IC UKTÜM-H v7.0 is developed in order to be used as national ID card. It aims to ensure EAL 5+ assurance level of CC and to be a national choice for smart card ICs on the market in terms of functionality, performance and security measures.

TOE Security Functions

Guarantee of Correct Operation

The TOE which can only be operated correctly under the specified conditions is equipped with different type of sensors monitoring the operating parameters to detect if the specified operating conditions are fulfiled. For this purpose, TOE includes temperature sensors, supply voltage sensor and external clock frequency sensor. If one of these sensors raises an alarm due to a violation in the operating conditions, than the circuit enters to reset state. Exposing the TOE to extreme operating conditions may be used by an attacker to modify TOE's behaviour to force information leakage or to affect the TOE to produce cryptographically bad random numbers. The presence of security sensors prevents such attacks.

These functions satisfy FPT_FLS.1 "Failure with Preservation of Secure State" requirement.

On the other hand, when these sensors do not raise any alarm, the TOE functions properly, thus, FRU_FLT.2 "Limited Fault Tolerance" requirement is satisfied.

Phase Management

During the chip development and production phases of the life cycle (Phase 2,3,4), the TOE is always in Test Mode enabling the operation of the IC Dedicated Software which is used to perform the die tests and to inject pre-personalisation data to the correctly working chips. After TOE delivery (Phase 5-7), the TOE is in User Mode where IC Dedicated Software is irreversibly disabled and the operation of the Smartcard Embedded Software is made available.

During start-up of the circuit, IC Dedicated Software decides whether it is in the User Mode or the Test Mode by checking some phase management flags. If it is in Test Mode, the TOE requests authentication before doing any other operation. Thus FMT.LIM.1 and FMT.LIM.2 requirements are satisfied.

Both in Test Mode and User Mode, the chip identification data and pre-personalisation data can be accessible satisfying FAU_SAS.1

Physical Protection Againts Physical Probing and Manipulation

There exist different measures to protect the design of the TOE and the user data stored in the TOE when the TOE is in operation and also when the power is not applied to the TOE. An active shield formed by the metal lines with active signals protects the entire surface of the TOE against physical attacks. Since physical attacks over the surface need to modify the active shield lines, the detection of opened or shortened lines will notify a physical attack causing the circuit to enter to reset state.

The entire surface of the TOE is covered by metal lines with active signals in order to prevent the attacker from probing and acquiring any useful data.

The layout of the logic circuit including the microprocessor core is effectively randomised making it difficult to determine specific functional areas for reverse engineering.

The microprocessor in UKTÜM-H v7.0 is designed in a unique and non standard way. Therefore, reverse engineering works need much more effort.

In the TOE, the data and address busses between microprocessor and the DES, the AES and the RSA blocks are encrypted against probing.

In the TOE, the data is encrypted in the SRAM and in the Flash memory. Thus, there are no plain data on the busses between microprocessor and memories.

In the TOE, the data and address busses are encrypted in the NVM where the operating system is embedded. Thus, the data and address busses are encrypted between NVM and the microprocessor.

Even if the attacker reads the content of the NVM by reverse engineering, since the data is encrypted, the attacker does not obtain any useful data about the microprocessors software.

The internal memory of the microprocessor and the external SRAM block are equipped with check bits to prevent the attacks aiming to modify memory contents.

The critical registers of the TOE are dual implemented againts manipulation attacks When a manipulation attack is detected, the chip enters reset state.

All these measures prevent forced information leakage which may be realised by physically manipulating and probing the critical lines of the TOE . The confidentiality of the random numbers provided by the TOE is also ensured by these measures preventing probing and manipulation.

These measures satisfy the security functional requirement of FPT_PHP.3, “Resistance to physical attack”.

The TOE will enter to reset state for any data read from internal RAM or SRAM with unmatched check bits satisfying FDP_SDI.2. The TOE is equipped with CRC hardware that the Security IC Embedded Software may use to calculate the total or partial cheksums of ROM and Flash Memory to control the stored data.

Logical Protection Against Data Leakage

In order to protect TOE against data analysis on stored and internally transferred data, the data is encrypted on chip before it is written in the SRAM and flash memories.

The use of encryption in the communication between the DES, the AES, the RSA blocks and the microprocessor prevents the interpretation of the leaked data. Random data is inserted into the data and address busses on the same purpose.

All these measures are implemented to prevent an attacker to be successful by measuring and analysing emanations, power consumption and other outputs produced by the TOE.

