COMMON CRITERIA RECOGNITION ARRANGEMENT
FOR COMPONENTS UP TO EAL 4

Certification Report

EAL 5+ (AVA_VAN.5)

Evaluation of

TÜBİTAK BİLGEM UEKAE
NATIONAL SMARTCARD IC (UKTÜM) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Date : **02.07.2012**
Pages : **41**
Certification Report Number : **14.10.01/2012-234**

This page left blank on purpose.

----- o -----

TABLE OF CONTENTS:

This page left blank on purpose.

----- o -----

CERTIFICATION REPORT

The Certification Report is drawn up to submit the Certification Committee 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 PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

1. INTRODUCTION

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 with respect to that standard by the Turkish Accreditation Agency (TÜRKAK), the national accreditation body in Turkey. The evaluation and tests related with the concerned product have been performed by TÜBİTAK-BİLGEM-OKTEM, which is a public/commercial 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) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE whose evaluation was completed on 06.04.2012 and whose evaluation technical report was drawn up by OKTEM(as CCTL), and with the Security Target document with version no 06 of the relevant product.

2. GLOSSARY

CCCS:	Common Criteria Certification Scheme
CCTL:	Common Criteria Test Laboratory
CCMB:	Common Criteria Management Board
CEM:	Common Evaluation Methodology
AKiS:	Smart Card Operating System (**A**kıllı **K**art **İ**şletim **S**istemi)
ETR:	Evaluation Technical Report
IT:	Information Technology
OKTEM:	Common Criteria Test Center (as CCTL)
PCC:	Product Certification Center
ST:	Security Target
TOE:	Target of Evaluation
TSF:	TOE Security Function
TSFI:	TSF Interface
SFR:	Security Functional Requirement
TÜBİTAK:	Turkish Scientific and Technological Research Council
TÜRKAK:	Turkish Accreditation Agency
BİLGEM:	Center of Research For Advanced Technologies of Informatics and Information Security
UEKAE:	National Electronics and Cryptology Research Institute
EAL:	Evaluation Assurance Level
PP:	Protection Profile

Table 1 - Glossary

3. EXECUTIVE SUMMARY

Evaluated IT product name:

NATIONAL SMARTCARD IC (UKTÜM) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE

IT Product version:

v4

Developer`s Name:

TÜBİTAK BİLGEM UEKAE YİTAL

Name of CCTL :

TÜBİTAK BİLGEM OKTEM Common Criteria Test Laboratory

Completion date of evaluation :

06.04.2012

Common Criteria Standard version :

- 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 Components, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009

Common Criteria Evaluation Method version :

- Common Methodology for Information Technology Security Evaluation v3.1 rev3, July 2009

Short summary of the Report:

1) **Assurance Package :**

EAL 5+(AVA_VAN.5)

2) **Functionality :**

UKT23T64H v4 is a contact-based smartcard IC which is designed and developed for security-based applications. 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 Smart Card IC, UKT23T64H v4, consists of an 8052-type microprocessor with a 256 Byte internal memory, a 64K ROM, a 6K Test ROM, a 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. The operating system software, embedded on 64 K ROM, is specifically developed for the TOE; however, it is not a part of the TOE. The Test ROM stores the IC Dedicated Software used to support testing of the TOE during production. The TOE includes hardware of UKT23T64H v4 smartcard IC, IC Dedicated Software, Flash memory access library, and user libraries of the DES-3DES, AES, and RSA algorithms, and related documentation. UKT23T64H v4 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.

TOE SECURITY FUNCTIONS

Operating State Checking	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 fulfilled. For this purpose, TOE includes temperature sensors, supply voltage sensor, internal voltage sensor and 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. In addition, the TOE enters to reset state when the contents of the critical registers

	ensuring the correct operation of the TOE are corrupted as a result of fault attacks. These functions satisfy FPT_FLS.1 "Failure with Preservation of Secure State" requirement. On the other hand, when the sensors and the critical registers 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, TOE decides whether it is in the User Mode or the Test Mode by checking some phase management flags. If it is in the 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 can be accessible satisfying FAU_SAS.1
Protection Against Snooping	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. 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. In case of sensing a short-circuit or an open-circuit on the active shield the smartcard IC enters to reset state. 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 UKT23T64H v4 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 ROM where the operating system is embedded. Thus, the data and address busses are encrypted between ROM and the microprocessor. Even if the attacker reads the content of the ROM by reverse engineering, since the data is encrypted, the attacker does not obtain any useful data about the microprocessors software. These measures satisfy the security functional requirement of FPT_PHP.3, "Resistance to physical attack".
Data Encryption and Data Disguising	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.

