



Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

**MT Bilgi Teknolojileri ve Dış Tic. A.Ş.
VERA APP_SSR-2 v0.1.3**

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**

Certificate Number: 21.0.03/TSE-CCCS-47



	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

TABLE OF CONTENTS

DOCUMENT INFORMATION	3
DOCUMENT CHANGE LOG	3
DISCLAIMER	4
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	5
1. EXECUTIVE SUMMARY	6
1.1 BRIEF DESCRIPTION	6
1.2 MAJOR SECURITY FEATURES	8
1.3 THREATS	9
2. CERTIFICATION RESULTS	12
2.1 IDENTIFICATION OF TARGET OF EVALUATION	12
2.2 SECURITY POLICY	13
2.3 ASSUMPTIONS AND CLARIFICATION OF SCOPE	14
2.4 ARCHITECTURAL INFORMATION	15
2.5 DOCUMENTATION	16
2.6 IT PRODUCT TESTING	16
2.7 EVALUATED CONFIGURATION	17
2.8 RESULTS OF THE EVALUATION	18
2.9 EVALUATOR COMMENTS / RECOMMENDATIONS	19
3. SECURITY TARGET	20
4. GLOSSARY	21
5. BIBLIOGRAPHY	23
6. ANNEXES	23

	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>	18.10.2017
<i>Approval Date</i>	20.10.2017
<i>Certification Report Number</i>	21.0.03/17-011
<i>Sponsor and Developer</i>	MT Bilgi Teknolojileri ve Dış Tic. A.Ş.
<i>Evaluation Facility</i>	BEAM Teknoloji A.Ş.
<i>TOE</i>	VERA APP_SSR-2 v0.1.3
<i>Pages</i>	23

<i>Prepared by</i>	İbrahim Halil KIRMIZI	
<i>Reviewed by</i>	Zümrüt MÜFTÜOĞLU	

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	18.10.2017	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 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.


FOREWORD

The Certification Report is drawn up to submit the Certification Committee 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 ITCDC 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 (IS) 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 public 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.

	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

This certification report is associated with the Common Criteria Certificate issued by the CCCS for VERA APP_SSR-2 v0.1.3 whose evaluation was completed on 29.09.2017 and whose evaluation technical report was drawn up by MT Bilgi Teknolojileri A.Ş. (as CCTL), and with the Security Target document with version no 1.1 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>

	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

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: VERA APP_SSR-2

IT Product version: v0.1.3

Developer's Name: MT Bilgi Teknolojileri Dış Tic. A.Ş.

Name of CCTL: BEAM Teknoloji A.Ş.

Assurance Package: EAL 4+ (ALC_DVS.2)

Completion date of evaluation: 29.09.2017

1.1 Brief Description

The TOE is the Application Firmware running on Type II SSR. The SSR is the identity verification terminal for the National eID Verification System (eIT.DVS).

As the Application Firmware, the TOE performs;

- 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 used for the identification & authentication purposes are also covered by the TOE.

The scenario in Figure 3 explains how Type II SSR performs Identity Verification Operation. As seen, Identity Verification Operation is initiated by the SPCA which is installed on a personal computer (PC). SPCA communicates to the TOE through the SAS via Ethernet interface.



