



Certification Report

EAL 4+ (ALC_DVS.2) Evaluation of

TÜBİTAK BİLGEM

**Protection Profile for Application Firmware of
Secure Smartcard Reader for
National Electronic Identity Verification System**

issued by

**Turkish Standards Institution
Common Criteria Certification Scheme**



	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	28/08/2015	No

TABLE OF CONTENTS

TABLE OF CONTENTS	2
Document Information	3
Document Change Log	3
DISCLAIMER	3
FOREWORD	4
RECOGNITION OF THE CERTIFICATE	5
1 - EXECUTIVE SUMMARY	6
2 CERTIFICATION RESULTS	10
2.1 PP Identification	10
2.2 Security Policy	10
2.3 Assumptions and Clarification of Scope	11
2.4 Architectural Information	13
2.5 Security Functional Requirements	16
2.6 IT Security Assurance Requirements	17
2.7 Results of the Evaluation	17
2.8 Evaluator Comments / Recommendations	17
3 PP DOCUMENT	18
4 GLOSSARY & ACRONYMS	19
5 BIBLIOGRAPHY	21

	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	28/08/2015	No

Document Information


<i>Date of Issue</i>	30.11.2015
<i>Version of Report</i>	v1.0
<i>Author</i>	Cem ERDİVAN
<i>Technical Responsible</i>	Zümrüt MÜFTÜOĞLU
<i>Approved</i>	Mariye Umay AKKAYA
<i>Date Approved</i>	03.12.2015
<i>Certification Report Number</i>	21.0.03/15-002
<i>Sponsor and Developer</i>	TÜBİTAK BİLGEM
<i>Evaluation Lab</i>	TÜBİTAK BİLGEM OKTEM
<i>PP Name</i>	Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.5
<i>Pages</i>	21

Document Change Log

<i>Release</i>	<i>Date</i>	<i>Pages Affected</i>	<i>Remarks/Change Reference</i>
1.0	30.11.2015	All	First Release

DISCLAIMER

This certification report and the 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 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the 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 PP 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 PP by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	28/08/2015	No

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.


The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) 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 PP have been performed by TÜBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a PP means that such PP meets the security requirements defined in its PP document that has been approved by the CCCS. The PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the PP should also review the PP document in order to understand any assumptions made in the course of evaluations, the environment where the PP will run, security requirements of the PP and the level of assurance provided by the PP.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.4 whose evaluation was completed on 13.11.2015 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM, and with the PP document with version no 2.5 of the relevant product.

The certification report, certificate of PP evaluation and PP document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).


	BİLİŞİM TEKNOLOJİLERİ TEST VE BELGELENDİRME DAİRESİ BAŞKANLIĞI / INFORMATION TECHNOLOGIES TEST AND CERTIFICATION DEPARTMENT	Doküman No	BTBD-03-01-FR-01	
	CCCS CERTIFICATION REPORT	Yayın Tarihi	30/07/2015	
		Revizyon Tarihi	28/08/2015	No

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. 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	28/08/2015	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: Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System

IT Product version: v2.5

Developer's Name: TÜBİTAK BİLGEM

Name of CCTL: TÜBİTAK BİLGEM OKTEM

Assurance Package: EAL4+ (ALC_DVS.2)

Completion date of evaluation: 13.11.2015

1.1 Brief Description


The TOE is the Secure Smartcard Reader (SSR) Application Firmware running on SSR Device. The SSR is the identity verification terminal for the National eID Verification System (eIDVS). As the application firmware of the SSR, the TOE performs identity verification of Service Requester and Service Attendee according to the eIDVS, securely communicating with the other system components and as a result of the identity verification, produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the SRR. The root certificates used for the identification & authentication purposes are also covered by the TOE.

This Protection Profile supports TOE on three different operational environments. Operation environment is the SSR Hardware and SSR User Environment including the other parties that SSR communicates to the SSR Application Firmware.

Properties of the three operational environments are compared in Table 1.

