TÜBİTAK
BİLGEM

CENTER OF RESEARCH FOR ADVANCED TECHNOLOGIES OF INFORMATICS AND INFORMATION SECURITY

NATIONAL RESEARCH INSTITUTE OF ELECTRONICS AND CRYPTOLOGY

COMMON CRITERIA PROTECTION PROFILE

for

ELECTRONIC IDENTITY CARD ACCESS DEVICE FIRMWARE

(KEC FIRMWARE PP)

TSE-CCCS/PP-001

Center of Research For Advanced Technologies of Informatics and Information Security

National Research Institute of Electronics and Cryptology

P.K. 74, 41470 Gebze / KOCAELİ

Tel: (0262) 648 10 00, Faks: (0262) 648 11 00

www.bilgem.tubitak.gov.tr

bilgem@bilgem.tubitak.gov.tr

:

CONTENTS

1. PP INTRODUCTION

This Protection Profile (PP) includes the following items:

- Description of The Target of Evaluation (TOE),
- The security environment of the TOE including the threats to be countered by the TOE and by the operational environment and the assumptions to be countered by the operatioal environment,
- The security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of sensitive data,
- The Information Technology (IT) security requirements which includes the TOE functional requirements and the TOE IT Assurance requirements.

1.1 PP reference

Title: Common Criteria Protection Profile for Electronic Identity Card Access Device Firmware (KEC FIRMWARE PP)

Sponsor:

TÜBİTAK BİLGEM

Center of Research For Advanced Technologies of Informatics and Information Security

National Research Institute of Electronics and Cryptology

Editor(s): Mustafa SELVİ - *National Research Institute of Electronics and Cryptology*, TÜBİTAK BİLGEM

CC Version: 3.1 (Revision 3)

Assurance Level: Minimum assurance level for this PP is EAL 4+ (ALC_DVS.2)

General Status: Final

Version Number / Revision Date: 1.0 / 06th August 2012

Registration: TSE-CCCS/PP-001

Key words : Smartcard, Smartcard Reader, Secure Smartcard Reader, Electronic Identity Card, eID, Identity Verification, Electronic Identity Verification System

Note: A glossary of terms used in the Protection Profile is given in **ACRONYMS** section of the document (section 7).

1.2 TOE Overview

1.2.1 TOE definiton and operational usage

TOE is the embedded application software within Electronic Identity Card Access Device (KEC - Kart Erişim Cihazı), which is the terminal device in Electronic Identity Verification System (EKDS – Elektronik Kimlik Doğrulama Sistemi). It performs smartcard based personal identity verification. TOE can provide the following main services:

- Validation of TCKK (Türkiye Cumhuriyeti Kimlik Kartı) and validation of KEC with the help of GEM,
- Cardholder verification by using PIN and biometrics (fingerprint, fingervein, or palmvein data).

TOE provides these services for Automation Software Interface (OYA – Otomasyon Yazılımı Arabirimi), Web Client Interface (WIA – Web İstemci Arabirimi) and Security Services Platform (GSP - Güvenlik Servisleri Platformu) softwares.

1.2.2 TOE major security features for operational use

The TOE can provide the following security features:

- Cardholder authentication by using PIN and/or biometrics (either fingerprint data and/or fingervein data) depending either on a policy rule defined by KDPS or on verification type directly defined by the application,
- Authentication of TCKK and authentication of KEC by using GEM,
- Integrity and confidentialty of TOE,
- Data encryption and decryption using 256-bit AES and 2048-bit RSA algorithms,
- Hash Message Authentication Code (HMAC) calculation using 256-bit SHA algorithm,
- Authentications and secure communication with TCKK, GEM, GSP, externally connected pinpad and biometric devices,
- Automatically remote and secure software upgrade,
- Personal idendity verification for different security levels,
- Auditing of critical events,
- Reporting alarms to OYA/WIA/GSP,

1.2.3 Non-TOE hardware/software/firmware

1.2.3.1 Software/Firmware Environment of TOE

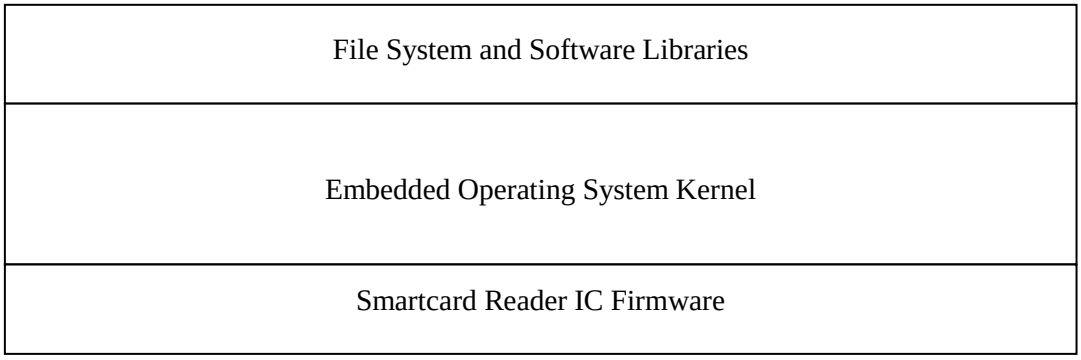

Figure 1. Typical Software/Firmware Architecture of TOE

In a typical software environment, TOE runs at the top of an embedded operating system, its file-system and software libraries. It communicates with a smartcard reader IC firmware within the device.

1.2.3.2 Hardware Environment of TOE

The TOE should be stored in a non-volatile memory location in KEC as an encrypted binary file. During power-up, encrypted TOE could be decrypted and loaded into the RAM region. Possible hardware environment of TOE is shown in Figure 2.

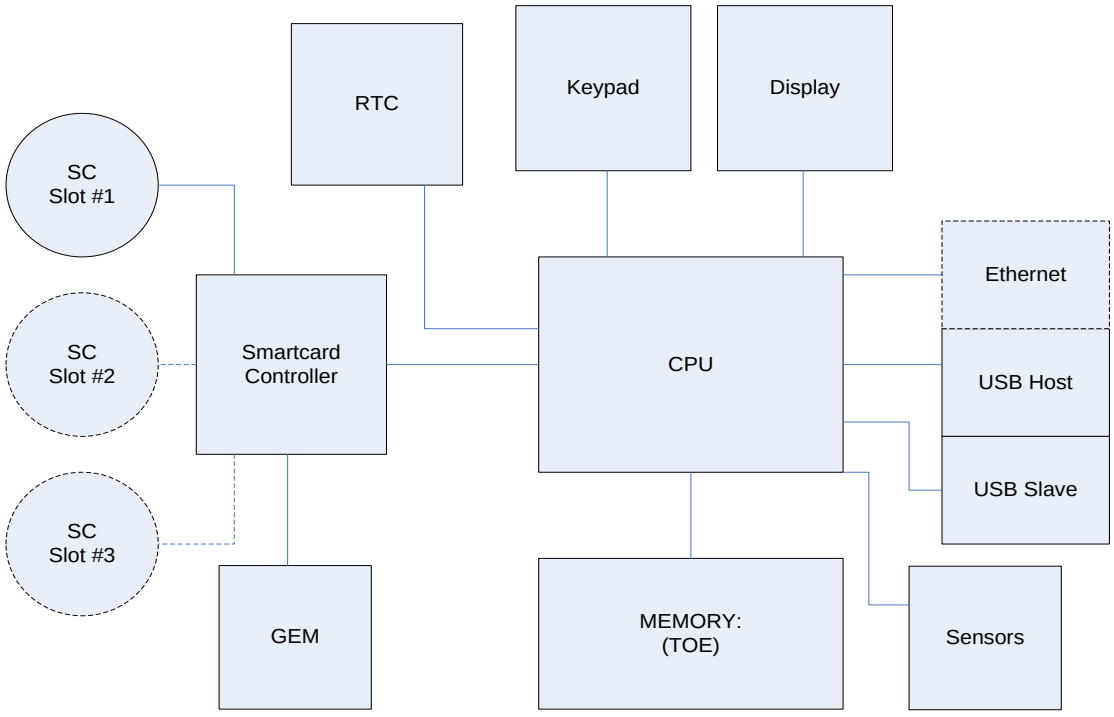

Figure 2. Possible Hardware Environment of TOE

Minimum hardware environment of TOE includes:

- I/O interfaces (USB and/or Ethernet),
- User interfaces (keypad, display, optional biometric sensor),
- CPU,
- Memory components (RAM, ROM, EEPROM, etc.),
- At least one smart card slot,
- GEM,
- Real Time Clock.
- Physical and logical security barriers (shields, temper switches etc.),

Some hardware components such as biometric sensor, ethernet port or second and third smartcard slots are optional depending on the device class. There are three possible smartcard reader device classes that TOE can be deployed. These classes are defined in the following section.

