EGA Elektronik Güvenlik Altyapısı A.Ş.

Security Target of

EGA Application Firmware v1.0

for SSR Type I, SSR Type II with/without SAS, SSR Type III

Version Lite

18.09.2018

DOCUMENT HISTORY

Version	Change Date	Author	Changes
1.0.1	21.12.2017	Ümit Yaşar USTA	Initial Version
1.0.2	24.01.2018	Ümit Yaşar USTA	Changes according to GR1 and changed TOE name
1.1.0	05.02.2018	Muhammet Ali EVCİ	Changes according to GR2 and correction typos
1.2.0	15.02.2018	Muhammet Ali EVCİ	Correction typos
Lite	18.09.2018	Muhammet Ali EVCİ	Lite version

CONTENTS

LIST OF TABLES

1 ST INTRODUCTION

1.1 ST AND TOE REFERENCE

Title: Security Target of EGA Application Firmware v1.0 for SSR Type I, SSR Type II with/without SAS, SSR Type III

ST Reference: Lite

TOE Identification: EGA Application Firmware for SSR Type I, SSR Type II with/without SAS, SSR Type III

TOE Version: v1.0

CC Conformance: Common Criteria for Information Technology Security Evaluation, Version 3.1 (Revision 5)

PP Conformance: Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for Electronic Identity Verification System, SSR_PP_2.8

Assurance Level: EAL4+ with ALC_DVS.2 augmentation

Keywords: Electronic Identity, Smartcard Reader, Identity Verification, Electronic Identity Card, Secure Smartcard Reader, Biometric Authentication

1.2 TOE OVERVIEW

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

As the Application Firmware of the SSR, the TOE performs;

- ✓ Identity verification of Service Requester and Service Attendee according to the eIDVS
- ✓ Securely communicating with the other system components
- ✓ As a result of the identity verification, produces an Identity Verification Assertion (IVA) signed by the Secure Access Module (SAM) inside the SSR.

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

1.2.1 MAJOR SECURITY FEATURES OF A TOE

The following security mechanisms are primarily mediated in the TOE:

❖ ***Identification and Authentication***

- Cardholder verification by using PIN and biometrics (fingerprint data).
- Authentication of eID Card,
- Authentication of Role Holder,
- Authentication of SAM,
- Authentication of the TOE by SAM and by Card Holder (Service Requester and Service Attendee) and by external entities (e.g. Role Holder, External Biometric Sensor and External PIN PAD etc.)

❖ ***Secure Communication between the TOE and***

- SAM
- eID Card

- Role Holder
- External Biometric Sensor and External PIN PAD
- SSR Access Server (SAS)

- ***Security Management***
- ***Self-Protection***
- ***Audit***

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

1.2.2 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

1.2.2.1 Typical Software/Firmware Environment of TOE

File System and Software Libraries
Embedded Operating System Kernel
Smartcard Reader IC Firmware

In a typical software environment, the TOE runs at the top of an embedded operating system, its file-system and software libraries. It communicates to a smartcard reader IC firmware within the device.

1.2.2.2 Hardware Environment of TOE (SSR Hardware and SAS)

The TOE is stored in a non-volatile memory location in the SSR Hardware as an encrypted binary file. During power-up, the encrypted TOE is decrypted before its execution. A Typical SSR Hardware environments of TOE are stated in Figure 1.

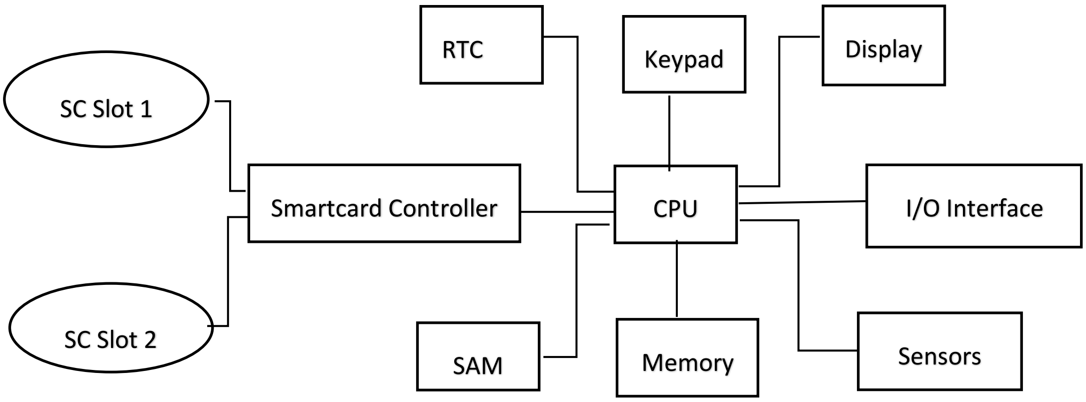


Figure 1 Typical SSR Hardware

Hardware environment of TOE consists of the following components:

- I/O interfaces
- User interfaces (keypad, display, optional biometric sensor)
- CPU
- Memory Components

- Two smartcard slots
- Secure Access Module
- Real Time Clock
- Physical and logical security barriers (shields, tamper switches etc.).

SSR Devices is developed that have the capability to operate together with additional hardware components, which are Internal Biometric Sensor, External Biometric Sensor (EBS) and External PIN PAD (EPP). Some hardware components such as biometric sensor, Ethernet port, WiFi, GPRS or Bluetooth are optional depending on the SSR type. In the case of usage of additional hardware components, the TOE authenticates the external device and protect the confidentiality and integrity of the communication between the TOE and the external device.

1.2.3 TOE TYPE

The TOE is the SSR Device firmware. The TOE covers Type I, Type II with or without SAS and Type III secure smart card readers. SAS usage for Type II is optional. External PIN PAD (EPP) and External Biometry Sensor (EBS) usage are optional.

1.2.4 ACTORS AND EXTERNAL ENTITIES

Actors: Service Requester (SR)**,** Service Attendee (SA), Identity Faker, Administrator

External Systems: Service Provider Client Application (SPCA)**,** Identity Verification Policy Server (IVPS), Application Server (APS), SSR Access Server (SAS), Identity Verification Server (IVS), Electronic Identity Card (eID Card), Service Requester (SR), Service Attendee (SA), Online Certificate Status Protocol (OCSP) Server, Identity Faker, Illegitimate eID Card, SSR Access Server, PC, SAM, External Biometric Sensor and External PIN PAD.

1.2.5 OPERATIONAL ENVIRONMENTS OF SSR

1.2.5.1 Operational Environment for SSR Type I

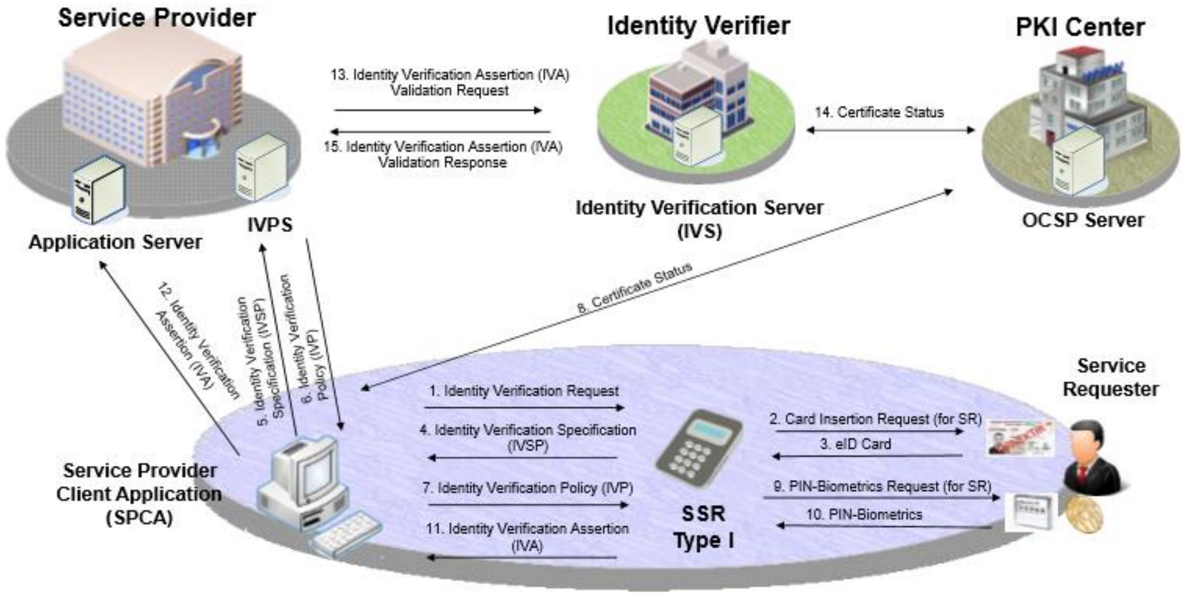

Service Provider
Identity Verifier
PKI Center
13. Identity Verification Assertion (IVA) Validation Request
15. Identity Verification Assertion (IVA) Validation Response
14. Certificate Status
Application Server
IVPS
Identity Verification Server (IVS)
OCSP Server
8. Certificate Status
12. Identity Verification Assertion (IVA)
5. Identity Verification Specification (IVSP)
6. Identity Verification Policy (IVP)
Service Requester
1. Identity Verification Request
4. Identity Verification Specification (IVSP)
7. Identity Verification Policy (IVP)
11. Identity Verification Assertion (IVA)
2. Card Insertion Request (for SR)
3. eID Card
9. PIN-Biometrics Request (for SR)
10. PIN-Biometrics
Service Provider Client Application (SPCA)
SSR Type I

Figure 2 User Environment for SSR Type I

User environment for SSR Type I is shown in Figure 2. 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 SR approves the displayed message, an Identity Verification Specification 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 that 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 checked online with the help of the Online Certificate Status Protocol (OCSP) Server. If the online certificate check cannot be achieved due to technical problems, there are two options to continue the operation: (i) the TOE checks 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 check 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, PIN verification and 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.

1.2.5.2 Operational Environment for SSR Type II with or without SAS

Two smartcard slots are required for Type II devices. The second smartcard slot is needed for Service Attendee support. The SPCA initiates the operation. If SSR Access Server (SAS) exists as shown in the Figure 3, the SPCA communicates to the TOE through the SAS via Ethernet interface. If SSR Access Server (SAS) does not exist as shown in the Figure 4, the SPCA communicates to the TOE via USB interface. 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. 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.

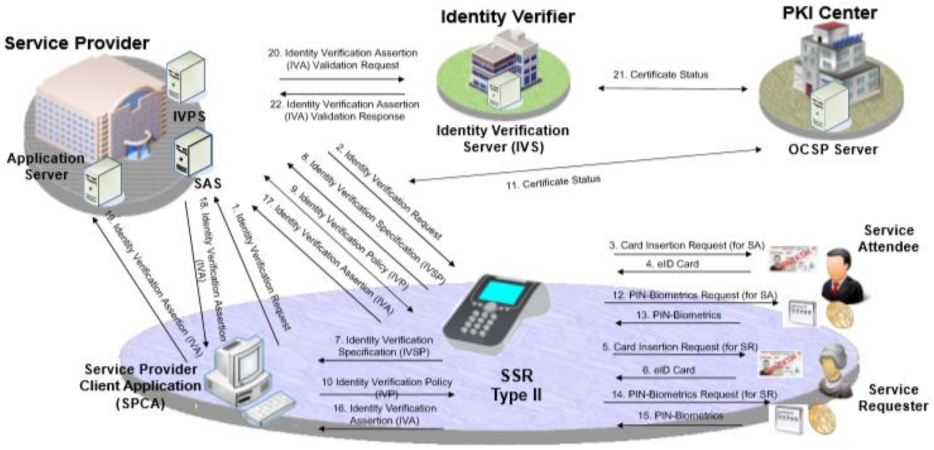

Service Provider
IVPS
Application Server
SAS
Identity Verifier
Identity Verification Server (IVS)
PKI Center
OCSP Server
20. Identity Verification Assertion (IVA) Validation Request
22. Identity Verification Assertion (IVA) Validation Response
21. Certificate Status
11. Certificate Status
2. Identity Verification Request
8. Identity Verification Specification (IVSP)
9. Identity Verification Policy (IVP)
17. Identity Verification Assertion (IVA)
1. Identity Verification Request
18. Identity Verification Assertion (IVA)
19. Identity Verification Assertion (IVA)
7. Identity Verification Specification (IVSP)
10 Identity Verification Policy (IVP)
16. Identity Verification Assertion (IVA)
Service Provider Client Application (SPCA)
SSR Type II
3. Card Insertion Request (for SA)
4. eID Card
12. PIN-Biometrics Request (for SA)
13. PIN-Biometrics
5. Card Insertion Request (for SR)
6. eID Card
14. PIN-Biometrics Request (for SR)
15. PIN-Biometrics
Service Attendee
Service Requester

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

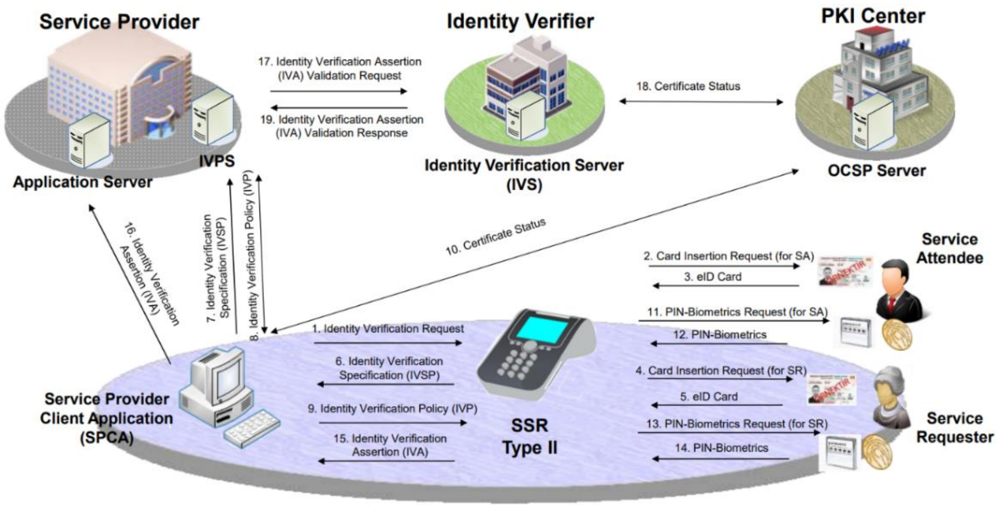

Service Provider
Identity Verifier
PKI Center
17. Identity Verification Assertion (IVA) Validation Request
19. Identity Verification Assertion (IVA) Validation Response
18. Certificate Status
IVPS
Application Server
Identity Verification Server (IVS)
OCSP Server
16. Identity Verification Assertion (IVA)
7. Identity Verification Specification (IVSP)
8. Identity Verification Policy (IVP)
10. Certificate Status
Service Attendee
2. Card Insertion Request (for SA)
3. eID Card
11. PIN-Biometrics Request (for SA)
12. PIN-Biometrics
1. Identity Verification Request
6. Identity Verification Specification (IVSP)
9. Identity Verification Policy (IVP)
15. Identity Verification Assertion (IVA)
Service Provider Client Application (SPCA)
SSR Type II
4. Card Insertion Request (for SR)
5. eID Card
13. PIN-Biometrics Request (for SR)
14. PIN-Biometrics
Service Requester

Figure 4 User Environment of Type II SSR (without SAS)

1.2.5.3 Operational Environment for SSR Type III

User environment for Type III devices is given in Figure 5. 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 OCSP Server, 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, TOE checks 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. 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 should be transmitted to APS securely before this time.

