Certification Report

EAL 4+ (ALC_DVS.2)
Evaluation of

TÜBİTAK BİLGEM UEKAE
SMART CARD OPERATING SYSTEM (AKiS) V 1.4N PASSPORT
AKILLI KART İŞLETİM SİSTEMİ (AKiS) V1.4N PASAPORT

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Date : 13 July 2011
Pages : 34
Certification Report Number :14.10.01/11-211

This page left blank on purpose.

----- o -----

TABLE OF CONTENTS:

LIST OF TABLES

FIGURES

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 (CCCS) 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-UEKAE-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 AKILLI KART İŞLETİM SİSTEMİ (AKiS) V1.4N PASAPORT - SMART CARD OPERATING SYSTEM (AKiS) V1.4N PASSPORT whose evaluation was completed on 13.06.2011 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:

Smart Card Operating System (AKiS) v 1.4N Passport

Akıllı Kart İşletim Sistemi (AKiS) v1.4N Pasaport

IT Product version:

V 1.4N

Developer`s Name:

TÜBİTAK BİLGEM UEKAE AKIS Project Group

Name of CCTL :

TÜBİTAK BİLGEM UEKAE OKTEM Common Criteria Test Laboratory

Completion date of evaluation :

13.06.2011

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

Other Mandatory Document version:

- Composite product evaluation for Smart Cards and similar devices v1.0 rev 1 Sep 2007

Short summary of the Report:

1) Assurance Package :

EAL 4+ (ALC_DVS.2)

2) Functionality :

AKiS-Pasaport v1.4N is a smart card application which is designed to be used as Machine Readable Travel Document (MRTD). The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel document (AKiS-Pasaport) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303'.

The TOE is a composite product comprising an integrated circuit (IC) AKiS Pasaport v1.4N application with a card operating system.

The TOE composes AKiS Pasaport v1.4N by combining NXP P5CD081. The integrated circuit of the MRTD's chip is NXP P5CD081. NXP-P5CD081 has CC EAL 5+ (AVA_VAN.5) certificate. AKiS-Pasaport v1.4N Operating System is loaded into the ROM of the NXP chip (P5CD081) during the manufacturing of the IC.

The evaluation has been performed according to the composition scheme as defined in the guide 15.7 in order to assess that no weakness comes from the integration of the software in the integrated circuit already certified.

Regarding Composite evaluation, smartcard specific prescription for evaluation and evaluation approach for assurance components which are not prescribed in CEM, they are based on the supporting documents.(15.7)

The TOE comprises

- the circuitry of the MRTD's chip (the integrated circuit, IC): NXP P5CD081
- the IC Embedded Software (AKiS-Pasaport v1.4N OS),
- the MRTD application and
- the MRTD User Manual.

TOE SECURITY FUNCTIONS

Cryptographic Operations	1. 3DES key generation according to Document Basic Access Control Key Derivation Algorithm with key sizes of 112 bit. 2. Hashing according to SHA-1 and SHA-256 that meets FIPS 180-2. For Basic Access Control SHA-1 is used. For active authentication manufacturer decides which algorithms will be used : SHA-1 or SHA-256. 3. Secure messaging: encryption and decryption with 3DES algorithm in CBC mode with key sizes of 112 bits. 8 bytes zero IV, padding mode 2 is used. 4. Secure messaging: message authentication with Retail MAC with key sizes 112 bits according to ISO 9797. MAC Algorithm 3 is used with block cipher 3DES. 5. Active authentication signature generation according to ISO/IEC 9796-2 scheme 1 with RSA algorithm RFC 3447 RSASSA-PSS key sizes 1024 to 1848 bits. 6. After each active authentication, active authentication keys are destroyed by writing 0. 7. After each BAC session both the 3DES encryption key and message authentication key are destroyed by writing 0. 8. After each initialization authentication and personalization authentication, initialization key and personalization key are destroyed by writing 0. 9. Random number generation according to ANSI X9.17, AIS20 Class K4 for key generation, authentication operations.
Identification and Authentication	1. Storage of IC Identification data by the Manufacturer (with PUT DATA command) 2. The following data can be read before identification and authentication a. Initialization data in Manufacturing phase b. ATS (Answer to Select) in all phases 3. TSF mediated actions require successful identification and authentication, because BAC is activated. 4. Authentication data (random numbers) are prevented to be reused. 5. User authentication is provided through: a. BAC authentication mechanism in Operation Phase through BAC Authentication mechanism with Document Basic Access keys. b. Symmetric authentication mechanism based on 3DES in

