	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No



Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

ETB Elektronik Teknoloji ve Bilişim Hizmetleri San. Tic. Ltd. Şti.

E-Bio KEC - Secure Smartcard Readers Firmware v1.1

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: 21.0.03/TSE-CCCS-60



	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No 05



TABLE OF CONTENTS

TABLE OF CONTENTS	2
DOCUMENT INFORMATION.....	3
DOCUMENT CHANGE LOG.....	3
DISCLAIMER.....	4
FOREWORD	5
RECOGNITION OF THE CERTIFICATE.....	6
1 - EXECUTIVE SUMMARY.....	7
1.1 TOE Overview	7
1.2 Threats	7
2 CERTIFICATION RESULTS.....	8
2.1 Identification of Target of Evaluation	8
2.2 Security Policy.....	8
2.3 Assumptions and Clarification of Scope	8
2.4 Architectural Information	9
2.4.1 Logical Scope	9
2.4.2 Physical Scope	11
2.5 Documentation.....	12
2.6 IT Product Testing	12
2.7 Evaluated Configuration	13
2.8 Results of the Evaluation	13
2.9 Evaluator Comments / Recommendations.....	14
3 SECURITY TARGET	15
4 BIBLIOGRAPHY	16

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

DOCUMENT INFORMATION


<i>Date of Issue</i>	July 9th, 2019
<i>Approval Date</i>	July 9th, 2019
<i>Certification Report Number</i>	21.0.03/18-006
<i>Sponsor and Developer</i>	ETB Elektronik Teknoloji ve Bilişim Hizmetleri San. Tic. Ltd. Şti.
<i>Evaluation Facility</i>	Beam Technology Test Center
<i>TOE</i>	E-Bio KEC - Secure Smartcard Readers Firmware v1.1
<i>Pages</i>	16

<i>Prepared by</i>	Cem ERDİVAN Common Criteria Inspection Expert	
<i>Reviewed by</i>	İbrahim Halil KIRMIZI Common Criteria Technical Responsible (Software Product Group)	

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


DOCUMENT CHANGE LOG

<i>Release</i>	<i>Date</i>	<i>Pages Affected</i>	<i>Remarks/Change Reference</i>
1.0	July 9th, 2019	All	First Release

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

DISCLAIMER

This certification report and the IT product in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 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. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

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

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by Beam Technology Testing Facility, 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 E-Bio KEC - Secure Smartcard Readers Firmware v1.1 whose evaluation was completed on July 5th, 2019 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 1.6 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).


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
		Yayın Tarihi	30/07/2015	
	CCCS CERTIFICATION REPORT	Revizyon Tarihi	29/04/2016	No

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>.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

1 - EXECUTIVE SUMMARY

1.1 TOE Overview

The TOE is the Secure Smartcard Reader (SSR) Application Firmware running on SSR Device. The SSR is the identity verification terminal for the eID Verification System (eIDVS) defined by TS 13584. As the application firmware 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 TOE also covers the root certificates used for the identification & authentication purposes.

The following security mechanisms are primarily mediated in the TOE:


- Identification and Authentication,
 - Cardholder verification by using PIN and biometrics (fingerprint, finger vein, or palm vein data).
 - Authentication of eID Card by the TOE,
 - Authentication of Role Holder by eID Card and by the TOE,
 - Authentication of SAM by the TOE and by eID Card,
 - Authentication of the TOE by SAM and by Card Holder (Service Requester and Service Attendee) and by external entities,
- Secure Communication between the TOE and
 - SAM
 - eID Card
 - Role Holder
 - other trusted IT Components
- Security Management,
- Self-Protection,
- Audit

Among the certificates used in the eID Verification System, certificates of the root CA, device management CA and eID management CA are included in the TOE.

TOE is the application firmware which is loaded into the embedded flash memory of E-Bio KEC. E-Bio KEC one of the terminal devices designed for eID Verification System. It provides personal identity verification and digital signature operations for smartcard based services over electronic media. E-Bio KEC will mainly used in public institutions like hospitals, pharmacies and banks.