	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 UKT23T64H v4 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 and SEF7 by the operating system software. The security enforcing function SEF5 can be tested directly

	from the operating system software. Since TSF self test will detect the attempts to modify sensor devices and random number generator, the covered security functional requirement is FPT_TST.2.
Notification of Physical Attack	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 covering the security functional requirement FPT_PHP.3.
Cryptographic Support	The TOE is equipped with the hardware implementations of the DES/DES3, AES and RSA cryptographic functions. The covered security functional requirement is FCS_COP.1.

Table 2 – TOE Security Functions

3) Summary of Threats addressed by the evaluated IT product:

Threats:

The TOE counter the threats presented in the table below and provide functions for countermeasure to them.

T. Leak-Inherent	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets. No direct contact with the Security IC internals is required here. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. One example is Differential Power Analysis (DPA). This leakage may be interpreted as a covert channel transmission but is more closely related to measurement of operating parameters, which may be derived either from direct (contact) measurements or measurement of emanations and can then be related to the specific operation being performed.
T. Phys-Probing	An attacker may perform physical probing of the TOE in order • to disclose User Data, • to disclose/reconstruct the Security IC Embedded Software or • to disclose other critical information about the operation of the TOE to enable attacks disclosing or manipulating the User Data or

	the Security IC Embedded Software. Physical probing requires direct interaction with the Security IC internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data may also be a prerequisite. This pertains to "measurements" using galvanic contacts or any type of charge interaction whereas manipulations are considered under the threat "Physical Manipulation (T.Phys-Manipulation)". The threats "Inherent Information Leakage (T.Leak-Inherent)" and "Forced Information Leakage (T.Leak-Forced)" may use physical probing but require complex signal processing as well.
T. Phys-Manipulation	An attacker may physically modify the Security IC in order to • modify User Data, • modify the Security IC Embedded Software, • modify or deactivate security services of the TOE, or • modify security mechanisms of the TOE

	to enable attacks disclosing or manipulating the User Data or the Security IC Embedded Software. The modification may be achieved through techniques commonly employed in IC failure analysis and IC reverse engineering efforts. The modification may result in the deactivation of a security feature. Before that hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data may also be a pre-requisite. Changes of circuitry or data can be permanent or temporary. In contrast to malfunctions (refer to T.Malfunction) the attacker requires to gather significant knowledge about the TOE's internal construction here.
T. Malfunction	An attacker may cause a malfunction of TSF or of the Security IC Embedded Software by applying environmental stress in order to • modify security services of the TOE or • modify functions of the Security IC Embedded Software • deactivate or affect security mechanisms of the TOE to enable attacks disclosing or manipulating the User Data or the Security

	IC Embedded Software. This may be achieved by operating the Security IC outside the normal operating conditions. The modification of security services of the TOE may e.g. affect the quality of random numbers provided by the random number generator up to undetected deactivation when the random number generator does not produce random numbers and the Security IC Embedded Software gets constant values. In another case, errors are introduced in executing the Security IC Embedded Software. To exploit this, an attacker needs information about the functional operation, e.g., to introduce a temporary failure within a register used by the Security IC Embedded Software with light or a power glitch.
T. Leak_Forced	An attacker may exploit information which is leaked from the TOE during usage of the Security IC in order to disclose confidential User Data as part of the assets even if the information leakage is not inherent but caused by the attacker. This threat pertains to attacks where methods described in “Malfunction due to Environmental Stress” (refer to T.Malfunction) and/or “Physical Manipulation” (refer to T.Phys-Manipulation) are used to cause

	leakage from signals which normally do not contain significant information about secrets.
T. Abuse-Func	An attacker may use functions of the TOE which may not be used after TOE Delivery in order to • disclose or manipulate User Data, • manipulate (explore, bypass, deactivate or change) security services of the TOE or • manipulate (explore, bypass, deactivate or change) functions of the Security IC Embedded Software or • enable an attack disclosing or manipulating the User Data or the Security IC Embedded Software.
T. RND	An attacker may predict or obtain information about random numbers generated by the TOE security service for instance because of a lack of entropy of the random numbers provided. An attacker may gather information about the random numbers produced by the TOE security service. Because unpredictability is the main property of random numbers this may be a problem in case they are used to generate cryptographic keys. Here the attacker is expected to take advantage of statistical

	properties of the random numbers generated by the TOE. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

Table 3 – Threats

4) Special Configuration Requirements:

National Smart Card IC, UKT23T64H v4, consists of an 8052-type microprocessor with a 256 Byte internal memory, a 64K ROM, a 6K Test ROM, a 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. The operating system, embedded on 64 K ROM memory, is specifically developed; however, it is not a part of the TOE. The Test ROM stores the IC Dedicated Software used to support testing of the TOE during production. The TOE includes hardware of UKT23T64H v4 smartcard IC, IC Dedicated Software, Flash memory access library, and user libraries of the DES-3DES, AES and RSA algorithms, and related documentation. UKT23T64H v4 communicate 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 detailed knowledge about the special configuration requirement can be found in the product guidance documents.