	Manufacturing Phase with initialization key. c. Symmetric authentication mechanism based on 3DES in Personalization Phase with personalization key. 6. Active authentication of the TOE is provided through Active authentication mechanism with active authentication keys.
User Data Protection	1. Allowing only the successfully authenticated Personalization Agent to read and write data groups DG1 to DG16 of the LDS. 2. Allowing the terminals to read data groups DG1 to DG 16 of the LDS after successful BAC authentication. 3. Not allowing anybody to modify any data groups DG1 to DG 16 of the LDS in Operation phase. 4. Not allowing anybody to write/modify/erase any data (keys, LDS data) in Operation phase. 5. Transmitted and received user data is protected from modification, deletion, insertion and replay errors through secure messaging. 6. Determination on receipt of user data if modification, deletion, insertion and replay have occurred through secure messaging. Not allowing anybody to read DG3 and DG4.
Security Management	1. Initialization, personalization and configuration of the TOE are only allowed for the manufacturer and the personalization agent. 2. Initialization data and pre-personalization data can only be written by the manufacturer. 3. Ability to enable attack counter and set its maximum value is restricted to the manufacturer and the personalization agent. 4. When attack counter exceeds the threshold, the TOE enters the Death phase and can no longer be used. 5. Ability to set maximum value of the BAC error counter and wait time for the BAC error is restricted to the manufacturer. 6. When BAC error counter exceeds the threshold, the TOE waits for a pre-configured wait time without any action. 7. Ability to set the hash algorithm for the active authentication, SHA-1 or SHA-256, is restricted to the manufacturer and the personalization agent. 8. Maintenance of the security roles: Manufacturer, personalization agent, Basic Inspection System. 9. Personalization Agent is allowed to write the Document Basic Access Keys.

	10. Manufacturer and Personalization Agent are allowed to write the Active Authentication keys. 11. After unsuccessfull authentication in INITIALIZATION START, INITIALIZATION END, and CHANGE KEY commands in Manufacturing phase, the initialization key error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used. 12. After unsuccessfull authentication in PERSONALIZATION START, PERSONALIZATION END, CHANGE KEY commands in Personalization phase, the personalization key error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used. 13. After unsuccessfull authentication in ERASE FILES command in Manufacturing and Personalization phase, the initialization key error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used. 14. After unsuccessfull authentication in EXCHANGE CHALLENGE command in Manufacturing phase, the EXCHANGE CHALLENGE error counter is incremented. When the counter reaches the threshold, the TOE enters the Death phase and can no longer be used which may enable other attacks. 15. Nobody is allowed to read Document Basic Access keys and Active Authentication keys. 16. Test features of the TOE are not available in Operation phase. If test features are performed by the TOE, no user data, TSF data can be disclosed or manipulated, no software can be reconstructed and no substantial information about TSF can be gathered. 17. Ability to disable read access for users to the Initialization Data to the Personalization Agent.
Protection	1. Hiding information about IC power consumption and command execution time. 2. Detection of the physical tampering of the TSF with sensors for operating voltage, clock frequency, temperature and electromagnetic radiation. If the TOE detects with the mentioned sensors, that it is not supplied within the specified limits, a security reset is initiated and the TOE is not operable until the supply is back in the specified limits. The hardware protects itself against analyzing and physical tampering. 3. Clock randomization 4. Not allowing any unauthorized users to use the following interface smart card circuit contacts to gain access to initialization and personalization authentication key and logical MRTD data.

	5. Preserve a secure state when a failure is detected by TSF according to FPT_TST.1. 6. Runs random number generator tests during initial start-up, when any command received, and at any cryptographic operation. Runs voltage level control test during initial start-up. 7. Provide authorized manufacturer and personalization agent with the capability to verify the integrity of ROM. 8. Verifies the integrity of the keys, header data of DFs, header and body data of EFs. If the integrity check of keys, header data of EFs and DFs fails, an error is returned to the user. If the integrity check of EF data fails, a warning returns to the user. If an integrity check of interior file system tables fails, the card enters the death phase and can no longer be used.

