Token ID Station (TIS) Protection Profile

Version 1.0

20 August 2002

Prepared By: SPRE Inc.

Prepared For: National Security Agency

Forward

Purpose: This Protection Profile (PP) was developed to identify and set forth the security requirements for a Token ID Station (TIS) in high risk environments. It is based on Version 2.1 of the "Common Criteria" International Standard 15408 (see references **[CC1999a], [CC1999b]** and **[CC1999c]**). The Common Criteria can also be found at http://csrc.nist.gov/cc.

Authors: W. W. Everett (SPRE, Inc.)

Comments: Please send comments on this PP to W. W. Everett at wwe@SPRE-Inc.com.

Authority: None specified at this time

Acknowledgements: Many of the concepts adopted in defining the Token ID Station (TIS) were borrowed from the Tokeneer System (references **[Tokeneer1998a]**, **[Tokeneer1998b]** and **[Tokeneer1998c]**). The CC Toolbox™ Version 6.0f (reference **[CCToolbox2000]**) along with the CC Profiling Knowledge Base™ (reference **[CCPKB2000]**) were used in defining this protection profile. Portions of this Protection Profile were heavily borrowed from the Biometrics Protection Profile (see reference **[BiometricPP2002]**), the Token Protection Profile (see reference **[TokenPP2002]**) and part 2 of the Common Criteria (reference **[CC1999b]**).

We wish to thank Mr □□□ □□ □□□ □□□□and Mr. □□□□□□□□□□□of the NSA for their countless hours in reviewing early versions of the protection profile and for providing useful feedback.

Revision History:

Version Number	***Date***	***Reason for Revision***
0.1	14 Aug 2002	Initial Draft of PP – Outline, title page, forward, conventions/terminology, document organization, table of contents, introduction, toe description.
0.2	20 Aug 2002	Add section 5.1, 5.2
0.3	22 Aug 2002	Filled out glossary, edited 2.2, expanded 2.3
0.4	29 Aug 2002	Include comment changes from BRET Rev Mtg 4. Modify TIS description in section 2. Focus on filling out Assumptions, Policy, Threats in section 3.
0.5	11 Sep 2002	Incorporated changes received through 11 September. Baselined version sent out on 12 September for review.
0.6	13 Sep 2002	Changes since 12 Sep. Baselined version sent out for review on 19 Sep.
0.7	19 Sep 2002	Changes since 19 Sep
0.8	25 Sep 2002	Changes since 25 Sep. Incorporate changes from 25 Sep review meeting. Complete Audit/Mgt tables for functional req'ts. Add section 5.3 on SOF. Complete section 5.4. Added caveat regarding the violation of some assurance components of the CCRA.
0.9	2 Oct 2002	Changes since 2 October.
1.0	10 Oct 2002	Baselined version

Conventions and Terminology

Conventions: The notation, formatting, and conventions used in this PP are consistent with those used in the Common Criteria (CC), Version 2.1. The CC allows several operations to be performed on security requirements; ***refinement***, ***selection, assignmen***t, ***iteration,*** and ***security-target-writer*** are defined in Paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this PP. ***Iteration*** is denoted by showing the iteration number in parenthesis following the component identifier (iteration_number). The ***security-target-writer*** operation is indicated by the words “determined by the security target (ST) writer”.

In addition, “Application Notes” have been selectively added to this PP to provide a discussion of the relationship between security requirements. They are provided so that the PP user can see why a component or group of components were chosen and what effect it is expected to have as a group of related functions.

Terminology: This PP uses terms that are defined in Section 2.3 of Part 1 of the Common Criteria (CC), Version 2.1. Section 7 (Glossary) provides a synopsis of CC terms used in this document and terms specific to Token ID Station (TIS) system.

Document Organization

Section 1: provides the introductory material for the protection profile

Section 2: provides general purpose and TOE description

Section 3: provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4: defines the security objectives for both the TOE and the TOE environment.

Section 5: contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6: provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

Section 7: provides a glossary of CC and Token ID Station terms used in this PP along with their definitions.

Section 8: provides a list of references with background material.

Table of Contents

List of Figures

List of Tables

1. Introduction

This section contains document management and overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The PP identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The PP overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The overview can also be used as a stand-alone abstract for PP catalogues and registers. The conventions section provides an explanation of how this document is organized and the terms section gives a basic definition of terms which are specific to this PP.

1.1. Identification

Title:	Token ID Station (TIS) Protection Profile.
Version:	1.0
Date:	20 August 2002.
Prepared by:	SPRE, Inc.
Authors:	W. W. Everett, SPRE, Inc.
Registration:	None specified at this time
Keywords:	access control, discretionary access control, information protection, enclave protection.

1.2. Protection Profile Overview

The Common Criteria (CC) Token ID Station (TIS) Protection Profile specifies a set of security functional and assurance requirements for systems that (1) authenticate individuals for entry into an enclave, (2) control the entry to and egress from an enclave of authenticated individuals, (3) issue certificates authorizing authenticated individuals to use resources within the enclave. TIS-compliant products also provide an audit capability which records the security-relevant events which occur within the system.

The TIS provides for a level of protection which is appropriate for an assumed non-hostile and well-managed end user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. TIS-compliant products are suitable for use in both commercial and government environments.

The TIS is for a generalized environment with a high level of risk to the assets. The assurance requirements and the minimum strength of function were chosen to be consistent with that level of risk. The assurance level is EAL 5 and the minimum strength of function is SOF-high.

1.3. Related Protection Profiles

Related profiles include the Biometric protection profile (reference **[BiometricPP2002])** and the Token protection profile (reference **[TokenPP2002]**)

2. TOE Description

The following section provides a overview of the Token ID Station (TIS) Target of Evaluation (TOE). Section 2.1 provides a functional/operational overview of a TIS system. Section 2.2 summarizes the TIS TOE which focuses on the security-related functions of the TIS.

2.1. TIS Overview

In the following, terms that are specific to TIS are *italicized* when first introduced. The glossary in section 7 contains a list of TIS terms and their definitions. A TIS system is used to secure a set of resources located within an *enclave* from unauthorized usage (see figure 1). Individuals who wish to use resources within the enclave must first be *authenticated* at the TIS *entry station* of the enclave's *portal*[1] (e.g., a door or turnstile). Individual's to be authenticated must possess a valid token. A token can be a *smart card*, *PCMCIA card* or other small device that can be conveniently carried by an individual. Tokens are used to carry *certificates,* i.e., electronic documents containing specified information.

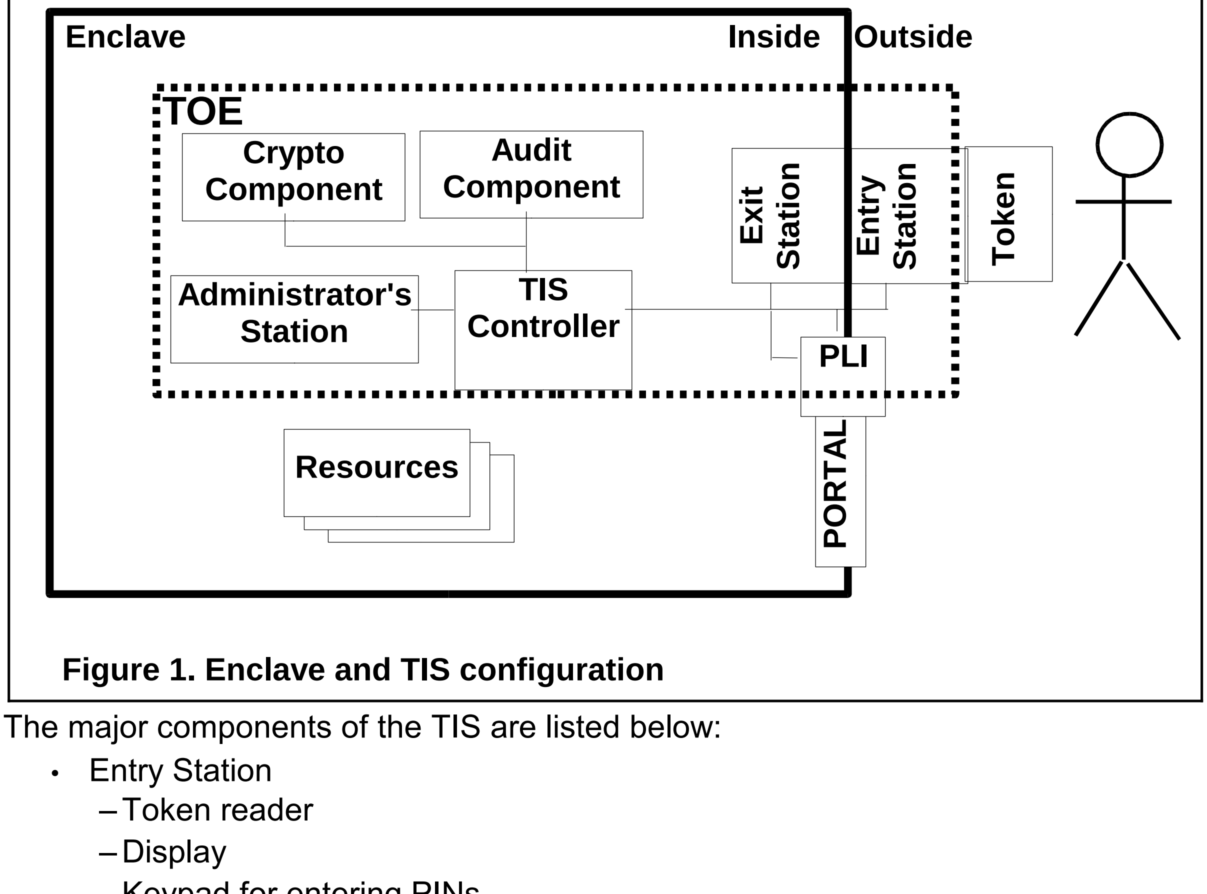

Figure 1. Enclave and TIS configuration

The major components of the TIS are listed below:

- Entry Station
  - Token reader
  - Display
  - Keypad for entering PINs
  - Biometric scanner

[1] Although only one portal is illustrated in figure1, a TIS system may manage several portals to an enclave.

  - Voice-box[2]
- Exit Station
  - Display
  - Token reader
- Portal Latch Interface
  - Can latch/unlatch the portal
  - Can sense if the portal is open or closed
- Administrator's Station
  - Keyboard
  - Display
  - Token reader
  - Voice-box
- Audit Component
  - Controls reading/writing audit records
- TIS controller
  - Biometric verifier (verifies a scanned biometric with a biometric template)
  - Removable storage media (for backups and long-term storage of audit files).
- Crypto component
  - Handles all encryption/decryption
  - Provides for entering/storing/destroying encryption keys

The *authentication* process uses an *authentication certificate* present on an individual's token. Once authenticated, an *authorization certificate* is placed on the individual's token. The authorization certificate allows an individual to access resources within the enclave when the individual presents his/her token to a resource. Once the individual is authenticated at the entry station, the *TIS controller*[3] will unlatch the portal via a *Portal Latch Interface (PLI)* to allow the individual to enter the enclave. The TIS controller can also monitor the state of the portal through the PLI to ensure the portal is not unlatched or open when it should not be.

When an individual leaves the enclave, he/she presents his/her token at the *exit station*. In emergencies, when the enclave must be evacuated rapidly, the organizational policy will allow individuals to leave the enclave without presenting their token carriers at the exit station. an individual can open the exit side of the portal even if it is latched. However, a TIS will raise an alarm when the portal is opened without a token being presented to the exit station.

Authentication of an individual by the TIS is founded on the notion of what an individual possesses (e.g., a token with a valid authentication certificate), what an individual knows (e.g., a *personal ID number (PIN)*) and what an individual is (e.g., a particular *biometric* associated with the Individual). The authentication process first

[2] Consists of a speaker, microphone and a buzzer button. An individual at the entry station can depress the buzzer button to gain the attention of the guard when he/she needs assistance. The individual and guard will be able to converse via the Voice Box.

[3] The portal controller may manage more than one portal of the enclave.

requires an individual to present his/her token at the entry station's token reader. A session is established between the token and the TIS. The TIS first checks that the token is not on the revocation list, it then retrieves the authentication certificate from the token. The TIS prompts the individual to enter a PIN via the entry station's keypad. The individual is also prompted to present his/her biometric to the entry station's biometric scanner. The entered PIN is validated with what is stored in the authentication certificate. The individual's scanned biometric is passed along with a biometric template retrieved from the authentication certificate to the TIS biometric verifier. The biometric verifier validates the scanned biometric with the biometric template. If both the scanned biometric and PIN are valid, TIS retrieves a role certificate[4] (if there is one) from the token. TIS then creates an authorization certificate with information on who the individual is, there PIN, roles they are allowed to assume while in the enclave and a validity time period for the individual using information retrieved from the authentication certificate and the role certificate. The authorization certificate is placed on the token, the session between the token and TIS is terminated and the portal is unlatched for a specified period of time to allow the individual to enter the enclave. If the individual is not authenticated the first time, the individual will be allowed a specified number of retries to authenticate. If the individual cannot authenticate after the specified number of retries, TIS terminates the session with the token, remembers the token ID so that token cannot be used again until a specified action is taken. If an individual encounters problems, he/she may contact the guard via the entry station's voice-box for assistance.