Table 1. Comparison of SSR types

	Type I	Type II	Type III
User Interface of SSR Device	Pinpad, Display, One smartcard slot, Biometric sensor (internal, external or does not exist) External pinpad (optional)	Pinpad, Display, Two smartcard slots, Biometric sensor (internal, external or does not exist) External pinpad (optional)	Pinpad, Display, One or two smartcard slots, Biometric sensor (internal, external or does not exist) External pinpad (optional)
Service Provider Client Application (SPCA)	Running on PC	Running on PC	Included in the TOE
SSR Access Server (SAS)	N/A	Optional	N/A
Communication Environment of SSR	SSR communicates to Service Provider Client Application (SPCA) through USB Interface. SPCA communicates to Identity Verification Policy Server (IVPS) / Application Server (APS)/ Online Certificate Status Protocol Server (OCSPS).	SSR communicates to Service Provider Client Application through USB interface or communicates to SAS through Ethernet interface. SPCA or SAS communicates to IVPS / APS/ OCSPS.	SSR directly communicates to IVPS / APS/ OCSPS through wireless 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	28/08/2015	No

Service Attendee Support	N/A	Yes	Optional
Secure Upgrade	Yes	Yes	Yes
Optional Online/Offline Mode	Offline Certificate Validation using Certificate Revocation List when the OCSP Server isn't reached	Offline Certificate Validation using Certificate Revocation List when the OCSP Server isn't reached	Offline Certificate Validation using Certificate Revocation List when the OCSP Server isn't reached Storing Identity Verification Assertions when the connection is failed

There are two offline use cases:

- (i) offline revocation list control and
- (ii) offline IVA generation & storage.

In first use case, only the certificate status control is performed offline, other identity verification steps are performed online. As it is explained in Table 1, this use case could be included in all three types of SSR Devices when OCSPS could not be reached. On the other hand, the second use case is an option only for SSR Type III Devices. If the SSR type III Device has the offline IVA generation and storage mode, the IVA can be generated and stored within the SSR when the SSR can not reach to the APS. The confidentiality and the integrity of the IVAs shall be assured during storage.

1.2 TOE Security Functions


The following security mechanisms are primarily mediated in the TOE:

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


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

1.3 Threats


1. **T.Counterfeit_eIDC:** 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.
2. **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.

	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	28/08/2015	No

3. **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.
4. **T.IVA_Fraud:** An attacker may create a fraudulent Identity Verification Assertion IVA (totally fake, build from scratch, or modified from a legitimate IVA).
5. **T.IVA_Eavesdropping:** The attacker may obtain Identity Verification Assertion by monitoring the communication line between Identity Verification Server and the Application Server or the communication line between Application Server and the Connected part (Service Provider Client Application for Type I, SPCA and SAS for Type II and TOE for Type III).
6. **T.IVA_Confidentiality_Integrity (valid only for offline mode of TOE on SSR Type III):** An attacker may steal or change the IVAs stored in the SSR Type III memory area during the offline operation of the SSR Type III.
7. **T.Repudiation:** The Service Requester (or the Service Attendee) may repudiate the Identification Verification Assertion.
8. **T.Fake_TOE_to_SR:** 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.
9. **T.Fake_TOE_to_External_Entities:** An attacker may introduce himself/herself as legitimate TOE to the external entities: eID Card, External Biometric Sensor, External PIN Pad. 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.
10. **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.
11. **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.
12. **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.
13. **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.
14. **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.
15. **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.
16. **T.Illegitimate_EBS:** An attacker may change the outcome of biometric verification or steal or modify the transmitted biometric template, thus collect biometric information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee by using an illegitimate biometric sensor.
17. **T.EBS_Comm:** An attacker may change the outcome of biometric verification; steal or modify the transmitted biometric template, thus collect biometric information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee through
 - a. eavesdropping and modifying the communication;
 - b. hijacking or replaying the authentication session between the TOE and the EBB.
18. **T.Illegitimate_EPP:** An attacker may change the outcome of PIN verification or steal or modify the transmitted PIN, thus collect PIN information from the Cardholders or damage the correct operation of the Identification and Authentication or Service Requester of Service Attendee by using an illegitimate external PIN-PAD.

	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	28/08/2015	No

- 19. T.EPP_Comm:** An attacker may steal or modify the transmitted PIN, thus collect PIN information from the Cardholders or damage the correct operation of the Identification and Authentication of Service Requester or Service Attendee through (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between SSR and EPP.
- 20. T.eIDC_Comm:** 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.
- 21. 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 SSR Type II.
- 22. T.Illegitimate_APS:** An attacker may use illegitimate Application Server (APS) 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 SSR Type III.
- 23. 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.
- 24. 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.
- 25. T.Audit_Data_Compromise:** An attacker may change or delete the audit data by physically accessing the audit memory area.
- 26. T.TOE_Manipulation:** An attacker may manipulate the operation or probe the internals of the SSR. SAM PIN could be obtained by probing the internals of the SSR, or DTN or Audit data could be manipulated. In addition, a counterfeit Identity Verification Assertion could be created.
- 27. T.Fake_SAM:** An attacker may issue a fake SAM to obtain the SAM-PIN.
- 28. T.Stolen_SAM:** An attacker may steal a SAM and use it to build an illegitimate SSR.
- 29. T.Revoked_SAM:** An attacker may use a Revoked SAM to build an illegitimate 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	28/08/2015	No