The hardware implementation of the DES, the AES and the RSA algorithms are implemented to be resistant against side channel attacks. This prevents the secure data leakage.

These security functions of the TOE cover the FDP_ITT.1 “Basic Internal Transfer Protection” and FTP_ITT.1 “Basic Internal TSF Data Transfer Protection”. The encryption covers the “Data Processing Policy” and FDP_IFC.1 “Subset Information Flow Control”.

Random Number Generation

The UKTÜM-H v7.0 is equipped with a physical random number generator which generates truly random numbers. The generated random numbers can be used by the operating system software and also by TOE’s security enforcing functions. The TOE has the capability to subject the generated numbers to the monobit, poker, runs, long run and auto correlation tests defined in FIBS-140-2. The covered security functional requirement is FCS_RND.1.

TSF Self-Test
The TOE has the hardware supports making available the test of its security enforcing functions SEF1, SEF5, SEF7 and partially SEF3 by the operating system software. Since TSF self-test will detect the attempts to modify sensor devices, random number generator, active shield and DES, AES, RSA cryptographic operations the covered security functional requirement is FPT_TST.2.

Cryptographic Support
The TOE is equipped with the hardware implementations of the DES/DES3, AES256, RSA1024 and RSA2048 cryptographic functions. The covered security functional requirement is FCS_COP.1.
The TOE shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [stated as in 'TCKK Akıllı Kartlarında RSA İmzalama Anahtar Çifti Üretimi', TKRD-501-11-TA-TR01, 23 Ocak 2012,BİLGEM-UEKAE] and specified cryptographic key sizes of [2048 bit] that meet [FIPS 186-3, 2009 June]. The covered security functional requirement is FCS_CKM.1/RSA.

The detailed information about thereats can be found in the Security Target v07, part 3.1.1

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Project Identifier	*21.0.01/TSE-CCCS-017*
TOE Name and Version	*NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE*
Security Target Title	*NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE Security Target*
Security Target Version	*06*
Security Target Date	*08.07.2013*
Assurance Level	*EAL 5+ (AVA_VAN.5)*
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, September 2012 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components,Version 3.1, Revision 3, September 2012

Methodology	- Common Criteria for Information Technology Security Evaluation, Evaluation Methodology Version 3.1 Revision 3, September 2012
Protection Profile Conformance	***None***
Common Criteria Conformance	- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3, July 2009. - Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 3, July 2009,extended. - Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 3, July 2009,conformant.
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE YİTAL***
Evaluation Facility	***TÜBİTAK BİLGEM OKTEM***
Certification Scheme	***TSE-CCCS***

2.2 Security Policy

Organisational Security Policies

P. Process-TOE: Protection during TOE Development and Production

The TOE Manufacturer must ensure that the development and production of the Smartcard Integrated Circuit (Phase 2 - 4) is secure so that no information is unintentionally made available for the operational phase of the TOE. For example, the confidentiality and integrity of design information and test data shall be guaranteed; access to samples, development tools and other material shall be restricted to authorised persons only; scrap will be destroyed etc. This not only pertains to the TOE but also to all information and material exchanged with the developer of the Smartcard Embedded Software and therefore especially to the Smartcard Embedded Software itself.

This includes the delivery (exchange) procedures for Phase 1 and the Phases after TOE Delivery as far as they can be controlled by the TOE Manufacturer.

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this unique identification. The accurate identification is introduced at the end of the production test in phase 3. Therefore the production environment must support this unique identification.

P. Add-Functions: Additional Specific Security Functionality

The TOE shall provide the following specific security functionality to the Smartcard Embedded Software:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES256)
- Rivest-Shamir-Adleman (RSA1024, RSA2048)
- Cryptographic Key Generation or RSA2048 algorithm

2.3 Assumptions and Clarification of Scope

	ASSUMPTION	BRIEF DESCRIPTION
1.	**A.Process-Sec-IC**	Security procedures are used after delivery of the TOE 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 unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately.
2.	**A.Plat-Appl**	The Security IC Embedded Software is designed so that the requirements from the following documents are met: • UKTÜM-H v7.0 Security Requirements for Operating System • Findings of the TOE evaluation reports relevant for the Security IC Embedded Software as referenced in the certification report. Since particular requirements for the Security IC Embedded Software are not clear before considering a specific attack scenario during vulnerability analysis of the Security IC (AVA_VAN), a summary of such results is provided in the document "ETR for composite evaluation" (ETR-COMP). This document can be provided for the evaluation of the composite product. The ETR-COMP may also include guidance for additional tests being required for the combination of hardware and software. The TOE evaluation must be completed before evaluation of the Security IC Embedded Software can be completed. The TOE evaluation can be conducted before and independent from the evaluation of the Security IC Embedded Software.
3.	**A.Resp-Appl**	All User Data are owned by Security IC Embedded