There is one variant to the authentication process. When an individual may not have a biometric, the individual will enter an over-ride access code on the keypad. TIS will validate the over-ride code and then prompt for the individual's PIN and proceed as in the previous paragraph.

TIS can import a token revocation list (a list of token IDs that are no longer valid) that is created by another system. This feature covers cases where tokens are lost and stolen and a mechanism is needed so they are not used by another individual.

There are a number of specific roles associated with managing the TIS. These roles are summarized in table . An individual who wants to use the TIS in the capacity of one of these roles must present his/her token to the TIS Administrator's Station token reader where the individual's authorization certificate will be checked to ensure he/she has on it the role he/she will assume. The TIS may prompt the individual for more information to authenticate him/her (e.g., his/her PIN).

[4] A role certificate contains a list of TIS roles that an individual can assume. Such a certificate is created by another entity.

Role		Responsibilities
1	System Security Officer	Is responsible and accountable for the security aspects of TIS. Configures the security attributes of TIS.
2	Guard	Is responsible for the day-to-day operation of TIS. Performs shutdowns and startups of TIS. Responds to TIS alarms.
3	Auditor	Is responsible for review audit records periodically or following a security breach.
4	System Administrator	Is responsible for the installation, upgrade and repair of TIS components. Configures the non-security attributes of TIS.

Table 1. Roles and Responsibilities in Managing TIS

There are other important aspects of the operation of a TIS. From the TIS's perspective,there are two operational periods during the day: in-hours and out-of-hours. During out-of-hours operation, access is limited to specified individuals. The TIS creates and stores *audit records* associated with specific events. Normal events (e.g., the authentication of an individual on entry to the enclave, a TIS function performed by the Guard, Security Officer, or Auditor) along with abnormal events (e.g., authentication of an individual fails after a specified number of retries, TIS detects the portal is open when it should not be, a failure of a TIS component) are audited. TIS may raise alarms for certain critical events. The alarms must be cleared by the Guard within a specified period of time. Audit records are created for alarm events and situations where the event is not cleared within a specified time by the guard. Included in each audit record in addition to a description of the event is an individual's name[5], an individual's role, severity level of the event and a date-time stamp. TIS provides means for an auditor to sort, search and filter audit records by date-time, user name, severity level, user's role and the ability to backup files of audit records to a removable media. Authentication revocation lists can be entered into TIS by the guard or system security officer. These lists are checked during the authentication process to determine if an authentication certificates has been revoked (i.e., are no longer valid).

2.2. TOE Overview

The Target of Evaluation (TOE) includes everything as outlined by the dashed box in figure 1. Security aspects of the biometric subsystem composed of the biometric scanner and biometric verifier are covered by the DoD Biometric System protection profile (reference **[BiometricPP2002**]). The token is outside the TOE and is assumed to conform to the DoD Token protection profile (reference **[Token2001**]). A TIS system will be used to secure Class 5 enclaves approved to process unclassified and some categories of classified information whether it is deemed mission critical, mission support, or administrative.

[5] When such can be determined.

Those responsible for managing the TIS are assumed to be trustworthy, competent and adequately trained in using the TIS and the organization's security policies although they may be prone to making mistakes. Likewise, individuals requesting entrance to the enclave are deemed to be trustworthy although they may also be prone to making mistakes. The enclave is physically secured. The periphery of the enclave is under surveillance so a protracted effort of tampering with the portal or entrance station is assumed not to be possible. Hence the TIS and and the communication links between TIS components can be assumed to be physically secure. There is no need for the TIS to communicate with other IT systems either within our outside the enclave. The only interface with another IT system is in reading revocation list files. TIS should authenticate the preparer of such files before they are read. Authorization certificates are encrypted by the TIS when they are placed on a token. The strength of function (SOF) of the encryption of certificates should be *high* as they could come under direct attack by an untrusted agent[6].

A TIS system should have an *integrity-checking* capability that would check that the TIS is operating in a secure state. A primary property of a secure state is that the portal is closed and latched when it should be. Such *integrity-checking* should be initiated automatically when the TIS is started up or when the TIS configuration is changed. The capability for initiating it manually should exist.

The TIS should have a backup/restore capability for storing key TIS operation parameters. The backup should be stored on removable media. As there is a possibility that the backup information may be stored in long-term off-premise storage, the backup information should be encrypted.

The TIS should be able to recover automatically from certain failures. The TIS should monitor its operation and the operation of its components and in particular, when the portal is unlatched. When it detects that part of the system is not operating or operating in an insecure manner, it should initiate a recovery back to a secure operational state.

The TIS will maintain an Audit File. Only someone in the auditor's role should have read access to the Audit File. No one should have write access to the Audit File. Someone in the guard's role should be able to backup an audit file and clear it in the event that Audit File space is depleted. If Audit File space is depleted and it is not backed-up and cleared, the Audit function should overwrite the oldest audit records first. Alarms should be raised for certain critical events. All alarmed events should be audited. An alarm can either be cleared automatically (after a specified period) or cleared by the guard[7] after a specified action is taken. Events that should be audited include:

- Alarm events
- TIS startup
- TIS shutdown
- Changes to the TIS configuration
- Access of TIS audit records
- TIS component failures
- Successful entries and exits through the portal

[6] E.g., someone who finds a lost token.

[7] Generally, an organization would require a guard to take a specified action and clear the alarm.

- Failure of a non-critical component.
- Unsuccessful entries and exits through the portal
- Depression of the voice-box's buzzer button at the entry station.

Alarm events include:

- Exits for which a token carrier was not presented
- TIS detects portal is unlatched when it should not be
- Failure of a TIS critical component.
- A specified number of unsuccessful entry attempts in a row.

As the TIS will be able to import token revocation lists, it must have the ability to authenticate the source of the list before using it.

3. TOE Security Environment

This section describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed. This description includes statements of assumptions, threats and organization policies (including detail policy statements levied on the TIS system).

3.1. Secure Usage Assumptions

This section includes descriptions of **assumptions on** the security aspects of the environment in which the TOE will be used or is intended to be used. This includes information about the intended usage of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use; and information about the environment of use of the TOE, including physical,personnel, and connectivity aspects. Assumptions are tagged with terms of the form **A.Xxxxxx.**

A.Admin_Docs: Administrators following documentation

TIS administrators follow the policies and procedures defined in TIS documentation for secure administration of TIS.

A.Biometrics: Biometrics subsystem security

The TIS biometrics subsystem (biometrics scanner and biometrics verifier) is certifiable under the DoD Biometric System Protection Profile for Medium Robustness Environments (reference [BiometricPP2002]).

The intent is not to have to replicate what is already covered in reference **[BiometricPP2002].**

A.Phys_Acc_to_Out: Physical access by Outsiders

A TIS is located within controlled access facilities that prevent unauthorized physical access by outsiders.

A.Token: Token security

Token security is certifiable under the DoD Public Key Infrastructure Token Protection Profile (reference [TokenPP2001]).

3.2. Threats to Security

This section includes all threats to the assets against which specific protection within a TIS or its environment is required. Only those threats which are relevant for secure TIS operation have been listed. A threat is described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threat agents are described by addressing aspects such as expertise, available resources, and motivation. Attacks are described by addressing aspects such as attack methods, any vulnerabilities exploited, and opportunity. Threats are tagged with terms of the form **T.Xxxxxx.** Corresponding detailed attacks are tagged with terms of the form **DA.Xxxxx.**

T.Admin_Err_Commit: Administrative errors of commission

An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

Administrators include those roles in table who are responsible for managing a TIS.

DA.Admin_Err_AC_Policy: Administrator error modifies access control.

An administrator's error in data entry changes the access control enforced by the system in such a way that it no longer serves its intended purpose.

DA.Admin_Err_Audit: Administrator error changes audit behavior

An administrator's error in data entry changes the audit behavior of the system in such a way that auditing no longer serves its intended purpose.

DA.Admin_Err_Authentic: Administrator error modifies authentication enforcement

An administrator's error in data entry changes the authentication-enforcement mechanism of the system in such a way that it no longer serves its intended purpose.

DA.Admin_Err_Crypto: Accidental mismanagement of cryptographic functions

An administrator misconfigures cryptographic functions or stores plaintext keys in insecure areas.

DA.Admin_Err_Info: Administrator error makes information unavailable

An administrator's error in data entry makes system or application information unavailable.

DA.Admin_Err_Resource: Administrator error makes resource unavailable

An administrator's error in data entry makes system or application resources unavailable.

DA.Admin_Err_Sys_Entry: Administrator error modifies entry policy

An administrator's error in data entry changes the intended entry policy of the system or application.

DA.Admin_Err_User_Attr: Administrator error modifies user security attributes

An administrator's error in data entry modifies a user's security attributes, which makes the attributes inappropriate under the security policy of the system or application.

T.Admin_Err_Omit: Administrative errors of omission

The system administrator fails to perform some function essential to security.

DA.Admin_Err_Crypto: Accidental mismanagement of cryptographic functions

An administrator misconfigures cryptographic functions or stores plaintext keys in insecure areas.

DA.Admin_Err_Omit_Trap: Back door left open

An administrator inadvertently leaves a back door port open after routine maintenance, allowing continuing unauthorized access by the service organization.

DA.Admin_Err_Update: Administrator fails to update security configuration

The organizational security policies changes but these changes are not reflected in all system configurations, resulting in circumvention and/or incorrect application of security policies.

DA.Adm_Misconfig_User: User privileges and/or authorizations are not updated upon reassignment

A change in the status of users duties do not get reflected in administratively controlled privileges and/or authorizations.

T.Biometric_Weak_Auth

A biometric device can only provide weak authentication of an individual.

DA.Biometric_Weak_Auth

An individual is able to circumvent biometric authentication because the False Acceptance Rate (FAR) of the biometric device cannot be set to a low enough level.

T.Component_Failure: A critical system component fails

Failure of one or more system components results in the loss of system-critical functionality.

DA.Hardware_Flaw: System hardware fails during system operation

System use uncovers a hardware flaw in a critical system component.

DA.Phys_CompFail_Res: Resource depletion failure

A system allocates so many resources that not enough are left for a critical component to function correctly.

DA.Software_Flaw: System use uncovers an intrinsic software flaw in a critical system component

An authorized user performs an operation or set of operations, exercising a software flaw in a security-critical component.

DA.TSF_Err_Conf_Crypto: Accidental release of cryptographic assets due to TSF flaw or malfunction

The TSF accidentally releases sensitive plaintext data, red keys, or other cryptographic assets to an inappropriate audience.

T.Dev_Flawed_Code: Software containing security-related flaws

A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

DA.Dev_FC_Attr_Interp: Inconsistent interpretation of audit data attributes

The security-critical (TSF) components inconsistently interpret audit data attributes exchanged with another trusted IT product.

DA.Dev_FC_Buff_Not_Clr: Buffers not cleared by the system

The system leaves user information in a system buffer for view by another unauthorized user.

DA.Dev_FC_Ctrl_Data: Incorrect modification of control data

A security-critical (TSF) component incorrectly modifies control data regarding a user process.

DA.Dev_FC_Data_Export: System data incorrectly exchanged

The system incorrectly exchanges system data with another trusted system.

DA.Dev_FC_Recovery: Non-secure recovery

A system failure may alter the behavior of the system's security functions in such a way that, upon recovery, it no longer properly enforces its security policy (TSP).

DA.Dev_FC_Replication: Inaccurate system-data replication

The system does not accurately replicate system data to different parts of the system where replication is required.

DA.Dev_FC_Self_Protect: System modification by unauthorized source

Software developer or hacker modifies system security functions resulting in a loss of security protection.

DA.Dev_FC_Trap_Door: Malicious developer creates secret trapdoor in system.

The system developer creates a secret back door in the system (TOE) that allows covert access by the developer. This allows the developer

to collect information, monitor user actions, modify the operation of the TOE, or just make unauthorized use of the TOE.

T.Power_Disrupt: Unexpected disruption of system or component power

A human or environmental agent disrupts power causing the system to lose information or security protection.

DA.Power_Disrupt_Reset: Unexpected power reset

An unintentional, malicious, or environmentally caused power reset occurs, resulting in the loss of critical information or the system to enter a non-secure state.

T.Repudiate_Transact: An individual denies performing a transaction

An individual in a transaction denies participation in the transaction to avoid accountability for the transaction or for resulting obligations.

This includes an individual requesting access to the enclave denying such a request or an administrator performing an administrator function and later denying it.

DA.Repudiate_Trans_Loc: Circumvent non-repudiation in a transaction involving a user and a local system

An authorized user participates in a transaction by responding to system/application prompts and then denies that the dialogue took place.

T.User_Err_Integrity: User errors cause integrity breaches

A user commits errors that induce erroneous actions by the system and/or erroneous statements its users.

DA.User_Err_MsngAttrXpt: Failure to provide object security attributes in data export

An authorized user deliberately or accidentally exports data so that the data is not accompanied by required handling information.

DA.User_Err_Object_Attr: Incorrectly set object attributes

An authorized user sets an object's security attributes inappropriately, misdirecting its use. The misdirection may allow unauthorized reading or modification, or it may prohibit authorized reading or modification.

