mtbilgiteknolojileri

VERA Type-II SSR Firmware with SAS v1.3.0

VERA KEC SECURITY TARGET V2.2

18.12.2021

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

Document History

Version	Change Date	Changes	Author
2.0	29.01.2021	Initial version	Aydın Çelik
2.1	14.12.2021	Updated according to the GR01	Aydın Çelik
2.2	18.12.2021	Updated according to the GR01	Aydın Çelik

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

Contents

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

List of Tables

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

List of Figures

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

1 ST INTRODUCTION

1.1 ST Reference

Title:	VERA Type-II SSR Firmware with SAS v1.3.0
Version:	2.2
Status:	Draft
Date:	18.12.2021
Developer:	MT Bilgi Teknolojileri ve Dış. Tic. A.Ş.
Keywords:	Electronic Identity, Smartcard Reader, Identity Verification, Electronic Identity Card, Secure Smartcard Reader, Biometric Authentication

1.2 TOE Reference

TOE Identification:	VERA Type-II SSR Firmware with SAS
TOE Version:	1.3.0
CC Identification:	Common Criteria for Information Technology Security Evaluations, Version 3.1R5

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

1.3 TOE Overview

This part of the ST describes VERA Type-II SSR Firmware with SAS (*TOE*) with its intended usage and general IT features as an aid to the understanding of its security requirements and addresses the different user environments.

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

As the Application Firmware, the TOE performs;

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

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

1.3.1 Major Security Features of the TOE

The following security mechanisms are primarily mediated in the TOE:

- ❖ ***Identification and Authentication***
  - Cardholder verification by using PIN and biometrics (*fingerprint data*).
  - Authentication of eID Card by the TOE,
  - Authentication of Role Holder by eID Card and by the TOE,
  - Authentication of SAM by the TOE and by eID Card,
  - Authentication of the TOE by SAM and by Card Holder (S*ervice Requester and Service Attendee*) and by external entity (*Role Holder*).
- ❖ ***Secure Communication between the TOE and***
  - SAM
  - eID Card
  - Role Holder
  - SAS
- ❖ ***Security Management***
- ❖ ***Self-Protection***
- ❖ ***Audit***

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

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

1.3.2 Non-TOE Hardware/ Software/ Firmware

1.3.2.1 Software/ Firmware Environment of TOE

The block diagram of the software environment architecture is shown in Figure 1.

File System and Software Libraries
Embedded Operating System Kernel
Kernel Drivers (Smart Card Reader, Biometric)

Figure 1: *Software/Firmware Environment of TOE*

The TOE runs at the top of Embedded Linux operating system v3.10 with a file-system in UBIFS format. The TOE makes use of some open source software libraries which are embedded in the file system. The TOE also communicates to a Smartcard Reader Driver within the Type II SSR.

1.3.2.2 Hardware Environment of TOE (SSR Hardware and SAS)

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

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

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

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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

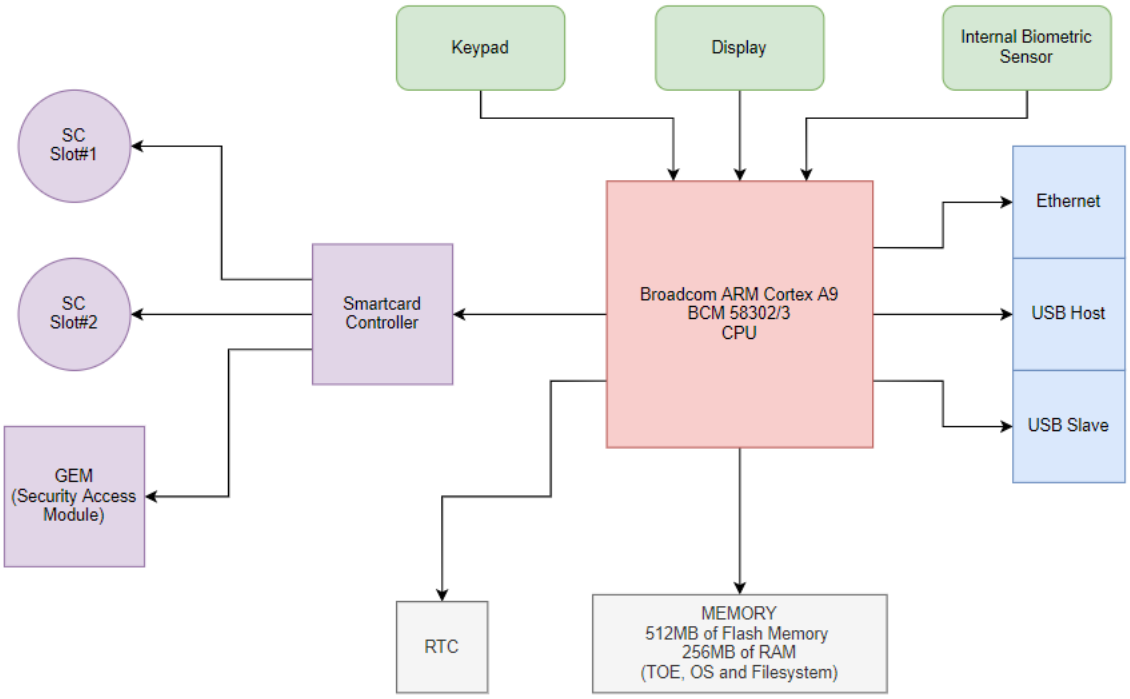


Figure 2: *Type II SSR Hardware*

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

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

1.3.3 TOE Type

The TOE is the Application Firmware running on Embedded Linux Operating System operating Type II SSR (with SAS). Root certificates of the CA, device management CA and eID management CA are also included in the TOE.

1.3.4 Actors and External Systems

Actors

- Service Requester (SR)
- Service Attendee (SA)
- Identity Faker
- Administrator (*This role has capability to read all auditable events from the audit storage*)

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 of National Republic (eID Card)
- Service Requester (SR)
- Service Attendee (SA)
- Online Certificate Status Protocol (OCSP) Server
- Illegitimate eID Card
- PC
- SAM

MT BİLGİ TEKNOLOJİLERİ A.Ş.

1.3.5 Operational Environments of Type II SSR

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

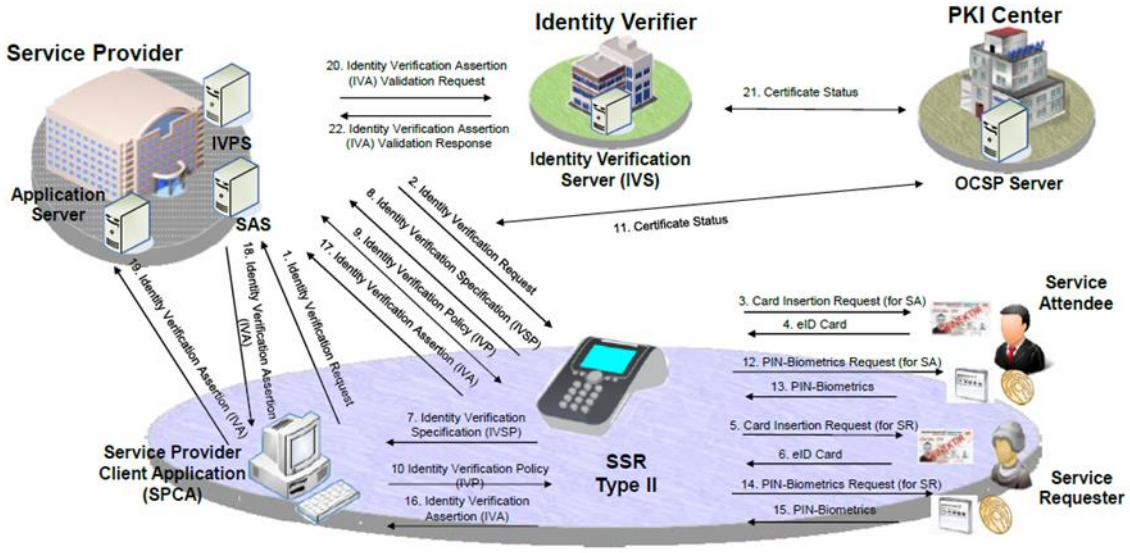


Figure 3: *User Environment of Type II SSR (with SAS)*

Operation is initiated by the Service Provider Client Application (SPCA) which is installed on a personal computer (PC).