5) Disclaimers:

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 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 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.

4. IDENTIFICATION

TOE is a contact-based smart card IC which is designed for security-based applications. TOE also includes IC Dedicated Software and DES v4.2, AES256 v4.2, RSA2048 v4.2 libraries. TOE is designed by Semiconductor Technologies Research Laboratory (YİTAL) division under National Research Institute of Electronics and Cryptology (UEKAE) of TUBİTAK-BİLGEM and fabricated with HHNEC's 0.25um eFlash technology process. It is aimed that this smart card IC is utilised as Turkish national ID Card and national Health Card where secrecy and security is an issue.

National Smart Card IC, UKT23T64H v4, consists of an 8052-type microprocessor with a 256 Byte internal memory, a 64K ROM, a 6K Test ROM, a 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 as shown in Figure 1.

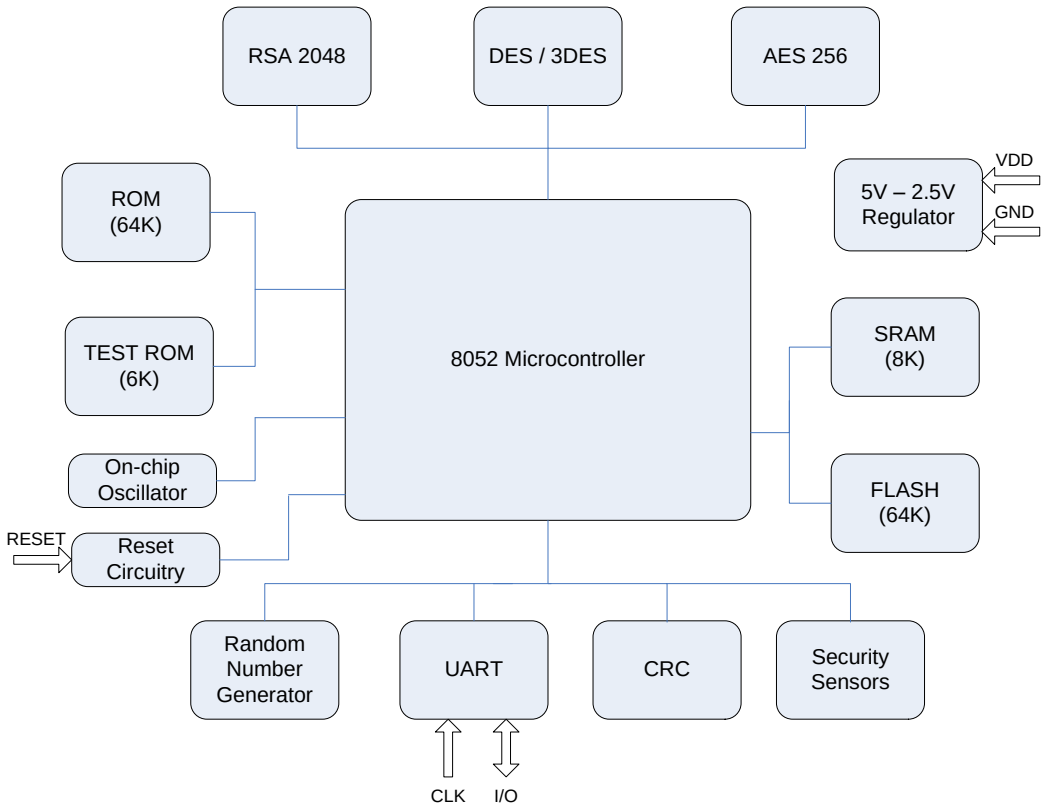

Figure 1 – Smartcard IC Block Diagram

The operating system, embedded on 64 K ROM memory, is specifically developed for the TOE; however, it is not a part of the TOE. The Test ROM stores the IC Dedicated Software used to support testing of the TOE during production. The TOE includes hardware of UKT23T64H v4 smartcard IC, IC Dedicated Software, Flash memory access library, and user libraries of the DES, AES and RSA algorithms, and related documentation. UKT23T64H v4 communicate 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.

UKT23T64H v4 smartcard IC is developed by YITAL in order to be used as national ID card, it aims to ensure EAL 5+ assurance level of CC. UKT23T64H v4 which has 7 design and manufacturing life cycle phases as shown in Figure 2 aims to be a national choice for smartcard ICs (which have EAL 5+ assurance level) on the market in terms of functionality, performance and security measures.