3.3. Organizational Security Policies

This section identifies and explains any organizational security policy statements or rules with which the TOE must comply. Explanation and interpretations have been included with individual policy statements in a manner that permits them to be used to set clear security objectives. In particular, detail policy statements providing TIS security functional policies for TIS have been included. Organizational policy statements are tagged with terms of the form **P.Xxxxxx**. Detail policy statements levied against the TIS by the corresponding organizational policy statement are listed immediately following and are tagged with terms of the form **DP.Xxxxxx**. A detailed system policy statement may address more than one organization policy statement.

P.Accountability: Individual accountability

Individuals shall be held accountable for their actions.

DP.Audit_Gen_User: Individual accountability

A TIS shall provide individual accountability for auditable actions.

DP.Audit_Generation: Audit data generation with identity

A TIS shall provide the capability to ensure that all audit records include enough information to determine the date and time of action, the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

DP.Audit_Protect: Protected audit data storage

A TIS shall protect the contents of the audit trails against unauthorized access, modification, or deletion.

DP.I&A_User: User identification and authentication

A TIS shall provide Identification and authentication (I&A) procedures which uniquely identify and authenticate individuals requesting access to the enclave and to administrators.

P.Authorities: Notification of threats and vulnerabilities

A TIS shall immediately notify appropriate authorities of any threats or vulnerabilities impacting the TIS.

DP.Authority_Notify: Notification of threats and vulnerabilities

A TIS shall address the notification of threats and vulnerabilities to the appropriate authorities.

In most situations, the authority being notified would be the guard.

P.Authorized_Use: Authorized use of information

Information shall be used only for its authorized purpose(s).

DP.Sys_Access_Banners: System access banners

A TIS shall notify individuals prior to gaining access to the enclave that the individual's actions may be monitored and recorded, that gaining access to the enclave consents to such monitoring, and that unauthorized use may result in criminal or civil penalties.

P.Availability: Information availability

Information shall be available to satisfy mission requirements.

DP.Config_Mgt_Plan: Implement operational configuration management

A TIS shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

DP.Documented_Recovery: Documented recovery

A TIS shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.

DP.Malicious_Code: Malicious code prevention

A TIS shall provide procedures and mechanisms to prevent the introduction of malicious code into the TIS.

DP.Sys_Assur_HW/SW/FW: Validation of security function integrity

A TIS shall provide features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

DP.Sys_Backup_Procs: System backup procedures

A TIS shall provide the capability to restore the system to a secure state after discontinuities of system operations.

DP.Sys_Backup_Restore: Restoration with minimal loss

A TIS shall provide backup procedures to allow restoration of the system with minimal loss of service or data.

DP.Sys_Backup_Storage: Effective backup restoration

A TIS shall provide procedures to ensure both the existence of sufficient backup storage capability and effective restoration (incremental and complete) of the backup data.

DP.Sys_Backup_Verify: Backup protection and restoration

A TIS shall provide appropriate physical and technical protection of the backup and restoration hardware, firmware, and software.

DP.System_Recovery: Trusted system recovery

A TIS shall provide procedures and features to assure that system recovery is done in a trusted and secure manner.

DP.User_Data_Storage: Protection of stored user data

A TIS shall provide appropriate storage, continuous personnel access control storage, or encrypted storage of data based on the sensitivity of the data.

P.Guidance: Installation and usage guidance

Guidance shall be provided for the secure installation and use of the system.

DP.Privileged_Doc: Privileged user documentation

TIS documentation shall include guides or manuals for the system's privileged users (e.g., TIS administrators).

DP.User_Documentation: General user documentation

TIS documentation shall include a user's guide for the general user.

A general user is an individual seeking entry into the enclave. User documentation could be simply a one page instruction sheet place at the entry and exit stations.

P.Information_AC: Information access control

Information shall be accessed only by authorized individuals and processes.

DP.Admin_Security_Data: Changes to security data by authorized personnel

A TIS shall provide mechanisms to assure that changes to security related data are executed only by authorized personnel.

DP.Screen_Lock: Screen locking

A TIS shall provide a screen lock mechanism for TIS administrators.

P.Integrity: Information content integrity

Information shall retain its content integrity.

DP.Admin_Security_Data: Changes to security data by authorized personnel

A TIS shall provide mechanisms to assure that changes to security related data are executed only by authorized personnel.

DP.Change_Control_Users: Notification of data content changes

A TIS shall notify users of the time and date of the last modification of data.

Here, users refer to TIS administrators.

DP.Config_Mgt_Plan: Implement operational configuration management

A TIS shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

DP.Documented_Recovery: Documented recovery

A TIS shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.

DP.Integrity_Data/SW: Strong integrity mechanisms

A TIS shall implement strong integrity mechanisms (integrity locks, encryption).

DP.Integrity_Practice: Operational integrity system function testing

A TIS shall provide system functional tests to periodically test the integrity of the hardware and code running system functions.

DP.Malicious_Code: Malicious code prevention

A TIS shall provide procedures and mechanisms to prevent the introduction of malicious code into the system.

DP.Storage_Integrity: Assurance of effective storage integrity

A TIS shall provide assurance that storage integrity is effective.

DP.Sys_Assur_HW/SW/FW: Validation of security function integrity

A TIS shall provide features and procedures to validate the integrity and the expected operation of the security-relevant software, hardware, and firmware.

DP.System_Protection: Protection from security function modification

A TIS shall provide features or procedures for protection of the system from improper changes.

DP.System_Recovery: Trusted system recovery

A TIS shall provide procedures and features to assure that system recovery is done in a trusted and secure manner.

DP.User_Data_Storage: Protection of stored user data

A TIS shall provide appropriate storage, continuous personnel access control storage, or encrypted storage of data based on the sensitivity of the data.

DP.User_Data_Transfer: Protection of transmitted user data

A TIS shall provide a protected distribution system for data transmitted.

P.Lifecycle: System lifecycle phases integrate security

Information systems security shall be an integral part of all system lifecycle phases.

DP.Lifecycle_Security: Security throughout lifecycle

Security shall be addressed throughout a TIS system's lifecycle.

P.Marking: Information marking

Information shall be appropriately marked and labeled.

DP.Config_Mgt_Plan: Implement operational configuration management

A TIS shall implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

DP.External_Labels: Labeling data

A TIS shall provide security parameters associated with information exchanged between systems.

P.Physical_Control: Physical protection

Information shall be physically protected to prevent unauthorized disclosure, destruction, or modification.

DP.Tamper_ID: Physical tampering detection and notification

A TIS shall detect physical tampering and notify the appropriate authority.

4. Security Objectives

This section defines the security objectives for the TOE and its environment. The security objectives address all of the security environment aspects identified. The security objectives reflect the stated intent and are suitable to counter all identified threats and cover all identified organizational security policies and assumptions[8]. The following categories of objectives are identified: security objectives for the TOE, security objectives for the environment. Security objective statements are tagged with terms of the form **O.Xxxxxx**.

4.1. Security Objectives for the TOE

This section lists the security objectives for the TOE. In section 6.1, these objectives are traced back to aspects of identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE.

O.AC_Admin_Limit: Limitation of administrative access control

TIS developers shall design administrative functions in such a way that administrators do not automatically have access to user objects, except for necessary exceptions.

For an audit administrator, the necessary exceptions include observation of audited actions. In general, the exceptions tend to be role specific.

O.Admin_Guidance: Administrator guidance documentation

A TIS shall deter administrator errors by providing adequate administrator guidance.

O.Atomic_Functions: Complete security functions or recover to previous state

A TIS shall recover automatically to a consistent, secure state if a security function does not complete successfully in the presence of certain types of failures.

O.Aud_Sys_Entry_Parms: Audit changes of system entry parameters

A TIS shall deter an administrator from changing system entry parameters to allow an unauthorized user access to organizational assets to which they are forbidden.

O.Audit_Account: Auditing for user accountability

A TIS shall provide information about past user behavior to an authorized user through system mechanisms. Specifically, during any specified time interval, the system is able to report to a user acting in an identified audit role selected auditable actions that a user has performed, and as a result, what auditable objects were affected and what auditable information was received by that user.

[8] Where a threat or organizational security policy is to be covered partly by the TOE and partly by its environment, the related objective is repeated in each category.

O.Audit_Admin_Role: Audit-administration role duties

A TIS shall deter modification or destruction of audit data through the creation of an audit-administration role.

O.Audit_ARP: Security Alarms

The TIS shall raise an alarm on detecting a potential security violation.

O.Audit_Gen_User: Individual accountability

A TIS shall provide individual accountability for audited events. Uniquely identify each user so that auditable actions can be traced to a user.

O.Audit_Generation: Audit records with identity

A TIS shall record in audit records: date and time of action, location of the action, and the entity responsible for the action.

O.Audit_Loss_Respond: Respond to possible loss of stored audit records

A TIS shall respond to possible loss of audit records when audit trail storage is full or nearly full.

O.Audit_Protect: Protect stored audit records

A TIS shall protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

O.Biometrics: Biometrics subsystem security[9]

The TIS biometrics subsystem (biometrics scanner and biometrics verifier) shall be certifiable under the DoD Biometric System Protection Profile for Medium Robustness Environments (reference [BiometricPP2002]).

The intent is not to have to replicate what is already covered in reference **[BiometricPP2002].**

O.Change_Control_Users: User notification of data content changes

A TIS shall notify users of changes to data content in order to make any adjustments to their own data.

O.Code_Signing: Code signing and verification

A TIS shall check verification of signed downloaded code prior to execution. A well-known example is checking digital signatures on signed Java applets.

O.Config_Management: Implement operational configuration management

A TIS shall implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).

O.Correct_Operation: Verify correct operation as designed

[9] See footnote 8.

A TIS shall provide the ability for the authorized user to verify that the system operates as designed.

O.Crypto_Data_Sep: Separation of cryptographic data

A TIS shall provide complete separation between plaintext and encrypted data and between data and keys. This requires separate channels and separate storage areas. The only place any data can pass between the plaintext and encrypted data modules is in the cryptographic engine. There should be no way for plaintext keys to reach either data module and no way for data to enter the key handling module. Eencrypted keys can be handled as encrypted data, but with limited user access.

O.Crypto_Dsgn_Impl: Cryptographic Design and Implementation

A TIS shall minimize or even eliminate design and implementation errors in the cryptographic modules and functions.

O.Crypto_Import_Export: Cryptographic import, export, and inter-TSF transfer

A TIS shall protect cryptographic data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

O.Crypto_Key_Man: Cryptographic Key Management

Fully define cryptographic components, functions, and interfaces. Ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.

O.Crypto_Manage_Roles: Management of cryptographic roles

A TIS shall provide one or more roles to manage cryptographic assets and attributes.

O.Crypto_Modular_Dsgn: Cryptographic Modular Design

A TIS shall prevent errors in one part of the TOE from influencing other parts, especially cryptographic parts. To this end, noncryptographic I/O paths must be well defined and logically independent of circuitry and processes performing key generation, manual key entry, key zeroizing, and similar key-related operations.

O.Crypto_Operation: Cryptographic function definition

TIS cryptographic components, functions, and interfaces shall be fully defined.

O.Crypto_Self_Test: Cryptographic self test

A TIS shall provide the ability to verify that the cryptographic functions operate as designed.

O.Crypto_Test_Reqs: Test cryptographic functionality

A TIS shall test cryptographic operation and key management.

O.External_Labels: Label or mark information for external systems

A TIS shall label or mark information for external systems to prevent the exchange of inappropriate data between systems.

O.Fail_Secure: Preservation of secure state for failures in critical components

A TIS shall preserve the secure state of the system in the event of a secure component failure.

O.Fault_Tolerance: Provide fault tolerant operations for critical components

A TIS shall provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.

O.General_Integ_Checks: Periodically check integrity

A TIS shall provide periodic integrity checks on both system and user data.

O.I&A_Domain: Identify and authenticate a user to support accountability

A TIS shall provide the basic I&A functions that will support user accountability.

O.I&A_Transaction: Transaction identification and authentication

A TIS shall associate each transaction between a user and a system/application with a unique transaction ID, allowing events associated with a given transaction to be distinguished from other events involving the user and/or system/application.

O.I&A_User_Action: User-action identification and authentication

A TIS shall associate each user-requested action with the user who requested the action.

O.Identify_Unusual_Act: Identify unusual user activity

A TIS shall identify unusual user activity on the system.

O.Info_Flow_Control: System enforced information flow

A TIS shall enforce an information flow policy whereby users are constrained from allowing access to information they control, regardless of their intent (e.g., mandatory access control).

This lattice property of security attributes is commonly associated with the U.S. DoD implementations of Mandatory Access Control (MAC).

O.Integ_Sys_Data_Ext: Integrity of system data transferred externally

A TIS shall ensure the integrity of system data exchanged externally with another trusted product by using a protocol for data transfer that will permit error detection and correction.

This includes detecting and possibly correcting errors in data received and encoding outgoing data to make it possible for the receiver to detect and possibly correct errors. The method for detecting and correcting errors is based on some method (protocol) that is agreed upon by participating parties.

O.Integ_Sys_Data_Int: Integrity of system data transferred internally

A TIS shall ensure the integrity of system data transferred internally.

O.Integrity_Data/SW: Integrity protection for user data and software

A TIS shall provide integrity protection for user data and software.

O.Integrity_Data_Rep: Integrity of system data replication

A TIS shall ensure that when system data replication occurs across the system the data is consistent for each replication.

O.Integrity_Practice: Operational integrity system function testing

A TIS shall provide system functional tests to periodically test the integrity of the hardware and code running system functions.

