Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

UDEA ELEKTRONİK SAN. TİC. A.Ş

SSR_Core v1.0

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-64

TABLE OF CONTENTS

Document Information

Date of Issue	*30.01.2020*
Approval Date	*31.01.2020*
Certification Report Number	*21.0.03/20-001*
Sponsor and Developer	*UDEA ELEKTRONİK SAN. TİC. A.Ş*
Evaluation Facility	*BEAM Teknoloji A.Ş*
TOE	*SSR_Core v1.0*
Pages	25

Prepared by	*Halime Eda BİTLİSLİ ERDİVAN*
Reviewed by	*İbrahim Halil KIRMIZI*

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	*30.01.2020*	*All*	*First Release*

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformant to Common Criteria for IT Security Evaluation, *version 3.1*, *revision 5*, using Common Methodology for IT Products Evaluation, *version 3.1*, *revision 5*. 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.

FOREWORD

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

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

CCTL 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 CCTL has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by, BEAM Teknoloji A.Ş which is a commercial CCTL.

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

This certification report is associated with the Common Criteria Certificate issued by the CCCS for *SSR_Core v1.0* whose evaluation was completed on *16.01.2020* and whose evaluation technical report was drawn up by *16.01.2020* (as CCTL), and with the Security Target document with version no 2.10 of the relevant product.

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

RECOGNITION OF THE CERTIFICATE

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

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL2. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org

1. EXECUTIVE SUMMARY

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

Evaluated IT product name: SSR_Core

IT Product version: 1.0

Developer's Name: UDEA ELEKTRONİK SAN. TİC. A.Ş

Name of CCTL: BEAM Teknoloji A.Ş

Assurance Package: EAL 4+ (ALC_DVS.2)

Completion date of evaluation: *16.01.2020*

1.1. Brief Description

The TOE is the Secure Smartcard Reader (SSR) Application Firmware running on SSR Device. The SSR is the identity verification terminal for the National eID Verification System (eIT.DVS).

As the application firmware which is run on microcontroller of the SSR, the TOE performs identity verification of Service Requester and Service Attendee according to the eIDVS, securely communicating with the other system components and as a result of the identity verification, produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the SRR. The root certificates used for the identification & authentication purposes are also covered by the TOE.

The TOE covers type I and II(with SAS/without SAS) secure smart card reader.

1.2. Major Security Features

The TOE provides the following security services;

- Security Audit
- Identification, Authentication and Authorization
- User Data Protection
- Protection of the TSF
- Security Management
- Communication
- Cryptographic Support
- Trusted Path/Channels

1.3. Threats

The related threats are:

T.Counterfeit_eIDC	An attacker (Identity Faker) may present a counterfeit eID Card (form of illegitimate eID Card) to the TOE for faking his or her identity. This action is also regarded as damaging the correct operation of the Identification and Authentication of the Service Requester and the Service Attendee.
T.Revoked_eIDC	An attacker (Identity Faker) may present a revoked eID Card (form of illegitimate eID Card) to the TOE for faking his or her identity. This action is also regarded as damaging the correct operation of the Identification and Authentication of the Service Requester and the Service Attendee.

T.Stolen_eIDC	An attacker (Identity Faker) may present a stolen (not an illegitimate eID Card) to the TOE for faking his or her identity. This action is also regarded as damaging the correct operation of the Identification and Authentication of the Service Requester and the Service Attendee.
T.IVA_Fraud	An attacker may create a fraudulent Identity Verification Assertion IVA (totally fake, build from scratch, or modified from a legitimate IVA).
T.IVA_Eavesdropping (valid for Type II TOE)	The attacker may obtain Identity Verification Assertion by monitoring the communication line between SAS and type II TOE.
T.Repudiation	The Service Requester (or the Service Attendee) may repudiate the Identification Verification Assertion.
T.Fake_TOE_to_SR	An attacker may prepare a fake SSR Hardware and introduce it to the Service Requesters (and/or Service Attendee). This way, the attacker may collect the Identity Verification Card-PIN and Biometric Information.
T.Fake_TOE_to_External_Entities	An attacker may introduce himself/herself as legitimate TOE to the external entities: eID Card, External Biometric Sensor, External PIN Pad. Thus obtain the PIN and biometric information of the Service Requester (or the Service Attendee) and gain access to eID Card on behalf of the Role Holder.
T.SA_Masquerader	An attacker may act as if he/she is a legitimate service attendee and perform the photo verification and thus damage the Identification and Authentication Service of the Service Requester.