First, SPCA sends an Identity Verification Request to TOE through the SAS via Ethernet interface (*1. Identity Verification Request & 2. Identity Verification Request*).

Once the TOE receives this request, it asks the SR and the SA to insert their eID card one by one into the smartcard slot.

After the eID cards are inserted, the TOE sets up a secure messaging session with the eID cards. Having read the cardholder's personal message from the eID card, the TOE displays it on the screen for the SR's and SA's approval.

If the displayed message is approved by the SR and SA, an Identity Verification Specification (IVSP), is generated by the TOE, and sent to IVPS through the SAS.

Next, the Identity Verification Policy Server (IVPS) sends the Identity Verification Policy (IVP) to the TOE through the SAS for the SR and SA specified in the IVSP.

MT BILGI TEKNOLOJILERI

Since the IVP is signed by the IVPS, the TOE checks the signature to make sure it comes from a legitimate IVPS and hasn't been modified. The IVP defines the Identity Verification Method (IVM) for the SR and SA and the organizational policies defined in TS 13584 [3].

If an IVPS doesn't exist, the SPCA defines the IVM itself. Otherwise, the TOE uses the predefined default IVM which has the highest security level. During identity verification, the Identity Verification Certificate within the eID Card is not only verified offline by the TOE, but also validated online with the help of the Online Certificate Status Protocol (OCSP) Server.

If the online certificate validation cannot be achieved due to technical problems, there are two options to continue the operation:

(i) The TOE validates the eID Card of the SR and the SA using the Certificate Revocation List downloaded on the Type II SSR. In this case, the information that "***OCSP check could not be achieved***" shall be included in the IVA.

(ii) The TOE does not validate the eID Card of the SR and the SA. In this case, the information that "***OCSP check and Revocation List control could not be achieved***" shall be included in the IVA.

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

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

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

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

1.3.6 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 are installed to the Type II SSR 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 Type II 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 and SAM PIN*) within the Type II SSR are deleted and the TOE becomes out of service; all TOE 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.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

1.4 TOE Description

This part of the ST describes the physical and logical scopes of the TOE as an aid to the understanding security capabilities of the TOE and to the separating of the TOE from non-TOE entities.

1.4.1 Physical Scope of TOE

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

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

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

The physical scope (*except TOE Documentation*) of the TOE is shown in green box in Figure 4.

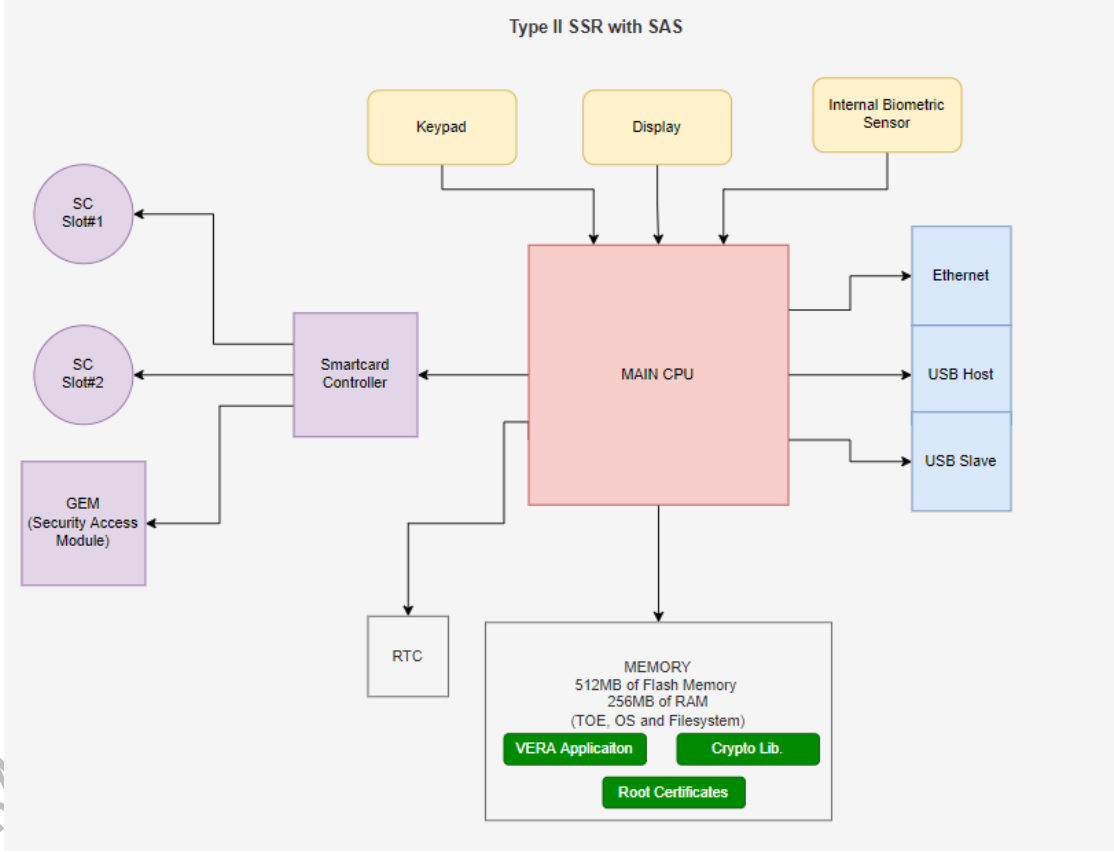


Figure 4: *Physical Scope (except TOE Documentation) of the TOE*

VERA Application

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

CONFIDENTIAL

Crypto Libraries

Crypto Libraries consist of OpenSSL v1.1.1i and Mbed TLS (2.16.6 and 2.7.15) libraries, which are embedded in the file system, are software library written in the C programming language as open-source and contains software crypto library for different crypto algorithm and implementation of the TLS protocols.

Secure communication and crypto operations are performed by the VERA Application using OpenSSL and Mbed TLS libraries.

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

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

- TOE Documentation consists of:
  - The TOE operational guidance
  - The TOE preparative procedures

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

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

1.4.2 Logical Scope of TOE

This section describes the logical security features of the TOE.

Table 1: *Logical Scope of TOE*

TOE Security Function	Description
Identification and Authentication	The TOE enforces identification mechanism that requires users (*eID Card, Role Holder Device, SSR Access Server and SAM*) identify themselves before any other action will be allowed by the TOE and also enforces multiple authentication mechanisms that requires different authentication mechanisms for Card Holders, eID Card, Role Holder Device, SSR Access Server and SAM. The TOE also performs re-authenticating mechanism with different scenario for different users. During the authentication process, the TOE provides only limited feedback information to the user in order to protect Card Holder authentication data. In cases of the number of unsuccessful biometric verification attempts exceeds the indicated threshold, the TOE performs biometric verification failure handling mechanism to take actions.
Secure Communication	The TOE performs secure communication with Role Holder Device, SSR Access Server, eID Card and SSR SAM Card for the protection of the channel data from modification or disclosure. The TOE produces digital signature of data using SAM Card for the verification of the evidence of origin of information to the recipients.
Cryptographic Operation	The TOE performs cryptographic operations such as cryptographic key generation, encryption, decryption, hash generation, signature verification and key destruction.
Security Management	The TOE associates users with Initialization Agent, SSR Access Server for TOE, Client Application for TOE, Identity Verification Policy Server, OCSP Server, Manufacturer service operator, Software Publisher roles. The TOE allows these roles to provide to control over the management of security functions behaviour of the TOE (*TOE upgrade function and Identity Verification Method determination*) and management of TSF data (*SAM PIN and DTN initialization, time and date setting*). It is also capable of performing the audit generation function.
TSF Protection	The TOE has the ability to verify that the defined imported TSF Data originates from the stated external entity and synchronize its internal state with another trusted external entity. The TOE also performs self-tests to demonstrate the correct operation of the TSF at start up. When the tampering event is detected and identification and authentication of the SAM are disturbed, it preserves secure state.

TEKNOLOJİLERİ - CONFIDENTIAL

Security Audit	The TOE generates an audit record of security events and records within each audit record detail information such as date and time (*reliable time*) of the event and also takes the actions to protect itself in case tampering of the Type II SSR is detected. In addition, The TOE protects the audit records stored in the audit trail from unauthorized deletion and detects unauthorized modifications. The TOE also enforces audit records storage rules to prevent audit record loss in case the audit storage is full. The TOE provides audit review functionality.
User Data Protection	The TOE provides Information Flow Control Policy when importing data exporting data during secure communication with SAS and SPCA (*through SAS*). It ensures that any previous information content of a resource is made unavailable upon the deallocation of the resource from the objects (*cryptographic credentials, IVA data fields, PIN, photo and biometric information*)

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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 and Package Claim

2.2.1 Protection Profile (PP) Claim

This Security Target claims strict conformance to '*Common Criteria Protection Profile for Application Firmware of Secure Smartcard Reader for National Electronic Identity Verification System*', Version 2.8, 1th August 2017.