O.Lifecycle_Security: Lifecycle security

TIS developers shall provide tools, techniques, and security employed during the development phase. TIS developers shall detect and resolve flaws during the operational phase. TIS developers shall provide safe destruction techniques.

O.Limit_Actions_Auth: Restrict actions before authentication

A TIS shall restrict the actions a user may perform before the TIS verifies the identity of the user.

O.Maintenance_Access: Controlled access by maintenance personnel

TIS administrators shall control access to the system by maintenance personnel who troubleshoot the system and perform system updates.

This refers to controlling the access of the the System Administrator role in table .

O.Maintenance_Recover: Expiration of maintenance privileges

A TIS shall terminate maintenance user system access privilege automatically after expiration of assigned timed interval.

O.Malicious_Code: Procedures for preventing malicious code

A TIS shall incorporate malicious code prevention procedures and mechanisms.

O.No_Repudiate_Transact: Counter an individual repudiating a transaction

A TIS shall be able to produce evidence when an individual denies performing a transaction that the transaction was executed by the user.

This includes an individual requesting access to the enclave denying such a request or an administrator performing an administrator function and later denying it.

O.No_Residual_Info: Eliminate residual information

A TIS shall ensure there is no "object reuse;" i.e., ensure that there is no residual information in some information containers or system resources upon their reallocation to different users.

O.Obj_Attr_Integrity: Basic object attribute integrity

A TIS shall maintain object security attributes with moderate to high accuracy (under the guidance of qualified users).

O.Priority_Of_Service: Provide priority of service

A TIS shall control access to resources so that lower-priority activities do not unduly interfere with or delay higher-priority activities.

O.Prvlg_IF_Status: Privileged-interface status

A TIS shall provide capability for an administrator to determine the use status of all privileged interfaces. This would include interfaces used by maintenance personnel.

O.Reference_Monitor: Provide reference monitor

A TIS shall always invoke mechanisms that enforce security policies (i.e., as for a traditional reference monitor).

O.Robust_Encryption: Robust encryption

A TIS shall produce cipher text that cannot be decrypted without either massive computational power or knowledge of the encryption key through robust encryption techniques.

O.Screen_Lock: Administrator screen locking

A TIS shall provide a screen lock function to prevent an unauthorized user from using an unattended computer where an administrator has an active session.

O.Secure_Configuration: Security-relevant configuration management

A TIS shall manage and update system security policy data and enforcement functions, and other security-relevant configuration data, in accordance with organizational security policies.

O.Secure_State: Protect and maintain secure system state

A TIS shall maintain and recover to a secure state without security compromise after system error or other interruption of system operation.

O.Security_Attr_Mgt: Manage security attributes

A TIS shall manage the initialization of, values for, and allowable operations on security attributes.

O.Security_Data_Mgt: Manage security-critical data

A TIS shall manage the initialization of, limits on, and allowable operations on security-critical data.

O.Security_Func_Mgt: Manage behavior of security functions

A TIS shall provide management mechanisms for security mechanisms.

O.Security_Roles: Security roles

A TIS shall maintain security-relevant roles and the association of users with those roles.

O.Source_Code_Exam: Examine the source code for developer flaws

Examinations shall be performed for accidental or deliberate flaws in code made by the developer. The accidental flaws could be lack of engineering detail or bad design. Where the deliberate flaws would include building trapdoors for later entry as an example.

O.Storage_Integrity: Storage integrity

A TIS shall provide integrity for data.

O.Sys_Access_Banners: System access banners

A TIS shall inform the user of the possibility of the system monitoring his actions, and that misuse of the system may result in criminal or civil penalties.

O.Sys_Assur_HW/SW/FW: Validation of security function

A TIS shall ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

O.Sys_Backup_Procs: System backup procedures

A TIS shall provide backup procedures to ensure that the system can be reconstructed.

O.Sys_Backup_Restore: Frequent backups to prevent minimal loss

A TIS shall provide through frequent backups, restoration of security-relevant changes to the system between backup and restore, and restoration of the security-relevant system state (e.g. access control list) without destruction of other system data.

O.Sys_Backup_Storage: Sufficient backup storage and effective restoration

A TIS shall provide sufficient backup storage and effective restoration to ensure that the system can be recreated.

O.Sys_Backup_Verify: Detect modifications of backup hardware, firmware, software

A TIS shall detect modifications to backup hardware, firmware, and software.

O.Sys_Self_Protection: Protection of system security function

A TIS shall protect the system security functions through technical features.

O.Tamper_ID: Tamper detection

A TIS shall provide system features that detect physical tampering of a system component, and use those features to limit security breaches.

O.Trusted_DS_Recov: Trusted distributed system recovery

A TIS shall ensure that a replaced failed component when re-integrated into the system will recover such that it will not cause errors or security breaches in other parts of the system.

O.Trusted_Recovery: Trusted recovery of security functionality

A TIS shall provide recovery to a secure state, without security compromise, after a discontinuity of operations.

O.Trusted_Recovery_Doc: Documentation of untrusted data recovery

A TIS shall provide trusted recovery to ensure that data cannot be lost or misplaced. Any circumstances which can cause untrusted recovery to be documented with mitigating procedures established.

O.User_Auth_Enhanced: Enhanced user authentication

A TIS shall execute enhanced measures to ensure that either user authentication data cannot be stolen or when it is stolen, it cannot be used to gain access to the system.

O.User_Auth_Management: User authorization management

A TIS shall manage and update user authorization and privilege data in accordance with organizational security and personnel policies.

O.User_Auth_Multiple: Require multiple authentication mechanisms

A TIS shall invoke multiple authentication mechanisms, which will provide confidence that the user is who they say they are.

TIS will use both PIN and biometric data to authenticate a user. Since the strength of function for biometric authentication specified in reference **[BiometricPP2002]** may not be of sufficient strength for this Protection Profile, the combination of both the PIN and biometric authentications should provide sufficient strenght.

O.User_Data_Integrity: Integrity protection of stored user data

A TIS shall provide appropriate integrity protection for stored user data.

O.User_Guidance: User guidance documentation

A TIS shall provide documentation for the general user.

4.2. Security Objectives for the Environment

This subsection states the security objectives for the environment. In section 6.1, these objectives are traced back to aspects of identified threats not completely countered by the TOE and/or organizational security policies or assumptions not completely met by the TOE. Some of these objectives are a re-statement, in whole or part, of the assumptions portion of the statement of the TOE security environment.

O.Biometrics: Biometrics subsystem security[10]

The TIS biometrics subsystem (biometrics scanner and biometrics verifier) shall be certifiable under the DoD Biometric System Protection Profile for Medium Robustness Environments (reference [BiometricPP2002]).

The intent is not to have to replicate what is already covered in reference **[BiometricPP2002].**

O.Phys_Acc_to_Out: Physical access by outsiders

A TIS shall be located within controlled access facilities that prevent unauthorized physical access by outsiders.

O.Token: Token security

Tokens used with a TIS shall have security that is certifiable under the DoD Public Key Infrastructure Token Protection Profile (reference [TokenPP2001]).

[10] See footnote 8.

5. IT Security Requirements

This section defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

5.1. TOE Security Functional Requirements

This section defines the functional security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. The section starts with a subsection specifying Security Function Policies referenced by other functional requirements. The remaining subsections provide functional requirements as functional components drawn from Part 2 of the Common Criteria **[CC1999b]** where applicable.

5.1.1. Security Function Policies

Several of the functional requirements reference Security Function Policies (SFPs). SFPs are are not organizational policies but rather named pieces of requirements.The short name for a SFP is preceded by a label of "SFP." Following each named SFP is an explanation that supplies additional information and interpretation. The SFPs used by the functional requirements in this PP are listed below:

SFP.DAC: Data Access Control Security Function Policy

Table 2 defines access privileges by role and information type. The Data Access Control Security Policy (SFP.DAC) is used in the access control, export, and import of data, and management of security attributes requirements. The administrator roles can only be assumed after successful authentication to the TOE.

	Information Type	***Role***	***Function***[11]
1	TIS security-sensitive configuration data[12]	Security Officer	View, initialize, modify
		Auditor	View
2	TIS non-security-sensitive configuration data	Security Officer	View, initialize, modify
		Guard	View, initialize, modify
		Auditor	View
		System Admin.	Initialize
3	Audit configuration data	Security Officer	View
		Auditor	View, initialize, modify
4	Audit Data	Auditor	View, backup, clear
5	Revocation Lists	Security Officer	View, import
		Guard	View, import, clear
		Auditor	View
6	Backup data	Security Officer	View, create, restore
		Guard	View, create, restore
		Auditor	View

Table 2. Access Control Table

5.1.2. Security audit (FAU)

5.1.2.1. Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall sound an audible alarm for a specified period of time upon detection of a potential security violation.

Application Notes: The list of potential security violations is determined by requirement FAU_SAA.1.1.

Management: The length of time that the alarm will sound should be settable by the Security Officer. An administrator should be able to reset the alarm from the Administrator's workstation.

Audit: TIS should audit when and why the alarm was raised. TIS should audit whether the alarm was reset after the time period expired or whether an Administrator reset it. If an Administrator reset the alarm, TIS should audit who reset the alarm.

5.1.2.2. Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

[11] Specifies what function (operation) can be performed on the information by the given role.

[12] E.g., cryptographic keys

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 detailed level of audit as defined in Table 3; and c) [assignment: other auditable events specific to the particular TIS system as defined by the ST writer].

Component	***Auditable Event***	***Additional Information***
FAU_ARP.1	• Alarm reset • Other actions taken due to imminent security violations.	• Indicate if alarm was reset after time-out or by an administrator
FAU_SAA.1 FAU_SAA.2 FAU_SAA.3 FAU_SAA.4	• Enabling and disabling of any of the analysis mechanisms • Automated responses performed by the tool (alarm raised).	•
FAU_SAR.1	• Reading of information from the audit records.	•
FAU_SAR.2	• Unsuccessful attempts to read information from the audit records.	•
FAU_SAR.3	• the parameters used for the viewing.	•
FAU_STG.4	• Actions taken due to the audit storage failure.	•
FCO_NRO.2	• The invocation of the non-repudiation service. Identification of the information, the destination, and a copy of the evidence provided. • The identity of the user who requested a verification of the evidence.	•
FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4	• Success and failure of the activity. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	•
FCS_COP.1	• Success and failure, and the type of cryptographic operation. • Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	•

Component	***Auditable Event***	***Additional Information***
FDP_ACF.1	• Successful requests to perform an operation on an object covered by the SFP. • All requests to perform an operation on an object covered by the SFP. • The specific security attributes used in making an access check.	•
FDP_ITC.1 FDP_ITC.2	• Successful import of user data, including any security attributes. • All attempts to import user data, including any security attributes. • The specification of security attributes for imported user data supplied by an authorized user.	•
FDP_SDI.1	• Successful attempts to check the integrity of user data, including an indication of the results of the check. • All attempts to check the integrity of user data, including an indication of the results of the check, if performed. • The type of integrity error that occurred.	•
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_UAU.2	• Unsuccessful use of the authentication mechanism All use of the authentication mechanism.	•
FIA_UAU.3	• Detection of fraudulent authentication data • All immediate measures taken and results of checks on the fraudulent data.	•

Component	**Auditable Event**	**Additional Information**
FIA_UID.1 FIA_UID.2	• Unsuccessful use of the user identification mechanism, including the user identity provided • All use of the user identification mechanism, including the user identity provided.	•
FMT_MOF.1	• All modifications in the behaviour of the functions in the TSF.	•
FMT_MSA.1	• All modifications of the values of security attributes.	•
FMT_MSA.2	• All offered and rejected values for a security attribute • All offered and accepted secure values for a security attribute.	•
FMT_MSA.3	• Modifications of the default setting of permissive or restrictive rules. All modifications of the initial values of security attributes.	•
FMT_MTD.1	• All modifications to the values of TSF data.	•
FMT_MTD.3	• All rejected values of TSF data.	•
FMT_REV.1	• Unsuccessful revocation of security attributes • All attempts to revoke security attributes.	•
FMT_SAE.1	• Specification of the expiration time for an attribute • Action taken due to attribute expiration.	•
FMT_SMR.2	• modifications to the group of users that are part of a role • unsuccessful attempts to use a role due to the given conditions on the roles • every use of the rights of a role.	•
FMT_SMR.3	• explicit request to assume a role.	•
FPT_AMT.1	• Execution of the tests of the underlying machine and the results of the tests.	•
FPT_FLS.1	• Failure of the TSF.	•

Component	***Auditable Event***	***Additional Information***
FPT_ITI.2	• the detection of modification of transmitted TSF data • the action taken upon detection of modification of transmitted TSF data. • the use of the correction mechanism.	•
FPT_ITT.3	• the detection of modification of TSF data; the action taken following detection of an integrity error.	•
FPT_PHP.3	• detection of intrusion.	•
FPT_RCV.1 FPT_RCV.2 FPT_RCV.3	• the fact that a failure or service discontinuity occurred • resumption of the regular operation; type of failure or service discontinuity.	•
FPT_RCV.4	• if possible, the impossibility to return to a secure state after failure of a security function • if possible, the detection of a failure of a security function.	•
FPT_RPL.1	• Detected replay attacks. • Action to be taken based on the specific actions.	•
FPT_STM.1	• changes to the time • providing a timestamp.	•
FPT_TRC.1	• restoring consistency upon reconnection. • Detected inconsistency between TSF data.	•
FPT_TST.1	• Execution of the TSF self tests and the results of the tests.	•
FRU_FLT.1	• Any failure detected by the TSF. • All TOE capabilities being discontinued due to a failure.	•
FRU_FLT.2	• Any failure detected by the TSF.	•
FTA_SSL.1 FTA_SSL.2	• Locking of an interactive session by the session locking mechanism. • Successful unlocking of an interactive session. • Any attempts at unlocking an interactive session.	•

Component	***Auditable Event***	***Additional Information***
FTA_SSL.3	• Termination of an interactive session by the session locking mechanism.	•
FTA_TSE.1	• Denial of a session establishment due to the session establishment mechanism. • All attempts at establishment of a user session. • Capture of the value of the selected access parameters (e.g. location of access, time of access).	•

Table 3. Auditable Events

Application Notes: A list of any additional auditable events shall be stated in the TOE Security Target by completing the assignment. An assignment of *none* is permissible, in which case paragraph c) should be omitted for the purposes of clarity.