T.SA_Abuse_of_Session	An attacker may abuse the service attendee's authentication session. Thus the attacker can validate the photo and/or accept negative result of biometric verification in an unauthorized way. This action therefore is regarded as damaging the correct operation of the Identification and Authentication of the Service Requester and the Service Attendee.
T.Fake_Policy	An attacker may send a fraudulent policy to manage the authentication process in an unauthorized manner. This action is also regarded as damaging the correct operation of the Identification and Authentication of the SA and the SR.
T.Fake_OCSP_Response	An attacker may mimic a legitimate Online Certificate Status Protocol Server (OCSPS) or manipulate the TSF Data transmitted by OCSPS. This action is also regarded as damaging the correct operation of the Identification and Authentication of the SA and the SR.
T.RH_Comm	An attacker may access or modify the eID Card contents through eavesdropping and manipulating the communication between the Role Holder and eID Card.
T.RH_Session_Hijack	An attacker may access or modify the eID Card contents through hijacking the authentication session between the eID Card and the Role Holder.
T.Illegitimate_EBS	An attacker may change the outcome of biometric verification1 or steal or modify the transmitted biometric template, thus collect biometric information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee by using an illegitimate biometric sensor.

T.EBS_Comm	An attacker may change the outcome of biometric verification; steal or modify the transmitted biometric template, thus collect biometric information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee through (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between the TOE and the EBB.
T.Illegitimate_EPP	An attacker may steal or modify the transmitted PIN, thus collect PIN information from the Cardholders or damage the correct operation of the Identification and Authentication or Service Requester of Service Attendee by using an illegitimate external PIN-PAD.
T.EPP_Comm	An attacker may steal or modify the transmitted PIN, thus collect PIN information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee through (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between SSR and EPP.
T.eIDC_Comm	An attacker may access or modify the eID Card contents, steal the PIN and biometric information, block the PIN and biometric verification through (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between the TOE and eID Card.

T.Illegitimate_SAS	An attacker may use illegitimate SSR Access Server (SAS) to undermine security policies. This action is also regarded as damaging the correct operation of the Identification and Authentication of third party IT Components for TOE on SSR Type II.
T.DTN_Change	An attacker may change the Device Tracking Number of the TOE through physically gaining access to the memories. This also damage the correctness of the IVA generated by the TOE.
T.SAM-PIN_Theft	An attacker may read or change the SAM-PIN of the TOE during normal operation by physically accessing the SAM PIN memory area or while TOE is entering the SAM PIN, i.e. sending the SAM PIN to the SAM.
T.Audit_Data_Compromise	An attacker may read, change or delete the audit data.
T.TOE_Manipulation	An attacker may manipulate the operation or probe the internals of the SSR. SAM PIN could be obtained by probing the internals of the SSR, or DTN or Audit data could be manipulated. In addition, a counterfeit Identity Verification Assertion could be created.
T.Fake_SAM	An attacker may issue a fake SAM to obtain the SAM-PIN.
T.Stolen_SAM	An attacker may steal a SAM and use it to build an illegitimate SSR.
T.Revoked_SAM	An attacker may use a Revoked SAM to build an illegitimate SSR.

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	*21.0.03/TSE-CCCS-64*
TOE Name and Version	*SSR_Core v1.0*
Security Target Title	*Security Target for SSR_Core v1.0*
Security Target Version	*2.10*
Security Target Date	*15.01.2020*
Assurance Level	*EAL 4+(ALC_DVS.2)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017*

Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017*
Protection Profile Conformance	*Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for National Electronic Identity Verification System, SSR_PP_2.8*
Sponsor and Developer	*UDEA ELEKTRONİK SAN. TİC. A.Ş*
Evaluation Facility	*BEAM Teknoloji A.Ş*
Certification Scheme	*TSE CCCS*

2.2. Security Policy

Organizational Security Policies are listed below;

P.IVM_Management	The TOE shall apply the identity verification methods defined by the IVPS. Otherwise if IVPS is not present, identity verification methods defined by the SPCA shall be applied. In absence of those, the TOE shall apply the default policy which has the highest security level.
P.TOE_Upgrade	The TOE will have mechanisms for secure field and remote upgrade.
P.Re-Authentication	Authentication of third party IT components will be renewed after 24 hours.