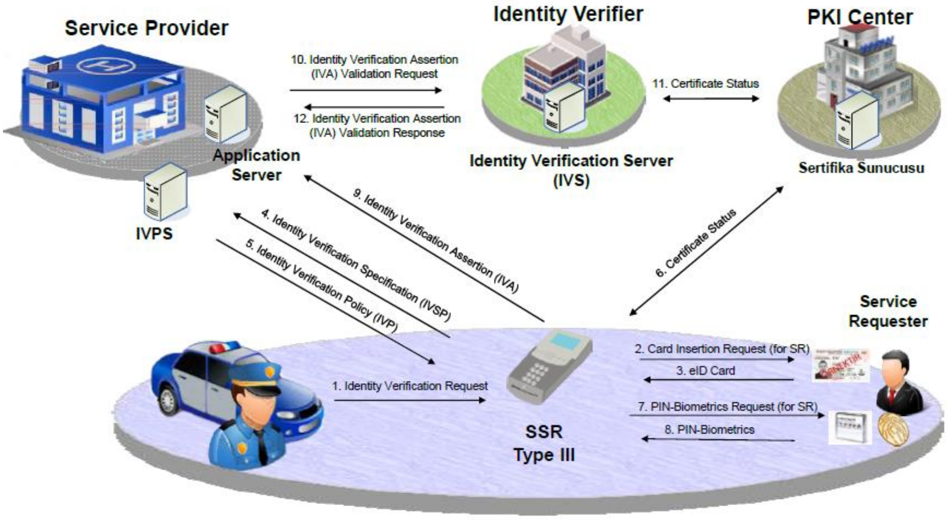

Service Provider
Identity Verifier
PKI Center
10. Identity Verification Assertion (IVA) Validation Request
12. Identity Verification Assertion (IVA) Validation Response
11. Certificate Status
Application Server
IVPS
Identity Verification Server (IVS)
Sertifika Sunucusu
9. Identity Verification Assertion (IVA)
4. Identity Verification Specification (IVSP)
5. Identity Verification Policy (IVP)
6. Certificate Status
Service Requester
2. Card Insertion Request (for SR)
3. eID Card
1. Identity Verification Request
7. PIN-Biometrics Request (for SR)
8. PIN-Biometrics
SSR Type III

Figure 5 User Environment of Type III

1.2.6 TOE LIFE CYCLE

The TOE shall support:

- Initialization & Configuration
- Operation Phases

After production, the TOE is in Initialization & Configuration Phase. In the Initialization & Configuration Phase, the TOE and all other SSR firmware including operating system and file system are installed to the SSR Device by Initialization agent in a secure environment. After the initialization and the configuration, the TOE switches to the Operation Phase and doesn't go back to the Initialization & Configuration Phase again except tampering of the SSR.

Tampering event is the only condition to set the TOE back to the Initialization & Configuration Phase. If a tampering event is detected, cryptographic data (keys, SAM Pin, etc.) within the SSR are deleted and the TOE becomes out of service; the TOE and other software including operating system, file system and other firmware need to be re-installed and it has to be initialized and configured by authorized personnel.

1.3 TOE DESCRIPTION

TOE is the application firmware which is loaded into the embeded flash memory of SSR. It provides personal identity verification (PIV) and digital signature operations for smartcard-based services over electronic media.

1.3.1 PHYSICAL SCOPE OF TOE

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

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

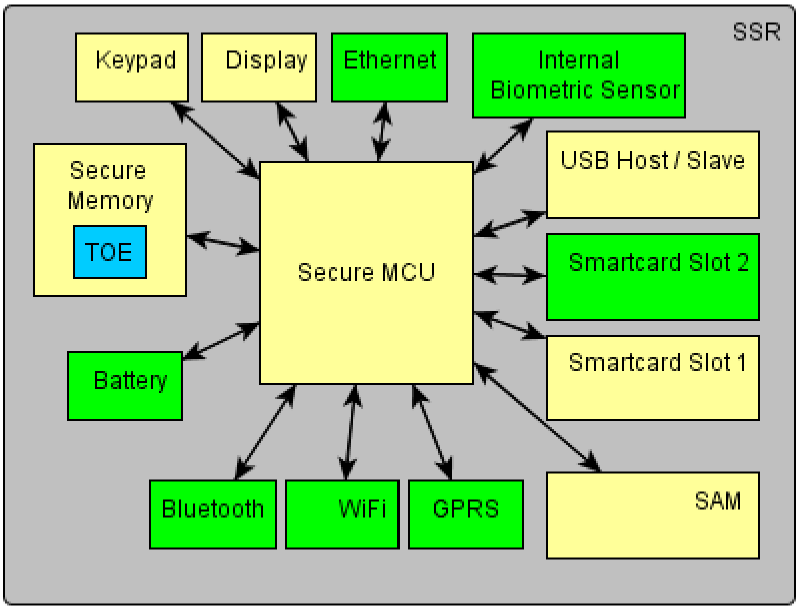


Figure 6 Physical Scope of the TOE

The physical scope of the TOE software is shown in Figure 6. The TOE is shown as blue and is stored in a non-volatile memory location in the SSR Hardware as an encrypted binary file. During power-up, the encrypted TOE is decrypted before its execution. At initialise phase of TOE, TOE reads configuration file and when the TOE boots up, operational environments are checked by TOE and operates according to hardware peripherals and config file.

While yellow components in Figure 6 take place on all SSR types, however green components show the optional parts of the SSRs. For example: when the TOE detects Ethernet and Smartcard Slot 2 at the boot-up, TOE operates as Type II with SAS functionality.

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

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

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

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

1.3.2 LOGICAL SCOPE OF TOE

This section describes the logical security features of the TOE. Details can be found in Section 7.1.

TRUSTED PATH

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

IDENTIFICATION AND AUTHENTICATION

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

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

SECURE COMMUNICATION

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

CRYPTOGRAPHIC OPERATION

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

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

SECURITY MANAGEMENT

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

TSF PROTECTION

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

SECURITY AUDIT

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

USER DATA PROTECTION

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

2 CONFORMANCE CLAIMS

2.1 CC CONFORMANCE CLAIM

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001 Version 3.1 Revision 5, April 2017, (CC Part 1)
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB--2017-04-002 Version 3.1 Revision 5, April 2017, (CC Part 2)
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB--2017-04-003 Version 3.1 Revision 5, April 2017, (CC Part 3) as follows
  - Part 2 extended
  - Part 3 conformant
- The Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB--2017-04-004 Version 3.1 Revision 5, April 2017, [CEM] has to be taken into account.

2.2 PP CLAIM

This ST claims strict conformance to

- Protection Profile for Application Firmware of Secure Smartcard Reader (SSR) for Electronic Identity Verification System, Version 2.8, 01.08.2017.

2.3 PACKAGE CLAIM

This ST is conforming to assurance package EAL4 augmented with ALC_DVS.2 defined in CC part 3 (CC Part 3).

EAL4 Assurance Class Assurance components and ALC_DVS.2 augmentation are listed below:

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

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

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 measure

ALC_LCD.1 Developer defined life-cycle model

ALC_TAT.1 Well-defined development tools

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

ATE_COV.2 Analysis of coverage

ATE_DPT.1 Testing: basic design

ATE_FUN.1 Functional testing

ATE_IND.2 Independent testing - sample

AVA_VAN.3 Focused vulnerability analysis

2.4 CONFORMANCE RATIONALE

The type of the TOE is consistent with TOE type of the PP.

The statement of the security problem definition is consistent with the statement of Type I, Type II with or without SAS and Type III security problem definition in the PP for which conformance is being claimed.

The statement of security objectives is consistent with the statement of Type I, Type II with or without SAS and Type III security objectives in the PP for which conformance is being claimed.

The statement of security requirements is consistent with the statement of Type I, Type II with or without SAS and Type III security requirements in the PP for which conformance is being claimed.

3 SECURITY PROBLEM DEFINITION

This part of the ST defines the security problem that is to be addressed by both the TOE and its environment. It consists of Assets, Subjects and External Entities, Organizational Security Policies, Threats and Assumptions.

3.1 ASSETS

The Secure Smart Card Reader (SSR) and the TOE is a part of eID Verification System. TOE carries out identification and authentication operations and accesses (reads out and performs management operations of) eID Card on behalf of authorized entities (Role Holder) who has privileges on the eID Card. TOE shall securely forward the user data read out from the eID Card; however, TOE does not store any user data. The TOE defined in this ST (the Application Firmware of the SSR) does not possess any user data.

Primary Assets: User Data		**Definition**	**Protected against loss of**
1	PIN and Biometry data	PIN and Biometry data of Service Requester and Service Attendee.	Integrity and confidentiality
2	SAM-PIN	Used to authenticate the TOE to the SAM	Integrity and confidentiality
3	Identity Verification Assertion (IVA)	Generated as the evidence of the identity verification operation.	Privacy, and authenticity
Secondary Assets: Security Services		**Definition**	**Protected against loss of**
4	Identification and Authentication of Service Requester and Service Attendee	Personal Identity Verification is performed by this service	Correct operation
5	Identification and Authentication of third party trusted IT Components	Identity Verification of third party IT Components are performed by this service. These components are Application Server (APS), SSR Access Server (SAS), External Biometric Sensor (EBS), External PIN PAD (EPP) and SAM	Correct operation
6	Access eID Card on behalf of Role Holder	Secure messaging session between the TOE and the Role Holder is setup. The TOE accesses the eID card on behalf of the Role Holder. Data transfer between the TOE and the Role Holder is managed in a secure manner using the secure messaging session.	Correct operation
Secondary Assets: TSF Data		**Definition**	**Protected against loss of**
7	Device Tracking Number of SSR	A number specific to each TOE that is written during initialization of TOE. Stored in the memory of the SSR	Integrity

8	Secure Messaging and Role Card Verifiable Certificates of SAM (in CVC Format)	Secure Messaging Certificate is used for Secure Messaging between the TOE and eID Card; Role Card Verifiable Certificate is used for Role Authentication of the SSR. These certificates are given by Device Management Certificate Authority and imported from SAM to the SSR Device and updated by the TOE before the expiry date.	Correctness
9	Current Time	The time defined by OCSP server. TOE uses this time for ID verification assertion.	Integrity
10	Audit Data	Audit Data	Integrity

Table 1 Primary and Secondary Assets

3.2 SUBJECTS AND EXTERNAL ENTITIES

The legitimate and the malicious actors and external entities are defined below in Table 2. The legitimate ones are given in the left column and the malicious ones are given in the right column of Table 2.

Legitimate subjects and entities	**Malicious subjects and entities**
Service Provider Environment	
Service Provider Client Application	See **Note 1**
Identity Verification Policy Server	Illegitimate Identity Verification Policy Server
Application Server	Illegitimate Application Server
SSR Access Server	Illegitimate SSR Access Server
Identity Verification Server	See **Note 2**
Identity Verification Environment	
eID Card	Illegitimate eID Card
Service Requester (SR)	Identity Faker (not real Service Requester)
Service Attendee (SA): validates photo of the card holder and has rights to proceed the operation even if the biometric verification fails	SA Masquerader (attacker acting as if Service Attendee)
SAM	Illegitimate SAM
External Biometric Sensor	Illegitimate External Biometric Sensor
External PIN PAD	Illegitimate External PIN PAD
Secure Smartcard Reader (SSR) hardware.	Illegitimate SSR hardware (manipulated and/or probed)
Role Holder	Illegitimate Role Holder (Malicious)

The Proxy Entities	
PC (on which the SPCA runs)	See **Note 3.**
Other Activities	
Initialization agent	-
Manufacturer service operator	Illegitimate service operator
Attacker	
Attacker (also covers the Identity Faker, SA Masquerader, Illegitimate Role Holder)	

Table 2 Legitimate and malicious actors and external systems

Note 1: It is assumed that no illegitimate Service Provider Client Application (SPCA) exists within the current context.

Note 2: It is assumed that no illegitimate Identity Verification Server (IVS) exists within the current context. The reason the IVS is taken into the scope this PP, is its required ability to distinguish the IVAs created by the TOE with the IVAs created by illegitimate TOEs.

Note 3: It is assumed that
(1) the PC is free of any malicious software and
(2) the environment between the USB Interface Software and the TOE is secure.
So no illegitimate USB Interface Software and illegitimate PC are defined within the system.

Note 4: Within the current system context, the role holder has privileges on the eID Card. The attacker will try to exploit these privileges to gain benefits.

Note 5: Initialization agent is assumed to pose no threat because the environment is secure and personal acts responsively.

Note 6: The attacker is the threat agent who tries to violate the security of the eID Verification System. Note that the attacker here is assumed to possess at most enhanced-basic attack potential (which means that the TOE to be tested against AVA_VAN.3).

Some of the entities defined in this section are valid for all the three types of SSR Device, however, some entities are irrelevant for one or two types of the SSR Device. Table 3 shows the relevance of these entities for three types of SSR Device.

Entity	**Applies To**
Service Provide Client Application	Applies to Type I and Type II.
Identity Verification Policy Server	Applies to all
Application Server	Applies to all (but only TOE on SSR Type III has direct contact)
SSR Access Server	Applies to Type II
Identity Verification Server	Applies to all
eID Card	Applies to all
Service Requester	Applies to all
Service Attendee	Applies to Type II and Type II
Online Certificate Status Protocol Server	Applies to all
PC	Applies to Type I and Type II

Security Access Module	Applies to all
SSR Hardware	Applies to all
External Biometric Sensor	Applies to configurations with External Biometric Sensor
External Pinpad	Applies to configurations with External Pin Pad

Table 3 Legitimate Entities vs SSR Types

3.3 THREATS

The threats that could be met by the TOE and its environment are given in Table 4.

Threat	Definition
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.
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 type III TOE and the Application Server or the communication line between SAS and type II TOE.
T. IVA_Confidentiality	An attacker may steal the IVAs stored in the SSR Type III memory area during the offline operation of the SSR Type III.
T. Repudiation	The Service Requester (or the Service Attendee) may repudiate the Identification Verification Assertion.
T. Fake_TOE_to_SR	An attacker may prepare a fake SSR 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 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.

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. 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.
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 (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between the TOE and the EBB.
T. Illegitimate_EPP	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 or Service Requester of Service Attendee by using an illegitimate External PIN-PAD.
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.

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.
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.
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.
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 SSR. SAM PIN could be obtained by probing the internals of the SSR, or DTN 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 SSR.
T. Revoked_SAM	An attacker may use a Revoked SAM to build an illegitimate SSR.

Table 4 Threats

3.4 ORGANIZATIONAL SECURITY POLICIES

The OSPs are given in the Table 5.

Policy	Policy Category and Definition
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 and remote upgrade.
P. Re-Authentication	Authentication of third party IT components will be renewed after 24 hours.

P. Terminal_Cert_Update	Terminal Certificate will be renewed within a period defined in TS 13584 [3]. 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.
P. Time_Update	The time shall be updated using the real time that is received only from trusted entities.
P. Offline_Operation	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.
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 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.
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.

Table 5 Organizational Security Policies

3.5 ASSUMPTIONS

The assumptions for the operational environment are given inTable 6.

Assumption	Definition

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
A.IVPS	It is assumed that the IVPS prepares and sends the policy correctly.
A.EBS-EPP	It is assumed that legitimate External Biometric Sensor (EBS) and legitimate External Pin Pad (EPP) work 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	It is assumed that the PIN value of the SAM in the SSR is defined in the 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.

Table 6 Assumptions for the Operational Environment

4 SECURITY OBJECTIVES

In this section, security objectives for TOE and security objectives for TOE Environment are given.