1.2.3.3 Smartcard Reader Classification

Secure card access devices, that TOE can be positioned, are classified according to their security functions, configurations and specifications. The following table summarizes the different device classes.

Device Class	*Class 1*	*Class 2*	*Class 3*
User Interface	Pinpad, Display, 1 smartcard slot, Biometric sensor(internal or external)	Pinpad, Display, 2 smartcard slots, Biometric sensor (internal or external)	Pinpad, Display, 2 smartcard slots, Biometric sensor (internal or external) Support for external pinpad with display
Communication environment	OYA/WIA	OYA/WIA, GSP	OYA/WIA, GSP
Security Functions	Card and cardholder authentication, GEM authentication, CVC based role authentication and secure messaging, Non-repudiation, Software integrity and confidentiality, 256-bit AES 2048-bit RSA	Card and cardholder authentication, GEM authentication, CVC based role authentication and secure messaging, Non-repudiation, Software integrity and confidentiality, 256-bit AES 2048-bit RSA	Card and cardholder authentication, GEM authentication, CVC based role authentication and secure messaging, Non-repudiation, Software integrity and confidentiality, 256-bit AES 2048-bit RSA
GEM	OK	OK	OK
Biometric Verification	OK	OK	OK
Service attender support	N/A	OK	OK
Representative support	OK	OK	OK
Secure Upgrade	OK	OK	OK

Table 1. The Device Classifications

1.2.3.4 TOE User Environments

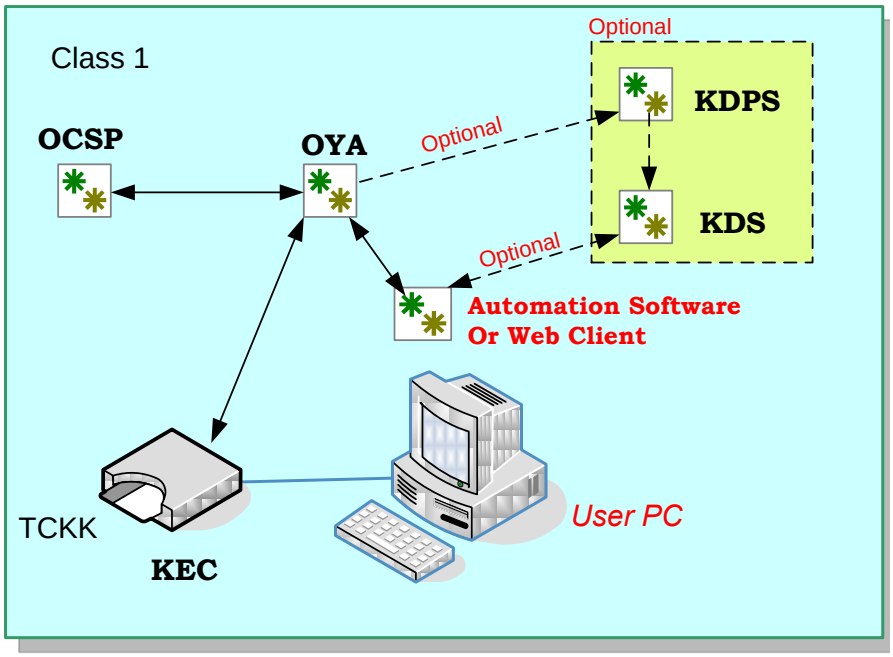

Figure 1. KEC environment of Class 1

The following scenario explains how Class 1 devices operate in the environment shown in figure 1:

The operation is initiated by an application software (or a web client) which is available on a personal computer. Application software communicates to KEC through a dll called OYA/WIA. OYA/WIA is a glue layer between TOE and the application software translating messages to TOE and securing the USB communication between TOE and OYA/WIA.

Authentication starts when the application software sends an authentication request to OYA/WIA. OYA/WIA directs this request to TOE. Once the TOE receives the request, it asks the user to insert his/her TCKK into the smart card slot. After TCKK is inserted, TOE begins a secure messaging session with TCKK and displays the user's personal message on the screen. If the displayed message is approved by the user, an identity specification package, prepared by TOE, is sent to OYA/WIA. OYA/WIA then communicates to KDPS to receive the policy that will be used. TOE gets the defined policy from OYA/WIA. If no policy is sent, a predefined default policy is applied by TOE. User authentication is performed according to security level (1to 5) specified in the policy package. During authentication, symmetric and asymmetric card verifications are performed and certificates of TCKK are validated online using OCSP to make sure the TCKK is valid and its certificate is not cancelled. Also according to security level in KDP, if requested, biometric verification of the user is carried out by TOE using fingerprint or fingervein biometrics depending on the environment. After the authentication, a KDB, which is electronically signed by TOE, is sent to OYA/WIA. Finally OYA/WIA forwards the KDB to KDS where they are stored for further examinations.

In the defined system, KDPS and KDS are optional. In their absence, their functions can be handled by the application software/web client applet and assertion packages (KDB) can be sent to application software/web client in spite of KDS.

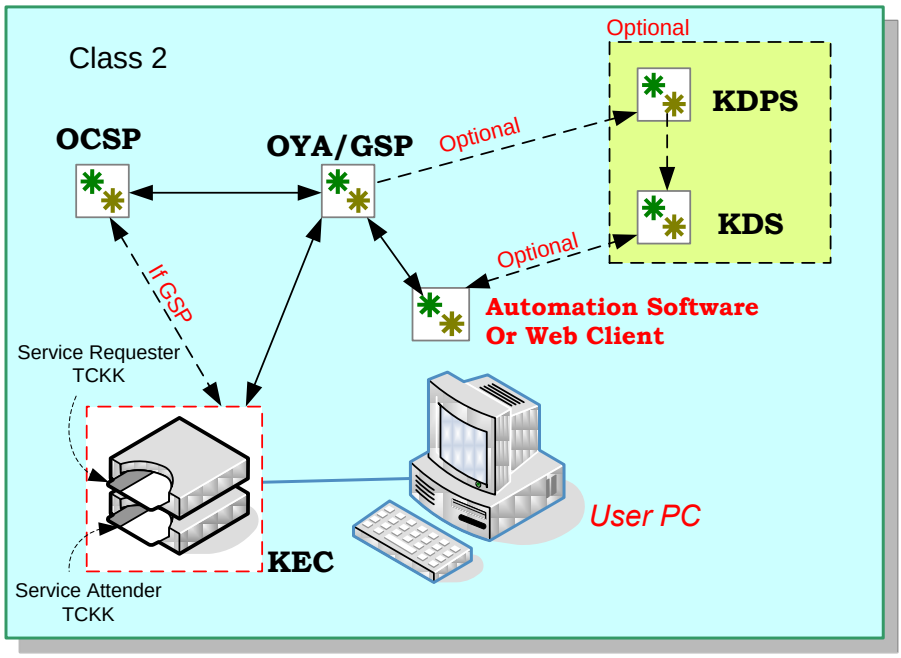

Figure 2. KEC environment of Class 2

KEC environmet for class 2 devices can be seen in figure 2 above. As seen, at least two smartcard slots are required by class 2 devices. The second smartcard slot is needed for service attender support. Operation is initiated by an application software (or a web client). Aplication software communicates to KEC through either a dll called OYA/WIA or GSP (Security services platform) depending on the environment. If the environment requires OYA/WIA, OYA/WIA has to be pre-installed on the user PC, otherwise, GSP has to be available on a remote network location.