1.2 Threats

Threats are provided in Table 5 of Security Target Document v1.6.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
		Yayın Tarihi	30/07/2015	
	CCCS CERTIFICATION REPORT	Revizyon Tarihi	29/04/2016	No

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation


<i>Certificate Number</i>	21.0.03/TSE-CCCS-60
<i>TOE Name and Version</i>	E-Bio KEC - Secure Smartcard Readers Firmware v1.1
<i>Security Target Title</i>	E-Bio KEC - Secure Smartcard Readers Firmware v1.1 Security Target
<i>Security Target Version</i>	V1.6
<i>Security Target Date</i>	February 22, 2019
<i>Assurance Level</i>	EAL4+ (ALC DVS.2)
<i>Criteria</i>	<ul style="list-style-type: none"> • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
<i>Methodology</i>	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
<i>Protection Profile Conformance</i>	Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for Electronic Identity Verification System, Version 2.8, 01.08.2017
<i>Common Criteria Conformance</i>	<ul style="list-style-type: none"> • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
<i>Sponsor and Developer</i>	ETB Elektronik Teknoloji ve Bilişim Hizmetleri San. Tic. Ltd. Şti.
<i>Evaluation Facility</i>	Beam Technology Test Center
<i>Certification Scheme</i>	TSE CCCS

2.2 Security Policy

TOE Security Policy consists of security functions described in section 2.4.1 Logical Scope.

2.3 Assumptions and Clarification of Scope

Please refer to Security Target Document v1.6 Table 6 for OSPs and Table 7 for Assumptions.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2.4 Architectural Information

2.4.1 Logical Scope

The primary security features of the TOE are:


- **Security audit:** TOE Security Functionality generates an audit record of the auditable events which will be explained in the ST.

Audit logs for the following events are provided:


- Insertion and removal of eID Card and SAM
 - Service requester authentication
 - Service attendee authentication
 - Start and end of secure messaging
 - Card authentication
 - Received data integrity failure
 - Role holder authentication
 - SAM authentication
 - SAM-PIN verification failure
 - TOE update
 - IVP verification
 - OCSP answer verification
 - Switching to offline mode (for TOE on SSR Type III)
 - SAS authentication (for TOE on SSR Type II)
 - Tamper event detection
- **Cryptographic Support:** Cryptographic support involves Cryptographic key generation, Encryption/Decryption, Cryptographic key destruction provided by the TOE.

Cryptographic operations are involved during the following functionalities:

- Secure Messaging are founded between TOE and eID; TOE and SAM; TOE and Role Holder
 - TLS Key Generation is performed between TOE and APS for TOE on SSR Type III;
 - between TOE and SAS for TOE on SSR Type II
 - To Encrypt/Decrypt the stored IVAs on SSR Type III
 - Service Attendee authentication
 - Service Requester authentication
 - eID Card authentication
 - SAM authentication
 - Role Holder Device authentication
 - SAS authentication for TOE on SSR Type II
 - APS authentication for TOE on SSR Type III
- **Identification and Authentication:** This feature contains that the users must be identified and authenticated before any action which related to security on the TOE. User roles are defined on system. Authentication failure handling, user identification and authentication, Multiple authentication mechanism for different users, reauthenticating, protected authentication feedback are supplied by the TOE. Identification and authentication functionalities for the followings are provided by the TOE:

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

- Service Attendee identification & authentication
 - Service Requester identification & authentication
 - eID Card identification & authentication
 - SAM identification & authentication
 - Role Holder Device identification & authentication
 - SAS identification & authentication for TOE on SSR Type II
 - APS identification & authentication for TOE on SSR Type III
- **Communication** : This feature contains communication methods between the TOE and other devices which the TOE can communicate. Following communications channels are provided by the TOE:
 - Communication between TOE and eID
 - Communication between TOE and SAM
 - Communication between TOE and Role Holder
 - Communication between TOE and SPCA (on SSR Type I – Type II without SAS)
 - Communication between TOE and SAS (on SSR Type II with SAS)
 - Communication between TOE and APS (on SSR Type III)
 - Communication between TOE and IVS (on SSR Type III)
 - Communication between TOE and IVPS (on SSR Type III)
 - Communication between TOE and OCSP (on SSR Type III)
 - **Security Management**: This feature contains managing security functions and data for different situations. Security roles, rules and conditions are identified and management is supplied according to roles, rules and conditions and only authorized people access the TOE.
 - **Protection of the TSF**: The TOE protects the TOE Security Functions and TSF data. This feature contains protection of cryptographic keys, digital signature protection/verification, data authentication, SAM-PIN, cryptographic credentials, IVA data fields, software integrity self-test and other TSF data protection. Temper protection is also supported by the TOE.
 - **User Data Protection**: This feature encloses monitoring user data stored in containers controlled by the TSF for any integrity error. Critical data in terms of keys, user passwords is used by the TOE and it is protected against losing and stealing. Integrity checking method, subset flow control rules, security attributes are provided by the TOE.
 - **Trusted Path/Channels**: This feature involves cryptographic communication protocols between itself and defined trusted products. Trusted channels supported by the TOE are the followings:
 - Trusted path/channel between TOE and eID
 - Trusted path/channel between TOE and SAM
 - Trusted path/channel between TOE and Role Holder
 - Trusted path/channel between TOE and SPCA (on SSR Type I – Type II without SAS)
 - Trusted path/channel between TOE and SAS (on SSR Type II with SAS)
 - Trusted path/channel between TOE and APS (on SSR Type III)
 - Trusted path/channel between TOE and IVS (on SSR Type III)
 - Trusted path/channel between TOE and IVPS (on SSR Type III)
 - Trusted path/channel between TOE and OCSP (on SSR Type III)