2.2.2 Package Claim

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

2.3 Conformance Rationale

The TOE type of the TOE is consistent with TOE type of the PP which is claimed in the section 2.2.1.

The statement of the security problem definition is consistent with the statement of Type II security problem definition in the PP for which conformance is being claimed.

The statement of security objectives is consistent with the statement of Type II security objectives in the PP for which conformance is being claimed.

The statement of security requirements is consistent with the statement of Type II security requirements in the PP for which conformance is being claimed.

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

3 SECURITY PROBLEM DEFINITION

This part of the ST defines the security problem that is to be addressed by the TOE and consists of following subsections:

- Assets
- Subjects and External Entities
- Organizational Security Policies
- Threats
- Assumptions

3.1 Assets

The Type II 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 (VERA Type-II SSR with SAS Firmware v1.0.0) does not possess any user data.

Table 2: *Primary and Secondary Assets*

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	Correct operation

MTBILGI TEKNOLOJILERI - CONFIDENTIAL

		Application Server (APS), SSR Access Server (SAS) and SAM.	
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 Type II SSR (with SAS).	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 Type II SSR. These certificates are given by Device Management Certificate Authority and imported from SAM to the Type II SSR 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

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

3.2 Subjects and External Entities

The legitimate and the malicious actors and external entities are defined as below:

Table 3: *Legitimate and malicious actors and external systems*

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
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)	

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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

Note 2: No illegitimate Identity Verification Server (IVS) exists within the current context. The reason the IVS is taken into the scope this ST, 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).

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

3.3 Threats

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

Table 4: *Threats*

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 SAS and the TOE.
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 Hardware and introduce it to the Service Requesters (and/or Service Attendee). This way, the attacker may collect the Identity Verification Card-PIN and Biometric Information.
T.Fake_TOE_to_External_Entities	An attacker may introduce himself/herself as legitimate TOE to eID Card. Thus obtain the PIN and biometric information of the Service Requester (or the Service Attendee) and gain access to eID Card on behalf of the Role Holder.

LOJILERI - CONFIDENTIAL

T.SA_Masquerader	An attacker may act as if he/she is a legitimate service attendee and perform the photo verification and thus damage the Identification and Authentication Service of the Service Requester.
T.SA_Abuse_of_Session	An attacker may abuse the service attendee's authentication session. Thus the attacker can validate the photo and/or accept negative result of biometric verification in an unauthorized way. This action therefore is regarded as damaging the correct operation of the Identification and Authentication of the Service Requester and the Service Attendee.
T.Fake_Policy	An attacker may send a fraudulent policy to manage the authentication process in an unauthorized manner. This action is also regarded as damaging the correct operation of the Identification and Authentication of the SA and the SR.
T.Fake_OCSP_Response	An attacker may mimic a legitimate Online Certificate Status Protocol Server (OCSPS) or manipulate the TSF Data transmitted by OCSPS. This action is also regarded as damaging the correct operation of the Identification and Authentication of the SA and the SR.
T.RH_Comm	An attacker may access or modify the eID Card contents through eavesdropping and manipulating the communication between the Role Holder and eID Card.
T.RH_Session_Hijack	An attacker may access or modify the eID Card contents through hijacking the authentication session between the eID Card and the Role Holder.
T.eIDC_Comm	An attacker may access or modify the eID Card contents, steal the PIN and biometric information, block the PIN and biometric verification through (1) eavesdropping and modifying the communication; (2) hijacking or replaying the authentication session between the TOE and eID Card.
T.Illegitimate_SAS	An attacker may use illegitimate SSR Access Server (SAS) to undermine security policies. This action is also regarded as damaging the correct operation of the Identification and Authentication of third party IT Components for TOE on Type II SSR

LOJİLERİ - CONFIDENTIAL

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

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

3.4 Organizational Security Policies

The OSPs are given in Table 5.

Table 5: *Organizational Security Policies*

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]. Client application and SSR Access Server shall update the Secure Messaging and Role Card Verifiable Certificates of SAM one day before the expiration day.
P.Time_Update	The time shall be updated using the real time that is received only from trusted entities.
P.Revocation_Control	In case SSR Device cannot reach to OCSP Server, downloading the Revocation List onto the SSR Device and checking the certificate revocation status of the Service Requester (and the Service Attendee if applicable) from this list is allowed. The revocation list shall be up to date. When the certificate revocation check is carried out without OCSP Server, the information regarding that OCSP check could not be realized shall be put in the IVA. If the OCSP Server is not reached and there is no downloaded revocation list, then the information that OCSP check and revocation list control could not be realized shall be put in the IVA. In this case, only the certificate status control is performed offline, other identity verification steps shall be performed online. Unless IVA is validated at IVS and revocation check is completed, Identity Verification is not regarded as completed.
P.DPM	The TOE shall support Initialization & Configuration and Operation lifecycle phases. The phase change shall be from Initialization & Configuration Phase to Operation Phase except tamper event detection case. If a tamper event is detected, TOE shall be out of service and require re-initialization. This shall be the only condition to go back to Initialization & Configuration

MOBİL ÖDEME TEKNOLOJİLERİ - CONFIDENTIAL

	Phase. DTN and SAM PIN shall be written to the Type II SSR during Initialization & Configuration Phase.
P.Tamper_Response	The SSR platform will be able to detect any tampering attempts and will notify the TOE. The TOE will respond to this notification by securely deleting the SAM-PIN and getting into Initialization & Configuration phase.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

3.5 Assumptions

The assumptions for the operational environment are given in Table 6.

Table 6: *Assumptions for the Operational Environment*

Assumption	Definition
A.SPCA	It is assumed that Service Provider Client Application is a trusted third party. For Type II SSR with SAS, there is no direct connection between the Type II SSR and the SPCA. SPCA communicates to the SSR through the SAS via Ethernet interface. When the Service Provider Client Application determines the identity verification method, it is assumed that the Service Provider Client Application selects the appropriate method. In addition, integrity and the confidentiality of the private data transferred from Type II SSR to the Client Application is preserved by the foundation sustaining the Client Application.
A.IVPS	It is assumed that the IVPS prepares and sends the policy correctly.
A.PC	It is assumed that the PC executing the Client Application is malicious code free and located in secure environment. In addition, the confidentiality of the private data that might be written into the IVA by the Application Owner as Application Specific Data is preserved by the Application Owner.
A.APS-IVPS	It is assumed that the Application Server and the Identity Verification Policy Server are malicious code free and located in secure environment.
A.Management_Environment	It is assumed that the environments, where initialization and configuration are performed, are secure. And the personal that hold initialization and configuration roles act responsively.
A.SAM_ PIN_Environment	It is assumed that the PIN value of the SAM in the Type II SSR is defined in the Type II SSR in secure environment.
A.SSR_Platform	The SSR platform supports the security functionality of the

MTBİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

	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.

Application Note: The SSR Platform consists of the physical enclosure, physical hardware, security elements, operating system and other dedicated software. A.SSR_Platform enables that Security Objectives of the TOE and the SSR Platform together are resistant to the attackers possessing Enhanced Basic Attack Potential.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

4 SECURITY OBJECTIVES

In this section part-wise solutions are given against the security problem defined in Part 3.

4.1 Securıty Objectives for the TOE

Security Objectives for the TOE are given in Table 7.

Table 7: *Security Objectives of 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 Type II SSR. 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.

MLOJILERI - CONFIDENTIAL

OT.Biometric_Verification	The TOE shall support Biometric Verification defined in TS 13584 [3] for Identification and Authentication of Service Requester and Service Attendee.
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.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 Type II 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 with authenticated SAS after 24 hours.
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.SAS_DA	Mutual authentication between the TOE on Type II SSR and the SAS shall be setup before TOE's doing any action.
OT.SAS_SC	The TOE on Type II SSR 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.

OLOJİLERİ - CONFIDENTIAL

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.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 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) SAS for online upgrade operation: 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 Type II SSR. 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.

