Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

MT Bilgi Teknolojileri ve Dış. Tic. A.Ş.

VERA Type-II SSR Application Firmware v1.5.2

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-83

TABLE OF CONTENTS

DOCUMENT INFORMATION

Date of Issue	**09.12.2022**
Approval Date	**09.12.2022**
Certification Report Number	**21.0.03/22-006**
Sponsor and Developer	**MT Bilgi Teknolojileri ve Dış. Tic. A.Ş.**
Evaluation Facility	**Beam Teknoloji A.Ş.**
TOE	**VERA Type-II SSR Application Firmware v1.5.2**
Pages	**17**

Prepared by	**Erkut BEYDAĞLI** **Common Criteria Inspection Expert**
	Merve Hatice KARATAŞ **Common Criteria Inspection Expert**
	Göktuğ İLISU **Common Criteria Candidate Inspection Expert**
Reviewed by	**Mehmet Kürşad ÜNAL** **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	**09.12.2022**	**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 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 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 VERA Type-II SSR Application Firmware v1.5.2 whose evaluation was completed on November 10th 2022 and

whose evaluation technical report was drawn up by Beam Teknoloji A.Ş. (as CCTL), and with the Security Target document with version no 2.6 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).

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 EAL 2. 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 II Secure Smartcard Reader (SSR). 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;

- identity verification of Service Requester and Service Attendee according to the eIDVS
- securely communicating with the other system components
- TLS communication with SAS through Ethernet interface
- as a result of the identity verification, produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the Type II SSR.

The root certificates which is 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 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 entity (*Role Holder*).
- ***Secure Communication between the TOE and***
  - SAM
  - eID Card
  - Role Holder
  - SAS
- ***Security Management***
- ***Self-Protection***
- ***Audit***

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

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-137
TOE and Version	VERA Type-II SSR Application Firmware v1.5.2
Security Target Title	VERA Type-II SSR Application Firmware v1.5.2 Security Target
Security Target Version	v2.6
Security Target Date	05.10.2022
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	MT Bilgi Teknolojileri ve Dış. Tic. 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 OSPs and assumptions, check the Table 5 & Table 6 in Security Target document v2.6.

2.4 Architectural Information

The physical scope of the TOE is an application firmware (VERA Type-II SSR Application Firmware) to be installed in Type II SSR, TOE Documentation and Root Certificates.

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

❖ The VERA Type-II SSR Application Firmware consists of:

- VERA Application
- Crypto Libraries

The physical scope (*except TOE Documentation*) of the TOE is shown in green box in Figure 1.