2 CERTIFICATION RESULTS

2.1 PP Identification

Certificate Number	21.0.03/TSE-CCCS/PP-010
PP Name and Version	Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.5
PP Document Title	Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System
PP Document Version	v2.5
PP Document Date	09.11.2015
Assurance Level	EAL4+ (ALC_DVS.2)
Criteria	<ul style="list-style-type: none"> Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	None
Common Criteria Conformance	<ul style="list-style-type: none"> Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant.
Sponsor and Developer	TÜBİTAK BİLGEM
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy


- 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.

	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	28/08/2015	No

4. **P.Terminal_Cert_Update:** Terminal Certificate will be renewed within a period defined in TS 13584 [3]. Client application (for TOE on SSR type I or II), SSR Access Server (for TOE on Type II with SAS) or Application Server (for TOE on SSR Type III) shall update the Secure Messaging and Role Card Verifiable Certificates of SAM one day before the expiration day.
5. **P.Time_Update:** The time shall be updated using the real time that is received only from trusted entities.
6. **P.Offline_Operation:** 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.
Additionally, in cases when the SSR Type III (mobile SSR) cannot reach to Application Server, TOE on SSR Type III is allowed to operate offline for at most maximum offline working time which is defined by the authorized foundation. IVAs shall be stored on the SSR Device securely and transmitted to APS before this time.
7. **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 the only condition to go back to Initialization & Configuration Phase.
DTN and SAM PIN shall be written to the SSR Device during Initialization & Configuration Phase.

2.3 Assumptions and Clarification of Scope


1. **A.SPCA:** It is assumed that Service Provider Client Application is a trusted third party and its communication with SSR occurs in a secure environment via USB interface. However, for SSR Type II with SAS, there is no direct connection between the SSR and the SPCA, SPCA communicates to the SAS through 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 SSR Device to the Client Application is preserved by the foundation sustaining the Client Application.
2. **A.IVPS:** It is assumed that the IVPS prepares and sends the policy correctly.
3. **A.EBS-EPP:** It is assumed that legitimate External Biometric Sensor (EBS) and legitimate External Pin Pad (EPP) work correctly.
4. **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.
5. **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.
6. **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.
7. **A.SAM_PIN_Environment:** It is assumed that the PIN value of the SAM in the SSR is defined in the SSR in secure 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	28/08/2015	No

Threats, OCPs and assumptions defined in the Security Problem Definition are matched with the three types of the SSR Device in Table .

Table 2. Relevance of Threats, OSPs and Assumptions to the three TOE types

Security Problem Definition	Applies to
T.Revoked_eIDC	Applies to all
T.Stolen_eIDC	Applies to all
T.IVA_Fraud	Applies to all
T.IVA_Eavesdropping	Applies to all
T.IVA_Confidentiality_Integrity	Applies to TOE on SSR Type III with offline mode feature
T.Repudiation	Applies to all
T.Fake_TOE_to_SR	Applies to all
T.Fake_TOE_to_External_Entities	Applies to all
T.SA_Masquerader	Applies to TOE on SSR Type II and Type III
T.SA_Abuse_of_Session	Applies to TOE on SSR Type II and Type III
T.Fake_Policy	Applies to all
T.Fake_OCSP_Response	Applies to all
T.RH_Comm	Applies to all
T.RH_Session_Hijack	Applies to all
T.Illegitimate_EBS	Applies to TOE on SSR with External Biometric Sensor
T.EBS_Comm	Applies to TOE on SSR with External Biometric Sensor
T.Illegitimate_EPP	Applies to TOE on SSR with External Pin Pad
T.EPP_Comm	Applies to TOE on SSR with External Pin Pad
T.eIDC_Comm	Applies to all
T.Illegitimate_SAS	Applies to TOE on SSR Type II
T.Illegitimate_APS	Applies to TOE on SSR Type III
T.DTN_Change	Applies to all
T.SAM-PIN_Theft	Applies to all
T.Audit_Data_Compromise	Applies to all
T.TOE_Manipulation	Applies to all
T.Fake_SAM	Applies to all
T.Stolen_SAM	Applies to all
T.Revoked_SAM	Applies to all
P.TOE_Update	Applies to all
P.Re-Authentication	Applies to all
P.Terminal_Cert_Update	Applies to all
P.Time_Update	Applies to all
P.Offline_Operation	Applies to TOE on SSR Type I, Type II and Type III but differently.
A.SPCA	Applies to all
A.IVPS	Applies to all
A.EBS-EPP	Applies to TOE on SSR with EBS and/or EPP
A.PC	Applies to all
A.APS-IVPS	Applies to all
A.Management_Environment	Applies to all
A.SAM PIN_Environment	Applies to all