4.1 SECURITY OBJECTIVES FOR THE TOE

Objective	Definition
OT.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.
OT.Security_Failure	When a tampering event is detected, or SAM-PIN authentication failure occurs the TOE shall delete all user and/or security related data and enter out of service mode becoming unusable until reinstallation and re-initialization of the TOE.
OT.eIDC_Authentication	The TOE shall support the Card Authentication mechanism defined in TS 13584 [3]. When OCSP Server is not reached, certificate revocation status control of the Service Requester and the Service Attendee could be done using the Revocation List downloaded to SSR Device. The revocation list shall be up to date. If the certificate status control of Service Requester or the Service Attendee is carried out without OCSP Server, the information that OCSP check could not be realized shall be put in the IVA. If the OCSP Server is not reached and the Revocation List does not exist within the SRR, then the information that OCSP check and Revocation List check could not be realized shall be put in the IVA.
OT.PIN_Verification	The TOE shall support PIN Verification mechanism defined in TS 13584 [3] for Identification and Authentication of Service Requester and Service Attendee.
OT. Photo_Verification	The TOE shall support Photo Verification defined in TS 13584 [3] for Identification and Authentication of Service Requester.
OT. Biometric_Verification	The TOE shall support Biometric Verification defined in TS 13584 [3] for Identification and Authentication of Service Requester and Service Attendee if applicable.
OT.IVA_Signing	The created Identity Verification Assertion shall be electronically signed by the TOE (using SAM) . Otherwise the secure channel is founded in between SPCA and IVS

OT.IVA_Privacy (Valid for Type III)	If the created IVA in the TOE on SSR Type III cannot be transmitted due to connection problems, this IVA shall be stored in the SSR Device in encrypted form. The keys for encryption/decryption are generated by the SAM and transferred to the TOE via secure messaging. The stored IVAs shall be transmitted to the APS (after being decrypted) as soon as possible and not later than the maximum offline working time.
OT.PM_Verification	The eID Card lets the TOE to access Personal Message of the service requester after the secure messaging session defined in TS 13584 [3] is established between the TOE and the eID Card. The TOE shall display the Personal Message to the Service Requester, so that, the Service Requester verifies the authenticity of the TOE and the SSR, since only legitimate TOE can access to the Personal Message.
OT.SA_Identity_Verification	The TOE shall support Identification and Authentication of Service Attendee as defined in TS 13585 [4].
OT.Session_Ending	The TOE shall end the authentication session of the Service Attendee whenever the session expires and/or the eID Card of the Service Attendee is taken out. In addition, TOE shall re-authenticate each authenticated third party IT product after 24 hours. (SAS for TOE on SSR Type II, APS for TOE on SSR Type III, EPP if applicable, EBS if applicable)
OT.Identity_Verification_Policy_Authentication	The TOE shall verify that the source of received Identity Verification Policy is a legitimate IVPS.
OT.OCSP_Query_Verify	The TOE shall verify that the source of received information is a legitimate OCSPS.
OT.APS_DA	Mutual authentication between the TOE on SSR Type III and the APS shall be setup before TOE's doing any action.
OT.SAS_DA	Mutual authentication between the TOE on SSR Type II and the SAS (if applicable) shall be setup before TOE's doing any action.
OT.APS_SC	The TOE on SSR Device Type III shall communicate to APS securely via SSL-TLS as defined in TS 13584 [3].
OT.SAS_SC	The TOE on SSR Device Type II shall communicate to SAS securely via SSL-TLS as defined in TS 13584 [3].
OT.RH_DA [Role Holder Device Authentication]	Mutual authentication between the TOE and Role Holder shall be setup as defined in TS 13584 [3] before TOE's doing any action.
OT.RH_SC Secure Communication with Role Holder	The communication between the TOE and the Role Holder shall be secured by AES-256 CBC and AES-256 CMAC

	algorithms, mutual authentication mechanisms and key exchange method defined in TS 13584 [3].
OT.RH_Session_Ending	The TOE shall end the role holder authentication session of eID Card when the secure communication between the TOE and Role Holder ends.
OT.EBS_DA	The TOE shall support mutual authentication with the External Biometric Sensor as defined in TS 13584 [3].
OT.EBS_SC	The TOE shall ensure the confidentiality, integrity and authenticity of the communication going between the TOE and the External Biometric Sensor as defined in TS 13584 [3].
OT.EPP_DA [External PIN-PAD Device Authentication]	The TOE shall support mutual authentication with the External PIN-PAD defined in SSR Standard TS 13584 [3].
OT.EPP_SC	The TOE shall ensure the confidentiality, integrity and authenticity of the communication going between the TOE and External PIN-PAD as defined in TS 13584 [3].
OT.SM_eID Card [Secure Messaging between TOE and eID Card]	The TOE shall ensure the confidentiality, integrity and authenticity of the communication going between the TOE and the eID Card.
OT.TOE_Upgrade	The TOE shall have TOE update security management function. The TOE shall accept only the Upgrade Package associated with the corresponding SSR SAM. The upgrade operation shall only be enabled by the following roles: (i) Manufacturer Service Operator for manual upgrade operation, (ii) The following third-party IT components for online upgrade operation: • SAS for TOE on SSR Type II, • APS for SSR Type III. TOE shall verify that the source of received upgrade package is a legitimate software publisher and TOE shall have a mechanism to decrypt the received TOE upgrade package as defined in TS 13584 [3].
OT.DPM [Device Phase Management]	The TOE shall support Initialization & Configuration and Operation lifecycle phases. The phase change shall be from Initialization & Configuration to Operation. The TOE shall not be switched to the Initialization & Configuration Phase from the Operation Phase unless a tamper event is detected, and the TOE becomes out of service.
OT.SAM-PIN_Mgmt	The TOE shall have a management function to write the SAM-PIN to the SSR Device. The SAM PIN shall be written only by the initialization agent during Initialization & Configuration phase.

OT.DTN_Mgmt	The TOE shall have a management function to write the Device Tracking Number to the TOE. The DTN shall be written only by the initialization agent during Initialization & Configuration phase.
OT.Time_Mgmt	The TOE shall have a management function to set the real time that is received only from the OCSP Server.
OT.SM_ TOE_and_SAM [Secure Messaging between TOE and SAM]	The TOE shall protect the confidentiality, integrity and the authenticity of the communication between the TOE and the SAM.
OT.SAM-PIN_Sec	The TOE shall protect the confidentiality and integrity of the SAM-PIN during storage and operation regardless of device power state with the help of the SSR platform.
OT.DTN_Integrity	The TOE shall protect the integrity of the Device Tracking Number.
OT.Audit_Data_Protection	The TOE shall control access to the audit data and shall not allow attackers to read, change or delete.
OT.RIP [Residual Information Protection]	PIN, Biometry data, other user data and TSF data shall be copied to only volatile memory and be deleted in a secure way right after the end of the usage.
OT.Auth_SAM_by_TOE [Authentication of SAM by TOE]	The TOE shall authenticate the SAM before doing any operation.
OT.Cert_Update	At each Identity Verification Operation, the TOE shall control the validity of the Secure Messaging and Role Card Verifiable Certificates of the SAM. If the expiration date of these certificate(s) are closer than one day, TOE shall request updated certificates from the SSR Access Server (for TOE on Type II with SAS) or the Application Server (for TOE on SSR Type III) and update the certificates.

Table 7 Security Objectives for TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

Security objectives for the SSR Hardware and the User Environment of the SSR are given below inTable 8.

Objective	Definition

OE. SPCA	Service Provider Client Application shall be developed and used by trusted parties thus accepted as a trusted third-party IT product. In addition, the communication between SPCA and the SSR shall occur in secure environment. For the cases when the SPCA determines the identity verification method, the SPCA shall select the appropriate method. SPCA shall encrypt the Identity Verification Assertion before sending it to the Application Server (APS).
OE. IVPS	The IVPS shall: • Prepare and send the correct policy, • Protect the integrity and the authenticity of the policy (it shall sign the policy using its signing certificate), • Protect the confidentiality of the private key of its signing certificate.
OE. eID Card	The eID Card shall have the following properties: • Support PIN verification, • prevent usage of IVC Certificate Private key prior to PIN verification, • store the cardholder's digital photo, • store the cardholder's biometric data (fingerprint, fingervein and palmvein), • support terminal authentication as defined in TS 13584 [3], • store the cardholder's personal message (shall not let any subject access to the personal message prior to terminal authentication), • support role holder authentication as defined in TS 13584 [3], • support secure messaging as defined in TS 13584 [3], • protect the integrity and confidentiality of the user data and TSF data.
OE.SAM	The SAM shall • store security credentials for eID Card Authentication, • support signing the IVA, • store security credentials for External Device Authentication to authenticate External Biometric Sensor and External PIN-PAD • support Secure Messaging key generation mechanisms for the communication between the TOE and the following entities: (1) eID Card, (2) Role Holder (3) External Biometric Sensor, (4) External PIN PAD as defined in TS 13584 [3], • store the private key (Key Encryption Key) to decrypt the TOE Upgrade package as defined in TS 13584 [3], • support SAM-PIN verification mechanism to authenticate the TOE, • require SAM-PIN verification to allow the TOE to use its services, • support Secure Messaging with the TOE as defined in TS 13584 [3], • support authentication of itself to the TOE, • offer Random Number Generation, • have minimum EAL4+ (AVA_VAN.5) Common Criteria Certificate.
OE. Service_Requester	The Service Requester shall: • Protect his/her PIN, • Not enter his/her PIN, or give his/her biometric data prior to personal message verification, • Immediately, inform his/her stolen or lost eID Card.

OE. Service_Attendee	The Service Attendee shall: - protect his or her PIN, - not enter his/her PIN, or give his/her biometric data prior to personal message verification, - immediately inform the stolen or lost eID Card, - act responsively during photo verification, - not leave the TOE unattended while his/her identity is verified (shall remove his/her eID Card whenever he/she leaves the environment).
OE.OCSPS	The OCSPS shall: - operate correctly, - sign the OCSP answer, - protect the confidentiality of the signing key.
OE.IVS	The IVS shall have the following properties: - Supports the verification of the authenticity of the IVA with the Authentication Reference Data (Public Key of IVA Signing Certificate's integrity is protected)
OE.SSR_Platform	The SSR platform will support 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, who is possessing enhanced basic attack potential, to manipulate or bypass the security functionality of the TOE. The TSF architecture will be resistant against attacks that can be performed by attackers possessing Enhanced-Basic attack potential (AVA_VAN.3), SSR Platform will 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. SSR Platform will have tamper detection mechanism and notify the TOE upon detection of a tamper event. SSR Platform will enable the TOE to securely delete the SAM-PIN and cryptographic keys when deleted SAM-PIN and cryptographic keys will be unrecoverable. SSR Platform will provide correct operation of the TOE. SSR platform will include a Real Time Clock (RTC) Unit with at most 20 seconds fault within 24 hours, providing hardware-based protection mechanisms to ensure the integrity and confidentiality of the TOE during storage, instantiation and operation.
OE.EBS	The EBS shall: - will perform biometric verification correctly - support Secure Communication between the EBS and the TOE as defined in TS 13584 [3], - support Terminal Authentication as defined in TS 13584 [3], - protect security credentials within the EBS. - display the personal message of the Service Requester prior to requesting biometric input

OE.EPP	The EPP shall: • support Secure Communication between the EPP and the TOE as defined in TS 13584 [3], • support Terminal Authentication as defined in TS 13584 [3], • protect security credentials within the EPP, • display the personal message of the Service Requester prior to PIN • protect the confidentiality of the PIN
OE.Role_Holder	The role holder shall: • act responsively • have the appropriate role certificate and its Private Key for Role Holder Authentication • protect the private key used within Role Holder Authentication • support Secure Communication between the Role Holder and the TOE as defined in TS 13584 [3].
OE.PC	The PC that executes the SPCA shall be malicious code free and be located in secure environment.
OE.Security_Management	The security management environment shall be secure and unauthorized personnel shall not access to the TOE. The security management roles shall act responsively.
OE.SAS	The SAS will support Secure Communication with the TOE on SSR Type II. SAS shall encrypt the Identity Verification Assertion before sending it to the SPCA.
OE.Terminal_Cert_Directory	SSR Access Server (for TOE on Type II with SAS) or Application Server (for TOE on SSR Type III) shall get the updated Secure Messaging and Role Card Verifiable Certificates of the SAM in periods defined in TS 13585 [4] and forward them to the TOE.
OE.PKI	The issuer of the eID Card shall establish a public key infrastructure for the authentication mechanisms of eID Card Authentication, External Biometric Sensor Authentication, External PIN PAD Authentication, Role Holder Device Authentication, OCSP Response Verification, Identity Verification Policy Verification, and the TOE Upgrade Package Verification.
OE.CM [Credential Management]	All credentials, certificates, authentication reference data, shall be securely created and distributed to the relevant entities. If Revocation List is used for certificate verification, this Revocation List shall be up to date.
OE.APS	The Application server (APS) shall support Secure Communication with the TOE on SSR Type III and with client application for SSR Type II without SAS. For the cases when the APS determines the identity verification method, the APS shall select the appropriate method. APS shall encrypt the Identity Verification Assertion before sending it to the IVS (if IVA received is decrypted in the APS).
OE.SSR_Initialization_Environment	The initialization environment of the SSR Device where SAM PIN is defined to the SSR shall be physically secure.

Table 8 Security Objectives for the Operational Environment

4.3 COVERAGE OF THREATS, OSPS AND ASSUMPTIONS BY THE SECURITY OBJECTIVES

Table 9,Table 10,Table 11 and Table 12 give the coverage of threats, OSPs and assumptions by the security objectives.

	OT.IVM_Management	OT.Security_Failure	OT.eIDC_Authentication	OT.PIN_Verification	OT_IVA_Signing	OT.PM_Verification	OT.Session_Ending	OT.Identity_Verification_Policy Autentication	OT.OCSP_Query_Verify	OT.RH_DA	OT.RH_SC	OT.RH_Session_Ending	OT.SM_eID Card	OT.TOE_Upgrade	OT. DPM	OT.SAM-PIN_Mgmt	OT.DTN_Mgmt	OT.Time_Mgmt	OT.SM_TOE_and_SAM	OT.SAM-PIN_Sec	OT.DTN_Integrity	OT_Audit_Data_Protection	OT.RIP	OT.Auth_SAM_by_TOE	OT. Cert_Update	OT.IVA_Privacy
T.Counterfeit_ eIDC	X		X										X													
T.Revoked_eIDC	X																									
T.Stolen_eIDC				X																						
T.IVA_Fraud					X																					
T.Repudiation				X																						
T.Fake_TOE_to_SR						X																				
T.Fake_Policy								X																		
T.Fake_OCSP_ Response									X																	
T.RH_Comm											X															
T.RH_Session_Hijack										X		X														
T.eIDS_Comm													X													
T.DTN_Change																	X									
T.SAM-PIN_Theft		X																	X	X						
T.Audit_Data_ Compromise		X																				X				
T.TOE_ Manipulation																			X	X	X	X	X			
T.Fake_SAM																								X		
T.Stolen_SAM																X			X	X				X		
T.Revoked_SAM																								X		
T.IVA_Confidentiality																										X
P.IVM_ Management	X																									
P.TOE_Upgrade														X												
P.Terminal_Cert_ Update																									X	
P.Re-Authentication							X																			
P.Time_Update																		X								
P.Revocation_Control			X																							

P.DPM															X	X	X									
P.Tamper_Response		X																								
P.Offline_Operation																										X

Table 9 Security Objective Rationale

	OE.SPCA	**OE.IVPS**	**OE.eID Card**	**OE.SAM**	**OE.Service_Attendee**	**OE.Service_Requester**	**OE.OCSP**	**OE.IVS**	**OE.SSR_Platform**	**OE.Role_Holder**	**OE.PC**	**OE.Security_Management**	**OE.SAS**	**OE.Terminal_Cert_Directory**	**OE.PKI**	**OE.CM**	**OE.APS**	**OE.SSR_Initialization_Environment**
T.Counterfeit_eID			X	X											X	X		
T.Revoked_eID			X				X								X	X		
T.Stolen_eID			X		X	X			X									
T.IVA_Fraud				X				X							X	X		
T.IVA_Confidentiality				X														
T.Repudiation			X			X									X	X		
T.Fake_TOE_to_SR			X	X		X									X	X		
T.Fake_TOE_to_External_Entities			X	X											X	X		
T.Fake_Policy		X													X	X		
T.Fake_OCSP_Response							X								X	X		
T.RH_Comm				X						X								
T.RH_Session_Hijack			X	X						X					X	X		
T.eIDC_Comm			X	X														
T.DTN_Change									X									
T.SAM-PIN_Theft									X									
T.Audit_Data_Compromise									X									
T.TOE_Manipulation									X									
T.Fake_SAM				X											X	X		
T.Stolen_SAM				X												X		
T.Revoked_SAM				X			X											
P.TOE_Upgrade	X			X									X				X	
P.Terminal_Cert_Update														X		X		
P.Revocation_Control																X		
P.Tamper_Response									X									

A.SPCA	X																	
A.IVPS		X																
A.PC											X							
A.APS																	X	
A.Management_Environment												X						
A.SAM_ PIN_Environment																		X
A.SSR_Platform									X									

Table 10 Environmental Security Objectives Rationale Table for TOE

TOE SSR Type II and Type III has Photo verification mechanism and Service Attendee and Security Service Provider entities. In addition, TOE on SSR Type II adds the SAS related objectives and TOE and SSR Type III adds the APS related objectives. These cannot fit the Table 9, so these coverage of threats, OSPs and assumtions are given in Table 11.