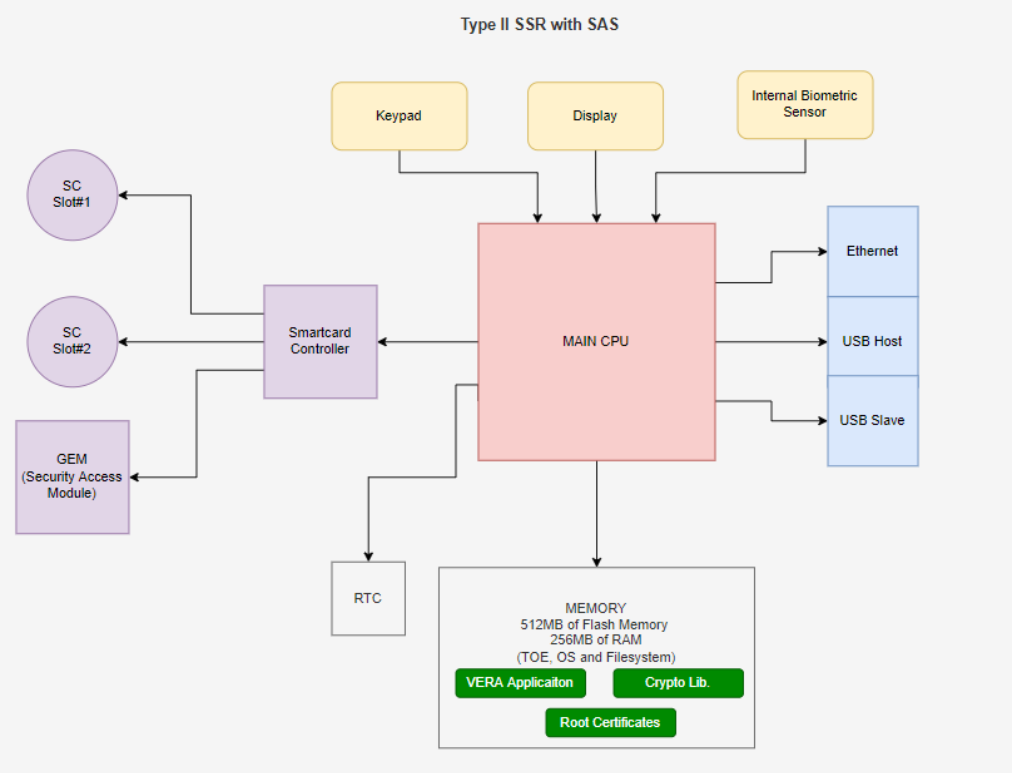

Figure 1: *Physical Scope (except TOE Documentation) of the TOE*

VERA Application

VERA Application is an application written in the C++ programming language and developed for running on Linux Operating System in the Type II SSR runs at the top of Embedded Linux operating system. VERA Application accesses SSR hardware components and Crypto Libraries via Embedded Linux Operating System.

Crypto Libraries

Crypto Libraries consist of OpenSSL v1.1.1m and Mbed TLS (3.1.0) libraries, which are embedded in the file system, are software library written in the C programming language as open-source and contains software crypto library for different crypto algorithm and implementation of the TLS protocols.
Secure communication and crypto operations are performed by the VERA Application using OpenSSL and Mbed TLS libraries.

❖ **Root Certificates consists of:**

- Root certificate of the Certificate Authority
- Device Management CA Sub-Root certificate
- eID Management CA Sub-Root certificate

These certificates are used for the Identification & Authentication purposes and are covered by the TOE as part of the TOE.

❖ **TOE Documentation consists of:**

- The TOE operational guidance
- The TOE preparative procedures

The Type II SSR hardware platform that the TOE is installed on and embedded operating systems are not part of the TOE.

Logical scope of the TOE are shown at Table 1.

TOE Security Function	Description
Identification and Authentication	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, 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 verification attempts exceeds the indicated threshold, the TOE performs biometric verification 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.
Security Management	The TOE associates users with Initialization Agent, SSR Access Server for TOE, Client Application for TOE, Identity Verification Policy Server, OCSP Server, Manufacturer service operator, Software Publisher roles. The TOE allows these roles to provide to control over the management of security functions behaviour of the TOE (*TOE upgrade function and Identity Verification Method determination*) and management of TSF data (*SAM PIN and DTN initialization, time and date setting*). It is also capable of performing the audit generation function.

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. When the tampering event is detected and identification and authentication of the SAM are disturbed, it preserves secure state.
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 also takes the actions to protect itself in case tampering of the Type II 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.
User Data Protection	The TOE provides Information Flow Control Policy when importing data 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 (*cryptographic credentials, IVA data fields, PIN, photo and biometric information*)

Table 1: *Logical Scope of TOE*

2.5 Documentation

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

Document Name	Version	Release Date
VERA Type-II SSR Application Firmware v1.5.2 Security Target	2.6	05.10.2022
Operational User Guidance	0.2	15.09.2022
Preparative Procedures	0.6	05.10.2022

2.6 IT Product Testing

- **Developer Testing:** All TSFIs and module behaviors have been tested by developer. Developer has conducted 23 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 16 developer tests. Additionally, evaluator has prepared 13 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, 14 penetration tests have been conducted. TOE proved that it is resistant to “Attacker with Enhanced-Basic Attack Potential”.

2.7 Evaluated Configuration

TOE configuration:

VERA Type-II SSR Application Firmware v1.5.2

Required Hardware Configuration:

The TOE is stored in a non-volatile 512 MB Flash Memory location in the Type II SSR Hardware as an encrypted binary file. During power-up, the encrypted TOE is decrypted before its execution. The hardware version of Type II SSR is 200-v2.4-001.