Table 2 – TOE Security Functions

3) Summary of Threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product:

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

T.Chip_ID	**Identification of MRTD's chip** *Adverse action:* An attacker trying to trace the movement of the MRTD by identifying remotely the MRTD's chip by establishing or listening to communications through the contactless communication interface. *Threat agent:* having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance *Asset:* Anonymity of user,
T.Skimming	**Skimming the logical MRTD** *Adverse action:* An attacker imitates an inspection system trying to establish a communication to read the logical MRTD or parts of it via the contactless communication channel of the TOE. *Threat agent:* having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance *Asset:* confidentiality of logical MRTD data
T.Eavesdropping	**Eavesdropping to the communication between TOE and inspection system** *Adverse action:* An attacker is listening to an existing communication between the MRTD's chip and an inspection system to gain the logical MRTD or parts of it. The inspection system uses the MRZ data printed on the MRTD data page but the attacker does not know these data in advance.

	Threat agent: having enhanced basic attack potential, not knowing the optically readable MRZ data printed on the MRTD data page in advance *Asset:* confidentiality of logical MRTD data
T.Forgery	**Forgery of data on MRTD's chip** *Adverse action:* An attacker alters fraudulently the complete stored logical MRTD or any part of it including its security related data in order to deceive on an inspection system by means of the changed MRTD holder's identity or biometric reference data. This threat comprises several attack scenarios of MRTD forgery. The attacker may alter the biographical data on the biographical data page of the passport book, in the printed MRZ and in the digital MRZ to claim another identity of the traveler. The attacker may alter the printed portrait and the digitized portrait to overcome the visual inspection of the inspection officer and the automated biometric authentication mechanism by face recognition. The attacker may alter the biometric reference data to defeat automated biometric authentication mechanism of the inspection system. The attacker may combine data groups of different logical MRTDs to create a new forged MRTD, e.g. the attacker writes the digitized portrait and optional biometric reference finger data read from the logical MRTD of a traveler into another MRTD's chip leaving their digital MRZ unchanged to claim the identity of the holder this MRTD. The attacker may also copy the complete unchanged logical MRTD to another contactless chip. *Threat agent:* having enhanced basic attack potential, being in possession of one or more legitimate MRTDs *Asset:* authenticity of logical MRTD data
T.Abuse-Func	**Abuse of Functionality** *Adverse action:* An attacker may use functions of the TOE which shall not be used in the phase "Operational Use" in order (i) to manipulate User Data, (ii) to manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or (iii) to disclose or to manipulate TSF Data. This threat addresses the misuse of the functions for the initialization and the personalization in the operational state after delivery to MRTD holder. *Threat agent:* having enhanced basic attack potential, being in possession of a legitimate MRTD *Asset:* confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF.
T.Information_ Leakage	**Information Leakage from MRTD's chip** *Adverse action:* An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential TSF data. The information leakage

	may be inherent in the normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. 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 measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are the Differential Electromagnetic Analysis (DEMA) and the Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis). *Threat agent:* having enhanced basic attack potential, being in possession of a legitimate MRTD *Asset:* confidentiality of logical MRTD and TSF data
T.Phys-Tamper	*Adverse action:* An attacker may perform physical probing of the MRTD's chip in order (i) to disclose TSF Data or (ii) to disclose/reconstruct the MRTD's chip Embedded Software. An attacker may physically modify the MRTD's chip in order to (i) modify security features or functions of the MRTD's chip, (ii) modify security functions of the MRTD's chip Embedded Software, (iii) modify User Data or (iv) to modify TSF data. The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. the biometric reference data for the inspection system) or TSF Data (e.g. authentication key of the MRTD's chip) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires direct interaction with the MRTD's chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary. *Threat agent:* having enhanced basic attack potential, being in possession of a legitimate MRTD *Asset:* confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

T.Malfunction	**Malfunction due to Environmental Stress** *Adverse action:* An attacker may cause a malfunction of TSF or of the MRTD's chip Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functions of the TOE or (ii) circumvent, deactivate or modify security functions of the MRTD's chip Embedded Software. This may be achieved e.g. by operating the MRTD's chip outside the normal operating conditions, exploiting errors in the MRTD's chip Embedded Software or misusing administration function. To exploit these vulnerabilities an attacker needs information about the functional operation. *Threat agent:* having enhanced basic attack potential, being in possession of a legitimate MRTD *Asset:* confidentiality and authenticity of logical MRTD and TSF data, correctness of TSF

Table 3 - Threats

4) Special Configuration Requirements:

The usage and security features are as defined in the MRTD with ICAO Application, Basic Access Control protection profile:

A State or Organization issues MRTDs to be used by the holder for international travel. The traveler presents a MRTD to the inspection system to prove his or her identity. The MRTD in context of this ST contains:

- visual (eye readable) biographical data and portrait of the holder,
- a separate data summary (MRZ data) for visual and machine reading using OCR methods in the Machine readable zone (MRZ) and
- data elements on the MRTD's chip according to LDS for contactless machine reading.