		Software. Therefore, it must be assumed that security relevant User Data (especially cryptographic keys) are treated by the Security IC Embedded Software as defined for its specific application context. The application context specifies how the User Data shall be handled and protected. The Security IC can not prevent any compromise or modification of User Data by malicious Security IC Embedded Software. The assumption A.Resp-Appl ensures that the Security IC Embedded Software follows the security rules of the application context. When defining the Protection Profile or Security Target for the evaluation of the Security IC Embedded Software appropriate threats must be defined which depend on the application context. These security needs are condensed in this assumption (A.Resp-Appl) which is very general since the application context is not known and the evaluation of the Security IC Embedded Software is not covered by this Security Target.
4.	**A.Key-Function**	Key-dependent functions (if any) shall be implemented in the Smartcard Embedded Software in a way that they are not susceptible to leakage attacks (as described under T.Leak-Inherent and T.Leak-Forced). Note that here the routines which may compromise keys when being executed are part of the Smartcard Embedded Software. In contrast to this the

		threats T.Leak-Inherent and T.Leak-Forced address • The cryptographic routines which are part of the TOE and • The processing of using data including cryptographic keys.

Table 1-Assumptions

2.4 Architectural Information

The physical scope of the TOE can best be depicted by the Figure 1 from the chap 1.4.2 of the ST. TOE has:

- 8052-type microprocessor with 256B internal RAM,

- 10K Test ROM storing IC Dedicated Software,

- 8K SRAM for volatile data storage,

- 3 x 64K Flash memory for non-volatile storage,

- RSA2048 crypto algorithm block,

- DES-3DES crypto algorithm block,

- AES crypto algorithm block,

- SHA-256 coprocessor block,

- UART block ensuring the communication between IC and card reader according to ISO/IEC 7816-3 protocol,

- Cyclic Redundancy Check module giving the opportunity to calculate 16 bit check sum according to ISO 3309 standard.

- Random Number Generator block producing true random numbers,

- Regulator converting external power supply of 5V to an internal supply of 2.5V,

- On Chip Oscillator which produces internal clock signal,

- Security sensors for sensing/preventing physical attacks,

- Reset Circuitry controlling the internal reset signal production according to RESET input and security sensor outputs.

Security Sensors subsystem includes the clock frequency sensor, the internal and external supply voltage sensors and the temperature sensor which sense the operating environment. These sensors cause the smartcard IC to enter to reset state when detected environmental conditions are out of specified ranges.

The crypto modules of the TOE has been designed to be resistant against SPA and DPA attacks. The microprocessor of the TOE is equipped with additional countermeasures against power analysis attacks.