**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

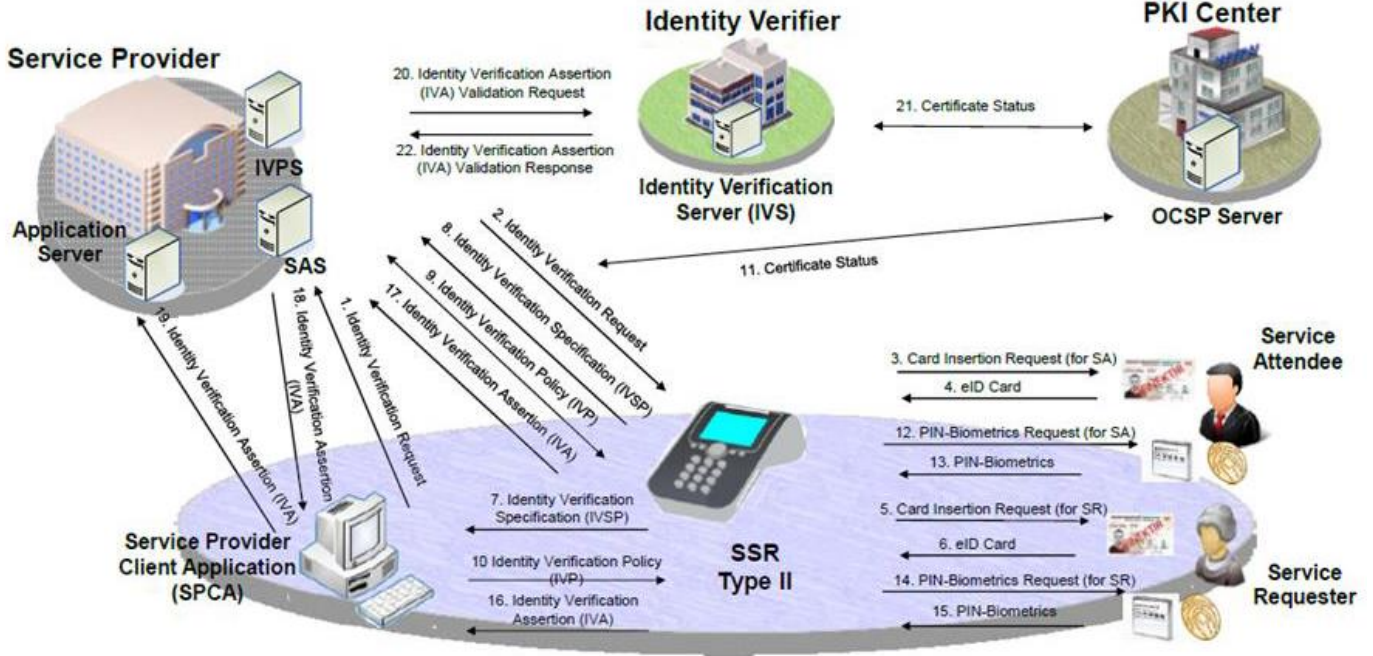



Figure 1 - User Environment of Type II SSR (with SAS)

Operation is initiated by the Service Provider Client Application (SPCA) which is installed on a personal computer (PC). First, SPCA sends an Identity Verification Request to TOE through the SAS via Ethernet interface (1. Identity Verification Request & 2. Identity Verification Request).

Once the TOE receives this request, it asks the SR and the SA to insert their eID card one by one into the smartcard slot. After the eID cards are inserted, the TOE sets up a secure messaging session with the eID cards. Having read the cardholder's personal message from the eID card, the TOE displays it on the screen for the SR's and SA's approval. If the displayed message is approved by the SR and SA, an Identity Verification Specification (IVSP), is generated by the TOE, and sent to IVPS through the SAS. Next, the Identity Verification Policy Server (IVPS) sends the Identity Verification Policy (IVP) to the TOE through the SAS for the SR and SA specified in the IVSP. Since the IVP is signed by the IVPS, the TOE checks the signature to make sure it comes from a legitimate IVPS and hasn't been modified. The IVP defines the Identity Verification Method (IVM) for the SR and SA and the organizational policies defined in TS 13584 [8]. If an IVPS doesn't exist, the SPCA defines the IVM itself. Otherwise, the TOE uses the predefined default IVM which has the highest security level. During identity verification, the Identity Verification Certificate within the eID Card is not only verified offline by the TOE, but also validated online with the help of the Online Certificate Status

	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

Protocol (OCSP) Server. If the online certificate validation cannot be achieved due to technical problems, there are two options to continue the operation:

- The TOE validates the eID Card of the SR and the SA using the Certificate Revocation List downloaded on the Type II SSR. In this case, the information that “**OCSP check could not be achieved**” shall be included in the IVA.
- The TOE does not validate the eID Card of the SR and the SA. In this case, the information that “**OCSP check and Revocation List control could not be achieved**” shall be included in the IVA.