As shown in the block diagram in Figure 2, Type II SSR includes:

- I/O interfaces:
  - ✓ USB 2.0 compliant full speed USB port for PC connection
  - ✓ USB 2.0 compliant full speed USB port for external device connection
  - ✓ 100 Mbit Ethernet port for network connection
  - ✓ +12V 2.5A power supply input
- User interfaces:
  - ✓ 480xRGBx272 or 320x240 resolution display, up to 16.7M colors with capacitive touch panel
  - ✓ 15-keys keypad
  - ✓ 320 x 480 pixels 500dpi / 256 gray resolution fingerprint sensor
- ARM Cortex A9 core based processing unit
- Memory components:
  - ✓ 512 MB of Flash Memory
  - ✓ 256 MB of DDR3 RAM
- Two smartcard slots & two SAM card slots[1] (*compatible to IEC/ISO 7816*)
- Security Access Module (*SAM*), placed into the SAM card slot
- Real Time Clock (*RTC*)
- Physical and logical security barriers (*shields and tamper switches*)

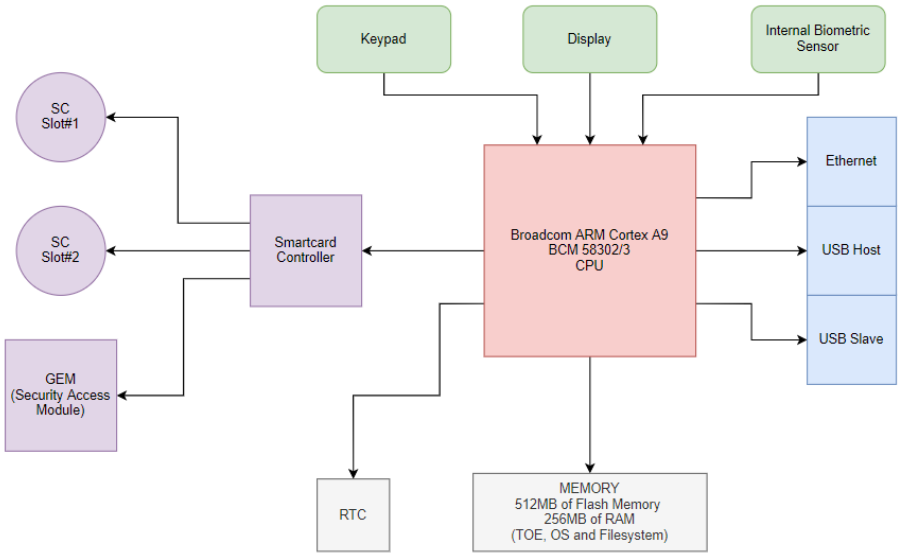

Figure 1: *Type II SSR Hardware*

The Type II SSR is developed to operate together with ***Internal Biometric Sensor*** that is used for biometric verification.

The Type II SSR communicates with SSR Access Server through Ethernet interface.

[1] *The second SAM slot is added to the SSR Hardware to be a backup in case of any hardware failure.*

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 “VERA Type-II SSR Application Firmware v1.5.2” 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: VERA Type-II SSR Application Firmware v1.5.2 Security Target

Version: v2.6

Date of Document: October 5, 2022

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

CCRA: Common Criteria Recognition Arrangement

ITCD: Information Techologies Test And Certification Department

EAL: Evaluation Assurance Level

IVA: Identity Verification Assertion

OSP: Organisational Security Policy

SAM: Secure Access Module

SSR: Secure Smartcard Reader

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 VERA Type-II SSR Application Firmware v1.5.2, Rel. Date: November 10, 2022

[4] VERA Type-II SSR Application Firmware v1.5.2Security Target, Version 2.6, Rel. Date: October 05, 2022.

6 ANNEXES

6.1 TOE and TEST ENVIRONMENT

TOE: VERA Type-II SSR Application Firmware v1.5.2

TOE Hash (SHA256): 0dc6087a48d5dfc71867072ff956dec1485c92d3017c175d84d80a2b5a1572cb

TEST ENVIRONMENT:

Hardware Version of the KEC: 200-v2.4-001

Serial Number of the KEC: 12000600

System Software Version: 1.0.2

KEC Software Version: 1.1

Kimlikizi.KaleKecTest.exe – Client Application to send Identity Verification Request (SPCA) (provided by Kale Yazılım): 20220124

KDP.Service.WebApi / Policy Server Version (provided by Kale Yazılım): KDP.Service.WebApi -> 1.2022.0411.1

KDB.Service.WebApi / Identity Verification Server Version (provided by Kale Yazılım): KDB.Service.WebApi -> 1.2022.0411.1

ROL.WebApi / Role Holder Server Version (provided by Kale Yazılım): ROL.WebApi -> 1.2022.0411.1

SAS Version (provided by Kale Yazılım): 1.2022.0914.3