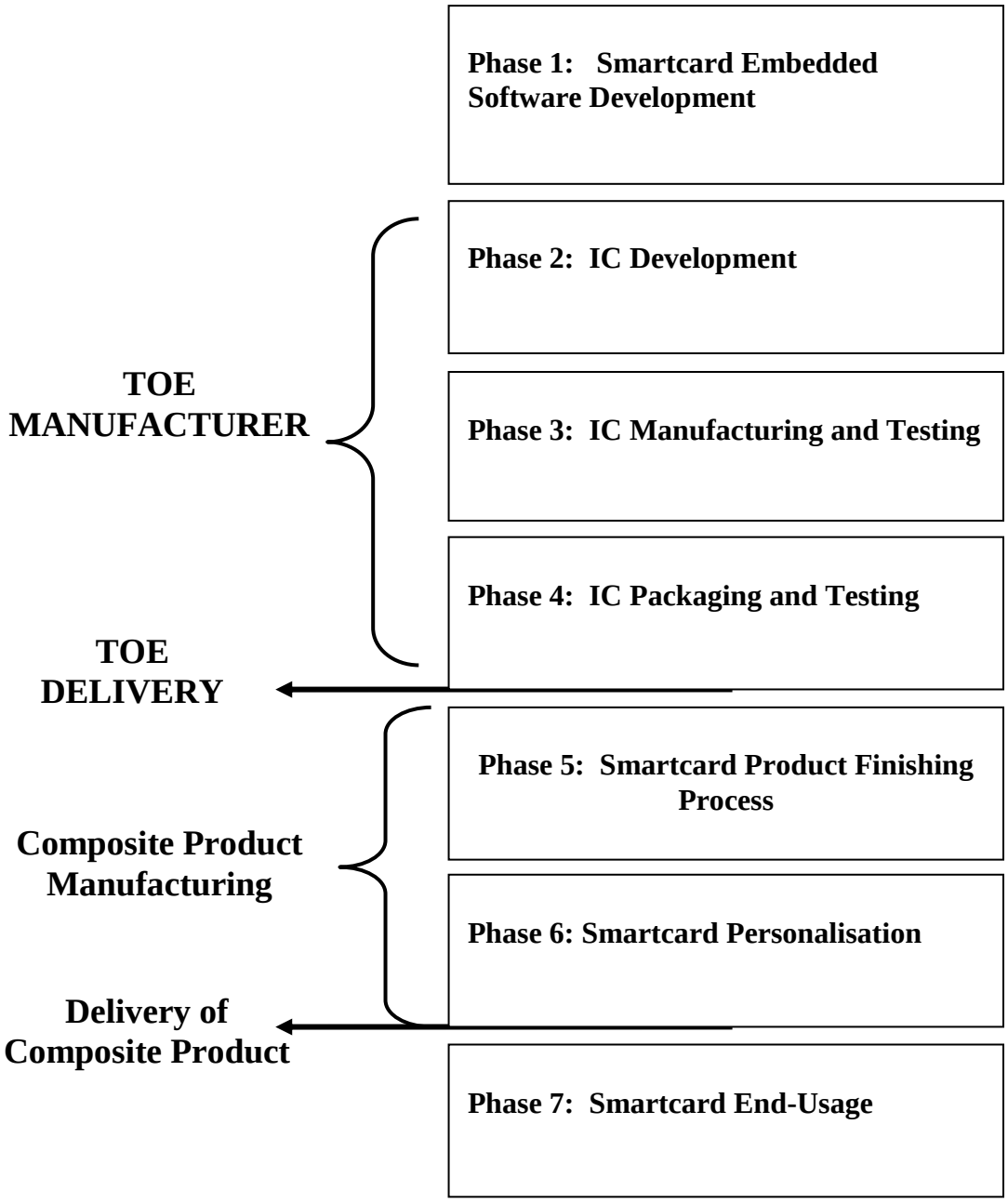

Figure 2 – Life Cycle

Phase 1: Smartcard Embedded Software Development

In this phase the **Smartcard Embedded Software Developer,** is in charge of

· the smartcard embedded software development and

· the specification of IC pre-personalisation requirements,

Since the operating system of the smartcard IC is developed in this phase, this phase will be out

of the scope of the ST.

Phase 2: IC Development

In this phase, the **IC Developer**

· designs the IC,

· develops IC Dedicated Software,

· provides information, software or tools to the Smartcard Embedded Software Developer, and

· receives the smartcard embedded software from the developer, through trusted delivery and verification procedures.