	OT.Photo_Verification	**OT.Biometric_Verification**	**OE.Service_Attendee**	**OT.SA_Identity_Verification**	**OT.Session_Ending**	**OT.SAS_DA**	**OT.SAS_SC**	**OT.APS_DA**	**OT.APS_SC**	**OE.APS**	**OE.SAS**	**OE.PKI**	**OE.CM**	**OE.SAM**
T.Illegitimate_SAS (SSR Type II)						X					X			
T.Illegitimate_APS (SSR Type III)								X		X				
T.IVA_Eavesdropping							X		X	X	X			
T.Fake_TOE_to_External_Entities						X		X						
T.Stolen_eIDC	X	X	X											
T.SA_Masquerader			X	X								X	X	X
T.SA_Abuse_of_Session			X		X									
T.Repudiation		X												

Table 11 Security Objective Rationale (additions)

For all SSR Device, External Biometric sensor or External PIN Pad could be connected. For the TOE on SSR device connected with an EBS or EPP, the additional threats, OSPs and assumptions are given in Table 12.

	OT.Biometric_Verification	OT.EPP_DA	OT.EPP_SC	OE.EPP	OE.PKI	OE.CM	OT.EBS_DA	OT.EBS_SC	OE.SAM	OE.EBS
T.Stolen_eIDC	X									
T.Fake_TOE_to_External_Entities		X		X			X			X
T.Repudiation	X									
T.Illegitimate_EPP		X		X	X	X			X	
T.EPP_Comm			X	X					X	
T.Illegitimate_EBS					X	X	X		X	X
T.EBS_Comm								X	X	X
A.EBS-EPP				X						X

Table 12 Security Objective Rationale for SSR with External/Internal Biometric Sensor and/or EPP (additions)

4.4 SECURITY OBJECTIVES RATIONALE

T.Counterfeit_eID:

The security objectives OT.eIDC_Authentication and OT.SM_eID Card protect the eID Card against counterfeiting by authentication of the eID Card and Secure Messaging with the card. These mechanisms brings about some requirements on eID card, which is addressed by OE.eID and the support of SAM, which is addressed by OE.SAM. The authentication mechanism requires the public key infrastructure and the secure credential management. The public key infrastructure is addressed by OE.PKI; the security of credential management is addressed by OE.CM.

Security Objectives: *OT.eIDC_Authentication, OT.SM_eID Card, OT.IVM_Management, OE.eID Card, OE.SAM, OE.PKI, OE.CM*

T.Stolen_eID:

At minimum PIN Verification mechanism verifies if the person presenting the card is legitimate owner of the eID Card or an attacker trying to masquerade the identity of legitimate card holder (OT.PIN_Verification adresses the features in the TOE for this operation, OE.eID_Card adresses the eID Card requirements for this operaiton, and OE.Service_Requester addresses the Service Requester requirements for this operaiton). Photo Verification and Biometric Verification strengthens the resistance against the T.Stolen_eID Card. (OT.Biometric_Verification for biometric verification; OT.Photo_Verification and OE.Service_Attendee for photo verification). In addition to this the SSR Platform shall prevent the attacker to steal the PIN or the biometric data of the user.

Security Objectives: OT.PIN_Verification, OT.Photo_Verification and OT.Biometric_Verification, OE.eID_Card, OE.Service_Requester, OE.Service_Attendee and OE.SSR_Platform.

T.Revoked_eID:

Authentication methods required by OT.IVM_Management prevent the revocation attack on the eID Card. OT.IVM_Management and OE.OCSPS cover the threat.

Security Objectives: OT.IVM_Management, OE.OCSPS, OE.eID Card, OE.PKI, OE.CM.

T.IVA_Fraud:

OT.IVA_Signing allows the IVS to verify the IVA and identify the SSR that created the IVA. Hence, if an illegitimate IVA is created by an attacker, the IVS can detect it. The signing of IVA is performed by the SAM. Therefore, the OT.IVA_Signing, OE.SAM and OE.IVS cover the current threat together with OE.PKI and OE.CM which also cover the required PKI and the secure creation and distribution of the credentials and authentication reference data respectively.

Security Objectives: OT.IVA_Signing, OE.SAM, OE.IVS, OE.PKI, OE.CM

T.IVA_Eavesdropping:

OT.APS_SC and OE.APS require the secure communication of the TOE with SAS and APS for SSR for Type III.OT.SAS_SC, and OE.SAS require the secure communication of the TOE with SAS and APS for SSR Type II. Secure communication prevents the attacker to obtain IVA by monitoring the communication.

Hence, T.IVA_Eavesdropping is covered by, OT.SAS_SC, OT.APS_SC, OE.APS and OE.SAS

Security Objectives: OT.APS_SC, OE.APS, OT.SAS_SC, OE.SAS

T.IVA_Confidentiality:

OT.IVA_Privacy addresses the secure storage of the IVAs in SSR Type III. The encryption keys are generated by SAM thus OE.SAM addresses the secure storage of this encryption keys. These keys shall be transferred to the TOE via the secure messaging which is addressed by OT.SM_TOE_and_SAM

Security Objectives: OT.IVA_Privacy, OT.SM_TOE_and_SAM, OE.SAM

T.Repudiation:

PIN Verification or Biometric Verification mechanisms ensure that Service Requester and eID Card had joined to the Identification Process. OE.CM covers the secure creation and distribution of the credentials and authentication reference data. Thus OT.PIN_Verification, OT.Biometric_Verification, OE.Service_Requester, OE.eID Card, OE.PKI, and OE.CM cover the T.Repudiation.

Security Objectives: OT.PIN_Verification, OT.Biometric_Verification, OE.Service_Requester, OE.eID Card, OE.PKI and OE.CM

T.Fake_TOE_to_SR:

OT.PM_Verification allows the Service Requester identifying a legitimate SSR. OE.Service_Requester protects the service requester from entering his or her PIN and interacting with the biometric sensor without Personal Message Verification. OE.eID Card prevents the fake SSR accessing the Personal Message and OE.SAM provides the TOE the ability of proving its identity to the eID Card. Finally, OE.PKI and OE.CM cover the required PKI and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives: OT.PM_Verification, OE.eID Card, OE.Service_Requester, OE.SAM, OE.PKI, OE.CM

T.Fake_TOE_to_External_Entities:

Authentication objectives for eID Card, Role Holder, SAS, APS, EBS, EPP are OT.SM_eIDCard, OT.RH_DA, OT.SAS_DA, OT.APS_DA, OT.EBS_DA, OT.EPP_DA correspondingly require TOE to prove its identity before doing any action. SAM card in the SSR Device is used to prove identity of the TOE to the external entities. OE.PKI and

OE.CM cover the required PKI and the secure creation and distribution of the credentials and authentication reference data. Thus, OE.SAM covers the threat with OE.eID Card, OE.EBS (depends on the configuration), and OE.EPP (depends on the configuration).

Security Objectives: OT.SM_eIDCard, OT.RH_DA, OT.SAS_DA, OT.APS_DA, OT.EBS_DA, OT.EPP_DA, OE.SAM, OE.eID Card, OE.EBS (depends on the configuration), OE.EPP (depends on the configuration), OE.PKI, OE.CM.

T.SA_Masquerader:

OT.SA_Identity_Verification addresses the verification of Service Attendee's identity. Service Attendee's identity verification is similar to the identity verification of Service Requester. OE.eID Card, OE.SAM and the OE.Service_Attender address the necessary contributions of the eID Card, SAM and Service Attendee to the mechanisms covered in Service Attendee identity verification. Finally, OE.PKI and OE.CM cover the required PKI and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives:OT.SA_Identity_Verification, OE.eID Card, OE.SAM OE.Service_Attendee, OE.PKI, OE.CM

T.SA_Abuse_of_Session:

OT.Session_Ending addresses the termination of authentication session of Service Attendee whenever the session expires or the Service Attendee removes the eID Card. OE.Service_Attendee states that the Service Attendee shall not leave his or her eID Card when he or she leaves the SRR environment.

Security Objectives: OT.Session_Ending, OE.Service_Attendee

T.Fake_Policy:

OT.Identity_Verification_Policy_Authentication addresses verifying the integrity and origin of Identity Verification Policy and OE.IVPS states that Identity Verification Policy shall be signed electronically by the IVPS. OE.PKI and OE.CM cover the required PKI and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives: *OT.Identity Verification Policy_Authentication, OE.IVPS, OE.PKI, OE.CM*

T.Fake_OCSP_Response:

OT.OCSP_Query_Auth addresses verifying the integrity and the origin of the OCSP response. OE.OCSPS states that OCSP response shall be signed by the OCSPS. OE.PKI and OE.CM cover the required PKI mechanism and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives: OT.OCSP_Query_Verify, OE.OCSPS, OE.PKI, OE.CM

T.RH_Comm:

The OT.RH_SC, OE.SAM and OE.Role_Holder together agree on the secure communication keys. OT.RH_SC and OE.Role_Holder addresses the secure communication between the Role Holder and the TOE.

Security Objectives: OT.RH_SC, OE.SAM, OE.Role_Holder

T.RH_Session_Hijack:

OT.RH_DA [Role Holder Device Authentication], OE.SAM and OE.Role_Holder provides mutual authentication of the TOE and the Role Holder. OT.RH_Session_Ending resets the authentication status of Role Holder in eID Card when the secure communication session is terminated. This prevents the attacker to abuse the authentication status present in the eID Card. OE.eID Card helps the OT.RH_Session_Ending by providing an authentication reset mechanism to the TOE. Finally OE.PKI and OE.CM cover the required PKI mechanism and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives:OT.RH_DA [Role Holder Device Authentication], OT.RH_Session_Ending, OE.Role_Holder, OE.SAM, OE.eID Card, OE.PKI, OE.CM.

T.eIDC_Comm:

OT.SM_eID Card and OE.eID Card create the cryptographic keys and perform secure communication. OE.SAM supports the cryptographic key agreement between the TOE and the eID Card. Hence the threat is covered by OT.SM_eID Card, OE.eID Card and OE.SAM.

Security Objectives: OT.SM_eID Card, OE.eID Card and OE.SAM.

T.RH_Session_Hijack:

OT.RH_DA [Role Holder Device Authentication], OE.SAM and OE.Role_Holder provides mutual authentication of the TOE and the Role Holder. OT.RH_Session_Ending resets the authentication status of Role Holder in eID Card when the secure communication session is terminated. This prevents the attacker to abuse the authentication status present in the eID Card. OE.eID Card helps the OT.RH_Session_Ending by providing an authentication reset mechanism to the TOE. Finally OE.PKI and OE.CM cover the required PKI mechanism and the secure creation and distribution of the credentials and authentication reference data.

Security Objectives: OT.RH_DA [Role Holder Device Authentication], OT.RH_Session_Ending, OE.Role_Holder, OE.SAM, OE.eID Card, OE.PKI, OE.CM.

T.Illegitimate_EBS:

OT.EBS_DA addresses the authentication of EBS by SAM. OE.PKI and OE.CM cover the required PKI echanism and the secure creation and distribution of the credentials and authentication reference data. So the threat is covered OT.EBS_DA, OE.SAM, OE.EBS, OE.PKI and OE.CM.

Security Objectives: OT.EBS_DA, OE.SAM, OE.EBS, OE.PKI, OE.CM

T.EBS_Comm:

OT.EBS_SC and OE.EBS addresses secure communication between the TOE and the EBS. The OE.SAM and OE.EBS contribute to the key agreement protocol between the TOE and the EBS.

Security Objectives: OT.EBS_SC, OE.SAM, OE.EBS

T.Illegitimate_EPP:

OT.EPP_DA, OE.EPP and OE.SAM addresses the authentication of EPP by SAM. OE.PKI and OE.CM cover the required PKI mechanism and the secure creation and distribution of the credentials and authentication reference data. So the threat is covered by OT.EPP_DA, OE.SAM, OE.EPP, OE.PKI, and OE.CM.

Security Objectives: OT.EPP_DA, OE.SAM, OE.EPP, OE.PKI, OE.CM

T.EPP_Comm:

OT.EPP_SC, OE.EPP and OE.SAM address the secure communication between the TOE and the EPP therefore cover the threat

Security Objectives: *OT.EPP_SC, OE.EPP, OE.SAM*

T.eIDC_Comm:

OT.SM_eID Card and OE.eID Card create the cryptographic keys and perform secure communication. OE.SAM supports the cryptographic key agreement between the TOE and the eID Card. Hence the threat is covered by OT.SM_eID Card, OE.eID Card and OE.SAM.

Security Objectives: *OT.SM_eID Card, OE.eID Card and OE.SAM.*

T.Illegitimate_SAS:

This threat is covered by OT.SAS_DA which guarantee the authentication of the SAS before any other action and OE.SAS which ensures that the SAS has the ability to be authenticated by the TOE.

Security Objectives: *OT.SAS_DA, OE.SAS.*

T.Illegitimate_APS:

This threat is covered by OT.APS_DA, which guarantee the authentication of the APS before any other action and OE.APS which ensures that the APS has the ability to be authenticated by the TOE.

Security Objectives: *OT.APS_DA, OE.APS.*

T.DTN_Change:

OT.DTN_Mgmt and OE.SSR_Platform address the protection against unauthorized modification to the DTN.

Security Objectives: *OT.DTN_Mgmt, OE.SSR_ Platform.*

T.SAM-PIN_Theft:

OT.Security_Failure, OT.SM_TOE_and_SAM, OE.SSR_ Platform and OT.SAM-PIN_Sec address the protection of SAM-PIN against theft and unauthorized change.

Security Objective: *OT.Security_Failure, OT.SAM-PIN_Mgmt, OT.SAM-PIN_Sec, OE.SSR_ Platform.*

T.Audit_Data_Compromise:

OT.Security_Failure, OT.Audit_Data_Protection and OE.SSR_ Platform cover the protection of audit data from unauthorized change.

Security Objective: *OT.Security_Failure, OT.Audit_Data_Protection, OE.SSR_ Platform*.

T.TOE_Manipulation:

OT.Security_Failure addresses protection of the TOE against physical tampering together with OE.SSR_Platform. OT.SM_TOE_and_SAM [Secure Messaging between TOE and SAM], addresses the protection of communication between the SAM and the TOE. OT.SAM-PIN_Sec protects the SAM-PIN against probing, OT.DTN_Integrity protects the DTN from manipulation, and the OT.Audit_Data_Protection protects the audit data from manipulation. OT.RIP provides protection against probing attacks and de-allocates any resources when they are no longer needed.

Security Objectives: *OT.SM_TOE_and_SAM [Security between TOE and SAM], OT.SAM-PIN_Sec, OT.DTN_Integrity, OT.Audit_Data_Protection , OT.RIP [Residual Information Protection], OE.SSR_Platform*

T.Fake_SAM:

OT.Auth_SAM_by_TOE addresses the authentication of SAM by TOE. OE.SAM provides the TOE for the capability to authenticate itself. Finally, OE.PKI and OE.CM cover the required PKI mechanism and the secure creation and distribution of the credentials and authentication reference data. Thus OT.Auth_SAM_by_TOE, OE.SAM, OE.PKI, and OE.CM cover the threat.

Security Objectives:OT.Auth_SAM_by_TOE [Authentication of SAM by TOE], OE.SAM, OE.PKI, OE.CM

T.Stolen_SAM:

OT.Auth_SAM_by_TOE addresses the authentication of SAM by TOE and OE.SAM requires the SAM-PIN verification before allowing the SSR (the legitimate or the fake) access its services. OT.SAM-PIN_Secand OT.SM_TOE_and_SAM requires the SAM PIN security during operation of the SSR Device. The OE.CM protects the SAM-PIN during generation and writing to the SAM and the TOE.

Security Objectives: OT.Auth_SAM_by_TOE, OT.SAM-PIN_Sec, OT.SAM-PIN_Mgmt, OT.SM_TOE_and_SAM, OE.SAM and OE.CM.

T.Revoked_SAM:

Authentication of SAM by TOE mechanism also involves the revocation query. The OT.Auth_SAM_by_TOE, OE.SAM, OE.OCSP cover the threat.

Security Objectives: OT.Auth_SAM_by_TOE, OE.SAM, OE.OCSPS.

P.IVM_Management:

OT. IVM_Management matches the requirement.

Security Objective: OT. IVM_Management

P.TOE_Upgrade:

OT.TOE_Upgrade covers the policy together with OE.SPCA, OE.SAM, OE.SAS and OE.APS since the upgrade package could be installed onto the SSR via SPCA, SAS or APS and SAM stores the certificates to validate the upgrade package.