For FMT_MTD.3, the interpretation of the audit requirement is that the audit record must indicate the reason for rejection of a biometric template. Note that successful enrollment is covered by the audit requirement for FMT_MTD.1.

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, 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 PP/ST, [assignment: other audit relevant information]

Application Notes: Any additional audit relevant information shall be stated in the TOE Security Target by completing the assignment. An assignment of *none* is permissible.

5.1.2.3. User identity association (FAU_GEN.2)

FAU_GEN.2.1

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Notes: *User* should be interpreted as either an individual entering or leaving the enclave, an administrator or the TIS system itself depending on the context of the event. In some cases, the TOE may not be able to identify the user associated with an event. For example, if an individual's authorization certificate cannot be interpreted, then the TOE can only record the event with an *unknown* identification. Therefore, this requirement should be interpreted as *when the user is known to the TOE*. The refinement operation has been applied by interpreting *user* as an individual entering or leaving the enclave, an administrator or the TIS system itself.

5.1.2.4. Security audit analysis (FAU_SAA.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 TSP.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events: a) Accumulation or combination of [assignment: *subset of defined auditable event*s] known to indicate a potential security violation; b) other rules that are known to indicate a potential security violation listed in table 4 or [assignment: *any other rule*s *listed by the ST writer*].

1. Portal is detected to be unlatched
2. Portal is detected to be open
3. TIS cannot determine that portal is latched or closed when it should be.

Table 4. Other rules indicating a security violation

5.1.2.5. Audit review (FAU_SAR.1)

FAU_SAR.1.1(1)

The TSF shall provide the auditor with the capability to read all audit information from the audit records.

FAU_SAR.1.1(2)

The TSF shall provide the [assignment: other administrators to be completed by the ST writer] with the capability to read [assignment: listed of audit record types by administrator role] from the audit records.

Application Notes: The ST writer may iterate this component leveling for each administrator role beyond the auditor who will be allowed to access audit records. When the list of audit record types is the same across two or more administrator role, the corresponding component levelings may be combined.

FAU_SAR.1.2

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.2.6. Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.2.7. Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1

The TSF shall provide the ability to perform searches, sorting, and filtering of audit data based as specified below:

1. **The TSF shall provide the ability to search records by the following criteria: (1) User ID, (2) date/time stamp, (3) whether the record is associated with an alarm event, (4) event type. The TSF shall allow for “and'ing” or “or'ing” multiple criteria.**
2. **The TSF shall provide the ability to sort by the following keys: (1) User ID, (2) date/time stamp, (3) whether the record is associated with an alarm event, (4) event type. The TSF shall allow for using multiple keys and specifying the order in which keys will be used in sorting.**
3. **The TSF shall provide the ability to filter records by the following criteria: (1) User ID, (2) date/time stamp range, (3) whether the record is associated with an alarm event, (4) event type. The TSF shall allow for “and'ing” and “or'ing” multiple criteria.**

5.1.2.8. Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to prevent modifications to the audit records.

FAU_STG.2.3

The TSF shall ensure that [assignment: metric for saving audit records specified by the ST writer] audit records will be maintained when the following conditions occur:audit storage exhaustion.

Application Notes: The metric could be a specified amount of space on a disk drive, a specified number of audit records or a specified period of time covered by audit records.

5.1.2.9. Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1

The TSF shall overwrite the oldest stored audit records and generate a security alarm if the audit trail is full.

5.1.3. Communications (FCO)

5.1.3.1. Enforced proof of origin (FCO_NRO.2)

FCO_NRO.2.1

The TSF shall enforce the generation of evidence of origin for transmitted authentication or authorization certificates at all times.

FCO_NRO.2.2

The TSF shall be able to relate the [assignment: *list of attribute*s] of the originator of the information, and the [assignment: *list of information field*s] of the information to which the evidence applies.

Application Notes: The TOE Security Target shall complete the assignments by stating the list of attributes of the originator and stating the list of information fields of a user's authentication certificate to which the evidence of origin applies.

FCO_NRO.2.3

The TSF shall provide a capability to verify the evidence of origin of information to recipient given [assignment: *limitations on the evidence of origi*n].

Application Notes: The TOE Security Target shall complete the assignment by stating any limitations on the evidence of origin.

5.1.4. Cryptographic support (FCS)

5.1.4.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: from list in table 5 and specified cryptographic key sizes [assignment: from table 6 that meet the following: FIPS 140-2 Level 3[13] and the X.509 Certificate Policy[14].

[13] See **[NIST2001]**

[14] See **[DoD2000]**

Signature Algorithms	• 1024 bit RSA • 2048 bit RSA • DSA 1024 (SHA-1) • Elliptic Curve Digital Signature Algorithm 384
Key Exchange Algorithms	• 1024 bit RSA • 2048 bit RSA • Diffie-Hellman 1024 • KEA 1024 • Elliptic Curve Key Exchange Algorithm 384
Symmetric Algorithms	• AES (128, 192 and 256 bit keys) • DES 64 • Triple DES 128 • Skipjack
Hash Algorithms	• SHA-1 • MD-5 • SHA 256 • SHA 384 • SHA 512
Any other NIST-approved cryptographic algorithms	

Table 5. Approved Cryptographic Algorithms

• At least 160 bit private key with at least 1024 bit prime modulus for Digital Signature Standard keys
• At least 1024 bit public key for key exchange algorithm (KEA)
• At least 2048 bit public key for RSA
• At least 384 bit for Elliptic Curve Digital Signature Algorithm key prime field (//p//)

Table 6. Approved Key Sizes

5.1.4.2. Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method encryption-with-key-exchange-keys-for-symmetric-keys that meets the following: FIPS 140-2 Level 3[15].

5.1.4.3. Cryptographic key access (FCS_CKM.3)

FCS_CKM.3.1

[15] See **[NIST2001]**

The TSF shall perform encryption of cryptographic keys in nonvolatile memory in accordance with a specified cryptographic key access method for cryptographic key storage that meets FIPS 140-2 Level 3[16].

5.1.4.4. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zerorization* that meets the following: FIPS 140-2 Level 3[16].

5.1.4.5. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1

The TSF shall perform signing of hash values and wrapping or unwrapping session keys in accordance with a specified cryptographic algorithm from table 5 and cryptographic key sizes from table 6 that meet the following: FIPS 140-2 Level 3[16] and the X.509 Certificate Policy[17].

5.1.5. User data protection (FDP)

5.1.5.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1

The TSF shall enforce the access control SFP SFP.DAC to objects as outlined in table 2.

5.1.5.2. Security attribute based access control (FDP_ACF.1)

FDP_ACF.1

The TSF shall enforce the access control SFP SFP.DAC to objects based on roles a per table 2.

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled objects is allowed: the role assigned is allowed to perform the operation as specified in table 2.

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects as specificed by ST writer*].

FDP_ACF.1.4

[16] See **[NIST2001]**

[17] See **[DoD2000]**

The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to object*s *as specified by ST writer*].

5.1.5.3. Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1

The TSF shall enforce the access control SFP SFP.DAC per table 2 when importing user data, controlled under the SFP, from outside of the TSC.

Application Notes: This refers to the revocation list.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rule*s *specified by ST writer*].

5.1.5.4. Full residual information protection (FDP_RIP.2)

FDP_RIP.2.1

The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource t*o, *deallocation of the resource fro*m] all objects.

Application Note: This SFR ensures residual biometric data (e.g., biometric samples stored temporarily in the capture device) or PIN data is not available after its use in the functional component. For example, clearing a biometric sample from the biometric scanner's memory after its operation.

5.1.5.5. Stored data integrity monitoring (FDP_SDI.1)

FDP_SDI.2.1

The TSF shall monitor user data stored within the TSC for integrity errors of revocation lists and lists of TIS administrator roles assigned to users.

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall generate an alarm.

5.1.6. Identification and authentication (FIA)

5.1.6.1. Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1(1)

The TSF shall detect when a specified number of unsuccessful authentication attempts occur related to authentication of an individual at the entry station.

FIA_AFL.1.2(1)

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall not allow the individual to attempt authentication until a specified amount of time has transpired.

Application Notes: The number of attempts allowed and the time period to disallow an individual to attempt to authenticate again are specified by the Security Officer when a TIS is configured.

FIA_AFL.1.1(2)

The TSF shall detect when a specified number of unsuccessful authentication attempts occur related to an administrator accessing the administrator's station.

FIA_AFL.1.2(2)

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall not allow the individual to attempt authentication until a specified amount of time has transpired.

Application Notes: The number of attempts allowed and the time period to disallow an administrator to attempt to authenticate again are specified by the Security Officer when a TIS is configured.

5.1.6.2. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to administrators: identifying name or number, roles and privileges allowed.

Application Notes: The identifying name or number must correspond to what is place in the authorization certificate on the token during authentication. The roles and privileges are TIS specific roles a privileges which may differ from the roles and privileges in the authorization certificate on the token.

5.1.6.3. User authentication before any action (FIA_UAU.2)

FIA_UAU.2.1

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

Application Notes: Typically, authentication is a function provided by a TOE whose main purpose is entirely different (e.g. an office automation network, a numerical analysis system, etc.). For a TIS system, however, authentication is the prime purpose of the TOE. There are no functions provided for the user other than authentication, or the single function of controlling access to a facility or information system, which does not form part of the TOE itself. This security functional requirement (SFR), therefore, expresses the prime objective of the TOE.

Although this SFR applies to authentication of regular users and administrators, the Security Target shall include FIA_UAU.5 as a TIS system support multi-factor authentication (e.g., biometric + PIN).

5.1.6.4. Unforgeable authentication (FIA_UAU.3)

FIA_UAU.3.1

The TSF shall detect and prevent use of authentication data that has been forged by any user of the TSF.

Application Notes: In this context, forgery generally refers to the use of an artifact such that the

biometric subsystem is spoofed into accepting the artifact as coming from a live human being. It is not possible to make definitive statements on the potential for forging of biometric characteristics. Most biometric characteristics could, in principle, be forged given sufficient resources and justification. The ease will depend on the nature of the biometric, the inherent characteristics of the capture device, and intentional countermeasures implemented in the TOE. For example,

in a fingerprint biometric subsystem, there may be some inherent rejection of an inanimate artifact due to the mode of operation of the finger reader (use of total internal reflection and the three dimensional property of a real finger pattern together with natural skin oil). The developer could also include measurements of temperature, surface conductivity and/or pulse to provide additional

countermeasures (i.e., liveness checks) to a fake or disembodied finger. All these would make it harder to produce a viable artifact but would not eliminate the possibility. The developer will need to provide information on inherent and intentional countermeasures to forgery.

The term biometric authentication data also includes the biometric template which is stored on a token. In such cases, the TOE is required to detect and prevent the forged use of a template by an imposter. This SFR does not explicitly require the ability to detect mimicry by an impostor. Such attacks are not considered as forgery of authentication data, rather the TOE meeting the FAR requirements in accordance with O.ADMIN counters these attacks.

FIA_UAU.3.2

The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

Application Notes: This security functional requirement may overlap in some instances with FIA_UAU.3.1 in the case of the biometric subsystem. The production of a forgery may also involve copying the biometric characteristics of an authorized user of a system (i.e. lifting a latent fingerprint from a glass). Most biometric characteristics are not secret and may therefore be vulnerable to being copied. There will be varying degrees of difficulty involved. For example, it may be hard to copy a retinal pattern. This form of copying requires the use of a forgery to exploit the copy. Replay attacks are not covered by this SFR. FPT_RPL.1 addresses this form of attack.

This SFR does not explicitly require the ability to detect mimicry of biometrics by an impostor. Such attacks are not considered as *copying* of authentication data, rather, these attacks are countered by the TOE meeting the FAR requirements identified with O.ADMIN.

5.1.6.5. Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1

The TSF shall provide only an indication that processing is underway to the user while the authentication is in progress.

Application Notes: This security functional requirement means, for example, that the biometric subsystem must not inform the user of any *score* against the threshold that might help the attacker to fool the device in subsequent verification or identification attempts. However, the TIS should provide feedback through an indication that is updated periodically (say every second) that processing is underway if there is a delay in completing authentication./m

5.1.6.6. User identification before any action (FIA_UID.2)

FIA_UID.2.1

The TSF shall require each user to identify him/herself before allowing any other TSF-mediated actions on behalf of that user.