The authentication of the traveler is based on

(i) the possession of a valid MRTD personalized for a holder with the claimed identity as given on the biographical data page and

(ii) optional biometrics using the reference data stored in the MRTD.

The issuing State or Organization ensures the authenticity of the data of genuine MRTD's. The receiving State trusts a genuine MRTD of an issuing State or Organization.

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

AKiS-Pasaport v1.4N is a smart card which is designed to be used as Machine Readable Travel Document (MRTD). The Target of Evaluation (TOE) is the contactless integrated circuit chip of machine readable travel document (AKiS-Pasaport) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control according to 'ICAO Doc 9303'.

AKiS v1.4N Operating System Phases

AKiS v1.4N Operating System also consists of some phases which will be called as "AKiS v1.4N Operating System Life cycle phases" (Figure 1) in order to obstruct a confusion. There are 5 different life cycle phases available on TOE. Relations and crossing between these life cycle phases are shown in the Figure 1. Also there are some several keys available on TOE in order to be used within the execution of the secure commands. Command interpreter of TOE is designed to execute some special commands for the different life cycle phases.

These phases are;

Activation:

Main purposes of the activation phase is; to check if TOE is correct (not corrupted) and load the initial values of the keys that will be used on the execution of the secure commands (initialization and personalization key). MF (Master File) is created in this phase.

Initialization:

Main purpose of the initialization phase is to load the initialization data into the card. Therefore the file system will begin to construct on the EEPROM on each command.

Personalization:

Main purpose of the personalization phase is to load the personalization data into the card. Henceforth the card will include unique data belonging to the end user.

Operation:

In the operation phase, TOE is available for the end user.

Death:

When the security conditions listed below are not satisfied or it is noticed that security is trying to be surpassed, TOE enters the death phase:

- When 64 unsuccessful authentication attempts occur related to loading of the system keys with Exchange Challenge command.
- When 10 unsuccessful authentication attempts occur related to changing of the initialization key with Change Key command, erasing of EEPROM with Erase Files command, Initialization Start and Initialization End commands.
- When 10 unsuccessful authentication attempts occur related to changing of the personalization key with Change Key command, Personalization Start and Personalization End commands.
- When 16 to 128 (configurable) unsuccessful authentication attempts occur related to BAC authentication protocol.
- When an integrity check of interior filesystem tables fails.