	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	28/08/2015	No

2.4 Architectural Information

1-Operational Environment for SSR Type I

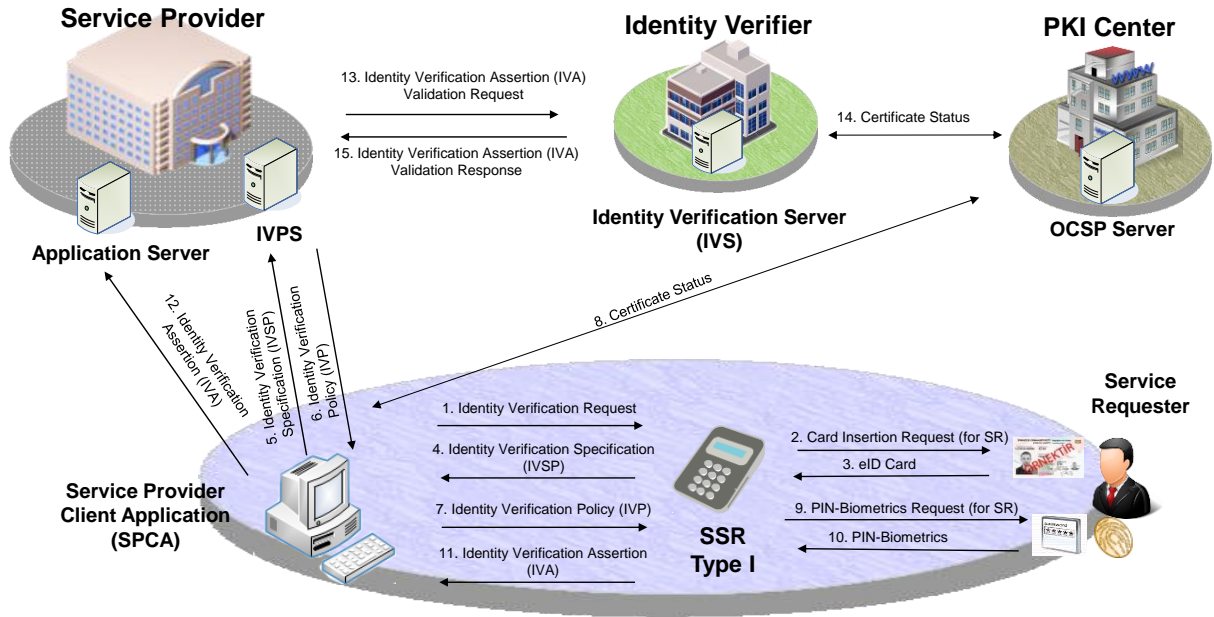



Figure 1. User Environment of Type I

The following scenario explains how Type I devices perform Identity Verification Operation in the environment shown in Figure 1. 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. Once the TOE receives this request, it asks the SR to insert his/her eID card into the smartcard slot. After the eID card is inserted, the TOE sets up a secure messaging session with the eID card. Having read the cardholder's personal message from the eID card, the TOE displays it on the screen for the SR's approval. If the displayed message is approved by the SR, an Identity Verification Specification (IVSP), is generated by the TOE, and sent to SPCA. Next, SPCA connects to the Identity Verification Policy Server (IVPS) and gets the Identity Verification Policy (IVP) for the SR specified in the IVSP. After that, SPCA sends the IVP to the TOE. Since the policy 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 the organizational policies defined in TS 13584. 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 Protocol (OCSP) Server. If the online certificate validation cannot be achieved due to technical problems, there are two options to continue the operation:

- (i) the TOE validates the eID Card of the Service Requester using the Certificate Revocation List downloaded on the SSR Device. In this case, the information that "OCSP check could not be achieved" shall be included in the IVA.
- (ii) The TOE does not validate the eID Card of the Service Requester. 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 verification of the SR is done by the TOE using fingerprint, fingervein or palmvein data. At the end of the authentication, an Identity Verification Assertion (IVA) 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 and finally, the SPCA forwards the IVA to the IVS, where it's further validated and kept as the evidence for the operation. Until the IVA is validated by the IVS, the Identification and Authentication of SR is regarded as incomplete.