Application Notes: This security functional requirement is one that needs special interpretation in the context of the biometric subsystem. For this consideration, biometric systems can be considered to divide into two broad categories, identification and authentication. Authentication is where a user makes a claim to be a specific individual and the system authenticates the claimant against the claim. This is analogous to the userid/password authentication in an IT system. Identification is where a user makes no specific claim of identity and the system has to determine who the individual is, or more generally, whether the individual is known to the system. Authentication systems are more common than identification systems but both types are used.

As the TOE is of the authentication type, then the security functional requirement has the same standard interpretation as for an IT password system. A specific claim of identity must be made before the TOE takes any further action. Most commonly, the next action after the user provides identification will be authentication. Note that this SFR applies to both users and administrators. Also, see application note under FIA_UAU.2 above.

5.1.7. Security management (FMT)

5.1.7.1. Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1

The TSF shall restrict the ability to determine the behavior (DE), disable (DI), enable (EN) or modify the behavior (MO) of functions by administrators as listed in table 7.

Component	***Function***	***Guard***	***Security Officer***	***Auditor***	***System Admin.***
FAU_ARP.1	• the management (addition, removal, or modification) of actions.	DE[18]	All[19]	DE	–
FAU_SAA.1	• maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.	DE	All	DE	–
FAU_SAR.1	• maintenance (deletion, modification, addition) of the group of users with read access right to the audit records.	–	DE	All	–
FAU_STG.2	• maintenance of the parameters that control the audit storage capability.	–	DE	All	–
FAU_STG.4	• maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	–	DE	All	–
FCO_NRO.1 FCO_NRO.2	• The management of changes to information types, fields, originator attributes and recipients of evidence.	DE	All	DE	–
FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4	• the management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).	–	All	DE	–
FDP_ACF.1	• Managing the attributes used to make explicit access or denial based decisions.	DE	All	DE	–
FDP_ITC.1 FDP_ITC.2	• The modification of the additional control rules used for import.	DE	All	DE	–
FDP_RIP.1 FDP_RIP.2	• The choice of when to perform residual information protection (i.e. upon allocation or deallocation) could be made configurable within the TOE.	–	All	DE	–
FDP_SDI.2	• The actions to be taken upon the detection of an integrity error could be configurable.	DE	All	DE	–

[18] DE = Determine the behavior of functions

[19] All = Determine the behavior (DE), disable (DI), enable (EN) or modify the behavior (MO) of functions

Component	***Function***	***Guard***	***Security Officer***	***Auditor***	***System Admin.***
FIA_AFL.1	• management of the threshold for unsuccessful authentication attempts • management of actions to be taken in the event of an authentication failure.	DE	All	DE	–
FIA_ATD.1	• if so indicated in the assignment, the authorized administrator might be able to define additional security attributes for users.	DE	All	DE	–
FIA_UAU.2	• management of the authentication data by an administrator • management of the authentication data by the user associated with this data.	DE	All	DE	–
FIA_UID.2	• the management of the user identities.	DE	All	DE	–
FMT_MOF.1	• managing the group of roles that can interact with the functions in the TSF;	DE	All	DE	–
FMT_MSA.1	• managing the group of roles that can interact with the security attributes.	DE	All	DE	–
FMT_MSA.3	• managing the group of roles that can specify initial values • managing the permissive or restrictive setting of default values for a given access control SFP.	DE	All	DE	–
FMT_MTD.1	• managing the group of roles that can interact with the TSF data.	DE	All	DE	–
FMT_REV.1	• managing the group of roles that can invoke revocation of security attributes • managing the lists of users, subjects, objects and other resources for which revocation is possible • managing the revocation rules.	DE	All	DE	–
FMT_SAE.1	• managing the list of security attributes for which expiration is to be supported • the actions to be taken if the expiration time has passed.	DE	All	DE	–
FMT_SMR.2	• managing the group of users that are part of a role • managing the conditions that the roles must satisfy.	DE	All	DE	–

Component	***Function***	***Guard***	***Security Officer***	***Auditor***	***System Admin.***
FPT_AMT.1	• management of the conditions under which abstract machine test occurs, such as during initial start-up, regular interval, or under specified conditions • management of the time interval if appropriate.	DE	All	DE	–
FPT_ITA.1	• management of the list of types of TSF data that must be available to a remote trusted IT product.	DE	All	DE	–
FPT_ITT.2	• management of the types of modification against which the TSF should protect • management of the mechanism used to provide the protection of the data in transit between different parts of the TSF • management of the separation mechanism.	DE	All	DE	–
FPT_ITT.3	• management of the types of modification against which the TSF should protect • management of the mechanism used to provide the protection of the data in transit between different parts of the TSF • management of the types of modification of TSF data the TSF should try to detect • management of the actions that will be taken.	DE	All	DE	–
FPT_PHP.3	• management of the automatic responses to physical tampering.	DE	All	DE	–
FPT_RCV.2 FPT_RCV.3	• management of who can access the restore capability within the maintenance mode • management of the list of failures/service discontinuities that will be handled through the automatic procedures.	DE	All	DE	–
FPT_RPL.1	• management of the list of identified entities for which replay shall be detecte • management of the list of actions that need to be taken in case of replay.	DE	All	DE	–

Component	***Function***	***Guard***	***Security Officer***	***Auditor***	***System Admin.***
FPT_STM.1	• management of the time.	DE	All	DE	–
FPT_TST.1	• management of the conditions under which TSF self testing occurs, such as during initial start-up, regular interval, or under specified conditions • management of the time interval if appropriate.	All	All	DE	–
FTA_SSL.1	• specification of the time of user inactivity after which lock-out occurs for an individual user • specification of the default time of user inactivity after which lock-out occurs • management of the events that should occur prior to unlocking the session.	All	All	DE	–
FTA_SSL.2	• management of the events that should occur prior to unlocking the session.	DE	All	DE	–
FTA_TAB.1	• maintenance of the banner by the authorized administrator.	All	All	DE	–
FTA_TSE.1	• management of the session establishment conditions by the authorized administrator.	DE	All	DE	–

Table 7. Functions allowed by administrators

5.1.7.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1

The TSF shall enforce the *access control SFP SFP.DAC* to restrict the ability to change_default, query, modify, delete the security attributes “roles” to the Security Officer.

5.1.7.3. Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.

5.1.7.4. Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the security function policy SFP.DAC to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the Security Officer to specify alternative initial values to override the default values when an object or information is created.

5.1.7.5. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1

The TSF shall restrict the ability to change_default (CD), query (QU), modify (MO), delete (DE) or clear (CL) the TIS configuration data, TIS security-related configuration data or Audit Files to administrators as listed in table 8.

Data	*Guard*	*Security Officer*	*Auditor*	*System Admin.*
Security sensitive configuration data[20]	-	All	QU	-
Operational, non-security sensitive data	All	CD, QU	QU	MO
Audit configuration data	-	QU	All	-

Table 8. Data Access allowed by administrators.

5.1.7.6. Secure TSF data (FMT_MTD.3)

FMT_MTD.3.1

The TSF shall ensure that only secure values are accepted for TSF data.

5.1.7.7. Revocation (FMT_REV.1)

FMT_REV.1.1

The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to the Security Officer or Guard.

FMT_REV.1.2

The TSF shall enforce the rules (1) deny access to those whose tokens appear on the revocation list.

5.1.7.8. Time-limited authorization (FMT_SAE.1)

FMT_SAE.1.1

The TSF shall restrict the capability to specify an expiration time for authorization certificates to the Security Officer.

FMT_SAE.1.2

The TSF shall be able to remove the authorization certificate after the expiration time for the authorization certificate has passed.

[20] E.g., cryptographic keys

5.1.7.9. Restrictions on Security roles (FMT_SMR.2)

FMT_SMR.2.1

The TSF shall maintain the roles Security Officer, Guard, Auditor and System Administrator.

FMT_SMR.2.2

The TSF shall be able to associate individuals authenticated at the entry station with these roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions [assignment: System Administrator can only access a TIS system when it is in a maintenance state and other conditions specified by the ST writer] are satisfied.

Application Notes: While in a maintenance state, the System Administrator shall not be able to access or change any of the TIS security-related attributes. As system administrators generally have unlimited access to system resources and may not have requisite clearances, TIS security attribute data should be physically removed before a System Administrator be allowed to work on a TIS system.

5.1.7.10.Assuming roles (FMT_SMR.3)

FMT_SMR.3.1

The TSF shall require an explicit request to assume the following roles: Security Officer, Guard and Auditor.

Application Notes: The request comes in the form of an administrator inserting their token in the Administrator's station token reader and authenticating by entering their PIN.

5.1.8. Protection of the TOE Security Functions (FPT)

5.1.8.1. Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1

The TSF shall run a suite of tests during initial start-up, periodically during normal operation and at the request of an authorized user to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.8.2. Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: power failure, TIS component failure.

5.1.8.3. TSF data transfer separation (FPT_ITT.2)

FPT_ITT.2.1

The TSF shall protect TSF data from disclosure and modification when it is transmitted between or stored in separate parts of the TOE.

Application Notes: The refinement operation has been performed to clarify that TSF data shall always be protected even when stored. In a TIS system, data flow security includes issues of confidentiality, integrity, and availability. A breach of data flow security could lead to unauthorized individuals being authenticated or authorized users failing to be authenticated. This security functional requirement deals with the confidentiality issues of data flow.

One major transmission of data in a TIS system takes place between the biometric scanner and the biometric verifier. A physically open channel in the form of a cable or possibly a remote network connection may separate these components. The possibility of monitoring the data flow between

the capture device and the recognition component must be considered as a potential area of vulnerability and the evaluators will be concerned to assess the means by which the TOE protects the data. Protective measures might include physical protection of the data path, detection of attempted monitoring, and data encryption.

A second major data flow comprises the communications of the result of the authentication process to the component which actions the result. An attack mounted on this path could bypass the authentication process altogether. The TOE Security Target will specify the scope of the TOE and will determine whether and how much of this path is included in the TOE.

Other internal data flows will likely exist and should be considered; e.g. that between the keypad and the component verifying an entered PIN.

FPT_ITT.2.2

The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.

5.1.8.4. TSF data integrity monitoring (FPT_ITT.3)

FPT_ITT.3.1

The TSF shall be able to detect the modification, substitution, re-ordering, or deletion of data for TSF data transmitted from the entry station token reader device.

FPT_ITT.3.2

Upon detection of a data integrity error, the TSF shall take the following actions: generate an alarm.

5.1.8.5. Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1

The TSF shall resist [assignment: *physical tampering scenario*s] to the TIS entry station devices by responding automatically such that the TSP is not violated.

Application Notes: The response should be generating an alarm.

5.1.8.6. Automated recovery (FPT_RCV.2)

FPT_RCV.2.1

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2

For power and TIS component failures, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

5.1.8.7. Function recovery (FPT_RCV.4)

FPT_RCV.4.1

The TSF shall ensure that power and TIS component failures have the property that the SF either completes successfully, or for the indicated failure scenarios, recovers to a consistent and secure state.

5.1.8.8. Replay detection (FPT_RPL.1)

FPT_RPL.1.1

The TSF shall detect replay for the following entities: [assignment: *list of identified entitie*s].

Application Notes: Part of detecting a replay attack on the biometric subsystem is to detect when an *exact match* comparison against a biometric template occurs.

FPT_RPL.1.2

The TSF shall generate an alarm when replay is detected.

5.1.8.9. Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Application Notes: The portal (whether physical or logical), once activated upon successful authentication, must not remain activated illicitly permitting unauthorized individuals access.

5.1.8.10.TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2

The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.8.11.Reliable time stamps (FPT_STM.1)

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps for its own use.

5.1.8.12.Internal TSF consistency (FPT_TRC.1)

FPT_TRC.1.1

The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

Application Notes: This would apply when TIS audit files and configuration files are backed up to removable media.

5.1.8.13.TSF testing (FPT_TST.1)

FPT_TST.1.1

The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, or at the request of an administrator to demonstrate the correct operation of the TSF.

FPT_TST.1.2

The TSF shall provide administrators with the capability to verify the integrity of TSF data.

FPT_TST.1.3

The TSF shall provide the Security Officer with the capability to verify the integrity of stored TSF executable code.

5.1.9. Resource utilization (FRU)

5.1.9.1. Limited fault tolerance (FRU_FLT.2)

FRU_FLT.2.1

The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: TIS component failures.

5.1.10.TOE access (FTA)

5.1.10.1.TSF-initiated session locking (FTA_SSL.1)

FTA_SSL.1.1

The TSF shall lock an interactive session after [assignment: a specified interval of time of administrator inactivity that is settable by the Security Officer] by: a) clearing or overwriting display devices, making the current

contents unreadable; b) disabling any activity of the administrator's data access/display devices other than unlocking the session.

FTA_SSL.1.2

The TSF shall require the following events to occur prior to unlocking the session: the administrator reinserts his/her token in the administrator's station token reader and reauthenticates using his/her PIN.

5.1.10.2.User-initiated locking (FTA_SSL.2)

FTA_SSL.2.1

The TSF shall allow administrator-initiated locking of the administrator's own interactive session, by: a) clearing or overwriting display devices, making the current contents unreadable; b) disabling any activity of the user's data access/display devices other than unlocking the session.

Application Notes: An administrator shall be able to initiate session locking by simply removing his/her token from the administrator's station token reader.