TEKNOLOJİLERİ CONFIDENTIAL

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 hardware.
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 under electronic mesh cover and 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 and update the certificates.

MT BILGI TEKNOLOJILERI CONFIDENTIAL

4.2 Security Objectives for the Operational Environment

Security objectives for the SSR Hardware and the User Environment of the Type II SSR.

Table 8: *Security Objectives for the Operational Environment*

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 Type II 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 data) • 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,

TOJİLERİ-CONFIDENTIAL

	• support signing the IVA, • support Secure Messaging key generation mechanisms for the communication between the TOE and the following entities: (1) eID Card, (2) Role Holder, 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

OJILERI - CONFIDENTIAL

	(Public Key of IVA Signing Certificate's integrity is protected)

OE.SSR_Platform	The Type II SSR platform shall not have vulnerabilities exploitable by attackers possessing Enhanced-Basic attack potential for the below mentioned security features:
	• including minimum hardware configuration to provide correct operation of the TOE,
	• possessing tamper-detection and response mechanisms that cause the Type II SSR to become immediately out of service and result in the automatic and immediate erasure of SAM PIN and cryptographic keys stored in tamper protected area, such that it becomes infeasible to recover these sensitive data.
	• being designed and implemented in a secure manner such that
	  • hardware components are chosen to prevent probing (they shall be BGA);
	  • it protects the unencrypted data and address busses carrying the user data and TSF data so that they are not directly reachable;
	• including 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.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,

OJILERI - CONFIDENTIAL

OE.SAS	The SAS will support Secure Communication with the TOE on Type II SSR. SAS shall encrypt the Identity Verification Assertion before sending it to the SPCA.
OE.Terminal_Cert_Directory	SSR Access Server 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, 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 Client Application. 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 Type II SSR where SAM PIN is defined to the Type II SSR shall be physically secure.

MT BILGİ - ÖZEL - CONFIDENTIAL

4.3 Coverage of Threats, OSPs and Assumptions by the Security Objectives

Table 9: *Security Objectives Rationale Table for TOE on Type II SSR with SAS and Internal Biometric Sensor*

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
T.Counterfeit_eIDC	✓		✓										✓																	
T.Revoked_eIDC	✓																													
T.Stolen_eIDC				✓																						✓	✓			
T.IVA_Fraud					✓																									
T.IVA_Eavesdropping																														✓
T.Repudiation				✓																							✓			
T.Fake_TOE_to_SR						✓																								
T.Fake_TOE_to_External_Entities										✓			✓																✓	
T.SA_Masquerader																												✓		
T.SA_Abuse_of_Session							✓																							
T.Fake_Policy								✓																						
T.Fake_OCSP_Response									✓																					
T.RH_Comm											✓																			

MT BİLGİ TEKNOLOJİ

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
T.RH_Session_Hijack										✓		✓																		
T.eIDC_Comm													✓																	
T.Illegitimate_SAS																													✓	
T.DTN_Change																	✓													
T.SAM-PIN_Theft		✓																	✓	✓										
T.Audit_Data_Compromise		✓																				✓								
T.TOE_Manipulation		✓																	✓	✓	✓	✓	✓							
T.Fake_SAM																								✓						
T.Stolen_SAM																✓			✓	✓				✓						
T.Revoked_SAM																								✓						
P.IVM_Management	✓																													
P.TOE_Upgrade														✓																
P.Terminal_Cert_Update																									✓					
P.Re-Authentication							✓																							

MT BILGI TEKNOLOJILERI

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
P.Time_Update																		✓												
P.Revocation_Control			✓																											
P.DPM			✓												✓	✓	✓													
P.Tamper_Response		✓																												

MT BILGI TEKNOLOJILERI

Table 10: *Environmental Security Objectives Rationale Table for TOE on Type II SSR with SAS and Internal Biometric Sensor*

	OE.SPCA	OE.IVPS	OE.eID Card	OE.SAM	OE.Service_Attendee	OE.Service_Requester	OE.OCSPS	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_eIDC			✓	✓											✓	✓		
T.Revoked_eIDC			✓				✓								✓	✓		
T.Stolen_eIDC			✓		✓	✓			✓									
T.IVA_Fraud				✓				✓							✓	✓		
T.IVA_Eavesdropping													✓					
T.Repudiation			✓			✓									✓	✓		
T.Fake_TOE_to_SR			✓	✓		✓									✓	✓		
T.Fake_TOE_to_External_Entities			✓	✓											✓	✓		
T.SA_Masquerader			✓	✓	✓										✓	✓		
T.SA_Abuse_of_Session					✓													
T.Fake_Policy		✓													✓	✓		
T.Fake_OCSP_Response							✓								✓	✓		
T.RH_Comm				✓						✓								
T.RH_Session_Hijack			✓	✓						✓					✓	✓		
T.eIDC_Comm			✓	✓														
T.Illegitimate_SAS													✓					

MTBİLGİ TEKNOLOJİLERİ

	OE.SPCA	OE.IVPS	OE.eID Card	OE.SAM	OE.Service_Attendee	OE.Service_Requester	OE.OCSPS	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.DTN_Change									✓									
T.SAM-PIN_Theft									✓									
T.Audit_Data_Compromise									✓									
T.TOE_Manipulation									✓									
T.Fake_SAM				✓											✓	✓		
T.Stolen_SAM				✓												✓		
T.Revoked_SAM				✓			✓											
P.TOE_Upgrade	✓			✓									✓				✓	
P.Terminal_Cert_Update														✓		✓		
P.Revocation_Control																✓		
P.Tamper_Response									✓									
A.SPCA	✓																	
A.IVPS		✓																
A.PC											✓							
A.APS-IVPS																	✓	
A.Management_Environment												✓						
A.SAM_ PIN_Environment																		✓

MTBİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

	OE.SPCA	OE.IVPS	OE.eID Card	OE.SAM	OE.Service_Attendee	OE.Service_Requester	OE.OCSPS	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
A.SSR_Platform									✓									

MT BILGI TEKNOLOJILERI

Justification about Table 9 and Table 10 are given below;

T.Counterfeit_eIDC:

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. Authentication methods required by OT.IVM_Management.

These mechanisms bring about some requirements on eID card, which is addressed by OE.eID Card 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 and OE.CM*

T.Stolen_eIDC

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 addresses the features in the TOE for this operation, OE.eID_Card addresses the eID Card requirements for this operation, and OE.Service_Requester addresses the Service Requester requirements for this operation).

Photo Verification and Biometric Verification strengthens the resistance against the T.Stolen_eIDC. (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_eIDC

Authentication methods required by OT.IVM_Management prevent the revocation attack on the eID Card. OE.OCSP covers that validity of certificate which belongs to eID. OE.eID Card covers that eID Card supports terminal authentication as defined in TS 13584. 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.IVM_Management, OE.OCSPS, OE.eID Card and 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.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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.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 and OE.SAS

Security Objectives: *OT.SAS_SC and OE.SAS*

T.Repudiation

OT.PIN_Verification requires PIN Verification mechanisms to ensure that SR/SA and eID Card had joined to the Identification Process. OT.Biometric_Verification requires Biometric Verification mechanisms to ensure that SR/SA 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. 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 and OE.CM*

T.Fake_TOE_to_External_Entities

Authentication objective for eID Card, Role Holder and SAS are OT.SM_eIDCard, OT. RH_DA, OT.SAS_DA correspondingly require TOE to prove its identity before doing any action. SAM card in the Type II SSR 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.

Security Objectives: *OT.SM_eID Card, OT. RH_DA, OT.SAS_DA, OE.SAM, OE. eID Card, OE.PKI and OE.CM*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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 and OE.CM*

T.Fake_OCSP_Response

OT.OCSP_Query_Verify 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 and 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 and OE.Role_Holder*

MT BİLGİ TEKNOLOJİLERİ- CONFIDENTIAL

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 and 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.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 and OE.SAS*

T.DTN_Change

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

Security Objectives: *OT.DTN_Mgmt and 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.SM_TOE_and_SAM, OT.SAM-PIN_Sec and OE.SSR_Platform.*

T.Audit_Data_Compromise

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

Security Objective: *OT.Security_Failure, OT.Audit_Data_Protection and 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],

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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.Security_Failure, 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] and 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, OE.SAM, OE.PKI and 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 Type II SSR (*the legitimate or the fake*) access its services. OT.SAM-PIN_Sec and OT.SM_TOE_and_SAM requires the SAM PIN security during operation of the Type II SSR. The OE.CM protects the SAM-PIN during generation and writing to the SAM and the TOE.