In this scenario, the precedures are similar to the senario for class 1 devices. The only difference is service attender support. Therefore TOE authenticates not only the service requester but also the service attender. After receiving the authentication request, TOE first asks the service attender to insert his/her TCKK into the smart card slot. After TCKK is inserted, TOE authenticates the card and the service attender in the same way as in the scenario of class 1 devices. Next, TOE asks the service requester to insert his/her TCKK into the smart card slot. Again once the card is inserted, TOE authenticates the card and the service requester in the same way as in the scenario of class 1 devices. After these authentications, a KDB, which is electronically signed by TOE, is sent to OYA/WIA. Finally OYA/WIA forwards the KDB to KDS where they are stored for further examinations.

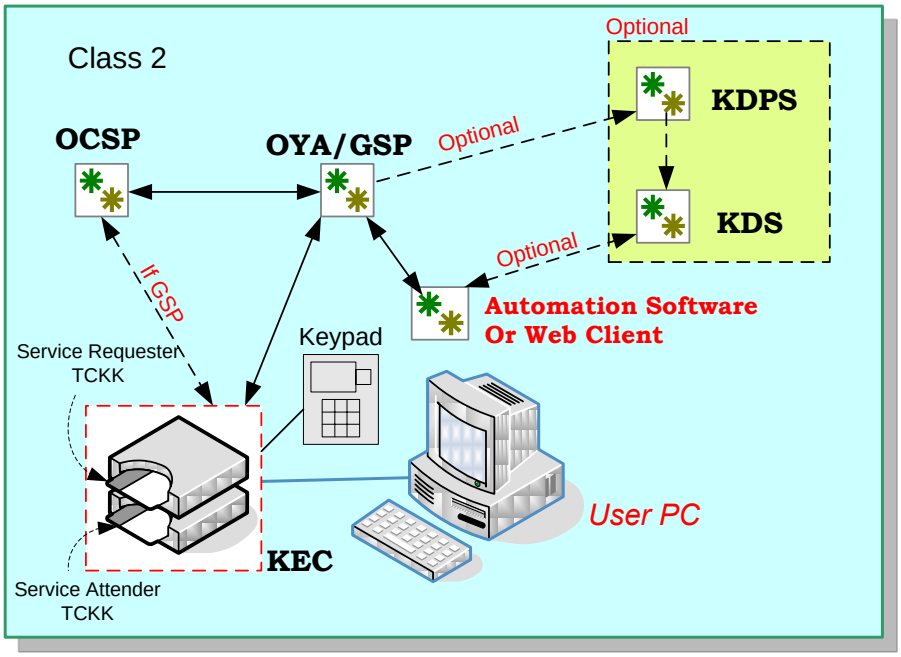

Figure 3. KEC environment of Class 3

As seen from the figure 3 above, class 3 devices have at least two smartcard slots too in order to provide service attender support. The operation of class 3 devices is the same of the operation of class 2 devices. Alternatively, by using Class 3 devices, an external pinpad can be connected to KEC so that the service requester can enter pin in a more comfortable way.

2. CONFORMANCE CLAIMS

2.1 CC Conformance Claim

This protection profile claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009 [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009 [2]
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009 [3]

As follows

- Part 2 conformant,
- Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009 [4]

has to be taken into account.

2.2 PP Claim

This PP does not claim conformance to any protection profile.

2.3 Package Claim

The current PP is conformant to the following security requirements package:

- Assurance package EAL4 augmented with ALC_DVS.2 as defined in the CC, part 3.

2.4 Conformance Claim Rationale

Since this PP does not claim conformance to any protection profile, this section is not applicable.

2.5 Conformance statement

This PP requires strict conformance of any ST or PP claiming conformance to this PP.

3. SECURITY PROBLEM DEFINITION

3.1 Threats

3.1.1 Threat Agents

A threat agent to the TOE can be:

- **User:** A person who has received a TOE in an authorized way and who wants to:
  - Alter the TOE so that it gives out PIN or biometric data of users or it loses its secure state.
  - Monitor the data transacted by the TOE to obtain security relevant data.
  - Tamper the TOE in order to obtain PIN or biometric data or GEM PIN.
  - Modify one of the external entities that the TOE communicates to such as TCKK, GEM, GSP, external pinpad device or biometric sensor, KDPS, SPS, OCSPS to obtain a TOE service in an unauthorized way.
- **Aggressor:** A person who has not received a TOE in an authorized way and who wants to:
  - Alter the TOE so that it gives out PIN or biometric data of users or it loses its secure state.
  - Monitor the data transacted by the TOE to obtain security relevant data.
  - Tamper the TOE in order to obtain PIN or biometric data of users or GEM PIN.
  - Modify one of the external entities that the TOE communicates to such as TCKK, GEM, GSP, external pinpad device or biometric sensor, KDPS, SPS, OCSPS to obtain a TOE service in an unauthorized way.

3.1.2 Threats covered by the TOE

T_ENTRY Sound and any visual output that the TOE produces during PIN or biometric data entry may help a threat agent to obtain PIN or biometric information of the user.

3.1.3 Threats covered by the TOE and the operational environment

T_KEC A threat agent may use a fake KEC-like device to obtain critical information such as GEM PIN and user's PIN or biometric information.

T_SC	A threat agent may use a counterfeit TCKK or modify the data between TOE and a valid TCKK in order to obtain a TOE service in an unauthorized way.
T_GSP	A threat agent may imitate GSP or modify the data between TOE and a valid GSP in order to obtain a service in an unauthorized way.
T_EXT_DEV	A threat agent may use an externally connected fake pinpad, smartcard reader or biometric device to collect PIN, biometrics and any other private information in an unauthorized way or modify the data sent by the external device to obtain a TOE service in an unauthorized way.
T_OCSPS	A threat agent may imitate OCSP Server (OCSPS) or modify the data sent by OCSPS in order to obtain a service in an unauthorized way.
T_SPS	A threat agent may imitate SPS or modify the data sent by SPS in order to modify TOE in an unauthorized way.
T_STOLEN_SC	A threat agent may steal somebody else's valid TCKK and use it to obtain a TOE service in an unauthorized way.
T_MNTR	A threat agent may monitor the data transferred between TOE and other external entities (GSP, TCKK/GEM and any externally connected pinpad, smartcard reader or biometric device) to discover security relevant information during the use stage.
T_PNTR	A threat agent may access inside of the TOE in an unauthorized way to obtain or modify security relevant data within TOE during the use stage.
T_REPU	A user may repudiate a TOE service that was given by KEC to the user.
T_RMODIF	Remote modification of the TOE by a threat agent. The TOE might be accessed by unauthorized connection from a remote location for modification purpose. After modification, TOE may send security related data in plain format or its security functions might be disabled.
T_CVCTIME	A cancelled GEM card may be used in a fake KEC by a threat agent in order to obtain a TOE service or collect user's PIN and biometric data in an unauthorized way

3.2 Assumptions

This section describes the assumptions that must be satisfied by the TOE operational environment.

3.2.1 Assumptions upon the development environment

A_DES.01 The designer issues and maintains a written procedure describing the security rules, and applies it in the development environment.

A_DES.02 The designer ensures protection of security relevant information involved in the design stage and during the software signature phase.

3.2.2 Assumptions upon the production environment

A_MAN.01 The manufacturer maintains a written procedure describing the security rules, and applies it in the production environment.

A_MAN.02 The manufacturer ensures protection of security relevant information involved in the manufacturing phase and the testing stage.

A_MAN.03 Security measures exist on the personal computer connected to TOE to ensure protection of the PC from viruses and unwanted programs and secure transfer of the TOE relevant data over the internet.

3.2.3 Assumptions upon the initialization and maintenance environment

A_INIT.01 Authorized service personnel maintain a written procedure describing the security rules, and apply it in pre-use and post-use environment.

A_INIT.02 Authorized service personnel protect security relevant information involved in personalization, delivery, maintenance phase and end of life processes.

A_INIT.03 Security measures exist on the personal computer connected to TOE to ensure protection of the PC from viruses and unwanted programs and secure communication of the TOE relevant data over the internet.