FTA_SSL.2.2

The TSF shall require the following events to occur prior to unlocking the session: the administrator reinserts his/her token in the administrator's station token reader and reauthenticates using his/her PIN.

5.1.10.3.Default TOE access banners (FTA_TAB.1)

FTA_TAB.1.1(1)

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application Notes: A user session would be an individual authenticating at an entry station. If the entry station display device is too small to display the warning message, then a paper copy of the warning could be posted at the entry station (there should be instructions in the administrator's guide to post such a warning). A TIS shall allow the Security Officer to compose the warning message.

FTA_TAB.1.1(2)

Before establishing an administrator session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Application Notes: Before establishing an administrator session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE. A TIS shall allow the Security Officer to compose the warning message.

5.1.10.4.TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1

The TSF shall be able to deny session establishment based on a user's token being on the TIS revocation list.

Application Notes: This includes a user attempting to initiate an authentication session at the entry station or an administrator attempting to initiate a session at the administrator's station.

5.2. TOE Security Assurance Requirements

This section states the assurance requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. The assurance requirements are stated for EAL level 5 as assurance components drawn from Part 3 of the Common Criteria **[CC1999c]** and are summarized in table 9. Not all signers of the CCRA (Common Criteria Recognition Agreement, formerly known as the Mutual Recognition Agreement or MRA) have agreed to all the components that should be included in EAL 5, 6 or 7. In particular, those assurance components followed by (*) in table 9 have not been accepted.in the CCRA. What this means is that this EAL 5 Protection Profile is valid but may not be accepted by some of the CCRA signers.

Assurance Class	***Assurance Components***
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.3*
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.3* ADV_HLD.3* ADV_IMP.2* ADV_INT.1* ADV_LLD.1 ADV_RCR.2* ADV_SPM.3*
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_FLR.1 ALC_LCD.2* ALC_TAT.2*
ATE	ATE_COV.2 ATE_DPT.2* ATE_FUN.1 ATE_IND.2
AVA	AVA_CCA.1* AVA_MSU.2 AVA_SOF.1 AVA_VLA.3*

Table 9. Assurance Requirements: EAL(5)

5.2.1. Configuration management (ACM)

5.2.1.1. Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1C

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.

ACM_AUT.1.1D

The developer shall use a CM system.

ACM_AUT.1.2C

The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.2D

The developer shall provide a CM plan.

ACM_AUT.1.3C

The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C

The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2. Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1C

The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.1D

The developer shall provide a reference for the TOE.

ACM_CAP.4.2C

The TOE shall be labeled with its reference.

ACM_CAP.4.2D

The developer shall use a CM system.

ACM_CAP.4.3C

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

ACM_CAP.4.3D

The developer shall provide CM documentation.

ACM_CAP.4.4C

The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C

The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C

The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C

The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C

The CM system shall provide measures such that only authorized changes are made to the configuration items.

ACM_CAP.4.11C

The CM system shall support the generation of the TOE.

ACM_CAP.4.12C

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3. Development tools CM coverage (ACM_SCP.3)

ACM_SCP.3.1C

The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, security flaws, and development tools and related information.

ACM_SCP.3.1D

The developer shall provide CM documentation.

ACM_SCP.3.2C

The CM documentation shall describe how configuration items are tracked by the CM system.

5.2.2. Delivery and operation (ADO)

5.2.2.1. Detection of modification (ADO_DEL.2)

ADO_DEL.2.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2C

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.2D

The developer shall use the delivery procedures.

ADO_DEL.2.3C

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2. Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1C

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.2.3. Development (ADV)

5.2.3.1. Semiformal functional specification (ADV_FSP.3)

ADV_FSP.3.1C

The functional specification shall describe the TSF and its external interfaces using a semiformal style, supported by informal, explanatory text where appropriate.

ADV_FSP.3.1D

The developer shall provide a functional specification.

ADV_FSP.3.2C

The functional specification shall be internally consistent.

ADV_FSP.3.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.3.4C

The functional specification shall completely represent the TSF.

ADV_FSP.3.5C

The functional specification shall include rationale that the TSF is completely represented.

5.2.3.2. Semiformal high-level design (ADV_HLD.3)

ADV_HLD.3.1C

The presentation of the high-level design shall be semiformal.

ADV_HLD.3.1D

The developer shall provide the high-level design of the TSF.

ADV_HLD.3.2C

The high-level design shall be internally consistent.

ADV_HLD.3.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.3.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.3.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.3.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.3.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.3.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing complete details of all effects, exceptions and error messages.

ADV_HLD.3.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3. Implementation of the TSF (ADV_IMP.2)

ADV_IMP.2.1C

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.1D

The developer shall provide the implementation representation for the entire TSF.

ADV_IMP.2.2C

The implementation representation shall be internally consistent.

ADV_IMP.2.3C

The implementation representation shall describe the relationships between all portions of the implementation.

5.2.3.4. Modularity (ADV_INT.1)

ADV_INT.1.1C

The architectural description shall identify the modules of the TSF.

ADV_INT.1.1D

The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interactions between the modules of the design.

ADV_INT.1.2C

The architectural description shall describe the purpose, interface, parameters, and effects of each module of the TSF.

ADV_INT.1.2D

The developer shall provide an architectural description.

ADV_INT.1.3C

The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

5.2.3.5. Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.10C

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

ADV_LLD.1.1C

The presentation of the low-level design shall be informal.

ADV_LLD.1.1D

The developer shall provide the low-level design of the TSF.

ADV_LLD.1.2C

The low-level design shall be internally consistent.

ADV_LLD.1.3C

The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C

The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C

The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C

The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.2.3.6. Semiformal correspondence demonstration (ADV_RCR.2)

ADV_RCR.2.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.2.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.2.2C

For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.

5.2.3.7. Formal TOE security policy model (ADV_SPM.3)

ADV_SPM.3.1C

The TSP model shall be formal.

ADV_SPM.3.1D

The developer shall provide a TSP model.

ADV_SPM.3.2C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.3.2D

The developer shall demonstrate or prove, as appropriate, correspondence between the functional specification and the TSP model.

ADV_SPM.3.3C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.3.4C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.3.5C

Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.

ADV_SPM.3.6C

Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.

5.2.4. Guidance documents (AGD)

5.2.4.1. Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2. User guidance (AGD_USR.1)

AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.1D

The developer shall provide user guidance.

AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5. Life cycle support (ALC)

5.2.5.1. Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1C

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.1D

The developer shall produce development security documentation.

ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2. Basic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.1D

The developer shall document the flaw remediation procedures.

ALC_FLR.1.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

5.2.5.3. Standardized life-cycle model (ALC_LCD.2)

ALC_LCD.2.1C

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.2.1D

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.2.2C

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.2.2D

The developer shall provide life-cycle definition documentation.

ALC_LCD.2.3C

The life-cycle definition documentation shall explain why the model was chosen.

ALC_LCD.2.3D

The developer shall use a standardized life-cycle model to develop and maintain the TOE.

ALC_LCD.2.4C

The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.

ALC_LCD.2.5C

The life-cycle definition documentation shall demonstrate compliance with the standardized life-cycle model.

5.2.5.4. Compliance with implementation standards (ALC_TAT.2)

ALC_TAT.2.1C

All development tools used for implementation shall be well-defined.

ALC_TAT.2.1D

The developer shall identify the development tools being used for the TOE.

ALC_TAT.2.2C

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.2.2D

The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.2.3C

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

ALC_TAT.2.3D

The developer shall describe the implementation standards to be applied.

5.2.6. Tests (ATE)

5.2.6.1. Analysis of coverage (ATE_COV.2)

ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2. Testing: low-level design (ATE_DPT.2)

ATE_DPT.2.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.

ATE_DPT.2.1D

The developer shall provide the analysis of the depth of testing.

5.2.6.3. Functional testing (ATE_FUN.1)

ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.1D

The developer shall test the TSF and document the results.

ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.2D

The developer shall provide test documentation.

ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4. Independent testing - sample (ATE_IND.2)

ATE_IND.2.1C

The TOE shall be suitable for testing.

ATE_IND.2.1D

The developer shall provide the TOE for testing.

ATE_IND.2.2C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7. Vulnerability assessment (AVA)

5.2.7.1. Covert channel analysis (AVA_CCA.1)

AVA_CCA.1.1C

The analysis documentation shall identify covert channels and estimate their capacity.

AVA_CCA.1.1D

The developer shall conduct a search for covert channels for each information flow control policy.

AVA_CCA.1.2C

The analysis documentation shall describe the procedures used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.1.2D

The developer shall provide covert channel analysis documentation.

AVA_CCA.1.3C

The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C

The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

AVA_CCA.1.5C

The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

5.2.7.2. Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1C

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.1D

The developer shall provide guidance documentation.

AVA_MSU.2.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.2D

The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.3C

The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C

The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.3. Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.4. Moderately resistant (AVA_VLA.3)

AVA_VLA.3.1C

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.1D

The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.3.2C

The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.2D

The developer shall document the disposition of identified vulnerabilities.

AVA_VLA.3.3C

The evidence shall show that the search for vulnerabilities is systematic.

5.3. Strength of TOE Security Function Requirements

5.3.1. Minimum SOF Rating

The minimum Strength of Function (SOF) rating provided in this PP is SOF-Medium at EAL4+. In the DoD, this refers to a minimum strength of mechanism level (SML) of 2 as defined in chapter 4 of the *Information Assurance Technical Framework,* which can be found at http://www.iatf.net/. As this TOE provides multiple authentication mechanisms, the minimum SOF rating shall apply to each mechanism.

5.3.2. Explicit SOF Metrics

Reference **[BiometricPP2002]** specifies the requirements shall satisfy the DoD biometric standards for False Acceptance Rates (FAR) and False Rejection Rates (FRR) appropriate for EAL4+. Specifically, it specifies a FAR of less than .0001 for biometric authentication to be validated mainly through statistical testing.

For this PP, we specify a metric of 0.000001 for the FAR of the combined biometric and PIN authentication mechanism. As the biometric and PIN FAR's are independent, the biometric FAR could be validated at 0.01[21] and the PIN[22] FAR at 0.0001 to give a combined FAR of 0.000001.

5.4. Environment Security Requirements

This section identifies the IT security requirements that are to be met by the IT environment of the TOE. There are no security requirements that must be satisfied by the IT environment for this PP. However, the Biometrics PP (reference **[BiometricPP2002])** may impose additional requirements on the environment.

[21] A FAR of 0.01 is closer to the current performance level of many biometric mechanisms.

[22] A four digit PIN would provide a FAR of 0.0001 under an attack involving “random guessing” of the PIN.

6. Rationale

The target of evaluation (TOE), a Token ID Station (TIS), has been defined in section 2. The description of the TOE supports the statement of threats, policies, and assumptions discussed earlier in this PP.

6.1. Introduction and TOE Description Rationale

This section presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The rationale includes the following: Security Objectives Rationale, Security Requirements Rationale.

6.2. Security Objectives Rationale

The **security objectives rationale** demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Table 6-1 and Table 6-2 map the security objectives to the security environment defined by the threats, policies, and assumptions. The mappings illustrate that each security objective covers at least one threat, policy, or assumption, and that each threat, policy, and assumption is covered by at least one security objective.

Policy/Threats/ Assumptions	***Objectives***
Security Objectives for the TOE	
A.Admin_Docs	O.Audit_Gen_User, O.Audit_Generation, O.Audit_Protect, O.I&A_Domain, O.User_Defined_AC, O.Admin_Guidance
A.Biometrics	O.Biometrics
P.Accountability	O.Audit_Gen_User, O.Audit_Generation, O.Audit_Protect, O.I&A_Domain, O.User_Defined_AC
P.Authorities	O.Admin_Guidance, O.User_Guidance
P.Authorized_Use	O.Sys_Access_Banners

Policy/Threats/ Assumptions	***Objectives***
P.Availability	O.Config_Management, O.Trusted_Recovery_Doc, O.Malicious_Code, O.Sys_Assur_HW/SW/FW, O.Sys_Backup_Procs, O.Sys_Backup_Restore, O.Sys_Backup_Storage, O.Sys_Backup_Verify, O.Info_Flow_Control, O.User_Data_Integrity, O.User_Defined_AC, O.Identify_Unusual_Act, O.User_Data_Transfer
P.Guidance	O.Admin_Guidance, O.User_Guidance
P.Information_AC	O.Security_Attr_Mgt, O.Security_Data_Mgt, O.Security_Func_Mgt, O.User_Defined_AC, O.Screen_Lock, O.User_Auth_Enhanced
P.Integrity	O.Change_Control_Users, O.Config_Management, O.Identify_Unusual_Act, O.Security_Attr_Mgt, O.Security_Data_Mgt, O.Security_Func_Mgt, O.Trusted_Recovery_Doc, O.Integrity_Data/SW, O.Integrity_Practice, O.Malicious_Code, O.Storage_Integrity, O.Sys_Assur_HW/SW/FW, O.Sys_Self_Protection, O.Info_Flow_Control, O.User_Data_Integrity, O.User_Defined_AC, O.User_Data_Transfer
P.Lifecycle	O.Lifecycle_Security
P.Marking	O.Config_Management, O.External_Labels
P.Physical_Control	O.Tamper_ID
T.Admin_Err_Commit	Security Objectives, O.Audit_Account, O.Crypto_Key_Man, O.Crypto_Manage_Roles, O.I&A_User_Action, O.Admin_Guidance, O.Security_Attr_Mgt, O.Security_Data_Mgt, O.Security_Func_Mgt, O.Security_Roles, O.Audit_Admin_Role, O.Audit_Loss_Respond, O.Audit_Protect, O.Limit_Actions_Auth, O.Priority_Of_Service
T.Admin_Err_Omit	O.Audit_Account, O.User_Auth_Management, O.Maintenance_Access, O.Maintenance_Recover, O.Prvlg_IF_Status, O.Secure_Configuration, O.Admin_Guidance, O.Crypto_Key_Man, O.Crypto_Manage_Roles, O.I&A_User_Action