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

2.4.2 Physical Scope

TOE: E-Bio KEC - Secure Smartcard Readers Firmware v1.1

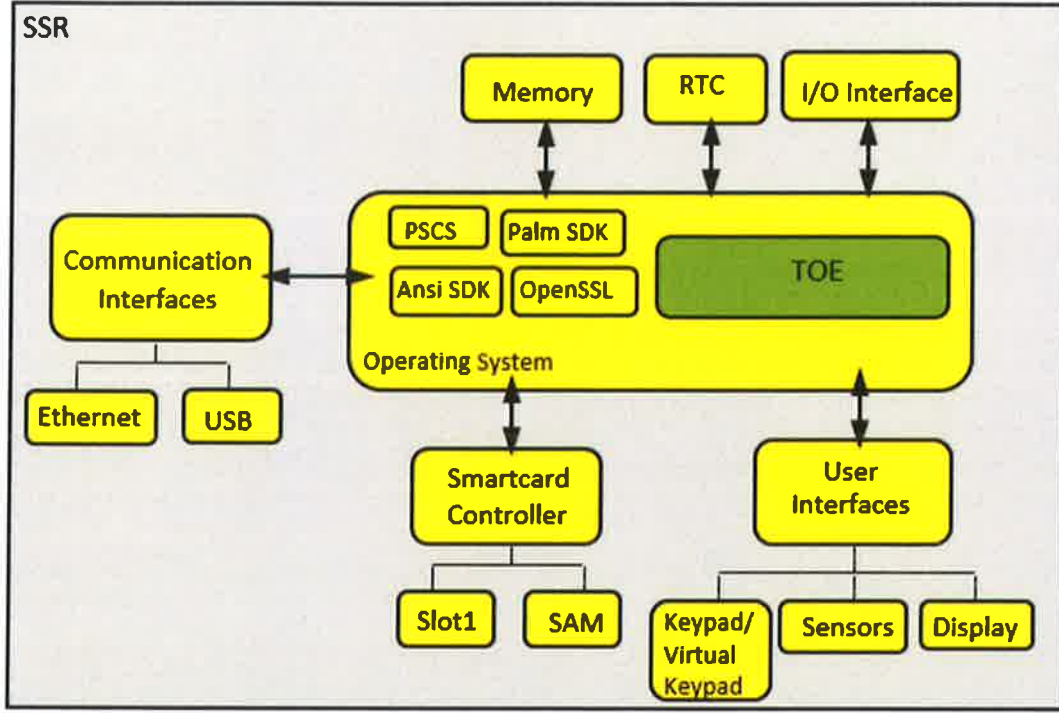
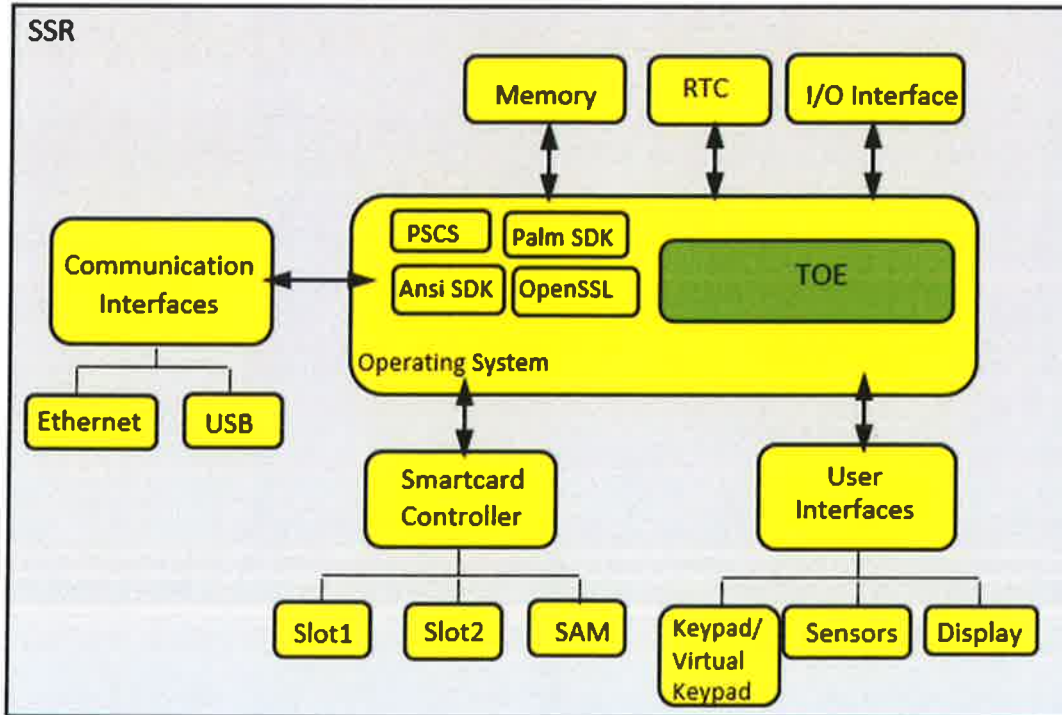