3.2.4 Assumptions upon the use environment

A_USE.01 Security measures exist on the personal computer connected to TOE to ensure protection of the PC from viruses and unwanted programs.

A_USE.02 PIN of any GEM card is never known by any user.

3.3 Organizational Security Policies

The current PP does not include any Organizational Security Policy.

3.4 Mapping of Assumptions and Threats To Device Classifications

As to device specifications differ, some assumptions or threats may not be applicable. The following table shows these differences between device classifications,

Assumption/Threat	Class 1	Class 2	Class 3
A_DES.01	✓	✓	✓
A_DES.02	✓	✓	✓
A_MAN.01	✓	✓	✓
A_MAN.02	✓	✓	✓
A_MAN.03	✓	✓	✓
A_INIT.01	✓	✓	✓
A_INIT.02	✓	✓	✓
A_INIT.03	✓	✓	✓
A_USE.01	✓	✓	✓
A_USE.02	✓	✓	✓
T_ENTRY	✓	✓	✓
T_KEC	✓	✓	✓
T_SC	✓	✓	✓
T_GSP	NA	✓	✓
T_EXT_DEV	NA	NA	✓
T_OCSPS	✓	✓	✓
T_SPS	✓	✓	✓
T_STOLEN_SC	✓	✓	✓
T_MNTR	✓	✓	✓
T_PNTR	✓	✓	✓
T_REPU	✓	✓	✓
T_RMODIF	✓	✓	✓
T_CVCTIME	✓	✓	✓

NA: not applicable

Table 2. Mapping of assumptions and threads to device classifications

4. SECURITY OBJECTIVES

The security objectives of the TOE and its environment cover principally the following aspects:

- Integrity and confidentiality of assets,

4.1 Security Objectives for the TOE

OT_INTEGRITY The TOE shall detect loss of integrity for security relevant data stored within the TOE.

OT_CONF The TOE shall ensure confidentiality of security relevant data during storage and data transfer between TOE and other trusted IT products**.**

OT_NON_REPU The TOE shall provide evidence for identity of origin, time of origin and location of origin for any KDB prepared by TOE.

OT_USER_AUTH The TOE shall authenticate users depending on either a policy rule specified by KDPS or a verification method directly defined by the application.

OT_TCKK_AUTH The TOE shall authenticate TCKK during each user authentication.

OT_GEM_AUTH The TOE shall authenticate GEM during each user authentication and device start-up. If GEM authentication fails, TOE shall not perform any operation.

OT_DEV_AUTH The TOE shall authenticate any externally connected pinpad, smartcard reader or biometric device before sensitive data transaction.

OT_GSP_AUTH The TOE shall authenticate GSP before executing any request from GSP.

OT_UPGRADE The TOE shall verify signature of the upgrade pack signed by SPS.

OT_AUDIT The TOE shall create audit records for critical events and detect security violations. The TOE shall also protect audit records against possible data loss or data overflow.

OT_PRS_MSG The TOE shall display the user's personal message before the user enters PIN or biometric data.

OT_CVCTIME The TOE shall update CV certificate of GEM before expiration date.

OT_ENTRY	When the user enters PIN or biometric data, the TOE shall not give any information, like audibale or visual outputs, which might be correlated with the entred data.
OT_SIGN_OCSP	The TOE shall verify signature of the data signed by OCSPS.

4.2 Security Objectives for the Operational Environment

OE_USR_AWR	Users shall be informed of their responsibility to protect their TCKK and its PIN/PUK information.
OE_SCARD	TCKK and GEM shall have necessary security certificates and keys for authentication of TCKK/GEM and cardholder by TOE and for confidentiality of personal private information and security relevant data. Private key of the certificates within TCKK/GEM shall be protected against unauthorized disclosure.
OE_PROCED	At each phase of its life cycle, the entity in charge of TOE shall issue and maintain a written procedure.
OE_PROTECT	In development, production, initialization (pre-use) and maintenance (post use) phases, the entity in charge of TOE shall ensure protection of security relevant data.
OE_PC	Personal computers used with TOE shall be protected against viruses and other unwanted programs.
OE_EXT_DEV	Any externally connected pinpad, smartcard reader or biometric device shall have security certificates and keys to provide mutual authentication with TOE and to ensure confidentiality of security relevant data transferred between TOE and itself. Private key of the certificate within these devices shall be protected against unauthorized disclosure. These external devices shall have tamper protection mechanism.
OE_GSP	GSP shall have a security certificate to provide mutual authentication with TOE and to ensure confidentiality of security relevant data transferred between TOE and GSP. GSP shall protect private key of its certificate against unauthorized disclosure.
OE_OCSPS	Private key of OCSPS certificate shall be protected against unauthorized disclosure.

OE_SPS	Private key of SPS certificate shall be protected against unauthorized disclosure.
OE_ACCESS	During production, initialization and maintenance stages, security relevant information shall be accessible by only authorized personnel.
OE_KEC_RTC	KEC shall have a RTC (Real Time Clock) hardware module.
OE_KEC_TEMP	KEC shall have a tamper protection mechanism. When a tamper event occurs, KEC shall erase encrypted GEM PIN stored within the device.
OE_GEM_PIN	GEM PIN shall be written within a non-volatile memory of KEC in an encrypted form by authorized personnel during production. This information will be accessed by only authorized personnel.
OE_AUTH_SRV	In the case of device tampering or loss of GEM PIN, the authorized service personnel shall reload all KEC software and firmware stored within the device.
OE_CVCTIME	Validity period of CV certificate within GEM shall not exceed one week.
OE_PRS_MSG	Any pinpad terminal device that is externally connected to TOE shall display the user's personal message before the user enters PIN or biometric data.
OE_GEM_SIGN	GEM shall have a sign certificate to sign KDB and KB prepared by TOE.

4.3 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all the identified threats and consistent with the identified assumptions.

The Table-3, on the following page, shows security objectives' relation to threats and assumptions. It demonstrates that at least one security objective is correlated to at least one threat or one assumption, and that each threat or each assumption is countered by at least one security objective.

Table 3. Mapping of the security objectives to the assumptions and the threats

	OT_INTEGRITY	OT_CONF	OT_NON_REPU	OT_USER_AUTH	OT_TCKK_AUTH	OT_GEM_AUTH	OT_GSP_AUTH	OT_DEV_AUTH	OT_UPGRADE	OT_AUDIT	OT_PRS_MSG	OT_CVC_TIME	OT_ENTRY	OT_SIGN_OCSP	OE_USR_AWR	OE_SCARD	OE_PROCED	OE_PROTECT	OE_PC	OE_EXT_DEV	OE_GSP	OE_OCSPS	OE_SPS	OE_ACCESS	OE_KEC_TEMP	OE_KEC_RTC	OE_GEM_PIN	OE_AUTH_SRV	OE_CVC_TIME	OE_PRS_MSG	OE_GEM_SIGN
A_DES.01																	✓							✓								
A_DES.02																		✓						✓								
A_MAN.01																	✓							✓								
A_MAN.02																		✓						✓								
A_MAN.03																			✓													
A_INIT.01																	✓							✓								
A_INIT.02																		✓						✓								
A_INIT.03																			✓													
A_USE.01																			✓													
A_USE.02																										✓						
T_ENTRY													✓																			
T_KEC		✓									✓														✓		✓					
T_SC					✓					✓						✓																
T_GSP		✓					✓			✓											✓											
T_EXT_DEV		✓						✓		✓										✓										✓		
T_OCSPS										✓				✓								✓										
T_SPS		✓							✓	✓													✓									
T_STOLEN_SC				✓						✓					✓																	
T_MNTR		✓																														
T_PNTR	✓	✓								✓															✓			✓				
T_REPU			✓	✓		✓				✓																✓					✓	
T_RMODIF	✓	✓								✓																						
T_CVCTIME												✓																	✓			

:

A_DES.01 This assumption is countered by OE_PROCED and OE_ACCESS environmental objectives. By OE_PROCED objective, in development stage the designer has to obey some security procedures that are maintained by the entity in charge of TOE development. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_DES.02 This assumption is countered by OE_PROTECT and OE_ACCESS environmental objectives. By OE_PROTECT objective, the designer has to protect the security relevant data during the development phase. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_MAN.01 This assumption is countered by OE_PROCED and OE_ACCESS environmental objectives. By OE_PROCED objective, in production stage the manufacturer has to obey some security procedures that are maintained by the entity in charge of TOE production. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_MAN.02 This assumption is countered by OE_PROTECT and OE_ACCESS environmental objectives. By OE_PROTECT objective, the manufacturer has to protect the security relevant data during the production phase. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_MAN.03 This assumption is countered by OE_PC objective.

