Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

EGA Elektronik Güvenlik Altyapısı A.Ş.

EGA Application Firmware v2.0 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-78

TABLE OF CONTENTS

Document Information

Date of Issue	**02.11.2021**
Approval Date	**02.11.2021**
Certification Report Number	**21.0.03/21-010**
Sponsor and Developer	**EGA Elektronik Güvenlik Altyapısı A.Ş.**
Evaluation Facility	**Beam Teknoloji A.Ş.**
TOE	**EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III**
Pages	**14**

Prepared by	**Mert LENGERLİOĞLU** **Common Criteria Inspection Expert**
Reviewed by	**İbrahim Halil KIRMIZI** **Common Criteria Technical Responsible**

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	**02.11.2021**	**All**	**First Release**

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1 revision 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/PP 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 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 EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III whose evaluation was completed on October 25th 2021 and whose evaluation technical report was drawn up by Beam Teknoloji A.Ş. (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 EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

The TOE is an Application Firmware running on Type I Secure Smartcard Reader device(SSR), Type II SSR device with or without SAS and Type III SSR device. The SSR is the identity verification terminal for the National eID Verification System. Security Target of TOE claims strict conformance to Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for Electronic Identity Verification System, SSR_PP_2.8, 2017.

The TOE performs the following, as the Application Firmware of the SSR;

- Produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the SSR because of the identity verification.
- Identity verification of Service Requester and Service Attendee according to the eIDVS
- Communicating with the other system components as a secure manner.

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

The TOE provides the following security mechanisms primarily:

- Security Management
- Self-Protection
- Audit
- Identification and Authentication
    - Authentication of the TOE by SAM and by Card Holder and by external entities
    - Cardholder verification by biometrics
    - Cardholder verification by using PIN
    - Authentication of Role Holder,
    - Authentication of SAM,
    - Authentication of eID Card,
- Secure Communication between the TOE and
    - Role Holder
    - External Biometric Sensor and External PIN PAD
    - SSR Access Server (SAS)
    - SAM
    - eID Card

The TOE includes the certificates of the root CA, device management CA and eID management CA and the certificates also used in the eID Verification System.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-78
TOE 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	05.05.2021
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	EGA Elektronik Güvenlik Altyapısı A.Ş.
Evaluation Facility	Beam Teknoloji A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

TOE Security Policy consists of security functions described in section 2.4 within logical scope.

2.3 Assumptions and Clarification of Scope

For assumption and OSPs, check the Table 5 & Table 6 in Security Target document v1.2.0.

2.4 Architectural Information

TOE operates on an embedded environment with a file-system. The kernel image comprises the OS kernel, the device drivers and the file-system. 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 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.

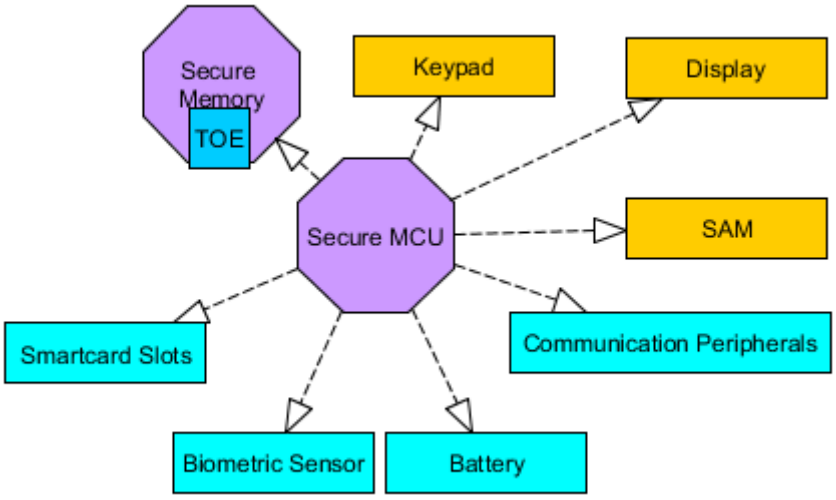

***Figure 1**: Physical Scope of the TOE*

In the figure above, 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 initialise 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 orange components in the figure take place on all SSR types, however turquoise components show the optional parts of the SSRs but only one smartcard slot is mandatory. The purple components

are mandatory for all types of SSRs. While Secure MCU is required for secure execution environment, the Secure Memory is used for deployment of encrypted TOE.

EGA Application Firmware as part of the TOE accesses SSR hardware components and the crypto libraries 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.

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, IVPS, OCSP (Type III).

The TOE enforces identification mechanism that requires users (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, APS, EBS, EPP, 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 biometric authentication attempts exceeds the indicated threshold, the TOE performs authentication failure handling mechanism to take actions.

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.

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

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.

The TOE associates the following roles with users

- Initialization Agent,
- SSR Access Server for TOE on SSR Type II,
- Client Application for TOE on SSR Type II,
- Application Server for TOE on Type III,
- Identity Verification Policy Server,
- OCSP Server,
- Manufacturer service operator
- Software Publisher.

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.

The TSF preserves secure state when the tampering event is detected and authentication services for SAM are disturbed.

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

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: the cryptographic credentials, IVA data fields, PIN, photo and biometric information.

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 v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target	V1.2.0	05.05.2021
User Manual	v1.2.0	13.08.2021
Installation Procedures	v1.2.0	25.06.2021

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and subsystem/module behaviors have been tested by developer. Developer has conducted 19 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 11 after merging of some developer tests. Additionally, evaluator has prepared 19 independent tests. TOE has passed all 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".

2.7 Evaluated Configuration

TOE configuration:

EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III.

Required Hardware Configuration:

TOE will run on SSR hardware which includes:

- 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 switches
- 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

Some hardware components such as biometric sensor, Ethernet port or second smartcard slot are optional depending on the SSR type.

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: 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 “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 v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target

Version: v1.2.0

Date of Document: May 5, 2021

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 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

ITCD: Information Techologies Test And Certification Department

EAL: Evaluation Assurance Level

OSP: Organisational Security Policy

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

ST: Security Target

TOE: Target of Evaluation

TSF: TOE Security Funcationality

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] ETR v1.2 of EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III, Rel. Date: October 21, 2021

[4] EGA Application Firmware v2.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III Security Target, Version 1.2.0, Rel. Date: May 05, 2021.

6 ANNEXES

There is no additional information or reference.