Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

EGA Elektronik Güvenlik Altyapısı A.Ş.

EGA Application Firmware v1.0
for SSR Type I, SSR Type II with/without SAS, SSR Type III

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-54

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	September 13, 2018
Approval Date	September 13, 2018
Certification Report Number	21.0.03/18-007
Sponsor and Developer	**Sponsor:** KAT Mekatronik Ürünleri A.Ş. **Developer:** EGA Elektronik Güvenlik Altyapısı A.Ş.
Evaluation Facility	Beam Technology Test Center
TOE	EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III
Pages	15

Prepared by	Cem ERDİVAN Common Criteria Inspection Expert
Reviewed by	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

Release	Date	Pages Affected	Remarks/Change Reference
1.0	September 13, 2018	All	First Release
2.0	September 27, 2018	Page #3,8	Sponsor Information Added

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.

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 EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III whose evaluation was completed on September 10th, 2018 and whose evaluation technical report was drawn up by Beam Technology (as CCTL), and with the Security Target document with version no 1.2.0 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

1.1 TOE Overview

The TOE is the Secure Smartcard Reader (SSR) Application Firmware running on Type I SSR, Type II SSR with or without SAS and Type III SSR Device. The SSR is the identity verification terminal for the Turkish National eID Verification System.

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
- As a result of the identity verification, produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the SSR.

The root certificates used for the identification & authentication purposes are also covered by the TOE.

The following security mechanisms are primarily mediated in the TOE:
- Identification and Authentication
    - Cardholder verification by using PIN and biometrics (fingerprint data).
    - Authentication of eID Card,
    - Authentication of Role Holder,
    - Authentication of SAM,
    - Authentication of the TOE by SAM and by Card Holder (Service Requester and Service Attendee) and by external entities (e.g. Role Holder, External Biometric Sensor and External PIN PAD etc.)
- Secure Communication between the TOE and
    - SAM
    - eID Card
    - Role Holder
    - External Biometric Sensor and External PIN PAD
    - SSR Access Server (SAS)
- 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.

1.2 Threats

Threats are provided in Table 4 of Security Target Document v1.2.0.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-54
TOE Name and Version	EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III
Security Target Title	EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target
Security Target Version	V1.2.0
Security Target Date	15.02.2018
Assurance Level	EAL4+ (ALC_DVS.2)
Criteria	• 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
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for Electronic Identity Verification System, Version 2.8, 01.08.2017
Common Criteria Conformance	• 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
Sponsor and Developer	Sponsor: KAT Mekatronik Ürünleri A.Ş. Developer: EGA Elektronik Güvenlik Altyapısı A.Ş.
Evaluation Facility	Beam Technology Test Center
Certification Scheme	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 v1.2.0 Table 5 for OSPs and Table 6 for Assumptions.

2.4 Architectural Information

2.4.1 Logical Scope

TRUSTED PATH: TOE initiates communication via the trusted channel for all functions. This feature involves trusted communication protocols between TOE and smart cards, role holder, External PINPAD and External Biometric Sensor, SAS (Type II) and APS, IVS, IVPS, OCSP (Type III).

IDENTIFICATION AND AUTHENTICATION: The TOE enforces identification mechanism that requires users (Cardholders, eID Card, Role Holder Device, SSR Access Server and SAM) identify themselves before any other action will be allowed by the TOE and also enforces multiple authentication mechanisms that requires different authentication mechanisms for Card Holders, eID Card, Role Holder Device, SSR Access Server and SAM.

The TOE also performs re-authenticating mechanism with different scenario for different users. During the authentication process, the TOE provides only limited feedback information to the user in order to protect Card Holder authentication data. In cases of the number of unsuccessful authentication attempts exceeds the indicated threshold, the TOE performs authentication failure handling mechanism to take actions.

SECURE COMMUNICATION: The TOE performs secure communication with Role Holder Device, SSR Access Server, eID Card and SSR SAM Card for the protection of the channel data from modification or disclosure. The TOE produces digital signature of data using SAM Card for the verification of the evidence of origin of information to the recipients.

CRYPTOGRAPHIC OPERATION: The TOE performs cryptographic operations such as cryptographic key generation, encryption, decryption, hash generation, signature verification and key destruction.

The TOE also guaranties the protection for secret data stored in and used by the TOE against Side Channel Attacks based on power consumption or timing information of the operation.

SECURITY MANAGEMENT: The TOE allows Manufacturer service operator, OCSP Server, Initialization Agent, Identity Verification Policy Server and Client Application control over the management of security functions of the TOE and management of TSF data, such as TOE upgrade function and Identity Verification Method determination and SAM-PIN setting, time and date setting.

TSF PROTECTION: The TOE has the ability to verify that the defined imported TSF Data originates from the stated external entity and synchronize its internal state with another trusted external entity. The TOE also performs self-tests to demonstrate the correct operation of the TSF at start up.

SECURITY AUDIT: The TOE generates an audit record of security events and records within each audit record detail information such as date and time (reliable time) of the event and takes the actions to protect itself in the case tampering of the SSR is detected. In addition, The TOE protects the audit records stored in the audit trail from unauthorized deletion and detects unauthorized modifications. The TOE also enforces audit records

	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** 05

storage rules to prevent audit record loss in case the audit storage is full. The TOE provides audit review functionality.