P.Revocation_Control	In case SSR Device cannot reach to OCSP Server, downloading the Revocation List onto the SSR Device and checking the certificate revocation status of the Service Requester (and the Service Attendee if applicable) from this list is allowed. The revocation list shall be up to date. When the certificate revocation check is carried out without OCSP Server, the information regarding that OCSP check could not be realized shall be put in the IVA. If the OCSP Server is not reached and there is no downloaded revocation list, then the information that OCSP check and revocation list control could not be realized shall be put in the IVA. In this case, only the certificate status control is performed offline, other identity verification steps shall be performed online. Unless IVA is validated at IVS and revocation check is completed, Identity Verification is not regarded as completed.
P.Tamper_Response	The SSR platform will be able to detect any tampering attempts and will notify the TOE. The TOE will respond to this notification by securely deleting the SAM-PIN and getting into Initialization & Configuration phase.
P.Terminal_Cert_Update	Terminal Certificate will be renewed within a period defined in TS 13584 [3]. Client application (for TOE on SSR type I or II), SSR Access Server (for TOE on Type II with SAS) or Application Server (for TOE on SSR Type III) shall update the Secure Messaging and Role Card Verifiable Certificates of SAM one day before the expiration day.
P.Time_Update	The time shall be updated using the real time that is received only from trusted entities.

P.DPM	The TOE shall support Initialization & Configuration and Operation lifecycle phases. The phase change shall be from Initialization & Configuration Phase to Operation Phase except tamper event detection case. If a tamper event is detected, TOE shall be out of service and require re-initialization. This shall be the only condition to go back to Initialization & Configuration Phase. DTN and SAM PIN shall be written to the SSR Device during Initialization & Configuration Phase.

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

A.SPCA	It is assumed that Service Provider Client Application is a trusted third party and its communication with SSR occurs in a secure environment via USB interface. However, for SSR Type II with SAS, there is no direct connection between the SSR and the SPCA, SPCA communicates to the SAS through Ethernet interface. When the Service Provider Client Application determines the identity verification method, it is assumed that the Service Provider Client Application selects the appropriate method. In addition, integrity and the confidentiality of the private data transferred from SSR Device to the Client Application is preserved by the foundation sustaining the Client Application
A.IVPS	It is assumed that the IVPS prepares and sends the policy correctly.
A.EBS-EPP	It is assumed that legitimate External Biometric Sensor (EBS) and legitimate External Pin Pad (EPP) work correctly.
A.PC	It is assumed that the PC executing the Client Application is malicious code free and located in secure environment. In addition, the confidentiality of the

	private data that might be written into the IVA by the Application Owner as Application Specific Data is preserved by the Application Owner.
A.APS-IVPS	It is assumed that the Application Server and the Identity Verification Policy Server are malicious code free and located in secure environment.
A.Management_Environment	It is assumed that the environments, where initialization and configuration are performed, are secure. And the personal that hold initialization and configuration roles act responsively.
A.SAM_ PIN_Environment	It is assumed that the PIN value of the SAM in the SSR is defined in the SSR in secure environment.
A.SSR_Platform	The SSR platform supports the security functionality of the TOE and does not undermine the security properties of it. The SSR platform does not provide any opportunities to the attacker to manipulate or bypass the security functionality of the TOE. The TSF architecture is resistant against attacks that can be performed by attackers possessing Enhanced-Basic attack potential (AVA_VAN.3), it is assumed that SSR Platform does not offer any attack interface to the attacker with enhanced basic attack potential to break the TSF architecture. SSR Platform will store TOE encrypted during nonoperation times. SSR Platform will decrypt and authenticate the TOE during starting up the TOE.

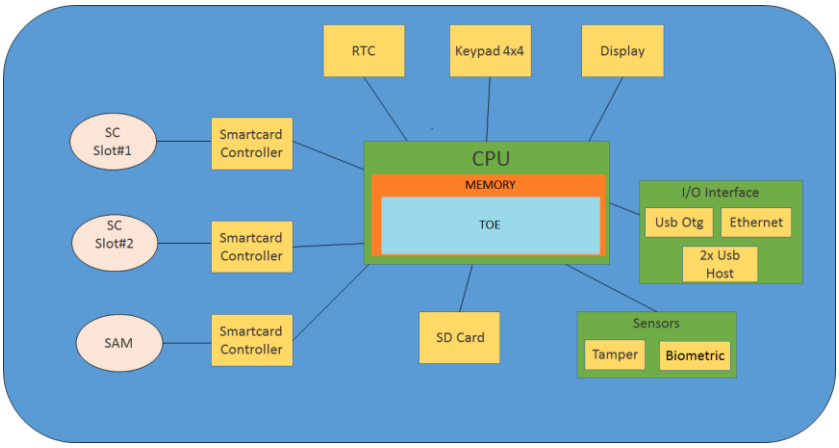
2.4. Architectural Information

The TOE is stored in a non-volatile memory location in the SSR Hardware as an encrypted binary file. During power-up, the encrypted TOE is decrypted before its execution.