The information, software and tools given to the Smartcard Embedded Software Developer are flash memory access driver, crypto hardware driver and RNG test software and related documents about the UKT23T64H v4 IC

Using the IC design, IC Dedicated Software and Security IC Embedded Software, **the IC Designer** constructs the Security IC database, necessary for the IC photomask fabrication.

Phase 3: Manufacturing and Testing

In this phase, the **IC Manufacturer** is responsible for

· producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalisation.

The **IC Mask Manufacturer**

· generates the masks for the IC manufacturing based upon an output from the smartcard IC database.

Since the Security IC Embedded Software is stored in the ROM, the development of the OS software is finished in Phase 1 and delivered to the **IC Manufacturer**. The security IC is manufactured with HHNEC's 0.25µm e-Flash process technology. When the manufacturing process is completed, wafer level tests are performed and the serial number which is specific for each individual chip is written on to the Flash memory of the chips passing the tests. This operation is performed through the IC Dedicated Software residing in the Test ROM. At the end of initilisation/pre-personalisation step, the security IC enters to user mode disabling the use of IC Dedicated Software forever.

Phase 4: IC Packaging and Testing

In this phase, the **IC Packaging Manufacturer** is responsible for the IC packaging and testing.

At the end of the manufacturing stage, IC Manufacturer sends wafers to **IC Packaging Manufacturer** for packaging. There, wafers are diced and separated into individual chips. These individual chips are placed into smartcard modules and wire bonding operation is performed. **TOE is delivered in form of smartcard modules at the end of Phase 4.**

Phase 5: Smartcard Product Finishing Process

In this phase, the Smartcard Product Developer is responsible for the smartcard product finishing process and testing.

Phase 6: Smartcard Personalisation

In this phase, **the Personaliser** is responsible for the smartcard personalisation and final tests.

Phase 7: Smartcard End-usage

In this phase, **the Smartcard Issuer** is responsible for the smartcard product delivery to the smartcard end-user, and the end of life process.

The Security IC Embedded Software is developed outside the TOE development in Phase 1. The TOE is developed in Phase 2 and produced in Phase 3. Then the TOE is packaged in Phase 4 and delivered in form of packaged products.

5. SECURITY POLICY

Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see sec3.3 of ST)

POLICY	DESCRIPTION
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 (DES3) • Advanced Encryption Standard (AES) • Rivest-Shamir-Adleman (RSA2048)
P.Key-Installation: Installation of Secret Keys	Keys used in specific functions stated in the policy "*P. Add-Functions"* are not produced and/or destroyed by the TOE, they are rather installed from outside.

Table 4 - OSPs

6. ARCHITECTURAL INFORMATION

The physical scope of the TOE can best be depicted by the Figure 1 from the chap 1.4 of the ST and ST lite.

TOE has:

- 8052 type microprocessor with 256 Byte internal RAM,
- 64KB ROM storing IC Embedded Software,,
- 6KB Test ROM storing IC Dedicated Software
- 8KB SRAM for volatile data storage,
- 64KB Flash memory for non-volatile data storage,
- RSA2048 crypto algorithm block,

- DES-3DES crypto algorithm block,
- AES crypto algorithm block,
- card reader interface(UART),
- sensors which sense/prevent physical attacks,
- random number generator module,
- cyclic redundancy check module,
- regulator which converts external supply of 5V to an internal supply of 2.5V
- on chip oscillator which produces internal clock signal,
- reset circuitry which controls the internal reset signal production according to RESET input and security sensor outputs

Internally, the TOE can be structured according to the following subsystems from the TOE Design documentation.