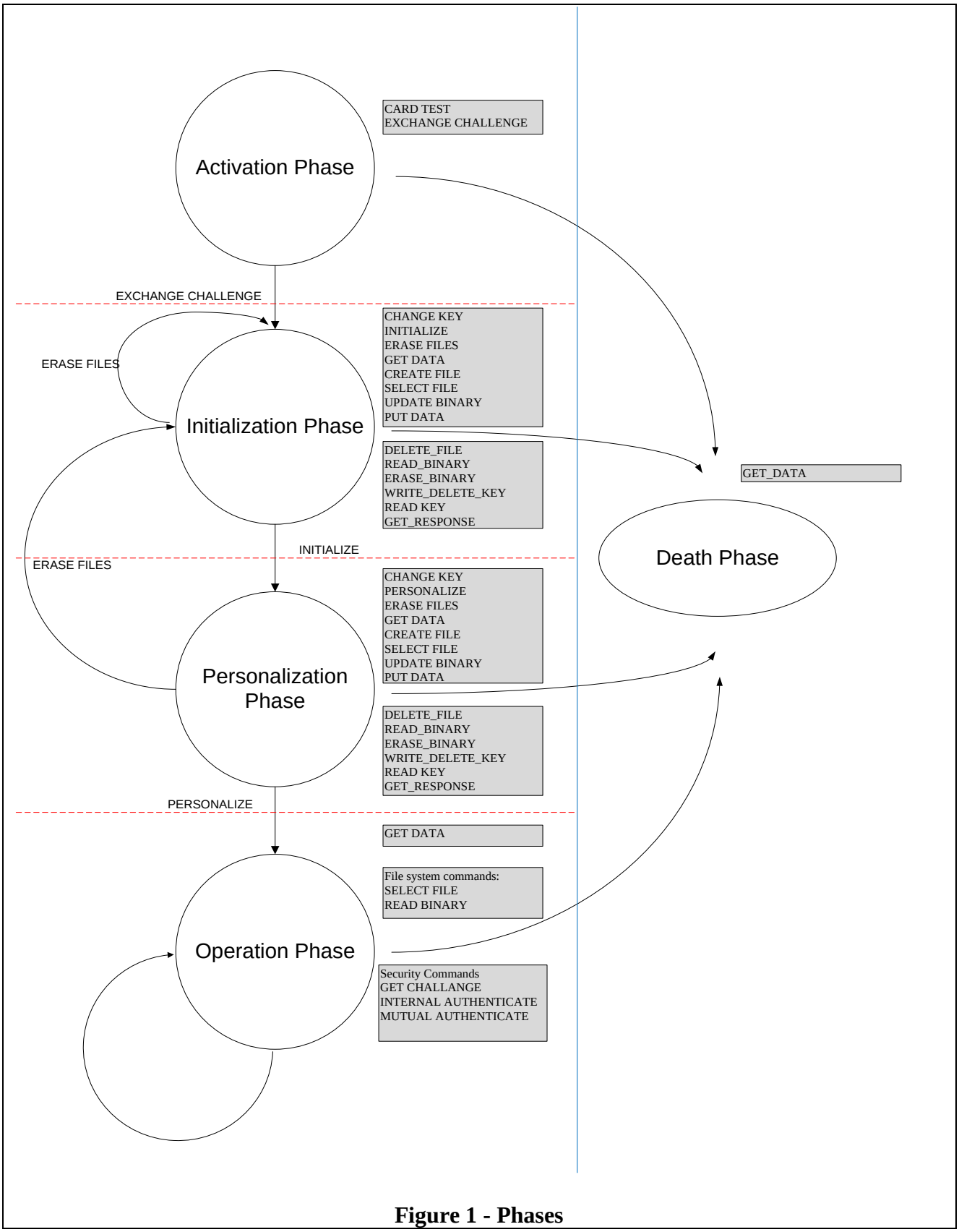

Figure 1 - Phases

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 CC part 1, sec. 3.2).

P.Manufact	**Manufacturing of the MRTD's chip** The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The MRTD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.
P.Personalization	**Personalization of the MRTD by issuing State or Organization only** The issuing State or Organization guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical MRTD with respect to the MRTD holder. The personalization of the MRTD for the holder is performed by an agent authorized by the issuing State or Organization only.
P.Personal	**Data Personal data protection policy** The biographical data and their summary printed in the MRZ and stored on the MRTD's chip (EF.DG1), the printed portrait and the digitized portrait (EF.DG2), the biometric reference data of finger(s) (EF.DG3), the biometric reference data of iris image(s) (EF.DG4) and data according to LDS (EF.DG5 to EF.DG13, EF.DG16) stored on the MRTD's chip are personal data of the MRTD holder. These data groups are intended to be used only with agreement of the MRTD holder by inspection systems to which the MRTD is presented. The MRTD's chip shall provide the possibility for the Basic Access Control to allow read access to these data only for terminals successfully authenticated based on knowledge of the Document Basic Access Keys.

Table 4 – Organizational Security Policies

6. ARCHITECTURAL INFORMATION

AKiS v1.4N algorithms and crypto specifications are;

Basic Access Control;

ISO/IEC11770-2 Key Establishment Mechanism 6

3DES CBC as block cipher

Cryptographic checksum ISO/IEC9797-1 MAC Algorithm 3

Active Authentication;

ISO/IEC9796-2 Digital Signature Scheme 1

MRTD Chip

The integrated circuit of the MRTD's chip is NXP P5CD081. NXP-P5CD081 has CC EAL 5+(AVA_VAN.5) certificate. AKiS-Pasaport v1.4N Operating System is loaded into the ROM of the NXP chip (P5CD081) during the manufacturing of the IC.