USER DATA PROTECTION: The TOE provides Information Flow Control Policy when importing data and exporting data during secure communication with SAS and SPCA (through SAS). It ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the objects such as PIN or biometric information.

2.4.2 Physical Scope

TOE operates on an embedded environment with a file-system. The compiled kernel image comprises the OS kernel and some of the device drivers while the file-system is composed of the system files, the software libraries and the rest of the device drivers required by TOE. The file system also includes the TOE. The TOE consists of EGA Application Firmware, crypto library and Root certificates to be installed in Type I, Type II and Type III SSRs.

TOE is installed to SSR hardware in the manufacturers secure room. After installation, the TOE is delivered to the customers in the SSR Platform via courier.
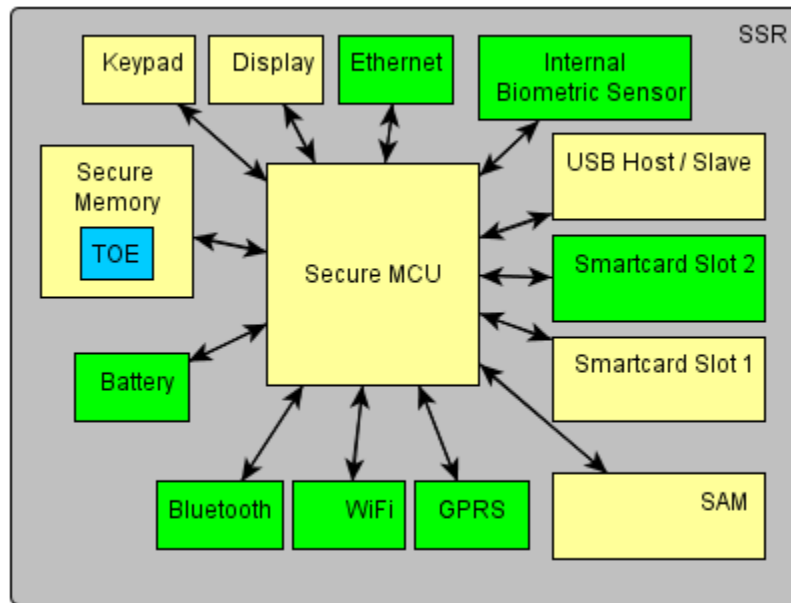

Figure 1: SSR Topography

The physical scope of the TOE software is shown in Figure 1. The TOE is shown as blue and 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. At initialize phase of TOE, TOE reads configuration file and when the TOE boots up, operational environments are checked by TOE and operates according to hardware peripherals and config file.

While yellow components in Figure 1 take place on all SSR types, however green components show the optional parts of the SSRs. For example: when the TOE detects Ethernet and Smartcard Slot 2 at the boot-up, TOE operates as Type II with SAS functionality.

EGA Application Firmware as part of TOE is an application written in the C++ programming language and accesses SSR hardware components and the crypto library via Embedded Operating System.

Secure communication and crypto operations are performed by the EGA Application Firmware using crypto library.

Root Certificates consists of root certificate of the Certificate Authority, Device Management CA Sub-Root certificate and eID Management CA Sub-Root certificates. These certificates are used for the Identification & Authentication purposes and are covered by the TOE.

For all type of SSR hardware platforms that the TOE is installed on and embedded operating systems are not part of the TOE.

2.5 Documentation

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

Document Name	Version	Release Date
EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target	V1.2.0	February 2, 2018
User Manual	v1.4.0	August 9, 2018
Installation Procedures	v1.2.0	June 5, 2018

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and subsystem/module behaviors have been tested by developer. Developer has conducted 18 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted all 18 developer tests. Additionally, evaluator has prepared 34 independent tests. TOE has passed all 52 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, 25 penetration tests have been conducted. TOE proved that it is resistant to "Attacker with Enhanced-Basic Attack Potential".

2.7 Evaluated Configuration

TOE configuration:

EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III.

Required Hardware Configuration:

- 528 MHz Arm Cortex-A7 single-core based processing unit with hardware-enabled Crypto Engine & Secure Boot features and secure RAM,
- 512 MB Flash and optional extra internal Micro-SD card support,
- 256 MB DDR memory (RAM),
- Secure Real Time Clock,
- 2 smart card slots & 1 SIM card slot (compatible to IEC/ISO 7816),
- Security Access Module (GEM), placed into the SIM card slot,
- 3.5-inch TFT-LCD,
- 12-keys keypad,
- +5V power supply input
- Tamper
- Optional internal fingerprint sensor,
- USB-A (host) port for External Biometric Sensor and External Pin Pad
- USB-mini AB (device) port for PC connection (for Type II),
- 10/100 Mbit Ethernet MAC + IEEE 1588 for network connection (for Type II),
- GPRS Quad-band and 1 GSM SIM card slot (for Type III),
- Optional Wi-Fi 802.11 and Bluetooth v4.2 module

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: Security Target evaluation	ASE_CCL.1	Conformance claims	PASS
	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:	ATE_COV.2	Analysis of coverage	PASS

Class Heading	Class Family	Description	Result
Tests	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 "EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III" 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: EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target
Version: v1.2.0
Date of Document: February 15, 2018

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.

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 EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III, Rel. Date: September 10, 2018

[5] EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target, Version 1.0.2, Rel. Date: February 15, 2018

[6] EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target, Version Lite, Rel. Date: September 18, 2018