OT.SAM-PIN_Mgmt requires the management function which ensures that the SAM PIN can only be written to the SSR Device by the ADMINISTRATOR during the Initialization and Configuration phase.
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.OCSPS cover the threat.

Security Objectives: *OT.Auth_SAM_by_TOE, OE.SAM and 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.*

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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.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 and 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.PC: OE. PC covers the assumption

Security Objective: *OE.PC*

A.APS-IVPS: 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*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

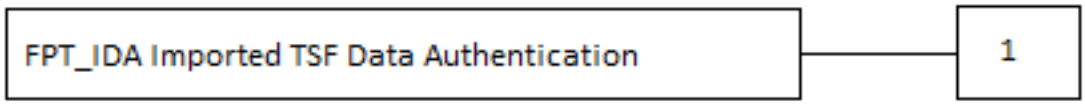
5 EXTENDED COMPONENTS DEFINITION

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 Levelling:



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].

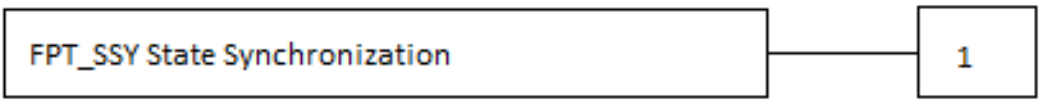
MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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 Levelling:



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].

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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[2] 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, SAM authentication, SAM-PIN verification failure, TOE update, IVP verification, OCSP answer verification, SAS authentication and tampering of the SSR*[3].

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)*[4].

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*[5] upon detection of a potential security violation.

6.1.1.3 FAU_SAR.1 Audit review

Hierarchical to: No other components.

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

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.

2[selection, choose one of: minimum, basic, detailed, not specified]

3[assignment: other specifically defined auditable events]

4[assignment: other audit relevant information]

5[assignment: list of actions]

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

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[6] 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[7] and *none*[8] 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*[9] known to indicate a potential security violation;

b) *none*[10].

6.1.2 Class FCS: Cryptographic Support

6.1.2.1 FCS_CKM.1/SM - Cryptographic key generation for secure messaging with eID, SA 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*

6 [selection, choose one of: prevent, detect]

7 [selection, choose one of: "ignore audited events", "prevent audited events, except those taken by the authorized user with special rights", "overwrite the oldest stored audit records"]

8 [assignment: other actions to be taken in case of audit storage failure]

9[assignment: subset of defined auditable events]

10[assignment: any other rules].

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

CMAC Key Generation Algorithm for Secure Messaging[11] and specified cryptographic key sizes *256 bits*[12] that meet the following: *TS 13584 [3]*[13].

Application Note 1: *Above mentioned Secure Messaging are founded between TOE and eID; TOE and SAM; TOE and Role Holder.*

6.1.2.2 FCS_CKM.1/SM_TLS - Cryptographic key generation for secure messaging with 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* [14] and specified cryptographic key sizes *256 Bits*[15] that meet the following: *RFC 5246*[16].

Application Note 2: *TLS Key Generation is performed between TOE and SSR Access Server.*

6.1.2.3 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 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 "*Secure::smemset" Method* [17] that meets the following: *none*[18].

Application Note 3: *FCS_CKM.4 destroys all cryptographic keys (secure messaging keys, the Upgrade Package key and TLS keys) with same key destruction method.*
The Method used in ***"void *Secure::smemset(void *v, int c, size_t n)"*** *function described below.*

- ***void * smemset (void *v, int c, size_t n)*** *function copies the character* ***c*** *(an unsigned char) to the first* ***n*** *characters of the string pointed to, by the argument* ***v.***

11[assignment: cryptographic key generation algorithm]
12[assignment: cryptographic key sizes]
13[assignment: list of standards]
14[assignment: cryptographic key generation algorithm]
15[assignment: cryptographic key sizes]
16[assignment: list of standards]
17[assignment: cryptographic key destruction method]
18[assignment: list of standards]

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

- ***v** is a pointer to the block of memory to fill.*
- ***c** is the value to be set. The value is passed as an **int**, but the function fills the block of memory using the unsigned char conversion of this value.*
- ***n** is the number of bytes to be set to the value.*
- *Return Value returns a pointer to the memory area **v**.*

6.1.2.4 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*[19] in accordance with a specified cryptographic algorithm *SHA-256 [5]*[20] and cryptographic key sizes *none*[21] that meet the following: *FIPS 180-4*[22].

6.1.2.5 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 and FCS_CKM.1/SM_TLS; [FCS_CKM.4 Cryptographic key destruction] **fulfilled** by FCS_CKM.4

Justification: *This SFR is used for decryption of the TOE Upgrade package but there is no FCS_CKM.1 to generate decryption key. 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. Thus, the first dependency (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) is not satisfied for the decryption requirement for the TOE Upgrade package.*

MT BILGI TEKNOLOJILERI CONFIDENTIAL

19[assignment: list of cryptographic operations]
20[assignment: cryptographic algorithm]
21[assignment: cryptographic key sizes]
22[assignment: list of standards]

FCS_COP.1.1	The TSF shall perform *encryption and decryption*[23] in accordance with a specified cryptographic algorithm *AES-256 CBC Mode*[24] and cryptographic key sizes *256 bits*[25] that meet the following: *FIPS 197 (for AES) [6], NIST Recommendation for Block Cipher Modes of Operations (for CBC mode)[7]*[26].

6.1.2.6 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, and 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*[27] in accordance with a specified cryptographic algorithm *AES-CMAC*[28] and cryptographic key sizes *256 bits*[29] that meet the following: *FIPS 197 (for AES) [6], RFC 4493 (for CMAC operation) [9]*[30].

6.1.2.7 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*[31] in accordance with a specified cryptographic algorithm *RSA OAEP* [32] and cryptographic key sizes

23[assignment: list of cryptographic operations]
24[assignment: cryptographic algorithm]
25[assignment: cryptographic key sizes]
26[assignment: list of standards]
27[assignment: list of cryptographic operations]
28[assignment: cryptographic algorithm]
29[assignment: cryptographic key sizes]
30[assignment: list of standards]
31 [assignment: list of standards]
32 [assignment: cryptographic algorithm]

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

2048[33] that meet the following: *TS 13584 [3]*, and *RSA Cryptography Standard [10]*[34].

6.1.2.8 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*[35] in accordance with a specified cryptographic algorithm *RSA, PKCS#1 v2.1 with PSS padding method* [36] and cryptographic key sizes *2048*[37] that meet the following: *ETSI TS 102 853[12] and TS 13584 [3]*[38].

Application Note 4: *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.

33 [assignment: cryptographic key sizes]
34 [assignment: list of standards]
35[assignment: list of cryptographic operations]
36[assignment: cryptographic algorithm]
37[assignment: cryptographic key sizes]
38[assignment: list of standards]

MT BİLGİ TEKNOLOJİLERİ CONFIDENTIAL

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*[39] unsuccessful authentication attempts occur related to *Biometric Verification*[40].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been met[41], the TSF shall not allow *further biometric verification*[42].

Application Note 5: *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~~ **Role Holder, Secure Access Module, eID Card and SAS** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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~~ **Role Holder, Secure Access Module, eID Card and SAS** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

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,*

39[selection: [assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]]

40[assignment: list of authentication events]

41[selection: met, surpassed]

42[assignment: list of actions]

MT BİLGİ TEKNOLOJİLERİ CONFIDENTIAL

- *SAS authentication*[43]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate ~~any user's~~ **Secure Access Module, Service Requester, Service Attendee, Role Holder Device, eID Card and SAS** 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 and biometric verification as defined in TS 13585 [4].*
- *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. 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 as defined in TS 13585 [4].*
- *eID Card, SAM and Role Holder Device are done by certificate verification.*
- *SAS authentication are done by SSL/TLS certificate authentication. SAS verification is a mutual authentication started by the TOE*[44].

Application Note 6: *Certificates stored in the SAM are used for the SSL/ TLS client authentication.*

Application Note 7: *eID Card is the smart card with the National 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.