Operating system components are shown in Figure2;

- Memory Manager
- File Manager
- Command Interpreter
- Communication Handler

Message is received by UART which is managed by communication handler in TOE. The message comes in TPDU format which is mentioned above. Incoming TPDU packet is analysed and block type decision is made by the communication handler. TPDU may include 3 different types of blocks, named R, S and I block. R and S blocks are used to control the transmission protocol (ISO 7816-3). I block carries the command which is transmitted to the command interpreter and executed in TOE. When command execution is finished, communication handler sends the answer to the reader via UART. If the command is related with the file system, command interpreter calls the file manager. File manager is responsible for the operations in the file field which is in the EEPROM.

Memory manager is used to open new file, close file, delete page and attach new page.

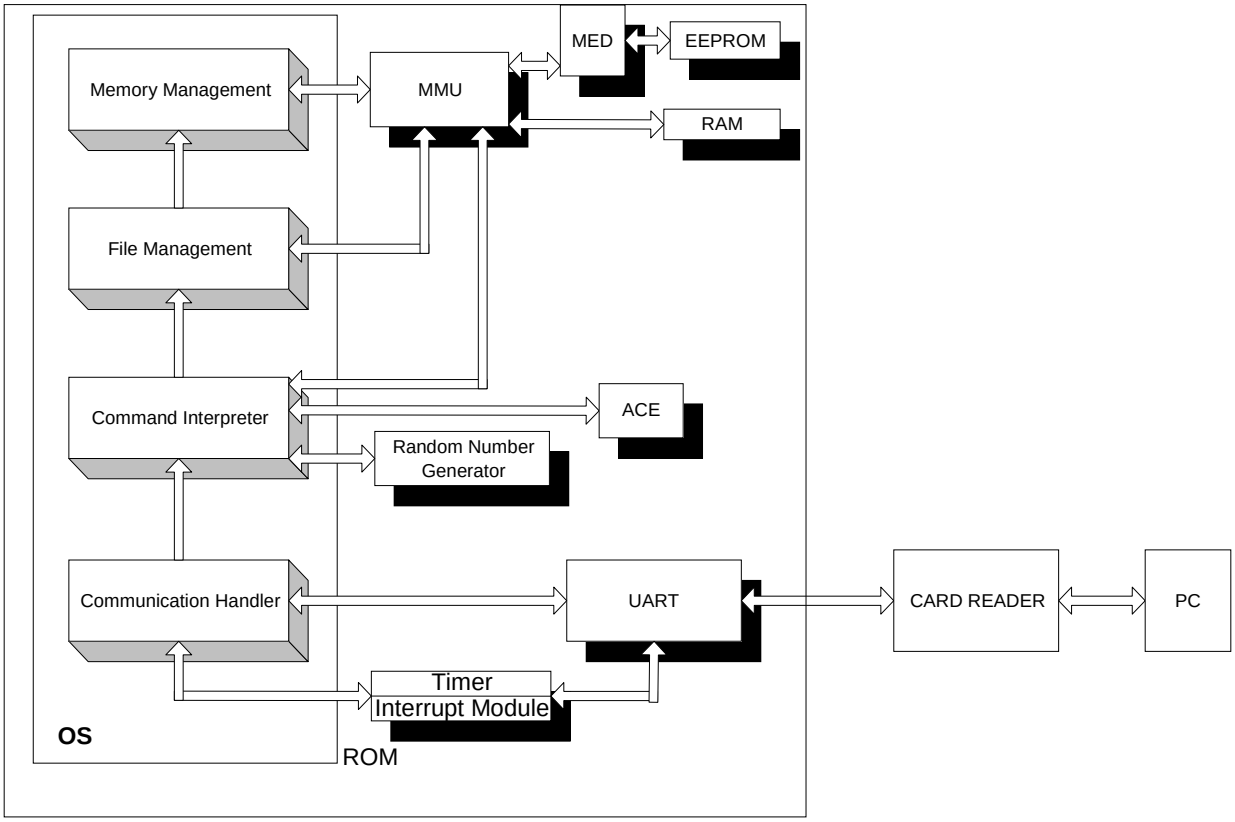

Figure 2 - AKiS v1.4N Operating System components and environment

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.MRTD_Manufact	**MRTD manufacturing on steps 4 to 6** It is assumed that appropriate functionality testing of the MRTD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRTD and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).
A.MRTD_Delivery	**MRTD delivery during steps 4 to 6** Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives: - Procedures shall ensure protection of TOE material/information under delivery and storage. - Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage. - Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.
A.Pers_Agent	**Personalization of the MRTD's chip** The Personalization Agent ensures the correctness of (i) the logical MRTD with respect to the MRTD holder, (ii) the Document Basic Access Keys, (iii) the Chip Authentication Public Key (EF.DG14) if stored on the MRTD's chip, and (iv) the Document Signer Public Key Certificate (if stored on the MRTD's chip). The Personalization Agent signs the Document Security Object. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by symmetric cryptographic mechanisms.