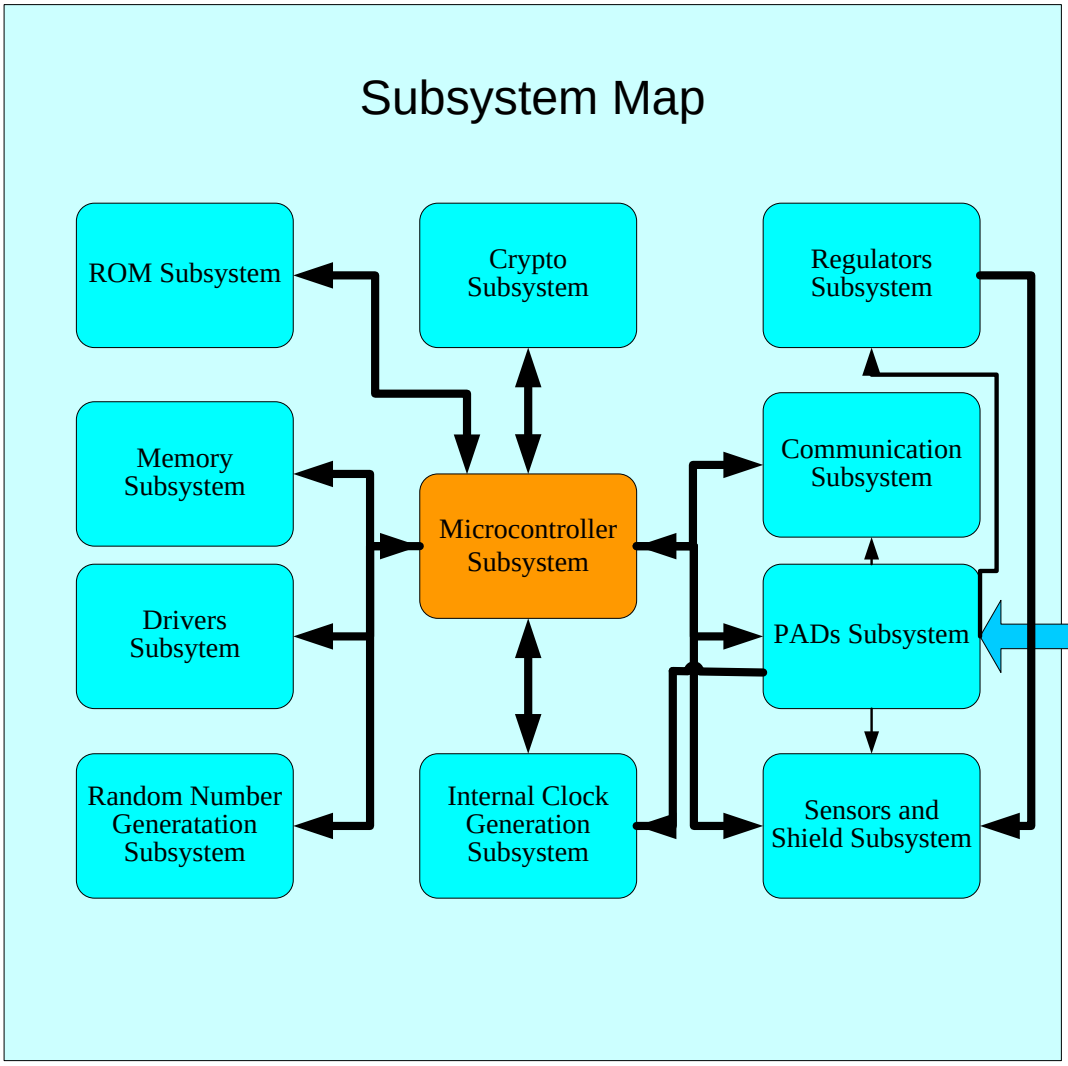

Figure 3 – The Subsystem Map of TOE

1.Microprocessor Subsystem : The microprocessor decodes and executes the operating system instructions that it reads from the ROM subsystem. During the execution of the instructions, it controls and use all other subsystems. For example, the microprocessor initiates the crypto subsystem to perform encryption/decryption operation after writing keys and data into it, and when the operation of the crypto subsystem is finished, the microcontroller reads the results and send them to other subsystems. All data exchange between different subsystems are realised through the microcontroller subsystem. The microcontroller subsystem is a TSF subsystem and its design includes countermeasures against side channel attacks and fault attacks.

2.Crypto Subsystem : Crypto subsystem is responsible from all of the cryptographic operations of the TOE. It supports DES, 3DES, AES, RSA1024 and RSA 2048 algorithms. The hardware implementation of these algorithms includes countermeasures against faults and side channel attacks. It is a TSF subsystem.

3. Sensors and Shield Subsystem : The TOE has security precautions against external attacks. These precautions are gathered under the sensors and shield subsystem. The TOE is equipped with different type of sensors and an active shield. These sensors are external supply sensor, internal supply sensor, frequency sensor and temperature sensor. The sensors monitor the operating condition of the TOE. Unless the TOE works under the specified conditions, the system resets the circuit and thus, stops the operation of the IC. The metal lines with active signals covering the chip surface forms the active shield which resets the IC when detects any physical attack to the TOE.

4. Random Number Generation Subsystem : This subsystem generates true random numbers to be used by the operating system software and by the security enforcing functions.

5.ROM Subsystem : ROM subsystem consists of 64KB ROM module storing Embedded Software and 6KB Test ROM module storing IC Dedicated Software. At the end of the production before TOE delivery the TOE is in Test Mode and the Test ROM is active. The die tests and pre-personalisation operations are performed using the IC Dedicated Software residing in the Test ROM. TOE is delivered in User Mode where 64KB ROM storing operating system code is active.
ROM subsystem delivers to the microcontroller subsystem the code instructions of the operating system software or the self test software depending on the operation mode of the TOE.