MT BİLGİ TEKNOLOJİLERİ CONFIDENTIAL

43[assignment: list of multiple authentication mechanisms]

44[assignment: rules describing how the multiple authentication mechanisms provide authentication]

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~~ **Service Attendee, Service Requester, SAM, Role Holder and SAS** 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,*
  - *SAS authentication*[45]

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 only

- *a dummy character for each entered PIN entry for authentication by PIN*
- *a dummy fingerprint representation for authentication by biometry*

on the SSR screen[46] to the ~~user~~ **Service Requester or Service Attendee** while the authentication is in progress.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

45[assignment: list of conditions under which re-authentication is required]

46[assignment: list of feedback]

6.1.4 Class FCO: Communication

6.1.4.1 FCO_NRO.2 Enforced proof of origin for Identity Verification Assertion

Hierarchical to: FCO_NRO.1 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*[47] at all times.
FCO_NRO.2.2	The TSF shall be able to relate the *identity of origin*[48] of the originator of the information, and the *Identity Verification Assertion Data*[49] 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*[50] given *immediately in online mode*[51].

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 8: *- IVS verifies the IVA. This is why the assignment is instantiated as "Identity Verification Server". However, the TOE gives the IVA to SPCA through SAS and SPCA sends the IVA to APS. Finally, APS sends the IVA to IVS.*

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

47 [assignment: list of information types]

48 [assignment: list of attributes]

49 [assignment: list of information fields]

50 [assignment: list of third parties]]

51 [assignment: limitations on the evidence of receipt]

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[52] the function *Identity Verification Operation*[53] to the *Identity Verification Policy Server or Client Application*[54].

Application Note 9: *Default Identity Verification Method is defined in the TOE during production for using 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[55] the function *TOE Upgrade*[56] to *Client Application for TOE and Manufacturer service operator*[57].

Application Note 10: *TOE allows only for the higher versions of the Upgrade Package associated with the SAM in the corresponding Type II 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*[58] the *SAM-PIN*[59] to *Initialization Agent*[60].

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

52[selection: determine the behavior of, disable, enable, modify the behavior of]
53[assignment: list of functions]
54[assignment: the authorized identified roles]
55[selection: determine the behavior of, disable, enable, modify the behavior of]
56[assignment: list of functions]
57[assignment: the authorized identified roles]
58[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
59[assignment: list of TSF data]
60[assignment: the authorized identified roles]

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*[61] the *Device Tracking Number*[62] to *Initialization Agent*[63].

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*[64] the *Time*[65] to *OCSP server*[66].

Application Note 11: *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*[67].

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

61[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
62[assignment: list of TSF data]
63[assignment: the authorized identified roles]
64[selection: change_default, query, modify, delete, clear, [assignment: other operations]]
65[assignment: list of TSF data]
66[assignment: the authorized identified roles]
67[assignment: list of management functions to be provided by the TSF]

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*
- *Client Application for TOE*
- *Identity Verification Policy Server,*
- *OCSP Server,*
- *Manufacturer service operator*
- *Software Publisher*[68].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

68[assignment: the authorized identified 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 12: *Reliable time stamp is provided from the OCSP server and stored in a real time clock on Type II SSR.*

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*[69] originates from *Card Publisher*[70] using *CVC Authentication Mechanism defined in TS 13584 [3]*[71].

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*[78] originates from *Card Publisher and Device Manager*[108] using *X509 Certificate Authentication Mechanism defined in TS 13584 [3]*[109].

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*[72] originates from *Identity Verification Policy Server*[73] using *IVP authentication mechanism defined in TS 13584 [3]*[74].

MT BILGI TEKNOLOJILERI CONFIDENTIAL

69[assignment: list of TSF Data]

70[assignment: list of external entities]

71[assignment: list of authentication mechanisms].

72[assignment: list of TSF Data]

73[assignment: list of external entities]

74[assignment: list of authentication mechanisms].

108[assignment: list of external entities]

109[assignment: list of authentication mechanisms].

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*[75] originates from legitimate *OCSP Server*[76] using *OCSP Response Verification Mechanism defined TS 13584 [3]*[77].

Application Note 13: *For offline Revocation Status Control from the Revocation List downloaded onto the Type II SSR 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*[78] originates from *legitimate Software Publisher*[79] using *TOE Upgrade Authentication mechanism defined in TS 13584 [3]*[80].

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* [81] **and request updated certificates** from the *SAS* in times*: at each Identity Verification Operation*[82].

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*[83] from the *OCSP Server*[84] in times*: immediately after opening of the SSR*[85].

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

75[assignment: list of TSF Data]
76[assignment: list of external entities]
77[assignment: list of authentication mechanisms].
78[assignment: list of TSF Data]
79[assignment: list of external entities]
80[assignment: list of authentication mechanisms].
81[assignment: security attributes]
82 [assignment: defined periods]
83[assignment: security attributes]
84[assignment: the external entities]
85 [assignment: defined periods]

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*[86] from the *OCSP Server or SSR Platform on which up-to-date Revocation List is present*[87] in times: *during Identity Verification Operation.*

Application Note 14: *The TOE downloads the revocation list onto the Type II SSR 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* [88] from the *eID Card*[89] in times: *after the secure communication between Role Holder and the TSF is terminated*[90].

Application Note 15: *The TSF resets 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[91] to demonstrate the correct operation of the TSF[92].

~~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[93].~~

~~FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [selection: [assignment: parts of TSF], TSF].~~

86[assignment: security attributes]

87[assignment: the external entities]

88[assignment: security attributes]

89[assignment: the external entities]

90 [assignment: defined periods]

91[selection: during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions[assignment: conditions under which self-test should occur]]

92[selection: [assignment: parts of TSF], the TSF].

93 [selection: [assignment: parts of TSF data], TSF data]

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

Application Note 16: *The TSF run self-tests, during initial start-up to verify its correct operation. Self-tests include the verification of the integrity of root certificates and verification of the integrity of stored executable TSF code.*

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*[94].

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

94 [assignment: list of types of failures in the TSF]

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*[95]on :

Subjects : SAS

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)[96].

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* [97]based on the following types of subject and information security attributes:

Subjects : SAS

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 [98].

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 SAS 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*[99].

95 [assignment: information flow control SFP]

96 [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

97 [assignment: information flow control SFP]

98 [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

99 [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

FDP_IFF.1.3	The TSF shall enforce the *none*[100].
FDP_IFF.1.4	The TSF shall explicitly authorize an information flow based on the following rules: *none*[101].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: *none*[102].

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*[103] 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*[104].

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[105] the following objects *cryptographic credentials, IVA data fields, PIN, photo and biometric information*[106].

6.1.8

MT BILGI TEKNOLOJILERI CONFIDENTIAL

100 [assignment: additional information flow control SFP rules]

101 [assignment: rules, based on security attributes, that explicitly authorize information flows]

102 [assignment: rules, based on security attributes, that explicitly deny information flows]

103 [assignment: access control SFP(s) and/or information flow control SFP(s)]

104 [assignment: additional exportation control rules]

105 [selection: allocation of the resource to, deallocation of the resource from]

106 [assignment: list of objects]

6.1.9 Class FTP: Trusted Path/Channels

6.1.9.1 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, eID Card, SSR SAM and SAS** 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[107] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for *all functions*[108].

Application Note 17: *The role holder certificate used to construct the trusted channel shall be kept in the HSM device. Trusted paths with SSR Access Server are founded using SSL-TLS using SSL- TLS certificates.*

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

107[selection: the TSF, another trusted IT product]

108[assignment: list of functions for which a trusted channel is required]

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. The security assurance requirements are listed in Table 11 below.