In addition to certificate verification and validation, according to the IVM, if requested, biometric verifications of the SR and the SA are done by the TOE using fingerprint data.


At the end of the authentication, an Identity Verification Assertion (IVA) includes SA and SR information is generated by the TOE. Since the IVA is signed by the SAM, it assures origin of identity, time and place. The TOE sends the IVA to the SPCA.

Finally, SPCA forwards the IVA to IVS, which validates it and keeps it as an evidence for the operation. Until the IVA is validated by the IVS, the Identification and Authentication of SR and SA is regarded as incomplete.

1.2 Major Security Features

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 entities such as Role Holder.
- Secure Communication between the TOE and
 - SAM
 - eID Card
 - Role Holder
 - SAS
- Security Management

	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

- 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.

1.3 Threats

The threats are;

- **T.AccessControl**

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**


The attacker may obtain Identity Verification Assertion by monitoring the communication line between;

- Identity Verification Server and the Application Server
- SPCA and the Application Server
- SPCA and the SAS

- **T.Repudiation**

The Service Requester (or the Service Attendee) may repudiate the Identification Verification Assertion.

- **T.Fake_TOE_to_SR**

	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

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 eID Card. 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.eIDC_Comm**

	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

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 Type II SSR

- **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 Type II SSR. SAM PIN could be obtained by probing the internals of the Type II 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 Type II SSR.

- **T.Revoked_SAM**


An attacker may use a Revoked SAM to build an illegitimate Type II SSR.

	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. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-47
TOE Name and Version	VERA APP_SSR-2 v0.1.3
Security Target Title	VERA Application Firmware v0.1.3 of Type II SSR with SAS Security Target
Security Target Version	V1.1
Security Target Date	29.09.2017
Assurance Level	EAL 4+ (ALC_DVS.2)
Criteria	<ul style="list-style-type: none"> • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 • 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	Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Identity Verification System TSE-CCCS/PP-012, version 2.8, August 10 th 2017

	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

2.2 Security Policy

Organizational Security Policies are;

- **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 upgrade.

- **P.Re-Authentication**

Authentication of third party IT components will be renewed after 24 hours.

- **P.Terminal_Cert_Upgrade**

Terminal Certificate will be renewed within a period defined in TS 13584 [8]. Type II SSR Access Server 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.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.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

	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

the only condition to go back to Initialization & Configuration Phase. DTN and SAM PIN shall be written to the Type II SSR during Initialization & Configuration Phase.

- **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.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the composite TOE are;

- **A.SPCA**

It is assumed that Service Provider Client Application is a trusted third party. For Type II SSR with SAS, there is no direct connection between the Type II SSR and the SPCA. SPCA communicates to the SSR through the SAS via 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 Type II SSR 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.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**

	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

It is assumed that the PIN value of the SAM in the Type II SSR is defined in the Type II 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 the 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 the Application Firmware running on Linux Operating System v3.2.0 within the SSR that is the identity verification terminal for the National eID Verification System.

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. Type II SSR includes;

- 2 USB 2.0 ports,
- 100 Mbit Ethernet port,
- +5V power supply port,
- Capacitive Touch Panel,
- Keypad,
- Fingerprint Sensor,
- CPU,
- Flash Memory,
- RAM,
- 2 Smartcard Slots,
- SAM,
- RTC,

	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

- Tamper switch mechanism

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 VERA Application Firmware v0.1.3 of Type II SSR with SAS (VERA APP_SSR-2)	V1.1	29.09.2017
VERA APP_SSR-2 Preparative Procedures	V0.6	08.09.2017
VERA APP_SSR-2 Operational User Guidance	V0.4	07.09.2017

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. 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 VERA APP_SSR-2 v0.1.3

It is concluded that the TOE supports EAL 4+ (ALC_DVS.2). There are 24 assurance families which are all evaluated with the methods detailed in the ETR.