	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	28/08/2015	No

2-Operational Environment for SSR Type II

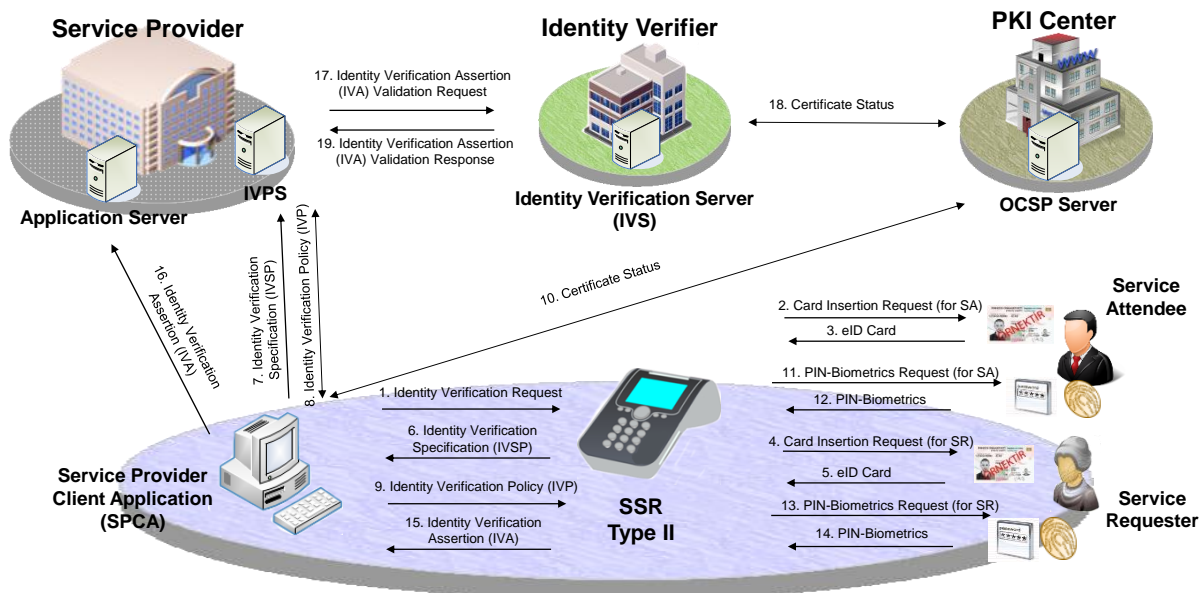


Figure 2. User Environment of Type II (without SAS)

User environments for Type II devices are given in Figure 2 and Figure 3. As seen, two smartcard slots are required for Type II devices. The second smartcard slot is needed for Service Attendee support. Operation is initiated by the SPCA. If SSR Access Server (SAS) exists as shown in Figure 3, the SPCA communicates to the TOE through the SAS via Ethernet interface, otherwise, it communicates to the TOE via USB interface.