Table 11: *Security Assurance Requirements Table*

Assurance Classes	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV.IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance Documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DVS.2 Sufficiency of security measures
	ALC_TAT.1 Well-defined development tools
	ALC_DEL.1 Delivery procedures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target Evaluation	ASE_INT.1 ST Introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

6.3 Security Requirements Rationale

6.3.1 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.*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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, FAU_GEN.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
SFRs: *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: *FAU_GEN.1, FIA_UID.2, FIA_UAU.2 and FIA_UAU.5*

OT.Session_Ending
FIA_UAU.6 and FAU_GEN.1 covers the objective.
SFRs: *FIA_UAU.6, FAU_GEN.1*

OT.Identity_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.*

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

OT.RH_DA [Role Holder Device Authentication]
FAU_GEN.1 audits the 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.
SFR: *FAU_GEN.1.FIA_UAU.5, FPT_IDA.1/CVC and FCS_COP.1/ Sign_Ver*

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.
SFR: *FPT_SSY.1/RH_Auth_Status*

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 and FCS_COP.1/AES-CMAC give the necessary cryptographic support for the secure communication.
SFRs: *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.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.
SFRs: *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.*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

OT.DPM
FMT_SMF.1 and FMT_SMR.1 covers the phase management functions and roles thus covers the objective.
SFRs: *FMT_SMF.1 and FMT_SMR.1*

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.
SFRs: *FMT_MTD.1/SAM-PIN, FMT_SMF.1 and 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
Time data may only be updated by the security role defined by the ST writer. 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*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

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_STG.1, FAU_SAR.1 and FAU_STG.4 covers the audit data protection.
SFR: *FAU_STG.1, 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.Cert_Update
Validity of certificates needs to be checked by the TOE. This is covered by FPT_SSY.1/ Cert State Synchronization. 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 State Synchronization, FDP_ETC.2, FDP_IFC.1 and FDP_IFF.1*

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, FCS_COP.1/SHA-256, FCS_COP.1/AES-CBC, and FTP_ITC.1*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

6.3.2 Security Functional Requirements Rationale Tables

The coverage of objectives by the SFRs are given in Table 11. Table 11 given below includes the objectives that are valid for TOE on Type II SSR with SAS and Internal Biometric Sensor.

Table 12: *Security Objectives Rationale Table for TOE on Type II SSR with SAS and Internal Biometric Sensor*

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
FAU_GEN.1		✓	✓	✓	✓	✓	✓	✓	✓	✓				✓						✓						✓	✓	✓	✓	
FAU_ARP.1																				✓										
FAU_SAR.1																						✓								
FAU_STG.1																						✓								
FAU_STG.4																						✓								
FAU_SAA.1		✓																												
FCS_CKM.1/SM						✓					✓		✓						✓											
FCS_CKM.1/SM_TLS																														✓
FCS_CKM.4						✓					✓		✓						✓											
FCS_COP.1/SHA-256					✓									✓																✓

MT BILGI TEKNO ... ENTIAL

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
FCS_COP.1/AES-CBC						✓					✓		✓	✓					✓												✓
FCS_COP.1/AES-CMAC						✓					✓		✓						✓												
FCS_COP.1/RSA																			✓												
FCS_COP.1/ Sign_Ver			✓					✓	✓	✓				✓																	
FIA_AFL.1																											✓				
FIA_UID.2			✓	✓										✓			✓	✓								✓		✓	✓	
FIA_UAU.2			✓	✓										✓			✓	✓								✓		✓	✓	
FIA_UAU.5	✓		✓	✓						✓														✓		✓	✓	✓	✓	
FIA_UAU.6							✓																								
FIA_UAU.7				✓																							✓				
FCO_NRO.2					✓																										
FMT_MOF.1/Verify	✓																														
FMT_MOF.1/Upgrade_Management														✓																	
FMT_MTD.1/SAM-PIN																✓															

MT BILGI TEKNOLOJILERI

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
FMT_MTD.1/DTN																	✓													
FMT_MTD.1/Time																		✓												
FMT_SMF.1	✓													✓	✓	✓	✓	✓												
FMT_SMR.1	✓													✓	✓	✓	✓	✓												
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 State Synchronization																									✓					
FPT_SSY.1/IVC			✓																											
FPT_SSY.1/SAM																								✓						
FPT_SSY.1/RH_Auth_Status												✓																		

MT BILGI TEKNOLOJILERI

	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_Autjentication	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.Photo_Verification	OT.Biometric_Verification	OT.SA_Identity_Verification	OT.SAS_DA	OT.SAS_SC
FPT_TST.1																					✓									
FPT_FLS.1		✓																		✓	✓									
FDP_ETC.2					✓			✓	✓					✓											✓					
FDP_IFC.1					✓			✓	✓					✓											✓					
FDP_IFF.1					✓			✓	✓					✓											✓					
FDP_RIP.1																							✓							
FTP_ITC.1					✓						✓		✓						✓											✓

MT BILGI TEKNOLOJILERI

6.3.3 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.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

7 TOE SUMMARY SPECIFICATION

7.1 TOE Security Functionality

This chapter provides a description of the Security Functionality of the TOE, which show how the TOE meets each Security Functional Requirement.

The Security Functionalities of the TOE are:

- Security Audit
- Cryptographic Operation
- Identification & Authentication
- Secure Communication
- Security Management
- TSF Protection
- User Data Protection

The following section explains how the security functions are implemented.

7.1.1 Security Audit

➢ **Audit Generation**

It generates an audit record of events (*start-up and shutdown of the audit functions, insertion and removal of eID Card, insertion and removal SAM, Service requester authentication, Service attendee authentication, start and end of secure messaging, Card authentication, received data integrity failure, Role holder authentication, SAM authentication, SAM-PIN verification failure, TOE update, IVP verification, OCSP answer verification, SAS authentication, tampering of the Type II SSR*) and records with associated data (success or failure of the event, subject identity (if applicable), date and time provided from the Real Time Clock (RTC) on the Type II SSR, and reason of the failure (if applicable).

Reliable time stamp is provided from the OCSP server by the TOE and stored in RTC on Type II SSR.

It also generates auditable events, based on the auditable event definitions of the functional components listed in Annex A and if available, these events are recorded with the data caused the failure.

➢ **Audit Trail Security**

It protects the stored audit records from unauthorized deletion and detects unauthorized modifications to the stored audit records in the audit storage. If the audit storage is full, it overwrites the oldest stored audit records.

➢ **Audit Alarm**

When the tampering event is detected and identification and authentication of the SAM are disturbed, it generates audit records. It takes the action of entering out of service mode and deletes SAM PIN upon detection of the tampering event. For returning Operation Phases, all TOE software including operating system, file system and other firmware need to be re-install and it has to be initialized and configured by authorized personnel.

➢ **Audit Review**

All audits are view on TOE by only administrator. It is protected and in order to read audit logs, authorized person must enter a password on the interface.

MT BİLGİ TEKNOLOJİLERİ CONFIDENTIAL

7.1.2 Cryptographic Operation

It provides following cryptographic mechanism:

- Generation and destruction[109] 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] ia used for confidentiality with communication of the external entities.
- AEC-CMAC generation defined in RFC 4493[9] is used for integrity control[110].
- 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].

And also it provides RSA (2048 bit) signature verification using PKCS#1 v2.1 with PSS padding method according to ETSI TS 102 853[12] and TS 13584 [3] for verification of Identity Verification Certificate (*eID Card Certificate*), the OCSP Answer signature, the Signature of the Identity Verification Policy sent by the Identity Verification Policy Server (IVPS) and, the Secure Access Module (SAM) certificate and TOE Upgrade Package signature.

7.1.3 Identification & Authentication

It requires each user Role Holder, Secure Access Module, eID Card and SAS to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that user.

Card holder authentication (either Service Requester or the Service Attendee is the person who possesses the eID Card) 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 is used which is the combination of certificate verification, PIN authentication, photo verification and biometric verification as defined in TS 13585 [4].

SAM, eID Card and Role Holder Device authentication are done by certificate verification.

SAS mutual authentication are done by SSL/TLS client authentication certificate stored in the SAM

It re-authenticates the Card holder, SAM, Role Holder Device and SAS 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.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

[109] *It destroys all cryptographic keys (secure messaging keys, the Upgrade Package key and TLS keys) with same key destruction method. The Method is described in Application Note 13.*

[110] *Encryption and CMAC Key Generation Algorithm that meets the TS 13584 for Secure Messaging with eID, SAM and Role Holder.*

- SAM authentication, Role Holder Device authentication, SAS authentication sessions' keys are renewed after 24 hours are exceeded.

It provides only 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.
Unsuccessful biometric verification number is written into the eID Card by the TOE and updated each time the counter is changed.

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

7.1.4 Secure Communication

For the protection of the channel data from modification or disclosure, It provides trusted channel for communication with SSR Access Server via TLSv1.2 standards according to RFC 5246 and TS 13584 document [3], and also communicates Role Holder Device, eID Card and SSR SAM via secure messaging method as defined in TS 13584 document [3].
For immediately verification of the SSR by Identity Verification Server in online mode, it sends the digital signature of the Identity Verification Assertion Data is produced by SAM Card within Type II SSR.