6.Memory Subsystem : Memory subsystem consists of the 8KB SRAM module and 64KB flash memory module. SRAM modules stores temporary data that the microcontroller subsystem needs during code execution. In the Flash memory module, the non-volatile data that must not be lost during the power-off is stored.

7. Internal Clock Generation Subsystem : This subsystem is responsible from generation of the internal clock signals of the circuit. The PLL module which is a part of this subsystem is used to generate the desired clock frequency. It is a non TSF subsystem.

8.Drivers Subsystem : Drivers subsystem consists of software codes needed for the use of Crypto Subsystem (DES, 3DES, AES, RSA1024, RSA2048), for performing self test of the Sensors and Shield subsystem, for performing the randomness test of the random numbers produced by the Random Number Generation subsystem and for accessing the flash memory module of the Memory subsystem It is a TSF subsystem..

9.Communication Subsystem : Communication subsystem is responsible from communication of the TOE with the outside world and is a non TSF subsystem. It consists of only UART (Universal Asynchronous Receiver Transmitter Interface) that provides communication of the microprocessor with the smartcard reader.

10.Pads Subsystem : Pads subsystem is responsible from making all connection of the TOE with the outside world (Data, Clock, Reset, Supply and Ground) and is a non TSF subsystem.

11.Regulator Subsystem : Regulator subsystem is responsible from generating internal power voltages of the circuit using the external power supply. and it is a non TSF subsystem.

7. ASSUMPTIONS AND CLARIFICATION OF SCOPE

TOE consists of the components which are defined in section 6 (Architectural information). Except these, Other components are not in the scope of Common Criteria Evaluation.

7.1 Usage Assumptions

A. Process-Sec-IC : Protection during Finishing and Personalisation (Phases 5 – 6)

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.

7.2 Environmental Assumptions

A.Plat-Appl : Usage of Hardware Platform

The Security IC Embedded Software is designed so that the requirements from the following documents are met:

- UKT23T64H v4 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.

A.Resp-Appl : Treatment of User Data

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.

A.Key-Function: Usage of key dependent Functions

Key-dependent functions (if any) shall be implemented in the smart card 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 smart card embedded software. In contrast to this the threads 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.

7.3 Clarification of Scope

Under normal conditions; there are no threats which TOE must counter but did not; however Operational Environment and Organizational Policies have countered. Information about threats that are countered by TOE and Operational Environmental are stated in the Security Target document.

8. DOCUMENTATION

Name of Document	Version Number	Publication Date
Security Target Document of National Smartcard IC (UKTÜM) UKT23T64H v4 with DES-3DES v4.2, AES256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software	6	07.06.2012
UKT23T64H v4 User Guidance	2	21.02.2012

Table 5 - Documents

9. 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 v4.

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.

IT Product Testing is mainly realized in two parts:

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 includes 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) **Evaluator Testing:**
   - **Independent Testing:** Evaluator has done a total of 38 sample independent tests. 14 of them are selected from developer`s test plans. The other 24 tests are evaluator`s independent tests. All of them are related to TOE security functions.
   - **Penetration Testing:** Evaluator has done 21 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-C 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.

10.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: TOE-UKT23T64H v4
Version Number: 4
Production Date: 10.02.2011

Evaluation Evidence: NATIONAL SMARTCARD IC (UKTÜM) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE Security Target Document

Version Number: 6
Date: 07.06.2012

Evaluation Evidence: NATIONAL SMARTCARD IC (UKTÜM) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE Security Target Lite Document

Version Number: 7
Date: 30.06.2012

Evaluation Evidence: UKT23T64H v4 Source Code
Version Number: 4
Date: 10.02.2011

Evaluation Evidence: UKT23T64H v4 Detailed Design Document(Ayrıntılı Tasarım Dokümanı)
Version Number: 18
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Security Architecture Design Document(Güvenli Mimari Tasarım Dokümanı)
Version Number:02
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Functional Specification Document(Fonksiyonel Belirtim Dokümanı)
Version Number: 4
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Modular Construction Document(Modüler Yapı Dokümanı)
Version Number: 2
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 User Manual Document(Kullanıcı Kılavuzu Dokümanı)
Version Number: 2
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Security Proposals Document(Güvenlik Önerileri Dokümanı)
Version Number: 03
Date: 29.02.2012

Evaluation Evidence: UKT23T64H v4 Installation Document(Kurulum Dokümanı)
Version Number: 2
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Delivery Document(Teslim Dokümanı)
Version Number: 2
Date: 21.02.2012

Evaluation Evidence: UKT23T64H v4 Application Standard Document(Uygulama Standardı Dokümanı)
Version Number: 1
Date: 24.02.2011