Security Objectives: OT.TOE_Upgrade, OE.SPCA, OE.SAM, OE.SAS, OE.APS.

P.Re-Authentication:

OT.Session_Ending requires necessary re-authentications for each authentication session.

Security Objectives: OT.Session_Ending

P.Terminal_Cert_Update:

OT.Cert_Update, OE.Terminal_Cert_Directory and OE.CM matches the policy. OE.Terminal_Cert_Directory requires the related server to obtain the updated certificates and OT.Cert_Update covers the update of the certificates by the TOE.

Security Objectives: OT.Cert_Update, OE.Terminal_Cert_Directory and OE.CM.

P.Time_Update:

OT.Time_Mgmt matches the time update requirement.

Security Objective:OT.Time_Mgmt

P.Offline_Operation:

OT.IVA_Privacy matches the offline identity verification with TOE on SSR Type III.

Security Objective: OT.IVA _Privacy

P.Revocation_Control:

OT.eIDC_Authentication defines the offline certificate verification together with OE.CM

Security Objectives: OT.eIDC _Authentication, OE.CM

P.DPM:

OT.DPM addresses the phase management policy of the P.DPM. DTN and PIN writing policy is addressed by OT.DTN_Mgmt and OT.SAM-PIN_Mgmt objectives correspondingly.

Security Objectives: OT.DPM, OT.DTN_Mgmt and OT.SAM-PIN_mgmt

P.Tamper_Response:

OT.Security_Failure and OE.SSR_Platform realize the tamper response together.

Security Objectives: OT.Security_Failure, OE.SSR_Platform

A.SPCA: The security objective OE.SPCA covers the assumption.

Security Objective: OE.SPCA

A.IVPS: The security objective OE.IVPS covers the assumption.

Security Objective: OE.IVPS

A.EBS-EPP: OE.EBS and OE.EPP covers the assumption.

Security Objective: OE.EBS, OE.EPP

A.PC:OE.PC covers the assumption

Security Objective: OE.PC

A.APS: The security objective OE.APS covers the assumption.

Security Objective: OE.APS

A.Management_Environment: OE.Security_Management covers the assumption.

Security Objective: OE.Security_Management

A.SAM_ PIN_Environment: OE.SSR_Initialization_Environment covers the assumption.

Security Objective: OE.SSR_Initialization_Environment

A.SSR_Platform: OE.SSR_Platform covers the assumption totally.

Security Objective: OE.SSR_Platform

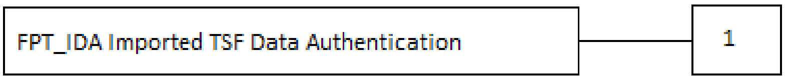
5 EXTENDED COMPONENTS DEFINITION

5.1 FPT_IDA IMPORTED TSF DATA AUTHENTICATION

Family Behavior:

This family requires that the TOE has the ability to verify that the defined imported TSF Data originates from the stated external entity.

Component Leveling:



5.1.1 FPT_IDA.1 IMPORTED TSF DATA AUTHENTICATION

Management: FPT_IDA.1

The following actions could be considered for the management functions in FMT:

- Management of authentication data by an administrator.

Audit: FPT_IDA.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimum: The final decision on authentication;

FPT_IDA.1 Imported TSF Data Authentication

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [assignment: list of TSF Data] originates from [assignment: list of external entities] using [assignment: list of authentication mechanisms

5.2 FPT_SSY STATE SYNCHRONIZATION

Family Behavior:

This family requires that the TOE has ability to synchronize its internal state with another trusted external entity.

Component Leveling:

FPT_SSY State Synchronization
1

5.2.1 FPT_SSY.1 STATE SYNCHRONIZATION

Management: FPT_SSY.1

The following actions could be considered for the management functions in FMT:

- Management of conditions where state synchronization is mandatory, not necessary if it fails, or not required

Audit: FPT_SSY.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimum: Result of synchronization: success or failure

FPT_SSY.1 State Synchronization

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SSY.1.1	The TSF shall check [assignment: status of the user security attributes] from the [assignment: the external entities] in times: [assignment: defined periods].

6 SECURITY REQUIREMENTS

6.1 SECURITY FUNCTIONAL REQUIREMENTS

This part of the ST defines the detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE needs to satisfy in order to meet the security objectives for the TOE. The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Section 8.1 of Common Criteria Part1 [17]. The following operations are used in the ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements are denoted in such a way that added words are in bold text and removed are ~~crossed out~~.

The **selection** operation is used to select one or more options provided by the CC instating a requirement. Selections having been made are denoted as underlined text.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted by *italicized* text.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.1 CLASS FAU: SECURITY AUDIT

6.1.1.1 FAU_GEN.1 - AUDIT DATA GENERATION

Hierarchical to: No other components.

Dependencies: [FPT_STM.1 Reliable time stamps] **fulfilled** by FPT_STM.1

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [minimum] level of audit; and c) *[Insertion and removal of eID Card and SAM, Service requester authentication, service attendee authentication, start and end of secure messaging, card authentication, received data integrity failure, role holder authentication, external biometric sensor authentication, external PIN PAD authentication, SAM authentication, SAM-PIN verification failure, TOE update, IVP verification, OCSP answer verification, Switching to offline mode (for TOE on SSR Type III), SAS authentication and tampering of the SSR.]*
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, ~~type of event~~, subject identity (if applicable), and the outcome (success or failure) of the event; and b) [*For each audit event type, based on the auditable event definitions of the functional components included in the ST, reason of the failure (if applicable)*.]

6.1.1.2 FAU_ARP.1- SECURITY ALARMS

Hierarchical to: no other components.

Dependencies: [FAU_SAA.1 Potential violation analysis] **fulfilled** by FAU_SAA.1

FAU_ARP.1.1	The TSF shall take *the [action of entering Out of Service Mode and delete SAM PIN and Cryptographic Keys used for storage security]* upon detection of a potential security violation.

Application Note 1: The instantiation "Cryptographic Keys used for storage security" matches the IVA Confidentiality Keys for TOE on SSR Type III with offline working feature.

6.1.1.3 FAU_SAR.1 AUDIT REVIEW

Hierarchical to: no other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1	The TSF shall provide *[Administrator]* with the capability to read [*all auditable events]* from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_STG.1 PROTECTED AUDIT TRAIL STORAGE

Hierarchical to: no other components.

Dependencies: [FAU_GEN.1 Audit data generation] **fulfilled** by FAU_GEN.1

FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to [detect] unauthorized modifications to the stored audit records in the audit trail.

6.1.1.5 FAU_STG.4 PREVENTION OF AUDIT DATA LOSS

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: [FAU_STG.1 Protected audit data storage] **fulfilled** by FAU_STG.1

FAU_STG.4.1	The TSF shall [overwrite the oldest stored audit records] and [*none]* if the audit trail is full.

6.1.1.6 FAU_SAA.1 POTENTIAL VIOLATION ANALYSIS

Hierarchical to: No other components.

Dependencies: [FAU_GEN.1 Audit data generation] **fulfilled** by FAU_GEN.1

FAU_SAA.1.1	The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2	The TSF shall enforce the following rules for monitoring audited events: a*) [Tampering of the SSR]* known to indicate a potential security violation; b) *[none]*.

6.1.2 CLASS FCS: CRYPTOGRAPHIC SUPPORT

6.1.2.1 FCS_CKM.1/SM-CRYPTOGRAPHIC KEY GENERATION FOR SECURE MESSAGING WITH EID, SA, EBS, EPP AND ROLE HOLDER

Hierarchical to: no other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by FCS_COP.1/AES-CBC and FCS_COP.1/AES-CMAC

[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Encryption and CMAC Key Generation Algorithm for Secure Messaging]* and specified cryptographic key sizes [*256 bits]* that meet the following: [*TS 13584* [3]*].*

Application Note 2: Above mentioned Secure Messaging are founded between TOE and eID; TOE and SAM, TOE and EBS; TOE and EPP; TOE and Role Holder.

6.1.2.2 FCS_CKM.1/SM_TLS- CRYPTOGRAPHIC KEY GENERATION FOR SECURE MESSAGING WITH IDENTITY VERIFICATION SERVER, APPLICATION SERVER AND SSR ACCESS SERVER

Hierarchical to: no other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by FCS_COP.1/AES-CBC and FCS_COP.1/AES-CMAC

[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*TLS v1.2 or above]* and specified cryptographic key sizes [*256 Bits]* that meet the following: [*RFC 5246]*.

Application Note 3: TLS Key Generation is performed between TOE and APS for TOE on SSR Type III; between TOE and SAS for TOE on SSR Type II.

6.1.2.3 FCS_CKM.1/IVA_KEYS - CRYPTOGRAPHIC KEY GENERATION FOR IVA CONFIDENTIALITY ON SSR TYPE III

Hierarchical to: no other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] **fulfilled** by FCS_COP.1/AES-CBC and FCS_COP.1/AES-CMAC

[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*True Random Number Generation*] and specified cryptographic key sizes [*256 bits]* that meet the following: [*none]*.

Application Note 4: True Random Numbers should be generated by the SAM. Since the communication between the TOE and the SAM is secure, these keys are securely transferred to the TOE and stored in the tamper proof area.
Refinement: Keys above refers to IVA Encryption/Decryption key used in AES CBC algorithm and the IVA Integrity key used in AES CMAC algorithm. These keys are used to Encrypt/Decrypt the stored IVAs on SSR Type III.

6.1.2.4 FCS_CKM.4 - CRYPTOGRAPHIC KEY DESTRUCTION

Hierarchical to: No other components.
Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by FCS_CKM.1/SM, FCS_CKM.1/IVA_Keys and FCS_CKM.1/SM_TLS

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*writing random values by the Secure MCU*] that meets following:[*none*]

Application Note 5: The dependency of FCS_CKM.4 is satisfied by the FCS_CKM.1/SM, FCS_CKM.1/IVA_Keys and FCS_CKM.1/SM_TLS. Note here that the coverage of these SFRs differs according to SSR Type and whether EBS, EPP and offline modes are included. Therefore, FCS_CKM.4 is required only for the covered SSR Configuration just as it is for FCS_CKM.1.
Application Note 6: FCS_CKM.4 determines the key destruction method for the secure messaging keys, secure storage keys and the Upgrade Package key (the decrypted key).

6.1.2.5 FCS_COP.1/SHA-256 - CRYPTOGRAPHIC OPERATION SHA 256

Hierarchical to: No other components.
Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **not fulfilled** but justified.
[FCS_CKM.4 Cryptographic key destruction] **not fulfilled** but justified.

Justification: SHA-256 hash function does not use a key so there is neither need to create nor need to destroy.

FCS_COP.1.1	The TSF shall perform [*hash value calculation]* in accordance with a specified cryptographic algorithm [*SHA-256 [*5*]]* and cryptographic key sizes [*none]* that meet the following: [*FIPS 180-4*.]

6.1.2.6 FCS_COP.1/AES-CBC - CRYPTOGRAPHIC AES CBC OPERATION

Hierarchical to: No other components.
Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by FCS_CKM.1/SM, FCS_CKM.1/IVA_Keys, FCS_CKM.1/SM_TLS
[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

Justification:

The first dependency is not satisfied for the decryption requirement for the TOE Upgrade package. The encrypted keys of the TOE Upgrade package are installed onto the TOE together with the Upgrade Package. The Key Decryption Keys for these keys are stored in the SAM. Therefore encrypted keys are decrypted in the SAM using the Key Decryption Keys and used in the TOE.

FCS_COP.1.1	The TSF shall perform [*encryption and decryption]* in accordance with a specified cryptographic algorithm [*AES-256 CBC Mode]* and cryptographic key sizes [*256 bits]* that meet the following: [*FIPS 197 (for AES) [6], NIST Recommendation for Block Cipher Modes of Operations (for CBC mode)[7]]* .

6.1.2.7 FCS_COP.1/AES-CMAC - CRYPTOGRAPHIC CMAC OPERATION

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **fulfilled** by FCS_CKM.1/SM, FCS_CKM.1/IVA_Keys, FCS_CKM.1/SM_TLS.

[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4.

FCS_COP.1.1	The TSF shall perform [*message authentication]* in accordance with a specified cryptographic algorithm [*AES-CMAC]* and cryptographic key sizes [*256 bits]* that meet the following: [*FIPS 197 (for AES) [6], RFC 4493 (for CMAC operation) [9]].*

6.1.2.8 FCS_COP.1/RSA - CRYPTOGRAPHIC RSA ENCRYPTION OPERATION

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **not fulfilled** but justified.
[FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

Justification:

RSA encryption operation is performed during the key agreement between the SAM and the TOE. Certificate of the secure messaging between the TOE and the SAM is stored in the SAM. This certificate contains the public RSA key needed for this RSA encryption operation and is read by the TOE before key agreement process starts.

FCS_COP.1.1	The TSF shall perform [*encryption]* in accordance with a specified cryptographic algorithm [*RSA OAEP]* and cryptographic key sizes [*2048]* that meet the following: [*TS 13584* [3]*,* and *RSA Cryptography Standard [10]].*

6.1.2.9 FCS_COP.1/SIGN_VER - CRYPTOGRAPHIC SIGNATURE VERIFICATION OPERATION

Hierarchical to: No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] **not fulfilled** but justified.

[FCS_CKM.4 Cryptographic key destruction] **not fulfilled** but justified.

Justification:

The public key needed to perform the cryptographic operation is imported to the TOE via FPT_IDA.1/X509. So neither key creation nor import operation is necessary within the SFR. Also the public key used in the operation does not have confidentiality requirements so FCS_CKM.4 is also not required here.

FCS_COP.1.1	The TSF shall perform [*Signature Verification by Cryptographic Validation and Certificate Validation]* in accordance with a specified cryptographic algorithm [*RSA, PKCS#1 v2.1 with PSS padding method]* and cryptographic key sizes [*2048]* that meet the following: [*ETSI TS 102 853[12] and TS 13584* [3]].

Application Note 8: This signature verification is performed by the TOE for the following signature verification operations:

- verification of Identity Verification Certificate (eID Card Certificate),
- verification of the OCSP Answer signature,
- verification of the Signature of the Identity Verification Policy sent by the Identity Verification Policy Server (IVPS) and,
- verification of the Secure Access Module (SAM) certificate,
- verification of upgrade package signature.

6.1.3 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

6.1.3.1 FIA_AFL.1 AUTHENTICATION FAILURE HANDLING

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 Timing of authentication] fulfilled by FIA_UAU.2, which is hierarchic to FIA_UAU.1

FIA_AFL.1.1	The TSF shall detect when [*limit of Biometric Verification Failure (defined in TS 13584 [3]) times]* unsuccessful authentication attempts occur related to [*Biometric Verification]*.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [met], the TSF shall not allow [*further biometric verification]*.

Application Note 9: Unsuccessful biometric verification number is written into the eID Card by the TOE and updated each time the counter is changed.

6.1.3.2 FIA_UID.2 USER IDENTIFICATION BEFORE ANY ACTION

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement: User above refers to Role Holder, Secure Access Module, External PIN Pad (if applicable), External Biometric Sensor (if applicable) and eID Card. In addition, for TOE on SSR Type II user also refers to SAS, for TOE on SSR Type III user also refers to APS.

6.1.3.3 FIA_UAU.2 USER AUTHENTICATION BEFORE ANY ACTION

Hierarchical to: FIA_UAU.1.

Dependencies: [FIA_UID.1 Timing of identification] **fulfilled** by FIA_UID.2 which is hierarchic to FIA_UID.1

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Refinement: User above refers to Role Holder, Secure Access Module, External PIN Pad (if applicable), External Biometric Sensor (if applicable) and eID Card. In addition, for TOE on SSR Type II user also refers to SAS, for TOE on SSR Type III user also refers to APS.