A_INIT.01 This assumption is countered by OE_PROCED and OE_ACCESS environmental objectives. By OE_PROCED objective, in pre-use stage the KECÖB personnel have to obey some security procedures that are maintained by the entity in charge of TOE initialization and personalization. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_INIT.02 This assumption is countered by OE_PROTECT and OE_ACCESS environmental objectives. By OE_PROTECT objective, the KECÖB personnel have to protect the security relevant data during the pre-use

:

phase. OE_ACCESS objective ensures that security relevant information must be accessible only by authorized personnel.

A_INIT.03	This assumption is countered by OE_PC objective.
A_USE.01	This assumption is countered by OE_PC objective.
A_USE.02	This assumption is countered by OE_GEM_PIN objective.

T_ENTRY This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent acquires PIN or biometric data of a user while the user enters it. Threat agent may achieve this information by processing the feedback information given by TOE during the entry. This threat is countered by OT_ENTRY objective.

T_KEC This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent replaces the KEC with a fake one that resembles the original. To do this, the threat agent must have a valid GEM card and he/she has to know GEM PIN. This threat is countered by OT_CONF, OT_PRS_MSG, OE_GEM_PIN and OE_KEC_TEMP objectives. OT_CONF objective makes sure that TOE keeps GEM PIN encrypted during storage and data transfer. OT_PRS_MSG objective requires TOE displays personal message of the user stored in TCKK in a secure area, before the user enters PIN. OE_KEC_TEMP objective requires the device will erase GEM PIN so that it needs initialization by authorized service personnel. OE_GEM_PIN objective is to unable the threat agent to learn GEM PIN from users.

T_SC This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent inserts a fake TCKK to KEC to get a TOE service in an unauthorized way. This threat is countered by OT_TCKK_AUTH, OT_AUDIT and OE_SCARD objectives. OT_TCKK_AUTH objective requires each TCKK to be authenticated before any operation is performed. OT_AUDIT objective is for auditing smartcard authentication failures. Finally, with OE_SCARD objective, TCKK cannot be copied.

T_GSP This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent uses a fake GSP to connect to TOE or modifies the critical data transferred between GSP and TOE such as policy information. This threat is countered by OT_CONF, OT_GSP_AUTH, OT_AUDIT and OE_GSP objectives. OT_GSP_AUTH objective requires authentication of GSP during

connections while OT_CONF objective necessitates a secure communication between TOE and GSP. OT_AUDIT objective is for auditing GSP connection and operation failures. Finally, with OE_GSP environment objective, it is assured that private key of GSP certificate is kept secret.

T_EXT_DEV This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a thread agent connects a modified pinpad or a modified external biometric device to TOE to collect PIN or biometric information or modifies the data sent by an authorized external pinpad or an authorized external biometric device in order obtain a TOE service in an unauthorized way. This threat is countered by OT_CONF, OT_DEV_AUTH, OT_AUDIT, OE_PRS_MSG and OE_EXT_DEV objectives. OT_DEV_AUTH objective requires authentication of the external device while OT_CONF objective necessitates a secure communication between TOE and external device. OT_AUDIT objective is for operation logs regarding connection information and failures. By OE_PRS_MSG environment objective, external pinpad device has to display personal message of the user stored in TCKK in a secure area before the user enters PIN. Finally, OE_EXT_DEV environment objective ensures that the external device has necessary security measure to be authenticated by TOE and private key within the external device is kept secret.

T_OCSPS This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when the TOE receives data packets singed by a fake OCSPS or modified by a thread agent. This threat is countered by OT_SIGN_OCSP, OT_AUDIT and OE_OCSPS objectives. OT_SIGN_OCSP objective assures that the data comes from an authorized OCSP server. OT_AUDIT objective is for reporting errors related to OCSP operations. Finally, by OE_OCSPS environment objective, it is assured that private key of OCSPS certificate is kept secret.

T_SPS This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent sends the TOE software upgrade packets singed by a fake SPS or modifies original software upgrade

packets sent by an authorized SPS in order to modify TOE to achieve sensitive data. This threat is countered by OT_CONF, OT_UPGRADE, OT_AUDIT and OE_SPS objectives. OT_CONF objective requires confidentiality of software upgrade packets through secure communication between TOE and GSP/OYA/WIA. By OT_UPGRADE objective, authorization of any software upgrade packet sent by SPS is obliged. OT_AUDIT objective is for reporting errors related to software upgrade operations. Finally, by OE_SPS environment objective, it is assured that private key of SPS certificate is kept secret.

T_STOLEN_SC This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent steals someone's TCKK and uses it to claim a TOE service in an unauthorized way. This threat is countered by OT_USER_AUTH, OT_AUDIT and OE_USR_AWR objectives. OT_USER_AUTH requires user authentication. OT_AUDIT objective is for reporting user authentication failures. Finally, OE_USR_AWR objective assures that users are aware of the importance of confidentiality of their TCKK, PIN and PUK.

T_MNTR This threat is especially applicable to "USE" phases of TOE life-cycle. The threat is realized by unauthorized monitoring of data transacted between TOE and other entities such as TCKK, GEM, GSP and Externally Connected Trusted Device to discover security relevant data. This threat is countered by OT_CONF objective. OT_CONF objective requires securing the communication between TOE and external entities.

T_PNTR This threat is especially applicable to "USE" phases of TOE life-cycle. The threat happens when a threat agent gets inside of KEC opening the device cover to insert a PIN enclosing bug or modify TOE. It is countered by OT_INTEGRITY, OT_CONF and OE_KEC_TEMP objectives. OT_INTEGRITY objective is to provide means of detecting loss of integrity for security relevant information stored within the device, OT_CONF objective ensures confidentiality of security relevant information that TOE manages during storage and use. OE_KEC_TEMP objective necessitates the ability to detect unauthorized opening of TOE.

T_REPU This threat is especially applicable to "USE" phase of TOE life-cycle. The threat is repudiation of an operation performed by a user. This threat is countered by OT_NON_REPU, OT_USER_AUTH, OT_GEM_AUTH, OT_AUDIT, OE_KEC_RTC and OE_GEM_SIGN objectives. OT_NON_REPU is to assure that TOE provides evidence of identity of origin, location of origin, and time of origin for each sign operation. To do this, OT_USER_AUTH objective provides proof of user identity, OT_GEM AUTH objective provides proof of device and location, OE_GEM_SIGN objective provides location of origin, and OE_KEC_RTC objective provides time of origin. Finally, OT_AUDIT objective is for logging each operation performed by TOE.

T_RMODIF This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent connects to TOE from a remote location to modify it. This is dangerous, because modified TOE may send some critical data in plain format or the security functions might be disabled. This threat is countered by OT_INTEGRITY, OT_CONF and OT_AUDIT objectives. OT_ INTEGRITY objective assures integrity of TOE. By OT_CONF, confidentiality of TOE stored in non-volatile memory is guaranteed. OT_AUDIT objectives require TOE records events of unauthorized connection and TOE modification.

T_CVCTIME This threat is especially applicable to "USE" phase of TOE life-cycle. The threat happens when a threat agent uses a cancelled GEM card (before its CVC certificate is expired) to produce a fake KEC. This threat is countered by OT_CVCTIME and OE_CVCTIME objectives. OT_CVCTIME objective requires that TOE updates CVC certificates of GEM card before it expires. OE_CVCTIME objective assures that expiration time of CVC certificate in GEM is short enough.