7.1.5 Security Management

The TOE associates users with Initialization Agent, SSR Access Server for TOE, Identity Verification Policy Server, OCSP Server, Manufacturer service operator, Software Publisher roles. The TOE allows these roles to provide to control over the management of security functions behavior of the TOE (*TOE upgrade function and Identity Verification Method determination*) and management of TSF data (*SAM PIN and DTN initialization, time and date setting*).
It restricts the ability to manage for following security functions and TSF data:

- SAM PIN and DTN writing operation, is performed by only Initialization Agent.
- Time and date setting is performed by only OCSP Server.
- TOE upgrade operation, is performed by only Manufacturer service operator and Client Application for TOE.

TOE Upgrade Package is not installed, if it is not higher version of the TOE.

Identity Verification Method determination, is performed by only Identity Verification Policy Server or Client Application. When Identity Verification Method is not determined by IVPS or Client Application, it applies default Identity Verification Method defined during the TOE production.
It is also capable of performing the audit generation function.

7.1.6 TSF Protection

It verifies;

- the Secure Messaging Card Verifiable Certificates and Role Card Verifiable Certificates originates from Card Publisher using CVC Authentication Mechanism defined in TS 13584 [3],

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

- the Identity Verification Policy originates from Identity Verification Policy Server using IVP authentication mechanism defined in TS 13584 [3],
- the OCSP Response originates from legitimate OCSP Server using OCSP Response Verification Mechanism defined in TS 13584 [3],
- the 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 Certificate and Role Card Certificate of the SAM and request updated certificates from the SAS at each Identity Verification Operation,
- SAM Card Certificate revocation status from the OCSP Server immediately after opening of the Type II SSR,
- Identity Verification Certificate revocation status from the OCSP Server or Type II 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 also runs a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF. When the tampering event is detected and identification and authentication of the SAM are disturbed, it preserves secure state.

7.1.7 User Data Protection

IVA is exported with associated security attributes (SAM Signature for IVA) for non-repudiation, only if communication channel with corresponding SPCA and SAS is established as defined in TS 13584 document [3].
TOE Upgrade Package, IVM, OCSP response, SAM Secure Messaging CVC and SAM Role CVC are imported and written if signature verification is completed successfully.
The initial value for Identity Verification Method is defined in the TOE during manufacturing.
It ensures that any 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. These objects are copied to only volatile memory under electronic mesh cover and deleted in a secure way right after the end of the usage.

7.2 TOE Summary Specification Mapping

Mapping of portions of the TOE security functionality to the Security Functional Requirements of the TOE are provided the following table.

Table 13: *Mapping of SFRs and the TOE Security Functionality*

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

	Security Audit	Cryptographic Operation	Identification & Authentication	Secure Communication	Security Management	TSF Protection	User Data Protection
FAU_GEN.1	✓						
FAU_ARP.1	✓						
FAU_STG.1	✓						
FAU_STG.4	✓						
FAU_SAA.1	✓						
FAU_SAR.1	✓						
FCS_CKM.1/SM		✓					
FCS_CKM.1/SM_TLS		✓					
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		✓					
FIA_AFL.1			✓				
FIA_UID.2			✓				
FIA_UAU.2			✓				
FIA_UAU.5			✓				
FIA_UAU.6			✓				
FIA_UAU.7			✓				
FCO_NRO.2				✓			
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					✓		
FPT_STM.1	✓						
FPT_IDA.1/CVC						✓	

JILERI - CONFIDENTIAL

	Security Audit	Cryptographic Operation	Identification & Authentication	Secure Communication	Security Management	TSF Protection	User Data Protection
FPT_IDA.1/IVP						✓	
FPT_IDA.1/OCSP						✓	
FPT_IDA.1/TOE_Upgrade						✓	
FPT_IDA.1/X509						✓	
FPT_SSY.1/Cert State Synchronization						✓	
FPT_SSY.1/IVC						✓	
FPT_SSY.1/SAM						✓	
FPT_SSY.1/RH_Auth_Status						✓	
FPT_TST.1						✓	
FPT_FLS.1						✓	
FDP_ETC.2							✓
FDP_IFC.1							✓
FDP_IFF.1							✓
FDP_RIP.1							✓
FDP_ETC.1							✓
FTP_ITC.1				✓			

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

8 GLOSSARY AND ACRONYMS

8.1 Glossary

Service Provider Environment

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

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

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

Identity Verification Environment:

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

SR (Service Requester):
Service requester is the person who claims and proves his or her identity. The service requester claim starts with presenting eID Card to the SSR. The TOE, the SAM and the Service Attendee[111] together verify the claim interacting with the Service Requester and the eID Card[112].

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

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

Malicious Actors and Malicious External Systems:

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

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

The Proxy Entities:

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

111The Service Attendee's presence and role depends on the Configuration of the TOE and the selected identity verification method.

112 PIN Verification involves interaction of Service Requester with eIDC.

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

SSR Environment

SAM (Secure Access Module):

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

The SSR Platform:

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

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

8.2 Acronyms

APS: Application Server

CRL: Certificate Revocation List

CVC: Card Verifiable Certificate

DA: Device Authentication

DTN: Device Tracking Number

eID: Electronic Identity

eIDMS: Electronic Identity Management System

eID Card: Electronic Identity Card of National Republic

eIDVS: Electronic Identity Verification System

eSign: Electronic Signature

IV: Identity Verification

IVA: Identity Verification Assertion

IVC: Identity Verification Certificate

IVP: Identity Verification Policy

IVPS: Identity Verification Policy Server

IVR: Identity Verification Request

IVS: Identity Verification Server

IVSP: Identity Verification Specification

OCSPS: Online Certificate Status Protocol Server

SAM: Security Access Module

SAS: SSR Access Server

SPCA: Service Provider Client Application

SPSA: Service Provider Server Application

SSR: Card Acceptance Device

TA: Terminal Authentication

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

8.3 References

1. TS 13582 - T.C Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı – Bölüm- 1: Genel Bakış, (Secure Smart Card Reader Standard - Part-1: Overview) 2017, Türk Standartları Enstitüsü
2. TS 13583 - T.C Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı – Bölüm-2: Arayüzler ve Özellikleri, (Secure Smart Card Reader Standard - Part-2: Interfaces and their characteristics) 2017, Türk Standartları Enstitüsü
3. TS 13584 - T.C Kimlik Kartları İçin Güvenli Kart Erişim Cihazları Standardı - Bölüm-3: Güvenlik Özellikleri (Secure Smart Card Reader Standard - Part-3: Security Properties), 2017, Türk Standartları Enstitüsü.
4. TS 13585 - T.C 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), 2017, 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. TST 2015101199 T.C. Kimlik kartları için elektronik kimlik doğrulama sistemi - Bölüm 1: Genel Bakış ve T.C. kimlik kartı
14. TST 2015101200 T.C. Kimlik Kartları İçin Elektronik Kimlik Doğrulama Sistemi - Bölüm 2: Kimlik Doğrulama Sunucusu
15. TST 2015101201 T.C. Kimlik Kartları İçin Elektronik Kimlik Doğrulama Sistemi - Bölüm 3: Kimlik Doğrulama Politika Sunucusu
16. TST 2015101202 T.C. Kimlik Kartları İçin 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-2017-04-002

MT BİLGİ TEKNOLOJİLERİ - CONFIDENTIAL

19. Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 3.1 Revision 5 CCMB-2017-04-003
20. Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, CCMB-2017-04-004
21. RFC 5246, The Transport Layer Security Protocol, https://tools.ietf.org/html/rfc5246.txt, August 2008, Internet Society Network Working Group.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL

9 ANNEX

9.1 Annex A

SFR Events for Minimum Level:

FAU_ARP.1	Actions taken due to potential security violations.
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms.
FAU_SAR.1	Reading of information from the audit records.
FCS_CKM.1	Success and failure of the activity.
FCS_CKM.4	Success and failure of the activity.
FCS.COP.1	Success and failure, and the type of cryptographic operation.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided.
FIA_UAU.2	Unsuccessful use of the authentication mechanism.
FIA_UAU.5:	The final decision on authentication;
FIA_UAU.6	Failure of reauthentication
FCO_NRO.2	The invocation of the non-repudiation service.
FMT_SMF.1	Use of the management functions.
FMT_SMR.1	Modifications to the group of users that are part of a role
FPT_STM.1	Changes to the time
FPT_IDA.1	The final decision on authentication;
FPT_SSY.1	Result of synchronization: success or failure
FDP_IFF.1	Decisions to permit requested information flows.
FDP_ETC.2	Successful export of information.
FTP_ITC.1	Failure of the trusted channel functions.

MT BILGI TEKNOLOJILERI - CONFIDENTIAL