6.1.3.4 FIA_UAU.5 MULTIPLE AUTHENTICATION MECHANISMS

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UAU.5.1	The TSF shall provide [*the following authentication mechanisms:* • *Service Attendee authentication,* • *Service Requester authentication,* • *eID Card authentication,* • *SAM authentication,* • *Role Holder Device authentication,* • *SAS authentication for TOE on SSR Type II,* • *APS authentication for TOE on SSR Type III,* • *external PIN PAD authentication (if applicable),* • *external biometric sensor authentication (if applicable)]* to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the following rules: [• *Service requester authentication is done by methods defined in TS 13585 [4]. Verification method is determined by the Identity Verification Policy Server (IVPS) or the Client Application. For the cases when there is no IVPS and Client Application does not determine the method, default method shall be used which is the combination of certificate verification, PIN authentication, photo verification (if applicable) and biometric verification (if applicable) as defined in TS 13585 [4].* • *Service Attendee authentication is done by methods defined in TS TS 13585 [4]. Verification method is determined by the Identity Verification Policy Server (IVPS) or the Client Application. For the cases when there is no IVPS and Client Application does not determine the method, default method shall be used which is the combination of certificate verification, PIN authentication and biometric verification (if applicable) as defined in TS 13585 [4].* • *eID Card, SAM, Role Holder, external PIN PAD and external biometric sensor authentications are done by certificate verification.* • *APS and SAS authentication are done by SSL/ TLS certificate authentication. SAS verification is a mutual authentication started by the TOE. APS verification is a one way server authentication.]*

Refinement: User above refers to Secure Access Module, External PIN Pad(if applicable), External Biometric Sensor(if applicable), Service Requester, Service Attendee, eID Card. In addition, for TOE on SSR Type II user also refers to SAS, for TOE on SSR Type III user also refers to IVPS and APS.
Refinement for TOE on SSR Type I: Exclude the Photo Verification and Service Attendee Authentication.

Application Note 10: Certificates stored in the SAM are used for the SSL/ TLS client authentication.

Application Note 11: eID Card is the smart card with the eID Application. Card holder (either Service Requester or the Service Attendee) is the person who possesses the eID Card. The authentication of the eID Card and the Card Holder are handled separately because the former is to validate that the card is not counterfeit, not forged or not revoked and the latter is to validate that the card is not stolen.

However, due to the authentication policy, in some cases Service Attendee and Service Requester authentication consist of certificate verification. In this case one refers to the other.

6.1.3.5 FIA_UAU.6 - RE-AUTHENTICATING

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions given below. [*When 4 hours is exceeded after Service Attendee authentication, this authentication process is repeated.* • *In each authentication request for Service Requester, Service Requester is re-authenticated even if the card is not removed.* *After 24 hours are exceeded the following sessions' keys are renewed:* • *SAM authentication,* • *Role Holder Device authentication,* • *APS authentication for TOE on SSR Type III,* • *SAS authentication for TOE on SSR Type II* • *external PIN PAD authentication (if applicable),* • *external biometric sensor authentication (if applicable)].*

Refinement for TOE on SSR Type I: Exclude the Photo Verification and Service Attendee Authentication

Refinement: User above refers to Service Attendee, Service Requester, SAM, Role Holder, APS for TOE on SSR Type III, SAS for TOE on SSR Type II, EPP (if applicable) or EBS (if applicable) according to the context.

6.1.3.6 FIA_UAU.7 PROTECTED AUTHENTICATION FEEDBACK

Hierarchical to: No other components.

Dependencies: [FIA_UAU.1 Timing of authentication] **fulfilled** by FIA_UAU.2, which is hierarchical to FIA_UAU.1.

FIA_UAU.7.1	The TSF shall provide [• *a dummy character for each entered PIN entry for authentication by PIN* • *a dummy fingerprint representation for authentication by biometry* *on the SSR screen]* to the ~~user~~ **Service Requester or Service Attendee** while the authentication is in progress.

6.1.4 CLASS FCO: COMMUNICATION

6.1.4.1 FCO_NRO.2 ENFORCED PROOF OF ORIGIN FOR IDENTITY VERIFICATION ASSERTION

Hierarchical to: Selective proof of origin.

Dependencies: [FIA_UID.1 Timing of identification] **fulfilled** by FIA_UID.1

FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted [Identity *Verification Assertion Data]* at all times.

FCO_NRO.2.2	The TSF shall be able to relate the [*identity of origin]* of the originator of the information, and the [*Identity Verification Assertion Data]* of the information to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [*Identity Verification Server]* given [*immediately in online mode, within a 24 hours period in offline mode for TOE on SSR Type III]*.

Refinement: Evidence above shall be the signature of the SAM card. Before sending the Identity Verification Assertion (IVA) to the Identity Verification Server (IVS), TOE shall ensure that the Identity Verification Assertion Data is signed by the SAM Signature Certificate as defined in TS 13584 [3].

Application Note 12: - IVS verifies the IVA. This is why the assignment is instantiated as *"Identity Verification Server"*. However, TOE on Type II gives the IVA to SPCA and SPCA sends the IVA to APS. TOE on SSR Type III directly sends the IVA to APS. In all cases APS sends the IVA to IVS.

6.1.5 CLASS FMT: SECURITY MANAGEMENT

6.1.5.1 FMT_MOF.1 /VERIFY- MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR – VERIFY

Hierarchical to: No other components.

Dependencies: [FMT_SMR.1 Security roles] **fulfilled** by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] fulfilled by FMT_SMF.1

FMT_MOF.1.1	The TSF shall restrict the ability to [determine the behavior of] the function [*Identity Verification Operation]* to the [*Identity Verification Policy Server or Client Application]*.

Application Note 13 A default Identity Verification Method shall be defined in the TOE during production for the cases when this method is not determined by IVPS or Client Application.

6.1.5.2 FMT_MOF.1 /UPGRADE-MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOR – UPGRADE

Hierarchical to: No other components.
Dependencies: [FMT_SMR.1 Security roles] **fulfilled** by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] **fulfilled** by FMT_SMF.1

FMT_MOF.1.1	The TSF shall restrict the ability to [enable] the function [*TOE Upgrade]* to [*Client Application for TOE on Type I and Type II, Application Server for TOE on Type III and Manufacturer service operator]*.

Refinement: TOE Upgrade above shall be allowed only for the higher versions and the Upgrade Package shall be associated with the SAM in the corresponding SSR.

6.1.5.3 FMT_MTD.1/SAM-PIN MANAGEMENT OF TSF DATA

Hierarchical to: No other components.
Dependencies: [FMT_SMR.1 Security roles] **fulfilled** by FMT_SMR.1

[FMT_SMF.1 Specification of Management Functions] **fulfilled** by FMT_SMF.1

FMT_MTD.1.1	The TSF shall restrict the ability to [write] the [*SAM-PIN]* to [*Initialization Agent]*.

6.1.5.4 FMT_MTD.1/DTN MANAGEMENT OF TSF DATA - DEVICE TRACKING NUMBER

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles **fulfilled** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions **fulfilled** by FMT_SMF.1

FMT_MTD.1.1	The TSF shall restrict the ability to [write] the [*Device Tracking Number]* to [*Initialization Agent]*.

6.1.5.5 FMT_MTD.1/TIME MANAGEMENT OF TSF DATA -TIME

Hierarchical to: No other components.
Dependencies:

FMT_SMR.1 Security roles **fulfilled** by FMT_SMR.1

FMT_SMF.1 Specification of Management Functions **fulfilled** by FMT_SMF.1

FMT_MTD.1.1	The TSF shall restrict the ability to [update]the *[Time]* to *[OCSP server]*.

Application Note 14: TOE gets the time information from OCSP Server and stores this time information on the SSR real time Clock (RTC). Upon use of time information in TSF functions, RTC provides time information.

6.1.5.6 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [• *TOE initialization (including SAM PIN and DTN initialization),* • *TOE upgrade,* • *time and date setting,* • *audit generation,* • *identity verification method determination.]*

6.1.5.7 FMT_SMR.1 SECURITY ROLES

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification **fulfilled** by FIA_UID.2 which is hierarchic to FIA_UID.1

FMT_SMR.1.1	The TSF shall maintain the roles [• *Initialization Agent,* • *SSR Access Server for TOE on SSR Type II,* • *Client Application for TOE on SSR Type II,* • *Application Server for TOE on Type III,* • *Identity Verification Policy Server,* • *OCSP Server,* • *Manufacturer service operator* • *Software Publisher.*]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.6 CLASS FPT: PROTECTION OF THE TSF

6.1.6.1 FPT_STM.1 RELIABLE TIME STAMPS

Hierarchical to: No other components

Dependencies: No dependencies

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note 15: Reliable time stamp shall be provided from the OCSP server and stored in a real time clock on SSR Device.

6.1.6.2 FPT_IDA.1/CVC – IMPORTED TSF DATA AUTHENTICATION - CARD VERIFIABLE CERTIFICATES

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [*Secure Messaging Card Verifiable Certificates and Role Card Verifiable Certificates*] originates from [*Card Publisher*] using [*CVC Authentication Mechanism defined in TS 13584 [3]*].

6.1.6.3 FPT_IDA.1/X509 - IMPORTED TSF DATA AUTHENTICATION – X509 CERTIFICATES

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [*Identity Verification Certificate, Identity Verification Policy Server Certificate, OCSP Server Certificate, Software Publisher Certificate*] originates from [*Card Publisher and Device Manager*] using [*X509 Certificate Authentication Mechanism defined in TS 13584 [3].*]

6.1.6.4 FPT_IDA.1/IVP - IMPORTED TSF DATA AUTHENTICATION - IDENTITY VERIFICATION POLICY

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [*Identity Verification Policy*] originates from [*Identity Verification Policy Server*] using [*IVP authentication mechanism defined in TS 13584 [3].*]

6.1.6.5 FPT_IDA.1/OCSP IMPORTED TSF DATA AUTHENTICATION – OCSP

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [*OCSP Response*] originates from legitimate [*OCSP Server*] using [*OCSP Response Verification Mechanism defined TS 13584 [3].*]

Application Note 16: For offline Revocation Status Control from the Revocation List downloaded onto the SSR Device this verification mechanism is still valid.

6.1.6.6 FPT_IDA.1/TOE_UPGRADE - IMPORTED TSF DATA AUTHENTICATION - TOE UPGRADE PACKAGE

Hierarchical to: No other components

Dependencies: No dependencies

FPT_IDA.1.1	The TSF shall verify that the [*TOE upgrade package*] originates from [*legitimate Software Publisher*] using [*TOE Upgrade Authentication mechanism defined in TS 13584 [3]*.]

6.1.6.7 FPT_SSY.1/CERT STATE SYNCHRONIZATION -SECURE MESSAGING AND ROLE CVC

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SSY.1.1	The TSF shall check [*the validity of the Secure Messaging and Role Card Certificates of the SAM*] **and request updated certificates** from the: [• SPCA for TOE on SSR Type I and Type II with no SAS • *SAS for TOE on SSR Type II with SAS* • *APS for TOE on SSR Type III*] in times*:* [*at each Identity Verification Operation*.]

6.1.6.8 FPT_SSY.1/SAM STATE SYNCHRONIZATION -SAM

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SSY.1.1	The TSF shall check [*SAM Card Certificate revocation status*] from the [*OCSP Server*] in times*:* [*immediately after opening of the SSR*.]

6.1.6.9 FPT_SSY.1/IVC STATE SYNCHRONIZATION -IVC

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SSY.1.1	The TSF shall check [*Identity Verification Certificate revocation status*] from the [*OCSP Server or SSR Platform on which up-to-date Revocation List is present*] in times: [*during Identity Verification Operation.*]

Application Note 17: TOE downloads the revocation list onto SSR device and do offline revocation controls. If a new update is present for the revocation list but the OSCP is not reached, in this case the foundation giving the service is responsible for defining the time for using old revocation list.

6.1.6.10 FPT_SSY.1/RH_AUTH_STATUS STATE SYNCHRONIZATION ROLE HOLDER AUTHENTICATION STATUS

Hierarchical to: No other components

Dependencies: No dependencies

FPT_SSY.1.1	The TSF shall check [*Role Holder authentication status in eID Card*] from the [*eID Card*] in times: [*after the secure communication between Role Holder and the TSF is terminated*.]

Application Note 18: The TSF shall reset the authentication status of the Role Holder in eID Card after the secure communication between Role Holder and the TSF is terminated as defined in TS 13584 [3]

6.1.6.11 FPT_TST.1 TSF TESTING

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1	The TSF shall run a suite of self tests [during initial start-up] to demonstrate the correct operation of [the TSF].
~~FPT_TST.1.2~~	~~The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data.~~
~~FPT_TST.1.3~~	~~The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF].~~

6.1.6.12 FPT_FLS.1 FAILURE WITH PRESERVATION OF SECURE STATE

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [*a tampering event is detected, identification and authentication services for SAM are disturbed*.]

6.1.7 CLASS FDP: USER DATA PROTECTION

6.1.7.1 FDP_IFC.1 SUBSET INFORMATION FLOW CONTROL

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes **fulfilled** by FDP_IFF.1

FDP_IFC.1.1	The TSF shall enforce the [*Information Flow Control Policy*] on : *[Subjects:* *SPCA (subject of TOE on SSR Type I and SSR Type II), SAS (subject for TOE on SSR Type II with SAS), APS (subject for TOE on SSR Type III), OCSP Server for TOE on SSR Type III, IVPS for SSR Type III.* *Information:* *TOE Upgrade Package, IVA, IVM, OCSP response, SAM Secure Messaging CVC and SAM Role CVC* *Operations:* *Write (installed to the TOE), read (sent by the TOE).]*

6.1.7.2 FDP_IFF.1 SIMPLE SECURITY ATTRIBUTES

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control **fulfilled** by FDP_IFC.1
FMT_MSA.3 Static attribute initialization **not fulfilled** but justified

Justification: The initial value for IVM is defined in the TOE during manufacturing. For other information under Information Flow Control Policy, initial value is not required, nor meaningful.

FDP_IFF.1.1	The TSF shall enforce the [*Information Flow Control Policy] based* on the following types of subject and information security attributes: [*Subjects:* *SPCA (subject of TOE on SSR Type I and SSR Type II), SAS (subject for TOE on SSR Type II with SAS), APS (subject for TOE on SSR Type III), OCSP Server for TOE on SSR Type III, IVPS for SSR Type III.* *Information:* *TOE Upgrade Package, IVA, IVM, OCSP response, SAM Secure Messaging CVC and SAM Role CVC* *Attributes:* *Software Publisher Signature for TOE Upgrade Package, SAM Signature for IVA, IVP Signature for IVM, OCSP signature for OCSP response, eID management CA Signature correspondingly* .]
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold*:* *[IVA is sent only if communication channel with corresponding SPCA, SAS or APS is established as defined in this ST and other information under the control of Information Flow Control Policy are accepted and written if signature verification is completed successfully].*
FDP_IFF.1.3	The TSF shall enforce the [*none*].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: [*none*].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [*none*].

6.1.7.3 FDP_ETC.2 EXPORT OF USER DATA WITH SECURITY ATTRIBUTES

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control] **fulfilled** by FDP_IFC.1

FDP_ETC.2.1	The TSF shall enforce the [*Information Flow Control Policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2	The TSF shall export the user data with the user data's associated security attributes
FDP_ETC.2.3	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4	The TSF shall enforce the following rules when user data is exported from the TOE: [*none*].

6.1.7.4 FDP_RIP.1 SUBSET RESIDUAL INFORMATION PROTECTION

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] the following objects [*cryptographic credentials, IVA data fields, PIN, photo and biometric information*].

6.1.8 CLASS FTP: TRUSTED PATH/CHANNELS

6.1.8.1 FTP_ITC.1 INTER-TSF TRUSTED CHANNEL

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **each one of the following trusted products: Role Holder Device, External Biometric Sensor (if applicable), External PIN PAD (if applicable), eID Card, SSR SAM, SAS for TOE on SSR Type II (with SAS) and APS for TOE on SSR Type III** that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit [the TSF] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for [*all functions*].

Application Note 19: TOE provides trusted paths with SSR Access Server and Application Server are founded using SSL-TLS using SSL- TLS certificates.

6.2 SECURITY ASSURANCE REQUIREMENTS

For the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level (EAL4) and augmented by taking the following component: ALC_DVS.2.

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE TABLES

The coverage of objectives by the SFRs are given in Table12, Table13, Table 14 and Table15.

Table 13 given below includes the objectives for the SSR Type I without Biometric Sensor and External PIN PAD, that are also valid for TOE on all of the three SSR Types where external PIN Pad and External/Internal Biometric Sensor is not present.