IT Product Testing is mainly described in 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 done total of 23 functional tests.

2.6.2 Evaluator Testing

- Independent Testing: Evaluator has done total of 52 tests. 21 of them were selected from developer's tests. The other 31 of them were evaluator's independent tests.

	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

- Penetration Testing: Evaluator has done 15 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes.

2.7 Evaluated Configuration

This evaluation was performed at the operational environment described below;

Name of the SSR within the Application Firmware: MTK 200

Processor within the SSR: Device uses ARM Cortex A8 processor with full implementation of the ARM architecture v7-A instruction set which has with a 1.0 Ghz core operating frequency.

Memory within the SSR has following features;

- 512 MB of Flash Memory
- 256 MB of DDR3 RAM

I/O and Peripherals;

- 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

Smartcard Controllers;


- Two smartcard slots
- 1 SAM card slot (compatible to IEC/ISO 7816)

Power;

- +5V Power Supply input

During the evaluation; the configuration of evaluation evidences which are composed of Common Criteria documents, guides are shown below;

Name of Document	Version Number	Publication Date
VERA APP_SSR-2	V0.1.3	
Security Target for VERA Application Firmware v0.1.3 of Type II SSR with SAS (VERA APP_SSR-2)	1.1	29.09.2017
VERA APP_SSR-2 Security Architecture	0.4	07.09.2017
VERA APP_SSR-2 Functional Specification Documentation	0.8	07.09.2017
VERA APP_SSR-2 TOE Design Documentation	0.7	07.09.2017


	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

Name of Document	Version Number	Publication Date
VERA APP_SSR-2 Preparative Procedures	0.6	08.09.2017
VERA APP_SSR-2 Operational User Guidance	0.4	07.09.2017
VERA APP_SSR-2 Configuration Management Documentation	0.7	08.09.2017
VERA APP_SSR-2 Configuration List Documentation	1.7	29.09.2017
VERA APP_SSR-2 Delivery Documentation	0.2	10.01.2017
VERA APP_SSR-2 Development Security Documentation	0.4	02.05.2017
VERA APP_SSR-2 Test Coverage Analysis	V0.5	07.09.2017
VERA APP_SSR-2 Depth of Testing Analysis	V0.4	07.09.2017
VERA APP_SSR-2 Test Documentation	V0.4	08.09.2017
VERA APP_SSR-2 Vulnerability Analysis Plan	V5.2	02.10.2017

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


	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

	ALC_TAT.1	Well-Defined Development Tools
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	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 “VERA APP_SSR-2 v0.1.3”, the results of the assessment of all evaluation tasks are “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 APP_SSR-2 v0.1.3” 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: VERA Application Firmware v0.1.3 of Type II SSR with SAS (VERA APP_SSR-2) Security Target

Version: 1.1


Date of Document: 29.09.2017

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

Title: VERA Application Firmware v0.1.3 of Type II SSR with SAS (VERA APP_SSR-2) Security Target v1.1

Lite

Date of Document: 18.10.2017

	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. 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

	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

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 : Opretional 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

TA : Terminal Authentication

TOE : Target of Evaluation

TSF : TOE Security Functionality

TSFI : TSF Interface

	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

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] BTTM-CCE-018 VERA APP_SSR-2 v0.1.3 Evaluation Technical Report v5.2
- [5] BTTM-CCE-018 VERA APP_SSR-2 v0.1.3 Vulnerability Analysis Plan v5.2
- [6] BTTM-CCE-018 VERA APP_SSR-2 v0.1.3 Functional Test Plan v3.2
- [7] 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
- [8] 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