Evaluation Evidence: UKT23T64H v4 Design Development Tools Document(Tasarım Geliştirme Araçları Dokümanı)
Version Number: 2
Date: 17.02.2012

Evaluation Evidence: UKT23T64H v4 Life Cycle Document(Yaşam Döngüsü Dokümanı)
Version Number: 2

Date: 13.02.2012

Evaluation Evidence: UKT23T64H v4 Development Environment Document(Geliştirme Ortam Güvenliği Dokümanı)
Version Number: 1
Date: 14.07.2009

Evaluation Evidence: UKT23T64H v4 Configuration Management Plan Document(Konfigürasyon Yönetim Planı Dokümanı)
Version Number: 4
Production Date: 09.11.2010

Evaluation Evidence: UKT23T64H v4 Test Document(Test Dokümanı)
Version Number: 4
Date: 12.03.2012

Evaluation Evidence: UKT23T64H v4 Test Scope and Depth Document(Test Kapsam ve Derinlik Dokümanı)
Version Number: 4
Date: 12.03.2012

Evaluation Evidence: UKT23T64H v4 Configuration Evidences(Konfigürasyon Kanıtları)
Date: 09.10.2010

11.RESULTS OF THE EVALUATION

Table 6 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.

Component ID	Component Title
ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance Claims
ASE_SPD.1	Security Problem Definition
ASE_OBJ.2	Security Objectives
ASE_ECD.1	Extended Components Definition
ASE_REQ.2	Derived Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_ARC.1	Security Architecture
ADV_FSP.5	Functional Specification
ADV_IMP.1	Implementation Representation
ADV_INT.2	TSF Internals
ADV_TDS.4	TOE Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Configuration Management Capabilities
ALC_CMS.5	Configuration Management Capabilities
ALC_DEL.1	Delivery
ALC_DVS.1	Development Security
ALC_LCD.1	Life-cycle Definition
ALC_TAT.2	Tools and Techniques
ATE_COV.2	Coverage
ATE_DPT.3	Depth
ATE_FUN.1	Functional Tests
ATE_IND.2	Independent Testing
AVA_VAN.5	Vulnerability Analysis

Table 6 – Security Assurance Requirements for 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) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE" the results of the assessment of all evaluation tasks are "Pass".

Results of the evaluation:

UKT23T64H v4 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.

12.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) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE" product, result of the evaluation, or the ETR.

13.CERTIFICATION AUTHORITY COMMENTS/ RECOMMENDATIONS

The certifier has no comments or recommendations related to the evaluation process of "NATIONAL SMARTCARD IC (UKTÜM) UKT23T64H v4 WITH DES – 3DES v4.2, AES256 v4.2, RSA2048 v4.2 LIBRARIES AND WITH IC DEDICATED SOFTWARE"product, result of the evaluation, or the ETR.

14.SECURITY TARGET

Information about the Security Target document associated with this certification report is as follows:

Name of Document: Security Target Document of "National Smartcard IC (UKTÜM) UKT23T64H v4 with DES-3DES v4.2, AES 256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software"

Version No.: 6

Date of Document: 07.06.2012

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.

Name of Document: Security Target Lite Document of "National Smartcard IC (UKTÜM) UKT23T64H v4 with DES-3DES v4.2, AES 256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software"

Version No.: 7

Date of Document: 30.06.2012

15.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) UKT23T64H v4 with DES-3DES v4.2, AES 256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software" Security Target Version: 06 Date: 07.06.2012

4)Evaluation Technical Report(Document Code: DTR 10 TR 01),v1.0,April 06,2012

5)Evaluation Technical Report(Document Code: DTR 10 TR 01),v1.1,June 07,2012

6)PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

7)CC Supporting Document Guidance, Mandatory Technical Document, Application of Attack Potential to Smartcards, Version 2.7 Revision 1, March 2009, CCDB-2009-03-001

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

9)Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, confidential Version 1.5, February 2009, BSI

10)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.

11) "National Smartcard IC (UKTÜM) UKT23T64H v4 with DES-3DES v4.2, AES 256 v4.2, RSA2048 v4.2 libraries and with IC Dedicated Software" Security Target Lite Version: 07 Date: 30.06.2012

16.APPENDICES

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

PREPARED BY

CC INSPECTION EXPERT(CANDIDATE)	
Name, Last Name:	Mehmet Kürşad ÜNAL
Title:	
Signature:	
CC INSPECTION EXPERT/TECHNICAL RESPONSIBLE	
Name, Last Name:	Mariye Umay AKKAYA
Title:	
Signature:	
APPROVED BY	
Name, Last Name:	Fatih ÇETİN
Title:	
Signature:	