	OT.IVM_Management	OT.Security_Failure	OT.eIDC_Authentication	OT.PIN_Verification	OT.IVA_Signing	OT.PM_Verification	OT.ID_Verification Policy_Authentication	OT.OCSP_Query_Verify	OT.RH_DA	OT.RH_SC	OT.RH_Session_Ending	OT.SM_eID Card	OT.DPM	OT.TOE_Upgrade	OT.SAM-PIN_Mgmt	OT.DTN_Mgmt	OT.Time_Mgmt	OT.SM_ TOE_and_SAM	OT.SAM-PIN_Sec	OT.DTN_Integrity	OT.Audit_Data_Protection	OT.RIP	OT.Auth_SAM_by_TOE	OT.Cert_Update
FAU_GEN.1		X	X	X		X	X	X	X					X					X					
FAU_ARP.1																			X					
FAU_SAR.1																					X			
FAU_STG.1																					X			
FAU_STG.4																					X			
FAU_SAA.1		X																						
FCS_CKM.1/SM						X				X		X						X						
FCS_CKM.1/SM_TLS																								
FCS_CKM.1/IVA_Keys																								
FCS_CKM.4						X				X		X						X						
FCS_COP.1/SHA-256					X									X										
FCS_COP.1/AES-CBC						X				X		X		X				X						
FCS_COP.1/AES-CMAC						X				X		X						X						
FCS_COP.1/RSA																		X						
FCS_COP.1/Sign_Ver			X				X	X	X					X										
FIA_UID.2			X	X										X		X	X							
FIA_UAU.2			X	X										X		X	X							
FIA_UAU.5	X		X	X					X														X	
FIA_UAU.7				X																				
FCO_NRO.2					X																			
FMT_MOF.1/Verify	X																							
FMT_MOF.1/Upgrade_Management														X										
FMT_MTD.1/SAM-PIN															X									
FMT_MTD.1/DTN																X								
FMT_MTD.1/Time																	X							
FMT_SMF.1	X												X	X	X	X	X							
FMT_SMR.1	X												X	X	X	X	X							
FPT_STM.1																	X							

FPT_IDA.1/CVC									X			X												
FPT_IDA.1/X509							X	X						X										
FPT_IDA.1/IVP							X																	
FPT_IDA.1/OCSP								X																
FPT_IDA.1/TOE_Upgrade														X										
FPT_SSY.1/IVC			X																					
FPT_SSY.1/SAM																							X	
FPT_SSY.1/RH_Auth_Status											X													
FPT_TST.1																				X				
FDP_RIP.1																						X		
FPT_FLS.1		X																	X	X				
FTP_ITC.1										X		X						X						
FPT_SSY.1/Cert																								X
FDP_ETC.2							X	X						X										X
FDP_IFC.1							X	X						X										X
FDP_IFF.1							X	X						X										X

Table 13 SFR Rationale Table for TOE on SSR Type I without Biometric Sensor and External PIN Pad

Table 14 gives the SFR Rational for additional objectives of TOE on SSR Type II and SSR Type III.

	OT.Photo_Verification	T.SA_Identity_Verification	OT.Session_Ending	OT.SAS_DA	OT.SAS_SC	OT.APS_DA	OT.APS_SC
FAU_GEN.1	X	X	X	X		X	
FCS_CKM.1/SM_TLS					X		X
FCS_COP.1/SHA-256					X		X
FCS_COP.1/AES-CBC					X		X
FIA_UID.2	X	X		X		X	
FIA_UAU.2	X	X		X		X	
FIA_UAU.5	X	X		X		X	
FIA_UAU.6			X			X	

FTP_ITC.1					X		X

Table 14 Rationale for additional objectives of TOE on SSR Type II and SSR Type III

Table 15 gives the SFR Rational for additional objectives of TOE on SSR with biometric sensor and/or external PIN PAD

	OT.Biometric_Verification	OT.EPP_DA	OT.EPP_SC	OT.EBS_DA	OT.EBS_SC	OT.Session_Ending
FAU_GEN.1	X	X		X		
FIA_AFL.1	X					
FIA_UID.2		X		X		
FIA_UAU.2		X		X		
FIA_UAU.5	X	X		X		
FIA_UAU.6						X
FIA_UAU.7	X					
FCS_CKM.1/SM			X		X	
FCS_CKM.4			X		X	
FCS_COP.1/AES-CBC			X		X	
FCS_COP.1/AES-CMAC			X		X	
FPT_SSY.1/IVC		X		X		
FTP_ITC.1			X		X	

Table 15 SFR rationale additions for TOE on SSR with External/Internal Biometric Sensor and/or EPP

	OT.IVA_Privacy
FAU_GEN.1	X
FAU_ARP.1	X
FCS_CKM.1/SM	X
FCS_CKM.1/SM_TLS	X
FCS_CKM.1/IVA_Keys	X
FCS_CKM.4	X
FCS_COP.1/AES-CBC	X
FCS_COP.1/AES-CMAC	X

FDP_RIP.1	**X**
FTP_ITC.1	**X**
FDP_ETC.2	**X**
FDP_IFC.1	**X**
FDP_IFF.1	**X**

Table 16 SFR Rationale for additional objectives of TOE on SSR Type III

6.3.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

OT.IVM_Management:
FIA_UAU.5 selects the rules for authentication of Service Requester and Service Attendee. FMT_MOF.1/Verify restricts the use of the management function to the security role: Identity Verification Policy Server and SPCA. FMT_SMF.1 and FMT_SMR.1 determines the management functions and roles.
SFRs: FIA_UAU.5, FMT_MOF.1/Verify, FMT_SMF.1, and FMT_SMR.1.

OT.Security_Failure:
This objective is covered by FPT_FLS. 1, FAU GEN.1 and FAU_SAA.1 which requires preserving the secure state, auditing and taking the action of entering out of service mode respectively upon detection of a security failure.
SFRs: FPT_FLS.1, FAU GEN.1 and FAU_SAA.1.

OT.eIDC_Authentication:
Card authentication mechanism is covered by the FIA_UAU.5, FIA_UID.2 and FIA_UAU.2. FCS_COP.1/Sign_Ver verifies the authenticity of the certificate and FPT_IDA.1/X509 verifies the authenticity of the certificate. FPT_SSY/IVC addresses that the eID Card certificate is not expired. Generation of audit data when failure of authentication happens is provided by FAU.GEN.1.
SFR: FIA_UAU.5, FAU_GEN.1, FIA_UID.2, FCS_COP.1/Sign_Ver, FPT_IDA.1/X509, FPT_SSY/IVC and FIA_UAU.2.

OT.PIN_Verification:
Identity Verification Certificate PIN verification is covered by the FIA_UAU.5, FIA_UAU.2 and FIA_UID.2 and protection of PIN during entry is addressed by the FIA_UAU.7. Generation of audit data when failure of authentication happens is provided by FAU.GEN.1.
SFRs: FIA_UAU.2, FIA_UID.2, FIA_UAU.5, FIA_UAU.7 and FAU_GEN.1

OT.Photo_Verification:
Authentication needs for Photo verification is covered by the FIA_UAU.5 FIA_UAU.2 and FIA_UID.2. Generation of audit data when failure of authentication happens is provided by FAU.GEN.1.
SFRs: FIA_UAU.5, FAU_GEN.1, FIA_UAU.2 and FIA_UID.2.

OT.Biometric_Verification:
Biometric verification is covered by the FIA_UAU.5. Generation of audit data when failure of authentication happens is provided by FAU.GEN.1. Authentication failure handling of biometric verification is handled by FIA_AFL.1. Protection of biometry data during entry is addressed by the FIA_UAU.7.
SFRs: FIA_UAU.5, FIA_AFL.1, FAU_GEN.1 and FIA_UAU.7.

OT_IVA_Signing:
FAU_GEN.1 requires auditing the created IVAs. The FCO_NRO.2 guaranties the authentication of the IVA. The hash value of the IVA is created and signed in SAM. This requirement is covered by FCS_COP.1/SHA-256.
SFRs: FCO_NRO.2, FCS_COP.1/SHA-256

OT.IVA_Privacy:

IVA is directly sent to APS in TOE on SSR Type III. Thus, confidentiality of the IVA during transmission is covered by FCS_CKM.1/SM_TLS, FCS_CKM.4 and FTP_ITC.1.

The cryptographic requirement for IVA confidentiality for the TOE on SSR Type III in the offline mode is guaranteed by FDP_RIP, FCS_COP.1/AES-CBC and FCS_COP.1/AES-CMAC. The generation and destruction of the encryption/decryption keys are addressed by FCS_CKM.1/IVA_Keys and FCS_CKM.4. These keys are generated by SAM and stored in the tamper proof area. The confidentiality of this key is guaranteed by FCS_CKM.1/SM, FCS_CKM.4 and FPT_ITC.1 during transmission from SAM to TOE and by FAU_ARP.1 during storage. The stored IVA integrity for TOE on SSR Type III in offline mode is addressed by FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1 define *Information Flow Control Policy* to sign IVA by SAM before sending it to IVS.

SFRs: FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC, FAU_GEN.1, FAU_ARP.1, FCS_COP.1/SHA-256, FCS_CKM.1/SM, FCS_CKM.1/IVA_Keys, FCS_CKM.1/SM-TLS, FCS_CKM.4, FPT_ITC.1, FDP_RIP.1, FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1.

OT.PM_Verification:

Since only the legitimate TOE could found secure messaging with eID Card and read personal message FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC and FCS_COP.1/AES-CMAC covers the OT.PM_Verification with FAU_GEN.1 which audits the confirmation of the personal message.

SFR: FAU_GEN.1, FCS_CKM.1/SM, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC and FCS_CKM.4.

OT.SA_Identity_Verification:

FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 covers the identity verification of Service Attendee and FAU_GEN.1 requires the auditing of the authentication.

SFR: FIA_UID.2, FIA_UAU.2, FIA_UAU.5 and FAU_GEN.1

OT.Session_Ending:

FIA_UAU.6 and FAU_GEN.1 covers the objective.

SFRs: FIA_UAU.6, FAU_GEN.1.

OT.ID_Verification_Policy_Authentication:

FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1 define *Information Flow Control Policy* for verifying the signature of the Identity Verification Policy sent by the IVPS. FPT_IDA.1/IVP covers the authentication of policy and FPT_IDA.1/X509 covers the authentication of the certificate of the policy server. The Identity Verification Policy Authentication mechanism addressed in the FPT_IDA.1/IVP and FPT_IDA.1/X509 require the cryptographic support of FCS_COP.1/ Sign_Ver. FAU_GEN.1 audits the authentication.

SFRs: FDP_ETC.2, FDP_IFC.1, FDP_IFF.1, FPT_IDA.1/IVP, FPT_IDA.1/X509, FCS_COP.1/ Sign_Ver and FAU_GEN.1.

OT.OCSP_Query_Verify:

FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1 define *Information Flow Control Policy* for verifying the signature of the OCSP Query Response sent by the OCSPS. FPT_IDA.1/OCSP covers the authentication of query response and FPT_IDA.1/X509 covers the authentication of the certificate of the OCSP server. The OCSP Query Response Verification Mechanism addressed in the FPT_IDA.1/OCSP requires the cryptographic support of FCS_COP.1/ Sign_Ver. FAU_GEN.1 audits the authentication.

SFRs: FDP_ETC.2, FDP_IFC.1, FDP_IFF.1 FPT_IDA.1/OCSP, FPT_IDA.1/X509, FCS_COP.1/ Sign_Ver and FAU_GEN.1.

OT.RH_DA [Role Holder Device Authentication]:

FIA_UAU.5 and FPT_IDA.1/CVC covers the authentication of role holder and role holder CVC certificate. This requires the cryptographic support of FCS_COP.1/ Sign_Ver. FAU_GEN.1 audits the authentication.

SFR: FIA_UAU.5, FPT_IDA.1/CVC, FCS_COP.1/ Sign_Ver and FAU_GEN.1.

OT.RH_SC [Secure Communication with Role Holder]:

FTP_ITC.1 covers the secure communication between the Role Holder and the TOE. FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC give the necessary cryptographic support for the secure communication.

SFRs: FTP_ITC.1, FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC.

OT.RH_Session_Ending:

FPT_SSY.1/RH_Auth_Status covers the objective.

<u>SFR</u>: FPT_SSY.1/RH_Auth_Status

OT.EBS_DA:
FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 covers the identity verification of EBS, FPT_SSY/IVC addresses that the EBS SAM certificate is not expired and FAU_GEN.1 requires the auditing of the authentication.
<u>SFRs:</u> FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FPT_SSY/IVC and FAU_GEN.1

OT.EBS_SC:
FTP_ITC.1 covers the secure communication between the EBS and the TOE. FCS_CKM.1/SM, FCS_CKM.4 FCS_COP.1/AES-256, FCS_COP.1/AES-CMAC give the necessary cryptographic support for the secure communication.
<u>SFRs:</u> FTP_ITC.1, FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC.

OT.EPP_DA [External PIN-PAD Device Authentication]:
FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 covers the identity verification of EPP, FPT_SSY/IVC addresses that the EPP SAM certificate is not expired and FAU_GEN.1 requires the auditing of the authentication.
<u>SFRs:</u> FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FPT_SSY/IVC and FAU_GEN.1

OT.EPP_SC:
FTP_ITC.1 covers the secure communication between the EPP and the TOE. FCS_CKM.1/SM, FCS_CKM.4 FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC give the necessary cryptographic support for the secure communication.
<u>SFRs</u>: FTP_ITC.1, FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC.

OT.SM_eID Card:
FTP_ITC.1 and FPT_IDA.1/CVC covers the secure communication between the eID Card and the TOE. FCS_CKM.1/SM, FCS_CKM.4 FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC give the necessary cryptographic support for the secure communication.

<u>SFRs</u>: FTP_ITC.1, FPT_IDA.1/CVC, FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC

OT.DPM:
FMT_SMF and FMT_SMR cover the phase management functions and roles thus covers the objective.
<u>SFRs</u>: FMT_SMF.1 and FMT_SMR.1.

OT.TOE_Upgrade:
The management function and roles of TOE upgrade is addressed by FMT_SMF.1 and FMT_SMR.1. Unauthorized TOE Update is protected by FMT_MOF.1/Upgrade_Management and FPT_IDA.1/TOE_Upgrade. FPT_IDA.1/X509 covers the authentication of the certificate of the software publisher server. FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1 define *Information Flow Control Policy* for verifying the signature of the Upgrade Package sent by the Software Publisher. The authentication before the upgrade is guaranteed by the FIA_UAU.2 and FIA_UID.2. Required cryptographic support is covered by FCS_COP.1/SHA-256, FCS_COP.1/AES-CBC and FCS_COP.1/Sign_Ver. Audit generation is needed thus FAU_GEN.1 is covered.
<u>SFRs:</u> FAU_GEN.1, FMT_SMF.1, FMT_SMR.1, FMT_MOF.1/Upgrade_Management, FPT_IDA.1/TOE_Upgrade, FPT_IDA.1/X509, FCS_COP.1/SHA-256, FCS_COP.1/AES-CBC, FCS_COP.1/Sign_Ver FIA_UAU.2 and FIA_UID.2, FDP_IFC.1, FDP_IFF.1, FDP_ETC.2.

OT.SAM-PIN_Mgmt:
The management function of writing the SAM-PIN is addressed by FMT_SMF.1; and protection of SAM-PIN from unauthorized access is provided by FMT_MTD.1/SAM-PIN. FMT_SMR.1 addresses the security role Initialization Agent who is allowed to write the SAM-PIN.
<u>SFRs</u>: FMT_MTD.1/SAM-PIN, FMT_SMF.1, FMT_SMR.1

OT.DTN_Mgmt:
The device tracking number can only have written by the configuration agent; this requirement is covered by FMT_MTD.1/DTN. Relevant management function and role are covered by FMT_SMF.1 and FMT_SMR.1. Authentication of the role before DTN writing is covered by FIA_UAU.2 and FIA_UID.2.

SFRs: FMT_MTD.1/DTN, FMT_SMF.1, FMT_SMR.1, FIA_UAU.2 and FIA_UID.2.

OT.Time_Mgmt:
This is addressed by FMT_MTD.1/Time. Security role and management function regarding the writing the Default Method is given in the SFRs: FMT_SMR.1 and FMT_SMF.1. Authentication of the role before time update is covered by FIA_UAU.2 and FIA_UID.2. Providing the real time for IVA data and audit data is fulfilled by FPT_STM.1.
SFRs: FMT_MTD.1/Time, FMT_SMF.1, FMT_SMR.1, FIA_UAU.2, FIA_UID.2 and FPT_STM.1.