The TOE runs at the top of an embedded Linux operating system and 528 MHz , ARM Cortex-A7 NXP Freescale imx6ul-2 microprocessor.

The physical scope of TOE is given below. TOE operates on memory while running in Operation Phase and cryptographic operations of TOE are performed on memory. Memory and CPU are combined in a single module. There are 3 card readers on the device, one for Service Requester, one for Service Attendee and one for SAM. There is an SD Card for extending memory on device. There is one fingerprint sensor

used for biometric validation and there are several sensors for detecting tamper event. There are two interfaces for communicating with Application Software, one is via Usb Otg and the other is via Ethernet. There are 2 Usb Hosts for external devices. There is a touch screen on the device for user interface and there are 16 keys on a 4x4 keypad. There exists a Real Time Clock for synchronizing time on device.



2.5. Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
Security Target for SSR_Core v1.0	*2.10*	*15.01.2020*
Operational User Manual	*1.6*	*13.01.2020*
Preparation Procedures	*1.2*	*22.01.2019*

2.6. IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections

between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report (ETR) of SSR_Core v1.0.

IT Product Testing is composed of two parts:

2.6.1. Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. Developer has conducted 24 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has conducted all 24 tests of developer and also has prepared 33 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.
- Penetration Testing: Evaluator has conducted 20 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes.

2.7. Evaluated Configuration

The evaluated TOE configuration is composed of;

- SSR_Core v1.0
- Guidance Documents

Also minimum Hardware/Software/OS requirements for the TOE are;

- Processor: Cortex-A7 @ 528MHz
- Flash Memory: 256 MB SLC NAND(Up to 2 GB NAND flash (SLC))
- RAM: 256 MB DDR3 (Up to 1 GB DDR3)
- Ethernet: 10/100 Mbit Ethernet MAC + IEEE 1588

- USB Connection: 2 Port USB 2.0 host, 1 Port USB 2.0 device
- LCD: 3.5" TFT LCD Capacitive Touch Screen, Resolution 320 x 240

2.8. Results of the Evaluation

Table 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

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.2	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction

Security Target Evaluation	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_DVS.2) 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 "SSR_Core v1.0", the results of the assessment of all evaluation tasks are "Pass".

2.9. Evaluator Comments / Recommendations

No recommendations have been communicated to CCCS by the evaluators related to the evaluation process of " SSR_Core v1.0" product, result of the evaluation, or the ETR.

3. SECURITY TARGET

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

Title: *Security Target for SSR_Core v1.0*

Version: *2.10*

Date of Document: *15.01.2020*

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

Title: *Security Target for SSR_Core v1.0*

Version: Lite

4. GLOSSARY

ADV : Assurance of Development

AES : Advanced Encryption Standard

APS : Application Server

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

APS : Application Server

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

CRL : Certificate Revocation List

CVC : Card Verifiable Certificate

DA : Device Authentication

DEL : Delivery

DES : Data Encryption Standard

DTN : Device Tracking Number

DVS : Development Security

EAL : Evaluation Assurance Level

EBS : External Biometric Sensor

eID : Electronic Identity

EPP : External Pin Pad

eIDMS : Electronic Identity Management System

eID Card : Electronic Identity Card

eIDVS : Electronic Identity Verification System

eSIGN : Electronic Signature

IV : Identity Verification

IVA : Identity Verification Assertion

IVC : Identity Verification Certificate

IVP : Identity Verification Policy

IVPS : Identity Verification Policy Server

IVR : Identity Verification Request

IVS : Identity Verification Server

IVSP : Identity Verification Specification

OCSPS : Online Certificate Status Protocol Server

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

PRE : Preperative Procedures

SAM : Security Access Module

SAR : Security Assurance Requirements

SAS : SSR Access Server

SFR : Security Functional Requirements

SPCA : Service Provider Client Application

SPSA : Service Provider Server Application

SSR : Card Acceptance Device

ST : Security Target

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017,

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: February 8th 2016

[4] Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Identity Verification System TSE-CCCS/PP-012, version 2.8, August 10th 2017

[5] TS 13584 - Elektronik Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı - Bölüm-3: Güvenlik Özellikleri (Secure Smart Card Reader Standard - Part-3: Security Properties), 2017, Türk Standartları Enstitüsü

6. ANNEXES

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