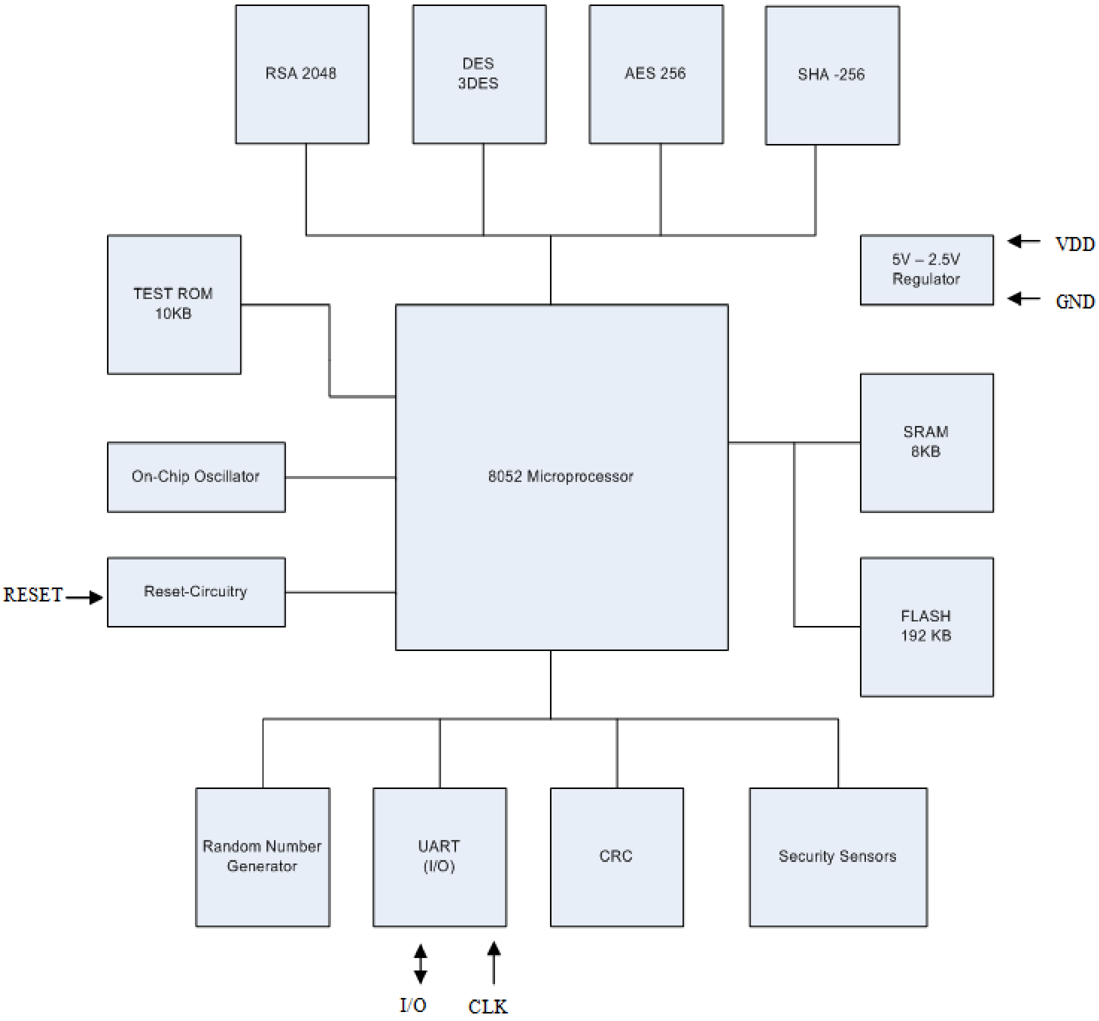

Figure 1 SmartCard IC Block Diagram

2.5 Documentation

Name of Document	Version Number	Publication Date
NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE SECURITY TARGET	06	08.07.2013
UKTUM-H V7.0 KULLANICI KILAVUZU	02	17.07.2013
UKTUM-H V7.0 TESLİM DOKÜMANI	01	06.11.2012

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 of 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 Evaluation Technical Report (ETR) of UKT23T64H v7.
It is concluded that the TOE supports EAL 5+ (AVA_VAN.5). There are 25 assurance families which are all evaluated with the methods detailed in the ETR. Scope of Test Assurance Class Evaluation :

- **TOE Test Coverage(ATE_COV.2):** Security Target Document,Functional Specification Document,Test Document, Test Coverage and Depth Document are used as evaluation evidence. The tests are in Test Document and the interfaces in Functional Specification Document are associated within the scope of test scope analysis inTest coverageand depth Document

- **TOE Test Depth(ATE_DPT.3):** Security Target Document,Functional Specification Document,Test Document, Test Coverage and Depth Document are used as evaluation evidence. Developer has prepared TOE System Test Document according to the TOE Design documentation which includes TSF subsystems and its interactions.
- **TOE Functional Testing(ATE_FUN.1):** Security Target Document,Functional Specification Document,Test Document are used as evaluation evidence.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.
- **Independent Testing(ATE_IND.2):** Security Target Document,Functional Specification Document,Test Document are used as evaluation evidence. Evaluator has done a total of 38 sample independent tests. 14 of them are selected from developer`s test plans.
- **Penetration Testing(AVA_VAN.5):** TOE**,**Security Target Document,Functional Specification Document,Design Document,Secure Architect Document, Implemetation Document,User Manual Document are used as evaluation evidence. Evaluator has done 24 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-A of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

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.