Table 5 – Usage Assumptions

7.2 Environmental Assumptions

A.Insp_Sys	**Inspection Systems for global interoperability** The Inspection System is used by the border control officer of the receiving State (i) examining an MRTD presented by the traveler and verifying its authenticity and (ii) verifying the traveler as MRTD holder. The Basic Inspection System for global interoperability (i) includes the Country Signing Public Key and the Document Signer Public Key of each issuing State or Organization, and (ii) implements the terminal part of the Basic Access Control. The Basic Inspection System reads the logical MRTD under Basic Access Control and performs the Passive Authentication to verify the logical MRTD.
A.BAC-Keys	**Cryptographic quality of Basic Access Control Keys** The Document Basic Access Control Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength. As a consequence of the 'ICAO Doc 9303' , the Document Basic Access Control Keys are derived from a defined subset of the individual printed MRZ data. It has to be ensured that these data provide sufficient entropy to withstand any attack based on the decision that the inspection system has to derive Document Access Keys from the printed MRZ data with enhanced basic attack potential.

Table 6 – Environmental Assumptions

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

AKiS v1.4N Pasaport Security Target
Ver. Number and Date: 06 – 18.04.2011

AKiS v1.4N Pasaport User Guidance
Ver. Number and Date: 01 – 30.12.2011

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 AKiS Pasaport v1.4N.

It is concluded that the TOE supports EAL 4+ (ALC_DVS.2) . There are 29 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 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) Evaluator Testing :

- **Independent Testing:** Evaluator has done a total of 37 sample independent tests. 19 of them are selected from developer`s test plans. The other 18 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- **Penetration Testing:** Evaluator has done 17 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.3 evaluation is given below:

- It is determined that TOE, in its operational environment, is resistant to an attacker possessing **"Enhanced-Basic"** attack potential.

For the product AKiS Pasaport v1.4N, **there is no residual vulnerability** (vulnerabilities can be used as evil actions by the hostile entities who have MEDIUM or HIGH level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

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 – AKiS Pasaport Application and NXP P5CD081 Contactless IC (AKiS Pasaport Uygulaması ve NXP P5CD081 Temazsız Yonga)
Version Number: 1.4N
Production Date : 05.11.2010

Evaluation Evidence: AKiS v1.4N Pasaport Source Code (Kaynak Kodu)
Version Number and Date: 1.0 – 30.12.2010

Evaluation Evidence: AKiS v1.4N Pasaport Design Specification Document (Tasarım Belirtim Dökümanı)
Version Number and Date: 03 –30.05.2011

Evaluation Evidence: AKiS v1.4N Pasaport Functional Specification Document (Fonksiyonel Belirtim Dokümanı)
Version Number and Date: 01 - 22.12.2010

Evaluation Evidence: AKiS v1.4N Pasaport Security Architecture Document (Güvenlik Mimarisi Dokümanı)
Version Number and Date: 01 – 27.12.2010

Evaluation Evidence: AKiS v1.4N Pasaport Delivery and Usage Document (Teslim ve İşletim Dokümanı)
Version Number and Date: 01 – 05.12.2010

Evaluation Evidence: AKiS v1.4N Pasaport Configuration Management Plan (Konfigürasyon Yönetim Planı)
Version Number and Date: 02 – 01.06.2011

Evaluation Evidence: AKiS v1.4N Pasaport Development Environment Security and Development Tools (Geliştirme Ortam Güvenliği ve Geliştirme Aletleri Dokümanı)
Version Number and Date: 01 – 05.01.2011

Evaluation Evidence: AKiS v1.4N Pasaport Life Cycle Document (Kullanım Ömrü Dokümanı)
Version Number and Date: 01 – 22.12.2010

Evaluation Evidence: AKiS v1.4N Pasaport Security Target Document (Güvenlik Hedefi)
Version Number and Date: 06 – 18.04.2011