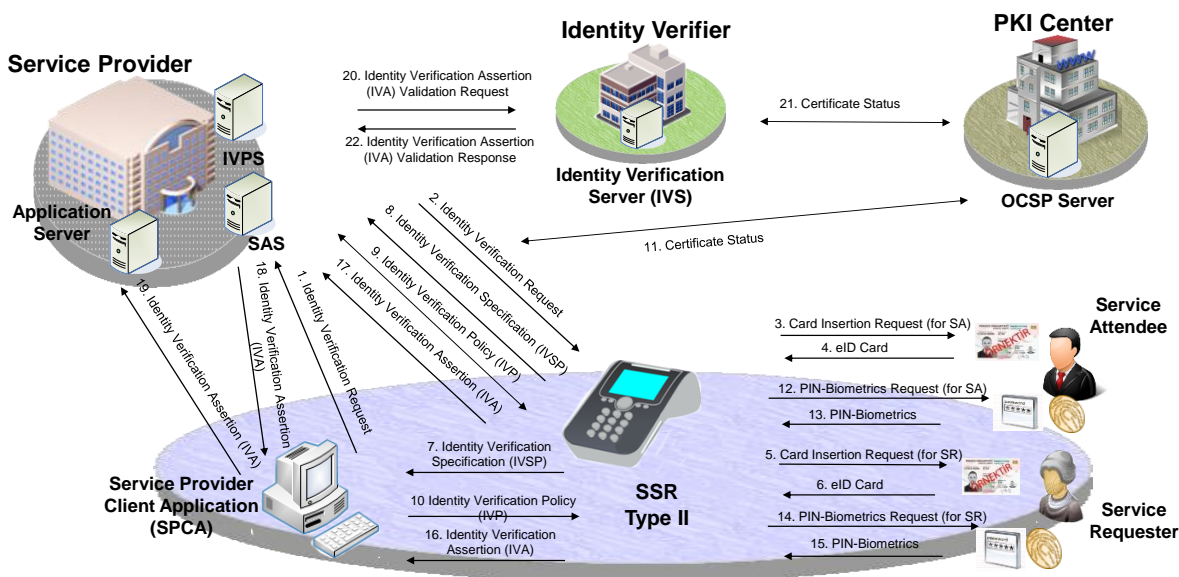



Figure 3. User Environment of Type II (with SAS)

In this scenario, the procedures are similar to the scenario for Type I SRR devices. However, in addition to Identification and Authentication of SR, Type II SRR devices also support Identification and Authentication of Service Attendee (SA) thanks to the second smartcard slot. At the end of the Identification and Authentication of SR and SA, an Identity Verification Assertion (IVA) is generated by the TOE. This time the IVA includes Service Attendee information as well. The TOE sends the IVA to the SPCA.

	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	28/08/2015	No

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.

3-Operational Environment for SSR Type III

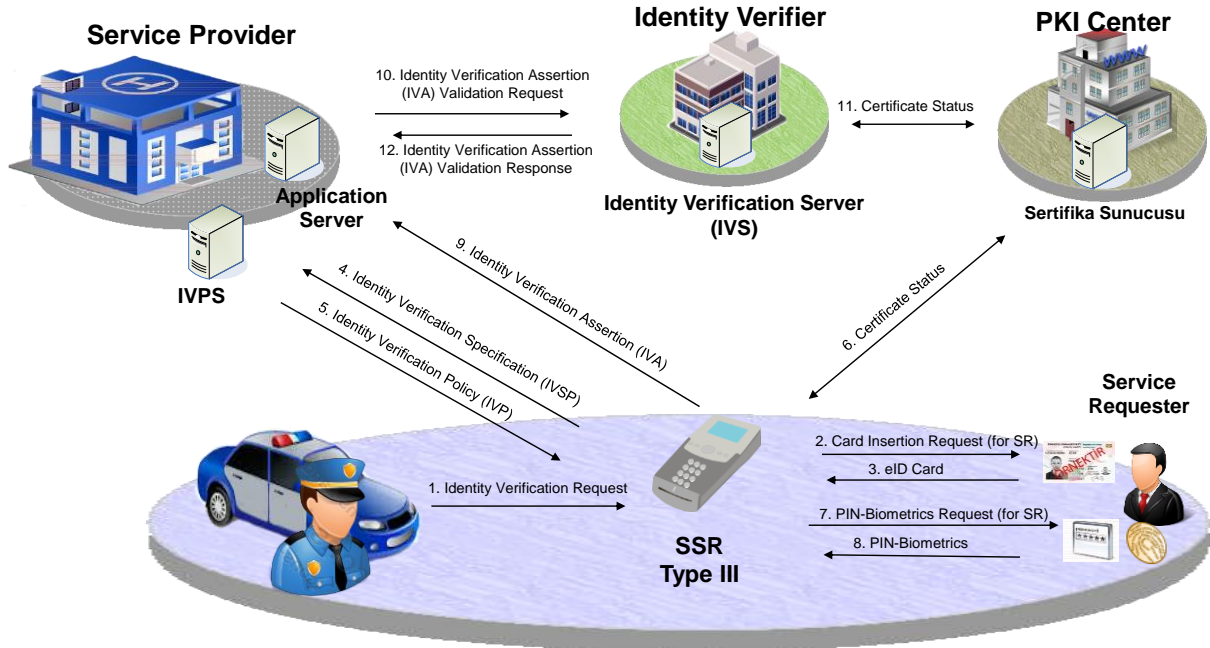



Figure 4. User Environment of Type III

User environment for Type III devices is given in Figure 4. Type III device is intended for mobile use. As seen, the environment doesn't require a PC. The TOE performs the functions of SPCA itself. It directly communicates to OSPCS, Application Server and IVPS. Type III devices may have one or two smartcard slots depending on usage. In the scenario, the procedures are similar to the scenario for Type I and Type II devices. However, the TOE itself initiates the Identification and Authentication Operation. In addition, offline usage scenarios are defined for mobile SSR Device. In case OCSP Server is not reached;


(i)TOE validates the eID Card of the Service Requester from the Revocation List downloaded on the SSR Device and puts the information that OCSP could not be achieved into the IVA.