Figure 1 Hardware Environment of TOE – Type 1




	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

Figure 2 Hardware Environment of TOE – Type 2

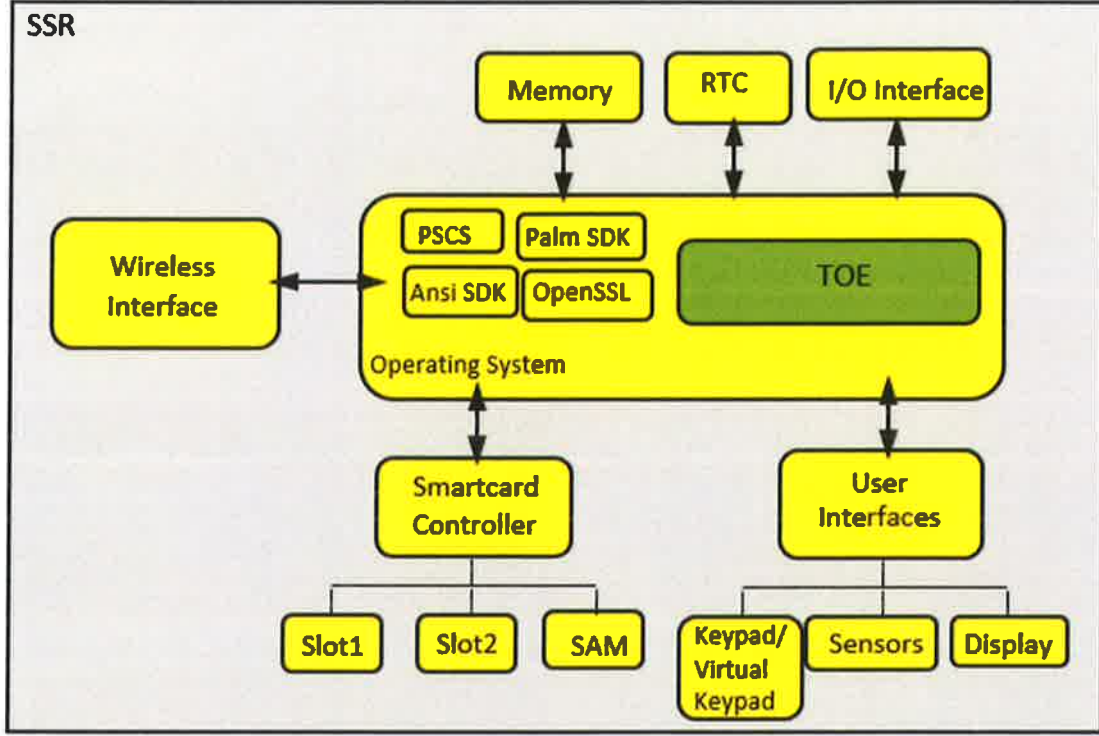


Figure 3 Hardware Environment of TOE – Type 3

More can be found in Security Target Document v1.6 in detail.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
E-Bio KEC - Secure Smartcard Readers Firmware v1.1 Security Target	V1.6	February 22, 2019
User Manual	v1.2	January 29, 2019
Installation Procedures	v1.0	January 28, 2019

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and subsystem/module behaviors have been tested by developer. Developer has conducted 25 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 14 of 25 developer tests. Additionally, evaluator has prepared 34 independent tests. TOE has passed all 48 functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 23 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with Enhanced-Basic Attack Potential”.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
		Yayın Tarihi	30/07/2015	
	CCCS CERTIFICATION REPORT	Revizyon Tarihi	29/04/2016	No

2.7 Evaluated Configuration

TOE configuration:

E-Bio KEC - Secure Smartcard Readers Firmware v1.1


Required Hardware Configuration:

- **Processing Unit:** Arm Cortex A9 1.2 Ghz processing unit support NEON/VFP
- **Memory:** 4 Gb Nand Flash Memory and 512 DDR SDRAM
Real Time Controller
Security Access Module (SAM), placed into the SIM card slot
- **Display:** 320X480 resolution TFT-LCD
- **Keypad:** 18 keys keypad/virtual keypad
- **Connections:**
 - Micro USB port for PC connection
 - 10/100 Mbit Ethernet port for network connection
 - Wi-Fi Module
 - GSM Module
 - USB device connection for biometric sensor
- **Power Supply:** +9V power supply input
- **Battery:** 7.4V 2500mAh

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL4+ (ALC_DVS.2) and the security target evaluation) is summarized in the following table:


Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation of the TSF	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.2	Sufficiency of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_TAT.1	Well-defined development tools	PASS
ASE:	ASE_CCL.1	Conformance claims	PASS

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No 05

Class Heading	Class Family	Description	Result
Security Target evaluation	ASE_ECD.1	Extended components definition	PASS
	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.2	Analysis of coverage	PASS
	ATE_DPT.1	Testing: basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.3	Focused vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “E-Bio KEC - Secure Smartcard Readers Firmware v1.1” product, result of the evaluation, or the ETR.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

3 SECURITY TARGET


The security target associated with this Certification Report is identified by the following terminology:

Title: E-Bio KEC - Secure Smartcard Readers Firmware v1.1

Version: v1.6

Date of Document: February 22, 2019

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	29/04/2016	No

4 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 8, 2016
- [4] ETR v2.2 of E-Bio KEC - Secure Smartcard Readers Firmware v1.1, Rel. Date: July 5th, 2019
- [5] E-Bio KEC - Secure Smartcard Readers Firmware v1.1 Security Target, Version 1.6, Rel. Date: February 22, 2019