4.4 Mapping of Security Objectives To Device Classifications

Securtiy objectives are mapped to device classes in the following table.

Objectives	Class 1	Class 2	Class 3
OT_INTEGRITY	✓	✓	✓
OT_CONF	✓	✓	✓
OT_NON_REPU	✓	✓	✓
OT_USER_AUTH	✓	✓	✓
OT_TCKK_AUTH	✓	✓	✓
OT_GEM_AUTH	✓	✓	✓
OT_GSP_AUTH	NA	✓	✓
OT_DEV_AUTH	NA	NA	✓
OT_UPGRADE	✓	✓	✓
OT_AUDIT	✓	✓	✓
OT_PRS_MSG	✓	✓	✓
OT_CVCTIME	✓	✓	✓
OT_ENTRY	✓	✓	✓
OT_SIGN_OCSP	✓	✓	✓
OE_USR_AWR	✓	✓	✓
OE_SCARD	✓	✓	✓
OE_PROCED	✓	✓	✓
OE_PROTECT	✓	✓	✓
OE_PC	✓	✓	✓
OE_EXT_DEV	✓	✓	✓
OE_GSP	NA	✓	✓
OE_OCSPS	✓	✓	✓
OE_SPS	✓	✓	✓
OE_ACCESS	✓	✓	✓
OE_KEC_TEMP	✓	✓	✓
OE_KEC_RTC	✓	✓	✓
OE_GEM_PIN	✓	✓	✓
OE_AUTH_SRV	✓	✓	✓
OE_CVCTIME	✓	✓	✓
OE_PRS_MSG	✓	✓	✓
OE_GEM_SIGN	✓	✓	✓

NA: not applicable

Table 4. Mapping of security objectives to device classifications

5. EXTENDED COMPONENTS DEFINITION

Since this PP has a conformance claim to CC part 2 and 3, this section is not applicable.

6. SECURITY REQUIREMENTS

6.1 Security Functional Requirements for the TOE

This chapter defines the security functional requirements for the TOE according to the functional requirements components drawn from the CC part 2 version 3.1 rev 3.

Class FAU: Security Audit

The Security audit data generation family includes requirements to specify the audit events that should be generated by the TSF for security-relevant events.

Security Alarms (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall take [assignment: *list of actions*] upon detection of a potential security violation.

list of actions:

- get into OUT OF SERVISE mode
- inform the user

Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection, choose one of: *minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

other specifically defined auditable events:

- GEM authentication failure
- wrong PIN entry for GEM
- TCKK authentication failure
- cardholder verification failure
- GSP authentication failure
- Externally Connected Trusted Device authentication failure
- online certificate status control failure

- integrity check error
- digital signature verification failure
- KD operations

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]

User Identity Association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Potential Violation Analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

- Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

  subset of defined auditable events:

  - GEM authentication failure
  - wrong PIN entry for GEM
  - integrity check error
- [assignment: *any other rules*].

Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Selectable Audit Review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [assignment: *methods of selection and/or ordering*] of audit data based on [assignment: *criteria with logical relations*].

Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [selection, choose one of: *prevent, detect*] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] stored audit records will be maintained when the following conditions occur: [selection**:** *audit storage exhaustion, failure, attack*].

Prevention of Audit Data Loss (FAU_STG.4)

FAU_ STG.4.1 The TSF shall *overwrite the oldest stored audit records* and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

Class FCO: Communication

Enforced Proof of Origin (FCO_NRO.2)

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: *list of information types*] at all times.

list of information types:

- KDB

FCO_NRO.2.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] of the information to which the evidence applies.

list of attributes:

- identity of origin
- time of origin

- location of origin

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to *recipient, [assignment: list of third parties]* given *no limitations*.

list of third parties:

- the association that gives the service
- legal body

Class FCS: Cryptographic Support

Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1/a TCKK Communication

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic key generation algorithm:

- session key generation for the communication between KEC and TCKK

cryptographic key sizes:

- 256-bit symmetric session key

list of standards:

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_CKM.1/b GEM Communication

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic key generation algorithm:

- session key generation for the communication between KEC and GEM

cryptographic key sizes:

- 256-bit symmetric session key

list of standards:

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_CKM.1/c Rol Certificate Holder Communication

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic key generation algorithm:

- session key generation for the communication between KEC and Role Certificate Holder

cryptographic key sizes:

- 256-bit symmetric session key

list of standards:

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_CKM.1/d GSP Communication

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic key generation algorithm:

- session key generation for the communication between KEC and GSP

cryptographic key sizes:

- 256-bit symmetric session key

list of standards:

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_CKM.1/e Externally Connected Trusted Device Communication

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic key generation algorithm:

- the session key generation for the communication between KEC and Externally Connected Trusted Devices

cryptographic key sizes:

- 256-bit symmetric session key

list of standards:

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

cryptographic key destruction method:

- Session key: Delete after use

Cryptographic Operation (FCS_COP.1)

FCS_COP.1/a Data Encryption and Decryption

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment:

cryptographic algorithm] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Data encryption/decryption

cryptographic algorithm:

- AES
- RSA

cryptographic key sizes:

- 256-bit key for AES
- 2048-bit key for RSA

list of standards:

- Advanced Ecryption Standard – FIPS 197
- Recommendation for Block Cipher Modes of Operation - NIST SP800-38A
- RSA Cryptography Standard - PKCS #1 v2.1
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/b Hash Computaiton

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure hash (message digest) computation

cryptographic algorithm:

- HMAC-SHA

cryptographic key sizes:

- 256-bit

list of standards:

- Secure Hash Standard - FIPS 180-3
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/c Digital Signature Verification

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Digital Signature Verification

cryptographic algorithm:

- RSA

cryptographic key sizes:

- 2048-bit

list of standards:

- RSA Cryptography Standard - PKCS #1 v2.1
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/d Secure Messaging with TCKK

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure messaging with TCKK

cryptographic algorithm:

- AES for data encryption/decryption
- RSA for key agreement

cryptographic key sizes:

- 256-bit key for AES
- 2048-bit key for RSA

list of standards:

- Advanced Ecryption Standard – FIPS 197
- RSA Cryptography Standard - PKCS #1 v2.1
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/e Secure Communication with GEM

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure messaging with GEM

cryptographic algorithm:

- AES for data encryption/decryption
- RSA for key agreement

cryptographic key sizes:

- 256-bit key for AES
- 2048-bit key for RSA

list of standards:

- Advanced Ecryption Standard – FIPS 197
- RSA Cryptography Standard - PKCS #1 v2.1
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/f Secure Communication with Role Certificate Holder

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment:

cryptographic key sizes] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure communication with role certificate holder

cryptographic algorithm:

- AES for data encryption/decryption
- RSA for key agreement

cryptographic key sizes:

- 256-bit key for AES
- 2048-bit key for RSA

list of standards:

- Advanced Ecryption Standard – FIPS 197
- RSA Cryptography Standard - PKCS #1 v2.1
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/g Secure Communication with GSP

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure socket communication

cryptographic algorithm:

- TLS v1.0

cryptographic key sizes:

- 256-bit key for data encrption/decryption
- 2048-bit key for key agreement

list of standards:

- RFC 5246 (The Transport Layer Security Protocol)

- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

FCS_COP.1/h Secure Communication with External Trusted Devices

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

cryptographic operations:

- Secure communication with external pinpad/biometric sensor

cryptographic algorithm:

- AES for data encryption/decryption
- RSA for key agreement

cryptographic key sizes:

- 256-bit key for AES
- 2048-bit key for RSA

list of standards:

- RFC 5246 (The Transport Layer Security Protocol)
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications [5]

Class FDP: User Data Protection

Basic Data Authentication (FDP_DAU.1)

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects*].

list of objects:

- GEM PIN
- CTN

FDP_DAU.1.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

list of subjects:

- user

Class FIA: Identification and Authentication

Authentication Failure Handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when *[assignment: positive integer number]* unsuccessful authentication attempts occur related to [assignment: *list of authentication evets*].

positive integer number:

- three

list of authentication events:

- user PIN verification

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [assignment: *list of actions*].

list of actions:

- cancel the operation
- display a message
- audit the event

Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

list of TSF mediated actions:

- authenticaiton and secure communcation with GEM
- authentication and secure messaging with TCKK

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Unforgeable Authentication (FIA_UAU.3)

FIA_UAU.3.1 The TSF shall *prevent* use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall *prevent* use of authentication data that has been copied from any other user of the TSF.