(ii)TOE does not validate the eID Card and puts the information that OCSP and Revocation List control could not be achieved in the IVA. This scenario is the same as the Type I and Type II Devices. However, the revocation list shall be downloaded onto the mobile SSR since SSR Device could run totally offline for maximum offline working time duration. In addition, if the connection with the APS is failed, IVAs could be stored in the SSR Device securely until the device becomes online again. The maximum offline working time is defined by the authorized foundations. Stored IVAs stored be transmitted to APS securely before this time.

	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	28/08/2015	No

2.5 Security Functional Requirements

Security Function Class	Function Family	Security Functional Component
CLASS FAU: SECURITY AUDIT	FAU_GEN	FAU_GEN.1
	FAU_ARP	FAU_ARP.1
	FAU_STG	FAU_STG.1
		FAU_STG.4
FAU_SAA	FAU_SAA.1	
CLASS FCS: CRYPTOGRAPHIC SUPPORT	FCS_CKM	FCS_CKM.1/SM - Cryptographic key generation for secure messaging with eID, SA, EBS, EPP and Role Holder
		FCS_CKM.1/SM_TLS - Cryptographic key generation for secure messaging with Identity Verification Server, Application Server and SSR Access Server
		FCS_CKM.1/IVA_Keys - Cryptographic key generation for IVA Confidentiality and Integrity
		FCS_CKM.4
	FCS_COP	FCS_COP.1/SHA-256 - Cryptographic operation SHA 256
		FCS_COP.1/AES-CBC - Cryptographic AES CBC operation
		FCS_COP.1/AES-CMAC - Cryptographic CMAC operation
		FCS_COP.1/RSA - Cryptographic RSA encryption operation
		FCS_COP.1/Sign_Ver - Cryptographic signature verification operation
	CLASS FIA: IDENTIFICATION AND AUTHENTICATION	FIA_AFL
FIA_UID		FIA_UID.2
FIA_UAU		FIA_UAU.2
		FIA_UAU.5
		FIA_UAU.6
		FIA_UAU.7
CLASS FCO: COMMUNICATION	FCO_NRO	FCO_NRO.2
CLASS FMT: SECURITY MANAGEMENT	FMT_MOF	FMT_MOF.1/Verify - Management of security functions behavior - verify
		FMT_MOF.1/Upgrade - Management of security functions behavior - upgrade
	FMT_MTD	FMT_MTD.1/SAM - PIN Management of TSF data
		FMT_MTD.1/DTN - Management of TSF data - Device Tracking Number
		FMT_MTD.1/Time - Management of TSF data -Time
	FMT_SMF	FMT_SMF.1
FMT_SMR	FMT_SMR.1	
CLASS FPT: PROTECTION OF THE TSF	FPT_STM.	FPT_STM.1
	FPT_IDA	FPT_IDA.1/CVC – Imported TSF Data Authentication - Card Verifiable Certificates
		FPT_IDA.1/IVP - Imported TSF Data Authentication - Identity Verification

	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	28/08/2015	No

	FPT_SSY	Policy
		FPT_IDA.1/OCSP - Imported TSF Data Authentication - OCSP
		FPT_IDA.1/TOE_Upgrade - Imported TSF Data Authentication - TOE Upgrade Package
		FPT_SSY.1/Cert - State Synchronization - Secure Messaging and Role CVC
	FPT_SSY.1/SAM - State Synchronization - SAM	
	FPT_SSY.1/IVC - State Synchronization - IVC	
	FPT_SSY.1/RH_Auth_Status - State Synchronization Role Holder Authentication Status	
	FPT_TST	FPT_TST.1
	FPT_EMSEC	FPT_EMSEC.1
	FPT_FLS	FPT_FLS.1
CLASS FDP: USER DATA PROTECTION	FDP_SDI	FDP_SDI.2
	FDP_IFC	FDP_IFC.1
	FDP_IFF	FDP_IFF.1
	FDP_ITC	FDP_ITC.1
	FDP_ETC	FDP_ETC.2
CLASS FTP: TRUSTED PATH/CHANNELS	FDP_RIP	FDP_RIP.1
	FTP_ITC	FTP_ITC.1

2.6 IT Security Assurance Requirements


Assurance requirements for Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.5 are consistent with assurance components in CC Part 3 and evaluation assurance level is EAL4+ (ALC_DVS.2).