OT.SM_TOE_and_SAM [Security between TOE and SAM]:
FTP_ITC.1 covers the secure communication between the TOE and the SAM. The necessary cryptographic support is given by FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/RSA, FCS_COP.1/AES-CBC, and FCS_COP.1/AES-CMAC.

SFRs: FTP_ITC.1, FCS_CKM.1/SM, FCS_CKM.4, FCS_COP.1/RSA, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC

OT.SAM-PIN_Sec:
The security of the SAM-PIN is satisfied by the deletion of the SAM PIN upon detection of a tamper event. This objective is covered by FPT_FLS.1, FAU GEN.1 and FAU_ARP.1
SFRs: FPT_FLS.1, FAU GEN.1 and FAU_ARP.1.

OT.DTN_Integrity:
The objective OT.DTN_Integrity is provided by FPT_TST.1 and FPT_FLS.1.
SFR: FPT_TST.1 and FPT_FLS.1.

OT.Audit_Data_Protection :
FAU_STG1, FAU_SAR.1 and FAU_STG.4 covers the audit data protection.
SFR: FAU_STG1, FAU_SAR.1 and FAU_STG.4

OT.RIP [Residual Information Protection]:
The SFR FDP_RIP.1 provides the protection aimed by OT.RIP.
SFR: FDP_RIP.1

OT.Auth_SAM_by_TOE [Authentication of SAM by TOE]:
FIA_UAU.5 addresses the authentication of SAM by the TOE. FPT_SSY.1/SAM addresses the revocation status control.
SFRs: FIA_UAU.5, FPT_SSY.1/SAM.

OT.SAS_DA:
FIA_UID.2, FIA_UAU.2 and FIA_UAU.5 covers the objective of device authentication of SAS with FAU_GEN.1
SFRs: FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FAU_GEN.1

OT.SAS_SC:
FCS_CKM.1/SM_TLS, FCS_COP.1/AES-CBC, FCS_COP.1/SHA-256 and FTP_ITC.1 covers the objective
SFRs: FCS_CKM.1/SM_TLS and FTP_ITC.1

OT.APS_DA:
FIA_UID.2, FIA_UAU.2 FIA_UAU.6, and FIA_UAU.5 covers the objective of device authentication of SAS with FAU_GEN.1
SFRs: FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FAU_GEN.1

OT.APS_SC:

FCS_CKM.1/SM_TLS, FCS_COP.1/AES-CBC, FCS_COP.1/SHA-256 and FTP_ITC.1 covers the objective.

SFRs: FCS_CKM.1/SM_TLS and FTP_ITC.1

OT.Cert_Update:

Validity of certificates needs to be checked by the TOE. This is covered by FPT_SSY.1/Cert. During certificate update, the integrity and authenticity of the new certificates replacing the old certificates are ensured. For this, FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1 define *Information Flow Control Policy* for verifying *eID management CA signature*.

SFRs: FPT_SSY.1/Cert, FDP_ETC.2, FDP_IFC.1, and FDP_IFF.1

6.4.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE

EAL4 is chosen to permit a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the TOE’s development and manufacturing especially for the secure handling of the TOE’s material.

The component ALC_DVS.2 augmented to EAL4 has no dependencies to other security requirements.

7 TOE SUMMARY SPECIFICATION

7.1 TOE SECURITY FUNCTIONALITY

7.1.1 SECURITY AUDIT

TOE Security Functionality generates an audit record of the following events:

- Insertion and removal of eID Card and SAM
- Service requester authentication
- Service attendee authentication
- Start and end of secure messaging
- Card authentication
- Received data integrity failure
- Role holder authentication
- EPP and EBS authentication
- SAM authentication
- SAM-PIN verification failure
- TOE update
- IVP verification
- OCSP answer verification
- Switching to offline mode (for TOE on SSR Type III)
- SAS authentication (for TOE on SSR Type II)
- Tamper event detection

For each audit event; date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and for each audit event type, based on the auditable event definitions of the functional components included in the, reason of the failure (if applicable) are stored. Reliable time stamp is provided from the OCSP server by the TOE and stored in RTC on SSR.

Audit trail is protected from unauthorized deletion. TOE is able to detect unauthorized modifications to the stored audit records in the audit trail. TOE overwrites the oldest stored audit records if the audit trail is full.

TOE provides the capability to read from the audit records in a manner suitable for the user to interpret the information.

TOE is able to enter Out of Service Mode and delete SAM PIN and Cryptographic Keys used for storage security upon detection of a potential security violation.

Functional Requirement Satisfied: FAU_ARP.1, FAU_GEN.1, FAU_SAR.1, FAU_STG.1, FAU_STG.4, FAU_SAA.1

7.1.2 CRYPTOGRAPHIC SUPPORT

Cryptographic support involves following cryptographic mechanism:

- Generation and destruction of cryptographic keys,
- SHA256 hash generation defined in FIPS 180-4[5],
- AES CBC encryption/decryption defined in FIPS 197 [6] and SP 800-38A [7],
- AEC-CMAC generation defined in RFC 4493[9],
- RSA encryption defined in RSA Cryptography Standard [10]and according to TS 13584 [3],

- Secure messaging between TOE-eID Card and TOE-SAM Card according to TS 13584 Document [3]
- TLS communication defined in RFC 5246 [21] between the TOE and SSR Access Server according to TS 13584 Document [3].

The TOE performs Signature Verification by Cryptographic Validation and Certificate Validation in accordance with a specified cryptographic algorithm RSA, PKCS#1 v2.1 with PSS padding method and cryptographic key sizes 2048 that meet the ETSI TS 102 853[12] and TS 13584 for Verification of Identity Verification Certificate (eID Card Certificate), verification of the OCSP Answer signature, verification of the Signature of the Identity Verification Policy sent by the Identity Verification Policy Server (IVPS) and, verification of the Secure Access Module (SAM) certificate, verification of upgrade package signature.

Secure messaging keys, secure storage keys and the Upgrade Package keys are destroyed as writing random values by the Secure MCU.

Functional Requirement Satisfied: FCS_CKM.1/SM, FCS_CKM.1/SM_TLS, FCS_CKM.1/IVA_Keys, FCS_CKM.4, FCS_COP.1/SHA-256, FCS_COP.1/AES-CBC, FCS_COP.1/AES-CMAC, FCS_COP.1/RSA, FCS_COP.1/Sign_Ver

7.1.3 IDENTIFICATION AND AUTHENTICATION

This feature contains that each user Role Holder, Secure Access Module, eID Card, SAS and APS must be successfully identified and authenticated before any action on behalf of that user. Authentication failure handling, user identification and authentication, multiple authentication mechanism for different users, reauthenticating, and protected authentication feedback are supplied by the TOE. Identification and authentication functionalities for the followings are provided by the TOE:

- Service Attendee identification & authentication
- Service Requester identification & authentication
- eID Card identification & authentication
- SAM identification & authentication
- Role Holder Device identification & authentication
- EPP and EBS identification & authentication
- SAS identification & authentication for TOE on SSR Type II
- APS identification & authentication for TOE on SSR Type III

When limit of Biometric Verification Failure times defined in TS 13584 [3] document has been met, the TSF does not allow further biometric verification.

Service requester and Service attendee authentication is done by methods defined in TS 13585 [4]. Verification method is determined by the Identity Verification Policy Server (IVPS) or the Client Application. eID Card, SAM, Role Holder authentications are done by certificate verification. APS and SAS authentication are done by SSL/ TLS certificate authentication. SAS verification is a mutual authentication started by the TOE. APS verification is a one way server authentication. It is able to reauthenticate the users Card holder, SAM, Role Holder Device, APS and SAS for certain conditions for each user type.

It provides a dummy character for each entered PIN entry for authentication by PIN and a dummy fingerprint representation for authentication by biometry on the SSR screen to the user Service Requester or Service Attendee while the authentication is in progress.

Functional Requirement Satisfied: FIA_AFL.1, FIA_UID.2, FIA_UAU.2, FIA_UAU.5, FIA_UAU.6, FIA_UAU.7

7.1.4. SECURE COMMUNICATION

The secure communication functionality provides following channels:

- Communication between TOE and eID
- Communication between TOE and SAM
- Communication between TOE and Role Holder
- Communication between TOE and EPP and EBS
- Communication between TOE and SAS (on SSR Type II with SAS)
- Communication between TOE and APS (on SSR Type III)
- Communication between TOE and IVS (on SSR Type III)
- Communication between TOE and IVPS (on SSR Type III)
- Communication between TOE and OCSP (on SSR Type III)

The identity of originator of the information, and the Identity Verification Assertion Data of the information to which the evidence applies. The Communication Security functions supply a competence to verify the evidence of origin of information to Identity Verification Server given immediately in online mode, within a 24 hours period in offline mode for TOE on SSR Type III.

Functional Requirement Satisfied: FCO_NRO.2

7.1.5. SECURITY MANAGEMENT

The Security Management function maintains the roles for users and associate such roles with users.

It restricts the ability to determine the behavior of the function Identity Verification Operation to the Identity Verification Policy Server or Client Application.

TOE upgrade function is only enabled to Client Application for TOE Type II, Application Server for TOE on Type III and Manufacturer service operator.

SAM-PIN and Device Tracking number written only in Initialization Agent. OCSP server has ability to update the TOE time.

Functional Requirement Satisfied: FMT_MOF.1 /Verify, FMT_MOF.1 /Upgrade_Management, FMT_MTD.1/SAM-PIN, FMT_MTD.1/DTN, FMT_MTD.1/Time, FMT_SMF.1, FMT_SMR.1

7.1.6. TSF PROTECTION

The TOE provides security mechanisms for the protection of TSF data.

It verifies that:

- Secure Messaging Card Verifiable Certificates and Role Card Verifiable Certificates originates from Card Publisher using CVC Authentication Mechanism
- Identity Verification Policy originates from Identity Verification Policy Server using IVP authentication mechanism
- OCSP Response originates from legitimate OCSP Server using OCSP Response Verification Mechanism
- TOE upgrade package originates from legitimate Software Publisher using TOE Upgrade Authentication mechanism defined in TS 13584[3].
- Identity Verification Certificate, Identity Verification Policy Server Certificate, OCSP Server Certificate, Software Publisher Certificate by using X509 Certificate Authentication Mechanism

It checks:

- The validity of the Secure Messaging and Role Card Certificates of the SAM and request updated certificates from the: SAS for TOE on SSR Type II with SAS, and APS for TOE on SSR Type III at each Identity Verification Operation.
- SAM Card Certificate revocation status from the OCSP Server immediately after opening of the SSR.
- Identity Verification Certificate revocation status from the OCSP Server or SSR Platform on which up-to-date Revocation List is present during Identity Verification Operation.
- Role Holder authentication status in eID Card from the eID Card after the secure communication between Role Holder and the TSF is terminated.

It runs a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF.

It preserves a secure state when any tampering event is detected, identification and authentication services for SAM are disturbed.

Functional Requirement Satisfied: FPT_STM.1, FPT_IDA.1/CVC, FPT_IDA.1/X509, FPT_IDA.1/IVP, FPT_IDA.1/OCSP, FPT_IDA.1/TOE_Upgrade, FPT_SSY.1/Cert, FPT_SSY.1/SAM, FPT_SSY.1/IVC, FPT_SSY.1/RH_Auth_Status, FPT_TST.1, FPT_FLS.1, FAU_ARP.1

7.1.7. USER DATA PROTECTION

Information Flow Control Policy on SAS (subject for TOE on SSR Type II with SAS), APS (subject for TOE on SSR Type III), OCSP Server for TOE on SSR Type III, IVPS for SSR Type III over TOE Upgrade Package, IVA, IVM, OCSP response, SAM Secure Messaging, CVC and SAM Role CVC during write (installed to the TOE) and read (sent by the TOE) operations.

Upon detection of a data integrity error, the TSF gives an error message to the APS indicating the integrity fault and do not continue offline Identity Verification Operation.

Information Flow Control Policy is applied when importing and exporting user data, controlled under the SFP, from outside of the TOE. Security attributes associated with the user data is ignored when imported from outside of the TOE. Previous information content of a resource is made unavailable upon the deallocation of the resource from the cryptographic credentials, IVA data fields, PIN, photo and biometric information.

Functional Requirement Satisfied: FDP_IFC.1, FDP_IFF.1, FDP_ETC.2, FDP_RIP.1,

7.1.8. TRUSTED PATH/CHANNELS

This feature involves trusted communication protocols between itself and defined trusted products. Trusted channels supported by the TOE are the followings:

- Trusted path/channel between TOE and eID
- Trusted path/channel between TOE and SAM
- Trusted path/channel between TOE and Role Holder
- Trusted path/channel between TOE and EPP and EBS
- Trusted path/channel between TOE and SAS (on SSR Type II with SAS)
- Trusted path/channel between TOE and APS (on SSR Type III)
- Trusted path/channel between TOE and IVS (on SSR Type III)
- Trusted path/channel between TOE and IVPS (on SSR Type III)
- Trusted path/channel between TOE and OCSP (on SSR Type III)

It initiates communication via the trusted channel for all functions.

Functional Requirement Satisfied: FTP_ITC.1

8 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
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: Secure Smartcard Reader
TA: Terminal Authentication

9 REFERENCES

1. TS 13582 - Elektronik Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı – Bölüm-1: Genel Bakış, (Secure Smart Card Reader Standard - Part-1: Overview) 2013, Türk Standartları Enstitüsü

2. TS 13583 - Elektronik Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı – Bölüm-2: Arayüzler ve Özellikleri, (Secure Smart Card Reader Standard - Part-2: Interfaces and their characteristics) 2013, Türk Standartları Enstitüsü

3. TS 13584 - Elektronik Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı - Bölüm-3: Güvenlik Özellikleri (Secure Smart Card Reader Standard - Part-3: Security Properties), 2013, Türk Standartları Enstitüsü.

4. TS 13585 - Elektronik Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı - Bölüm-4: SSR Uygulama Yazılımı Özellikleri, (Secure Smart Card Reader Standard - Part-4: Secure Smart Card Reader Application Firmware Specifications), 2013, Türk Standartları Enstitüsü.

5. FIPS 180-4, Secure Hash Standard (SHS), March 2012, U.S. Department of Commerce, National Institute of Standards and Technology

6. FIPS 197, Advanced Encryption Standard (AES), November 2001, National Institute of Standards and Technology

7. Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology Special Publication 800-38A 2001 ED Natl. Inst. Stand. Technol. Spec. Publ. 800-38A 2001 ED, 66 pages (December 2001)

8. NIST Special Publications 800-38A, Recommendation for Block Cipher Modes of Operations, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf, 2001.

9. RFC 4493, The ESP CBC-Mode Cipher Algorithms, https://tools.ietf.org/html/rfc4493, June 2006, Internet Society Network Working Group.

10. PKCS #1 v2.1, RSA Cryptography Standard, September 2012, RSA Laboratories.

11. RFC 3447, RSA Cryptography Specifications, https://www.ietf.org/rfc/rfc3447.txt, Feb 2003, Internet Society Network Working Group.

12. ETSI TS 102 853, Electronic Signatures and Infrastructures (ESI); Signature verification procedures and policies, V1.1.1, July 2012.

13. TS 13678 Elektronik Kimlik Doğrulama Sistemi - bölüm 1: Genel Bakiş

14. TS 13679 Elektronik Kimlik Doğrulama Sistemi - Bölüm 2: Kimlik Doğrulama Sunucusu

15. TS 13680 Elektronik Kimlik Doğrulama Sistemi - Bölüm 3: Kimlik Doğrulama Politika Sunucusu

16. TS 13681 Elektronik Kimlik Doğrulama Sistemi - Bölüm 4: Kimlik Doğrulama Yöntemleri

17. Common Criteria for Information Technology Security Evaluation Part I: Introduction and General Model; Version 3.1 Revision 5 CCMB-2017-04-001

18. Common Criteria for Information Technology Security Evaluation Part II: Security Functional Requirements; Version 3.1 Revision 5 CCMB-2017-04-001

19. Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 3.1 Revision 5 CCMB-2017-04-001

20. Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5 CCMB-2017-04-001