Single Use Authentication Mechanism (FIA_UAU.4)

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanisms*].

identified authentication mechanisms:

- authenticaiton of GEM
- authentication of TCKK
- authentication of GSP
- authentication of External Trusted Devices

Multiple Authentication Mechanism (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.

list of multiple authentication mechanisms:

- authenticaiton and secure communication with GEM
- authentication and secure messaging with TCKK
- verification of KD certificate
- digital photograph verification
- PIN verification
- biometric data verification

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].

rules describing how the multiple authentication mechanisms provide authentication:

- Secure Card Access Devices for T.C. Identity Cards — Part 4: KEC Application Software Specifications [5]

Re-Authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].

list of conditions under which re-authentication is required:

- each KD operation

Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.

list of feedback:

- result of the authentication
- reason of failure if it fails

Timing of Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is identified.

list of TSF mediated actions:

- authenticaiton and secure communcation with GEM
- authenticaiton and secure messaging with TCKK

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Class FPT: Protection of the TSF

Inter-TSF Confidentiality During Transmission (FPT_ITC.1)

FPT_ITC.1.1 The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.

Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Inter-TSF Basic TSF Data Consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.

list of TSF data types:

- TSF data types described in [5]

FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

list of interpretation rules to be applied by the TSF:

- the interpretation rules to be applied by the TSF are described in [5]

Class FTP: Trusted Path/Channels

Inter-TSF Trusted Channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*].

list of functions for which a trusted channel is required:

- *data exchange with GEM*
- *data exchange with TCKK*
- *data exchange with GSP*
- *data exchange with remote role certificate holder*
- *data exchange with external biometric devices*
- *data exchange with external pinpad devices*

6.2 Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following component:

- ALC_DVS.2 (Sufficiency of security measures)

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements rationale

The following table provides an overview for security functional requirements coverage also giving an evidence for *sufficiency* and *necessity* of the SFRs chosen.

	OT_INTEGRITY	OT_CONF	OT_NON_REPU	OT_USER_AUTH	OT_TCKK_AUTH	OT_GEM_AUTH	OT_GSP_AUTH	OT_DEV_AUTH	OT_UPGRADE	OT_AUDIT	OT_PRS_MSG	OT_CVCTIME	OT_ENTRY	OT_SIGN_OCSP
FAU_ARP.1										✓				
FAU_GEN.1										✓				
FAU_GEN.2										✓				
FAU_SAA.1										✓				
FAU_SAR.1										✓				
FAU_SAR.3										✓				
FAU_STG.2										✓				
FAU_STG.4										✓				
FCO_NRO.2			✓											
FCS_CKM.1/a		✓												
FCS_CKM.1/b		✓												
FCS_CKM.1/c		✓												
FCS_CKM.1/d		✓												
FCS_CKM.1/e		✓												
FCS_CKM.4		✓												
FCS_COP.1/a		✓												
FCS_COP.1/b	✓													
FCS_COP.1/c				✓	✓	✓	✓	✓	✓			✓		✓
FCS_COP.1/d		✓												
FCS_COP.1/e		✓												
FCS_COP.1/f		✓												
FCS_COP.1/g		✓												
FCS_COP.1/h		✓												
FDP_DAU.1	✓													
FIA_AFL.1				✓										
FIA_UAU.1				✓										
FIA_UAU.3					✓	✓	✓	✓						
FIA_UAU.4					✓	✓	✓	✓						
FIA_UAU.5				✓										
FIA_UAU.6				✓	✓	✓								
FIA_UAU.7				✓									✓	
FIA_UID.1				✓										
FPT_ITC.1		✓									✓			
FPT_STM.1			✓							✓				
FPT_TDC.1		✓												
FTP_ITC.1		✓									✓			

Table 5. Mapping of TOE SFRs to TOE security objectives

OT_INTEGRITY This objective is satisfied by FCS_COP.1/b and FDP_DAU.1 SFRs. FDP_DAU.1 requires the functions to generate and verify evidence that can be used as a guarantee of the validity of security relevant data stored within the TOE. FCS_COP.1/b is for hash calculation to provide integrity check.

OT_CONF This objective is satisfied by FCS_CKM.1/a, FCS_CKM.1/b, FCS_CKM.1/c, FCS_CKM.1/d, FCS_CKM.1/e, FCS_CKM.4, FCS_COP.1/a, FCS_COP.1/d, FCS_COP.1/e, FCS_COP.1/f, FCS_COP.1/g, FCS_COP.1/h, FPT_ITC.1, FPT_TDC.1 and FTP_ITC.1 SFRs. FCS_CKM.1/a/b/c/d/e SFRs are for key generation that will be used for secure communication with TCKK/GEM/GSP, role certificate holder and external pinpad/biometric sensor. FCS_CKM.4 provides destruction of session keys after use. FCS_COP.1/d/e/f/g/h SFRs provides key agreement protocol with TCKK/GEM/GSP, role certificate holder and external pinpad/biometric sensor. FCS_COP.1/a is for encryption and decryption between the TOE and these other trusted IT products. FTP_ITC.1 provides confidentiality of transmitted data between TOE and TCKK/GEM, GSP, external biometric sensor or other trusted IT product. FPT_TDC.1 is for data consistency between TOE and other external trusted entities. Finally, FTP_ITC.1 defines a trusted channel between them assuring identification of its end points.

OT_NON_REPU This objective is satisfied by FCO_NRO.2 and FPT_STM.1 SFRs. FCO_NRO.2 requires the functions to generate and verify evidence of origin for KDB, KB. FPT_STM.1 provides reliable time stamps for KD operations.

OT_USER_AUTH This objective is satisfied by FCS_COP.1/c, FIA_AFL.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7 and FIA_UID.1 SFRs. FCS_COP.1/c is for signature verification operations. FIA_UAU.5 provides requirements to support user authentication. FIA_UAU.6 defines the conditions to re-authenticate users. FIA_UAU.7 is for protection of feedback information during user PIN or biometric data entry. FIA_AFL.1 SFRs are for describing user authentication failure

situations and course of action taken by TOE. FAU_UAU.1 is for timing of user authentication and FIA_UID.1 is for timing of user identification.

OT_TCKK_AUTH This objective is satisfied by FCS_COP.1/c, FIA_UAU.3, FIA_UAU.4 and FIA_UAU.6 SFRs. FCS_COP.1/c is for signature verification operations. FIA_UAU.3, FIA_UAU.4 and FIA_UAU.6 SFRs are the requirements to provide TCKK authentication.

OT_GEM_AUTH This objective is satisfied by FCS_COP.1/c, FIA_UAU.3, FIA_UAU.4 and FIA_UAU.6 SFRs. FCS_COP.1/c is for signature verification operations. FIA_UAU.3, FIA_UAU.4 and FIA_UAU.6 SFRs are the requirements to provide GEM authentication.

OT_GSP_AUTH This objective is satisfied by FCS_COP.1/c, FIA_UAU.3 and FIA_UAU.4 SFRs. FCS_COP.1/c is for signature verification operations. FIA_UAU.3 and FIA_UAU.4 SFRs are the requirements to provide GSP authentication.

OT_DEV_AUTH This objective is satisfied by FCS_COP.1/c, FIA_UAU.3 and FIA_UAU.4 SFRs. FCS_COP.1/c is for signature verification operations. FIA_UAU.3 and FIA_UAU.4 SFRs are the requirements to provide Externally Connected Trusted Device authentication.

OT_UPGRADE This objective is satisfied by FCS_COP.1/c SFR. FCS_COP.1/c requires necessary cryptographic operations to verify the signature of software upgrade packets.