Evaluation Evidence: AKiS v1.4N Pasaport System and Test Document (Sistem ve Test Dokümanı)

Version Number and Date: 01 – 25.01.2011

Evaluation Evidence: AKiS v1.4N Pasaport System Test Pre-usage Document (Sistem Test Dokumani Isletim Oncesi)
Version Number and Date: 01 – 23.01.2011

Evaluation Evidence: AKiS v1.4N Pasaport Administrator and User Manual Document (Yönetici ve Kullanıcı Kılavuzu Dokümanı)
Version Number and Date: 02 – 03.06.2011

11. RESULTS OF THE EVALUATION

Table 7 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 ALC_DVS.2.

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	Security Requirements
ASE_TSS.1	TOE Summary Specifiation
ASE_COMP.1	Consistency of Security Target
ADV_ARC.1	Security Architecture
ADV_COMP.1	Composite Design Compliance
ADV_FSP.4	Functional Specification
ADV_IMP.1	Implementation Representation
ADV_TDS.3	TOE Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.4	Configuration Management Capabilities
ALC_CMS.4	Configuration Management Scope
ALC_DEL.1	Delivery
ALC_DVS.2	Development Security
ALC_LCD.1	Life-Cycle Definition
ALC_TAT.1	Tools and Techniques
ALC_COMP.1	Integration of composition parts and Consistency of delivery procedures
ATE_COV.2	Coverage
ATE_DPT.1	Depth
ATE_FUN.1	Functional Tests
ATE_IND.2	Independent Testing
ATE_COMP.1	Composite Testing
AVA_VAN.3	Vulnerability Analysis
AVA_COMP.1	Composite Vulnerability Analysis

Table 7 - Security Assurance Requirements for the 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 AKiS Pasaport v1.4N the result of the assessment of all evaluation tasks are "Pass".

Results of the evaluation:

AKiS Pasaport v1.4N product was found to fulfill the Common Criteria requirements for each of 29 assurance families and provide the assurance level EAL 4+ (ALC_DVS.2) .This result shows that TOE is resistant against the "ENHANCED-BASIC'' level attack potential and it countervails the claims of the functional and assurance requirements which are defined in ST document.

There is no residual vulnerability (vulnerabilities can be used as evil actions by the hostile entities who have MEDIUM or HIGH level attack potential), that they do not affect the evaluation result, found by CCTL(OKTEM) laboratory under the conditions defined by the evaluation evidences and developer claims.

12. EVALUATOR COMMENTS/ RECOMMENDATIONS

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of AKiS Pasaport v1.4N 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 AKiS Pasaport v1.4N 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 : AKiS-PASAPORT v1.4N Security Target
Version No. : 06
Date of Document : 18.04.2011

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.

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] AKiS v1.4N Pasaport Security Target Version: 06 Date: 18.04.2011

[4] Evaluation Technical Report (Document Code: DTR 16 TR 01), June 13, 2011

[5] Evaluation Technical Report (Document Code: DTR 16 TR 02), July 11, 2011

[6] Composite product evaluation for Smart Cards and similar devices v1.0 rev 1 Sep 2007 (CCDB-2007-09-001)

[7] ETR for composition according to AIS36, as summary of ETR for NXP P5CD081V1A Secure Smart Card Controller

[8] PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 2.0

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

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

[11] P5CD016/021/041/051 and P5Cx081 - Delivery and Optional Manual

[12] P5CD016/021/041/051 and P5Cx081 – Product Data Sheet

[13] Assurance Continuity Maintenance Report (BSI-DSZ-CC-0555-2009-MA-01)

[14] NXP Secure Smart Card Controllers - P5CD016/021/041/051V1A and P5Cx081V1A Security Target Lite

[15] P5CD081 Order Entry Forms

[16] Common Criteria Protection Profile Machine Readable Travel Document with “ICAO Application”, Basic Access Control, BSI-CC-PP-0055, Version 1.10, 25th March 2009

[17] Common Criteria Protection Profile Machine Readable Travel Document with,,ICAO Application", Extended Access Control, BSI-CC-PP-0026, Version 1.2, 19 November 2007, BSI

[18] Certification Report for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software, BSI-DSZ-CC-410-2007, 05 July 2007, BSI

[19] Joint Interpretation Library, Attack Methods for Smartcards and Similar Devices, confidential Version 1.5, February 2009, BSI

16. APPENDICES

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