2.7 Results of the Evaluation

The evaluation is performed with reference to the CC v3.1 and CEM v3.1. The verdict of Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.5 is “pass” as it satisfies all requirements of APE class of CC. Therefore, the evaluation results were decided to be “suitable”.

2.8 Evaluator Comments / Recommendations

There are no recommendations concerning the Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System v2.5.

	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	28/08/2015	No


3 PP DOCUMENT

Information about the Protection Profile document with associated with this certification report is as follows:

Name of Document: Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System

Version No: 2.5

Date of Document: 09.11.2015

	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	28/08/2015	No

4 GLOSSARY & ACRONYMS

4.1 Glossary

Service Provider Environment:

SCPA (Service Provider Client Application): The external system that requests the identity verification. The SCPA may directly state the method that will be used in the identity verification process or may state the method will be declared by the IVPS. And as a final option the SCPA may state that the default method stored in the TOE should be used in the identity verification process.

IVPS (Identity Verification Policy Server): The external system that prepares the Identity Verification Policy (Identity Verification Policy) and sends it to the TOE. The TOE performs the identity verification method defined in the policy.

IVS (Identity Verification Server): The external entity that validates the IVAs created by the TOE.

Identity Verification Environment:

eID Card (Electronic Identity Card): The national identity card used by service requester for claiming and proving his or her identity. eID Card is issued by or on behalf of General Directorate of Civil Registration and Nationality – Ministry of the Interior.

SR (Service Requester): Service requester is the person who claims and proves his or her identity. The service requester claim starts with presenting eID Card to the SSR. The TOE, the SAM and the Service Attendee together verify the claim interacting with the Service Requester and the eID Card.

SA (Service Attendee): Service Attendee is the person who attends the identity verification process and approves if the photo displayed by the SSR belongs to the service requester. Service Attendee is also subject to prove his or her identity one of the methods.

OCSPS (Online Certificate Status Protocol Server): The server that keeps the revocation status of the IVCs. The OCSPS responds to the OCSP queries with the revocation status of the queried IVC.

Malicious Actors and Malicious External Systems:

Identity Faker: The attacker who tries to masquerade his or her identity with someone else's identity.

Illegitimate eID Card: An identity faker may use three types of illegitimate eID Card: a counterfeit eID Card, a forged eID Card and a revoked eID Card.


The Proxy Entities:

PC (Personal Computer): The computer the UIS or NIS is running on.

SSR Environment:

SAM (Secure Access Module): The SAM is the secure element of the SSR. The critical security functionality of the SSR is performed by the SAM. Since the TOE is the application software of the SSR, the SAM is an external element. The TOE accesses the SAM services through PIN verification.

The SSR Platform: The SAM and the SSR Environment are the non-TOE hardware, software and firmware that the TOE needs to function. The SSR environment at minimum consists of USB Interface, the smart card interfaces, graphic display, Service Requester interface, real time clock, execution environment and file system. Optionally depending on the configuration, the TOE may have Service Attendee interface, biometric sensor, Ethernet interface and interfaces for EBS and EPP. The SSR environment should also include security features to protect itself from tampering.


	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	28/08/2015	No

EBS (External Biometric Sensor): Optional external entity connected to the TOE. Depending on the sensor type, it sends the biometric template or biometric verification result to the TOE.

EPP (External PIN-PAD): Optional external entity connected to the TOE. The EPP is present only for TOE of Configuration Type III. External PIN_PAD offers convenience to the Service Requester. When external PIN-PAD is available, the Service Requester inserts his or her eID Card and enters IVC-PIN to external PIN-PAD.

4.2 Acronyms

APS: Application Server
CRL: Certificate Revocation List
CVC: Card Verifiable Certificate
DA: Device Authentication
DTN: Device Tracking Number
EBS: External Biometric Sensor
eID: Electronic Identity
EPP: External pin Pad
eIDMS: Electronic Identity Management System
eID Card: Electronic Identity Card of Turkish Republic
eIDVS: Electronic Identity Verification System
eSign: Electronic Signature
IV: Identity Verification
IVA: Identity Verification Assertion
IVC: Identity Verification Certificate
Identity Verification Policy: 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
SAM: Security Access Module
SAS: SSR Access Server
SPCA: Service Provider Client Application
SPSA: Service Provider Server Application
SSR: Card Acceptance Device
TA: Terminal Authentication

	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	28/08/2015	No

5 BIBLIOGRAPHY

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012
- [2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012
- [3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: August,4,2015
- [4] Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System
- [5] ETR 48 TR 02 /13.11.2015