OT_AUDIT This objective is satisfied by FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.2 and FAU_STG.4 SFRs. FAU_ARP.1 defines the actions in case a potential security violation is detected. FAU_GEN.1 defines the level of auditable events, and specifies the list of data that shall be recorded in each record. FAU_GEN.2 defines how audit records are associated with individual users. FAU_SAA.1 is for detecting security violations by monitoring the listed events in FAU_SAA.1 description. FAU_SAR.1 defines the capability to read audit information from the audit records. FAU_SAR.3 states that there will be methods of ordering based on time of origin for audit records.FAU_STG.2 defines the requirement for protecting audit

records from unauthorized deletion and modification, Finally, FAU_STG.4 is the requirement for preventing data loss in case the audit trail is full.

OT_PRS_MSG This objective is satisfied by FPT_ITC.1 and FTP_ITC.1 SFRs. FPT_ITC.1 provides confidentiality of data transferred between TOE and TCKK. FTP_ITC.1 provides a trusted communication channel between TOE and TCKK assuring identification of of its end points.

OT_CVCTIME This objective is satisfied by FCS_COP.1/c SFR. FCS_COP.1/c requires necessary cryptographic operations to verify the signature of new certificates that will be replaced with old GEM certificate.

OT_ENTRY This objective is satisfied by FIA_UAU.7 SFR.

OT_SIGN_OCSP This objective is satisfied by FCS_COP.1/c SFR. FCS_COP.1/c requires necessary cryptographic operations to verify the signature of OCSPS.

6.3.2 Rationale for SFR's Dependencies

The selected security functional requirements include related dependencies. Table 6 below provides a summary of the TOE security functional requirements dependency analysis.

Table 6. TOE Security Functional Requirements Dependencies

Component	Dependencies	Which is:
FAU_ARP.1	FAU_SAA.1	Included
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1	Included
	FIA_UID.1	Included
FAU_SAA.1	FAU_GEN.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_SAR.3	FAU_SAR.1	Included
FAU_STG.2	FAU_GEN.1	Included
FAU_STG.4	FAU_STG.1	FAU_STG.2 Included FAU_STG.2 is hierarchical to FAU_STG.1
FCO_NRO.2	FIA_UID.1	Included
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1 Included
	FCS_CKM.4	Included
FCS_COP.1	FCS_CKM.4	Included
	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1 included
FDP_DAU.1	None	-
FIA_AFL.1	FIA_UAU.1	Included
FIA_UAU.1	FIA_UID.1	Included
FIA_UAU.3	None	-
FIA_UAU.4	None	-
FIA_UAU.5	None	-
FIA_UAU.6	None	-
FIA_UAU.7	FIA_UAU.1	Included
FIA_UID.1	None	-
FPT_ITC.1	None	-
FPT_STM.1	None	-
FPT_TDC.1	None	-
FTP_ITC.1	None	-

6.3.3 Security Assurance Requirements Rationale

The current assurance package was chosen based on the pre-defined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the KEC's development and manufacturing, especially for the secure handling of sensitive material.

The set of assurance requirements being part of EAL4 fulfils all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance component and it does not any dependency:

- ALC_DVS.2. (No dependency)

6.3.4 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual supportiveness and internal consistency demonstrates:

- The dependency analysis in section 6.3.2 'Rationale for SFR's Dependencies' for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.
- All subjects and objects addressed by more than one SFR in section 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these 'shared' items.

- The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.3 'Security Assurance Requirements Rationale' shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.2 'Rationale for SFR's Dependencies' and 6.3.3 'Security Assurance Requirements Rationale'. Furthermore, as also discussed in section 6.3.3 'Security Assurance Requirements Rationale', the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

6.4 Mapping of SFR's To Device Classifications

SFR's are defined in the table as to device classification.

SFR	Class 1	Class 2	Class 3
FAU_ARP.1	✓	✓	✓
FAU_GEN.1	✓	✓	✓
FAU_GEN.2	✓	✓	✓
FAU_SAA.1	✓	✓	✓
FAU_SAR.1	✓	✓	✓
FAU_SAR.3	✓	✓	✓
FAU_STG.2	✓	✓	✓
FAU_STG.4	✓	✓	✓
FCO_NRO.2	✓	✓	✓
FCS_CKM.1/a	✓	✓	✓
FCS_CKM.1/b	✓	✓	✓
FCS_CKM.1/c	✓	✓	✓
FCS_CKM.1/d	NA	✓	✓
FCS_CKM.1/e	NA	NA	✓
FCS_CKM.4	✓	✓	✓
FCS_COP.1/a	✓	✓	✓
FCS_COP.1/b	✓	✓	✓
FCS_COP.1/c	✓	✓	✓
FCS_COP.1/d	✓	✓	✓
FCS_COP.1/e	✓	✓	✓
FCS_COP.1/f	✓	✓	✓
FCS_COP.1/g	NA	✓	✓
FCS_COP.1/h	NA	NA	✓
FDP_DAU.1	✓	✓	✓
FIA_AFL.1	✓	✓	✓
FIA_UAU.1	✓	✓	✓
FIA_UAU.3	✓	✓	✓
FIA_UAU.4	✓	✓	✓
FIA_UAU.5	✓	✓	✓
FIA_UAU.6	✓	✓	✓
FIA_UAU.7	✓	✓	✓
FIA_UID.1	✓	✓	✓
FPT_ITC.1	✓	✓	✓
FPT_STM.1	✓	✓	✓
FPT_TDC.1	✓	✓	✓
FTP_ITC.1	✓	✓	✓

NA: not applicable

Table 7. Mapping of SFR's to device classifications

7. ACRONYMS

AES	Advanced Encryption Standard
BİLGEM	Bilgi ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
CC	Common Criteria
CPU	Central Processing Unit
CTN	Cihaz Takip Numarası (Device Track Number)
EAL	Evaluation Assurance Level
TCKK	Türkiye Cumhuriyeti Kimlik Kartı (Turkish Republic Identity Card)
EKDS	Elektronik Kimlik Doğrulama Sistemi (Electronic Identity Verification System)
GEM	Güvenli Erişim Modülü (Secure Access Module)
GSP	Güvenlik Servisleri Platformu (Security Services Platform)
HMAC	Hash Message Authentication Code
IC	Integrated Circuit
KD	Kimlik Doğrulama (Identity Verification)
KDB	Kimlik Doğrulama Bildirimi (Identity Verification Assertion)
KDP	Kimlik Doğrulama Politikası (Identity Verification Policy)
KDPS	Kimlik Doğrulama Politika Sunucusu (Identity Verification Policy Server)
KDS	Kimlik Doğrulama Sunucusu (Identity Verification Server)
KEC	Kart Erişim Cihazı (Elektronic Identity Card Access Device)
KECÖB	Kart Erişim Cihazı Özelleştirme Birimi (KEC Personalization Unit)
OCSP	Online Certificate Status Protocol
OCSPS	Online Certificate Status Protocol Server
OYA	Otomasyon Yazılımı Arabirimi (Automation Software Interface)
PIN	Personal Identification Number
RSA	Rivest – Shamir – Adleman (RSA Algorithm)
RTC	Real Time Clock
SC	Smartcard
SFR	Security Functional Requirement
SPS	Software Publisher Server
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (Scientific and Technologic Research Association of Turkey)
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (National Research Institute of Electronics and Cryptology)
USB	Universal Serial Bus
WIA	Web İstemci Arabirimi (Web Client Interface)

8. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2009-07-001, Version 3.1, Revision 3, July 2009

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2009-07-002, Version 3.1, Revision 3, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2009-07-003, Version 3.1, Revision 3, July 2009

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2009-07-004, Version 3.1, Revision 3, July 2009

[5] TSE-Product Certification Center-Information Technology-CCCS Beneficial Documents: (http://tse.tse.org.tr/kalitedoc/ubmdb/bilgi_teknolojisi/ok.htm)

- Secure Card Access Devices for Turkish National Identity Cards — Part 1: Overview
- Secure Card Access Devices for Turkish National Identity Cards — Part 2: Interfaces and their characteristics
- Secure Card Access Devices for T.C. Identity Cards — Part 3: Security Specifications
- Secure Card Access Devices for T.C. Identity Cards — Part 4: KEC Application Software Specifications