2.7 Evaluated Configuration

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

Evaluation Evidence	Version Number	Date
TOE-UKT23T64H v7	7.0	
NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE Security Target Document	6	08.07.2013
UKT23T64H v7 Source Code	7.0	
UKTÜM-H V7.0 ULUSAL AKILLI KART TÜMDEVRESİ GÜVENLİ YÜKLEME YAPABİLEN TESTROM MODÜLÜ (YROMV01.02) TASARIM TANIMLAMA DOKÜMANI(Design Specification Document)	1	18.07.2012
UKTÜM-H v7.0 GÜVENLİ MİMARİ DOKÜMANI(Secure Architecture Document)	2	21.03.2013
UKTÜM-H V7.0 FONKSİYONEL SPESİFİKASYON DOKÜMANI(Functional Specification Document)	3	08.07.2013
UKTÜM-H v7.0 MODULER YAPI DOKÜMANI(Modular Construction Document)	1	20.11.2012
UKTÜM-H V7.0 KULLANICI KILAVUZU(User Manual Document)	2	17.07.2013

UKTÜM-H v7.0 GÜVENLİK ÖNERİLERİ DOKÜMANI (Security Proposals Document)	2	01.10.2012
UKTÜM-H v7.0 KURULUM DOKÜMANI(Installation Document)	2	19.07.2013
UKTÜM-H v7.0 TESLİM DOKÜMANI (Delivery Document)	1	06.11.2012
UKTÜM-H v7.0 TÜMDEVRE TASARIM GELİŞTİRME ARAÇLARI DOKÜMANI (Design Development Tools Document)	1	06.11.2012
UKTÜM-H v7.0 YAŞAM DÖNGÜSÜ DOKÜMANI (Life Cycle Document)	1	06.11.2012
UKTÜM-H v7.0 GELİŞTİRME ORTAM GÜVENLİĞİ DÖKÜMANI (Development Environment Document)	1	06.11.2012
UKTÜM-H v7.0 KONFİGÜRASYON YÖNETİMİ DOKÜMANI (Configuration Management Document)	1	06.11.2012
UKTÜM-H v7.0 TEST DOKÜMANI (Test Document)	1	12.11.2012
UKTÜM-H v7.0 TEST KAPSAM ve DERİNLİK DOKÜMANI (Test Scope and Depth Document)	2	19.07.2013

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 5 (EAL 5) components as specified in Part 3 of the Common Criteria, augmented with AVA_VAN.5.

Assurance Class	**Component ID**	**Component Title**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.5	Complete Semi-Formal functional specification with additional error information
	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT.2	Well-Structured Internals
	ADV_TDS.4	Semiformal 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.5	Development Tools CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.2	Compliance With Implementation Standards
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.3	Testing: modular design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.5	Advanced Methodological Vulnerability Analysis

Table 2- Security Assurance Requirements of the TOE

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 5 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 “NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE” the results of the assessment of all evaluation tasks are “Pass”.

As a result,UKTÜM-H v7.0 product was found to fulfill the Common Criteria requirements for each of 25 assurance families and provide the assurance level EAL 5+ (AVA_VAN.5) .This result shows that TOE is resistant against the “HIGH “level attack potential and it countervails the claims of the functional and assurance requirements which are defined in ST document.

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of "NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE" product, result of the evaluation, or the ETR.

3 SECURITY TARGET

Information about the Security Target document associated with this certification report is as follows:
Name of Document: NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE SECURITY TARGET
Version No.: 6
Date of Document: 08.07.2013
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

CCCS:	Common Criteria Certification Scheme (TSE)
CCTL:	Common Criteria Test Laboratory (OKTEM)
CCMB:	Common Criteria Management Board
CEM:	Common Evaluation Methodology
ETR:	Evaluation Technical Report
IT:	Information Technology
IC:	Integrated Circuit
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function
TSFI:	TSF Interface
SFR:	Security Functional Requirement
EAL:	Evaluation Assurance Level
AES:	Advanced Encryption Standard
DES:	Data Encryption Standard
RSA:	Rivest, Shamir and Adleman
SHA:	Secure Hash Algorithm
UEKAE:	National Electronics and Cryptology Research Institute

FIPS:	Federal Information Processing Standard
TÜBİTAK:	Turkish Scientific and Technological Research Council
OKTEM:	Common Criteria Test Center (as CCTL)
BİLGEM:	Center of Research For Advanced Technologies of Informatics and Information Security
UKTÜM:	National Smart Card Integrated Circuit

5 BIBLIOGRAPHY

1)Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009

2)Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009

3) "NATIONAL SMARTCARD IC UKTÜM-H v7.0 WITH DES – 3DES v7.0, AES256 v7.0, RSA2048 v7.0 LIBRARIES AND WITH IC DEDICATED SOFTWARE" Security Target Version: 06 Date: 08.07.2013

4)Evaluation Technical Report(Document Code: DTR 19 TR 02),v02,September 03,2013

5)CC Supporting Document Guidance, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.8 Revision 1, April 2012, CCDB-2012-04-002

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

7)Common Criteria Protection Profile as a guidance, 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.

6 ANNEXES

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