Policy/Threats/ Assumptions	***Objectives***
T.Component_Failure	O.Crypto_Data_Sep, O.Crypto_Dsgn_Impl, O.Crypto_Key_Man, O.Crypto_Modular_Dsgn, O.Crypto_Operation, O.Crypto_Self_Test, O.Crypto_Test_Reqs, O.Fail_Secure, O.Fault_Tolerance, O.Priority_Of_Service, O.Secure_State
T.Dev_Flawed_Code	O.No_Residual_Info, O.Integ_Sys_Data_Int, O.Integ_Sys_Data_Ext, O.Secure_State, O.Integrity_Data_Rep, O.Correct_Operation, O.Sys_Self_Protection, O.Audit_Account, O.Audit_Admin_Role, O.Code_Signing, O.Source_Code_Exam
T.Failure_DS_Comp	O.Fault_Tolerance, O.Integrity_Data_Rep, O.Trusted_DS_Recov
T.Power_Disrupt	O.Atomic_Functions, O.Trusted_Recovery
T.Repudiate_Transact	O.I&A_Transaction, O.No_Repudiate_Transact
T.User_Err_Integrity	O.Crypto_Import_Export, O.Crypto_Manage_Roles, O.Audit_Generation, O.Info_Flow_Control, O.User_Defined_AC
T.User_Err_Slf_Protect	O.Obj_Attr_Integrity
T.User_Modify	O.Audit_Gen_User, O.Audit_Generation, O.Audit_Protect, O.Security_Roles, O.Audit_Account, O.Security_Data_Mgt, O.Info_Flow_Control, O.User_Defined_AC, O.Config_Management, O.General_Integ_Checks, O.Integ_Sys_Data_Int, O.Integrity_Practice, O.Maintain_Sec_Domain, O.Reference_Monitor
Security Objectives for the Environment	
A.Biometrics	O.Biometrics
A.Phys_Acc_to_Out	O.Phys_Acc_to_Out
A.Token	O.Token

Table 10. Mapping the TOE Security Environment to Security Objectives

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
Security Objectives for the TOE		
O.AC_Admin_Limit	T.Admin_Err_Commit T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Admin_Guidance	P.Authorities P.Guidance T.Admin_Err_Commit T.Admin_Err_Omit	DP.Authority_Notify DP.Privileged_Doc DP.User_Documentation DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Atomic_Functions	T.Power_Disrupt	DA.Power_Disrupt_Reset
O.Aud_Sys_Entry_Parms	T.Admin_Err_Commit	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.Audit_Account	T.Admin_Err_Commit T.Admin_Err_Omit T.Dev_Flawed_Code T.User_Modify	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Audit_Admin_Role	T.Admin_Err_Commit T.Dev_Flawed_Code	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.Audit_Gen_User	P.Accountability T.User_Modify	DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Audit_Generation	P.Accountability T.User_Err_Integrity T.User_Modify	DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC DA.User_Modify_Data DA.Hack_Ext_CryptoAsset DA.User_Err_AttrXpt DA.User_Err_Data_Export DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Audit_Loss_Respond	T.Admin_Err_Commit	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Audit_Protect	P.Accountability T.Admin_Err_Commit T.User_Modify	DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Biometrics	A.Biometrics	
O.Change_Control_Users	P.Integrity	DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.Code_Signing	T.Dev_Flawed_Code	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.Config_Management	P.Availability P.Integrity P.Marking T.User_Modify	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DP.Config_Mgt_Plan DP.External_Labels DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Correct_Operation	T.Dev_Flawed_Code	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure
O.Crypto_Data_Sep	T.Component_Failure	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto
O.Crypto_Dsgn_Impl	T.Component_Failure	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.Crypto_Import_Export	T.User_Err_Integrity	DA.User_Modify_Data DA.Hack_Ext_CryptoAsset DA.User_Err_AttrXpt DA.User_Err_Data_Export
O.Crypto_Key_Man	T.Admin_Err_Commit T.Admin_Err_Omit T.Component_Failure	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto
O.Fail_Secure	T.Component_Failure	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto
O.Fault_Tolerance	T.Component_Failure T.Failure_DS_Comp	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto DA.Failure_DS_Comm
O.General_Integ_Checks	T.User_Modify	DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.I&A_Domain	P.Accountability	DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC
O.I&A_Transaction	T.Repudiate_Transact	DA.Repudiate_Trans_ Loc

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.I&A_User_Action	T.Admin_Err_Commit T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Identify_Unusual_Act	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Info_Flow_Control	P.Availability P.Integrity T.User_Err_Integrity T.User_Modify	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.User_Modify_Data DA.Hack_Ext_CryptoAsset DA.User_Err_AttrXpt DA.User_Err_Data_Export DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Integ_Sys_Data_Ext	T.Dev_Flawed_Code	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Integ_Sys_Data_Int	T.Dev_Flawed_Code T.User_Modify	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Integrity_Data/SW	P.Integrity	DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.Integrity_Data_Rep	T.Dev_Flawed_Code T.Failure_DS_Comp	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure DA.Failure_DS_Comm

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Integrity_Practice	P.Integrity T.User_Modify	DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Lifecycle_Security	P.Lifecycle	DP.Lifecycle_Security
O.Limit_Actions_Auth	T.Admin_Err_Commit	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Maintain_Sec_Domain	T.User_Modify	DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Maintenance_Access	T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Maintenance_Recover	T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Malicious_Code	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.No_Residual_Info	T.Dev_Flawed_Code	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure
O.No_Repudiate_Transact	T.Repudiate_Transact	DA.Repudiate_Trans_ Loc
O.Obj_Attr_Integrity	T.User_Err_Slf_Protect	DA.User_Err_MsngAttrXpt DA.User_Err_Object_Attr
O.Priority_Of_Service	T.Admin_Err_Commit T.Component_Failure	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Prvlg_IF_Status	T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Reference_Monitor	T.User_Modify	DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.Robust_Encryption		
O.Screen_Lock	P.Information_AC	DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC
O.Secure_Configuration	T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.Secure_State	T.Component_Failure T.Dev_Flawed_Code	DA.Ext_Crypto_Failure DA.Hardware_Flaw DA.Phys_CompFail_Res DA.Software_Flaw DA.TSF_Err_Conf_Crypto DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Security_Attr_Mgt	P.Information_AC P.Integrity T.Admin_Err_Commit	DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr

Objectives	*Policies/Threats/ Assumptions*	*Detailed Policies Detailed Attacks*
O.Security_Data_Mgt	P.Information_AC P.Integrity T.Admin_Err_Commit T.User_Modify	DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Security_Func_Mgt	P.Information_AC P.Integrity T.Admin_Err_Commit	DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr
O.Security_Roles	T.Admin_Err_Commit T.User_Modify	DA.Adm_Err_Crypto DA.Admin_Err_AC_Policy DA.Admin_Err_Audit DA.Admin_Err_Authentic DA.Admin_Err_Info DA.Admin_Err_Resource DA.Admin_Err_Sys_Entry DA.Admin_Err_User_Attr DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Source_Code_Exam	T.Dev_Flawed_Code	DA.Dev_FC_Attr_Interp DA.Dev_FC_Buff_Not_Clr DA.Dev_FC_Ctrl_Data DA.Dev_FC_Data_Export DA.Dev_FC_Recovery DA.Dev_FC_Replication DA.Dev_FC_Self_Protect DA.Dev_FC_Trap_Door DA.Ext_Crypto_Failure
O.Storage_Integrity	P.Integrity	DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.Sys_Access_Banners	P.Authorized_Use	DP.Sys_Access_Banners
O.Sys_Assur_HW/SW/FW	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.Sys_Backup_Procs	P.Availability	DP.Config_Mgt_Plan

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.Sys_Backup_Restore	P.Availability	DP.Config_Mgt_Plan
O.Sys_Backup_Storage	P.Availability	DP.Config_Mgt_Plan
O.Sys_Backup_Verify	P.Availability	DP.Config_Mgt_Plan
O.Sys_Self_Protection	P.Integrity T.Dev_Flawed_Code	DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.Tamper_ID	P.Physical_Control	DP.Tamper_ID
O.Trusted_DS_Recov	T.Failure_DS_Comp	DA.Failure_DS_Comm
O.Trusted_Recovery	T.Power_Disrupt	DA.Power_Disrupt_Reset
O.Trusted_Recovery_Doc	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security

Objectives	***Policies/Threats/ Assumptions***	***Detailed Policies Detailed Attacks***
O.User_Auth_Enhanced	P.Information_AC	DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC
O.User_Auth_Management	T.Admin_Err_Omit	DA.Adm_Err_Crypto DA.Adm_Misconfig_User DA.Admin_Err_Omit_Trap DA.Admin_Err_Update
O.User_Auth_Multiple	T.Biometric_Weak_Auth	
O.User_Data_Integrity	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security
O.User_Data_Transfer	P.Availability P.Integrity	DP.Config_Mgt_Plan DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security

Objectives	Policies/Threats/ Assumptions	Detailed Policies Detailed Attacks
O.User_Defined_AC	P.Accountability P.Availability P.Information_AC P.Integrity T.User_Err_Integrity T.User_Modify	DP.Config_Mgt_Plan DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC DP.Audit_Gen_User DP.Audit_Generation DP.Audit_Protect DP.I&A_User DP.User_Defined_AC DP.Admin_Security_Data DP.Need_To_Know DP.Screen_Lock DP.User_Auth_Enhanced DP.User_Defined_AC DP.Admin_Security_Data DP.Change_Control_Users DP.Config_Mgt_Plan DP.Documented_Recovery DP.Integrity_Data/SW DP.Integrity_Practice DP.Malicious_Code DP.Non-Repudiation DP.Storage_Integrity DP.Sys_Assur_HW/SW/FW DP.System_Protection DP.System_Recovery DP.User_Data_Dial-in DP.User_Data_Storage DP.User_Data_Transfer DP.Lifecycle_Security DA.User_Modify_Data DA.Hack_Ext_CryptoAsset DA.User_Err_AttrXpt DA.User_Err_Data_Export DA.User_Modify_Audit DA.User_Modify_Auth DA.User_Modify_Data DA.User_Modify_TSFData
O.User_Guidance	P.Authorities P.Guidance	DP.Authority_Notify DP.Privileged_Doc DP.User_Documentation

Objectives	*Policies/Threats/ Assumptions*	*Detailed Policies Detailed Attacks*
Security Objectives	A.Admin_Docs A.Admin_Errors A.No_Abuse_By_Admin A.Outsider_Hi A.Review_Audit_Log A.User_Access A.User_Mistakes A.Well_Behaved_Admin	
Security Objectives for the Environment		
O.Biometrics	A.Biometrics	
O.Phys_Acc_to_Out	A.Phys_Acc_to_Out	
O.Token	A.Token	

Table 11. Tracing of Security Objectives to the TOE Security Environment

6.3. Security Requirements Rationale

This section demonstrates that the set of security requirements (TOE and environment) is suitable to meet and traceable to the security objectives.

Security Objectives	*Requirement Components*
O.AC_Admin_Limit	FDP_ACC.1 FDP_ACF.1
O.Admin_Guidance	AGD_ADM.1
O.Atomic_Functions	FPT_RCV.4
O.Aud_Sys_Entry_Parms	FAU_GEN.1 FMT_MTD.1 FMT_MTD.3
O.Audit_Account	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FMT_MOF.1
O.Audit_Admin_Role	AGD_ADM.1 FAU_STG.2 FMT_MTD.1 FMT_SMR.2
O.Audit_Gen_User	FAU_GEN.2

Security Objectives	***Requirement Components***
O.Audit_Generation	FAU_GEN.1
O.Audit_Loss_Respond	FAU_STG.4
O.Audit_Protect	FAU_STG.2
O.Change_Control_Users	
O.Code_Signing	FDP_UIT.1
O.Config_Management	FMT_MOF.1 FMT_MTD.1
O.Correct_Operation	FPT_TST.1
O.Crypto_Data_Sep	ADV_INT.1
O.Crypto_Dsgn_Impl	ADV_LLD.1 ALC_TAT.2
O.Crypto_Import_Export	AGD_ADM.1 AGD_USR.1 FDP_ITC.1
O.Crypto_Key_Man	FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_CKM.4 FDP_ACC.1 FDP_ACF.1 FDP_ITC.1 FMT_MSA.1 FMT_MTD.1 FPT_SEP.1
O.Fail_Secure	FPT_FLS.1
O.Fault_Tolerance	FRU_FLT.2
O.General_Integ_Checks	FPT_TST.1
O.I&A_Domain	FIA_ATD.1 FIA_UAU.2 FIA_UAU.7 FIA_USB.1 FTA_TAB.1
O.I&A_Transaction	
O.I&A_User_Action	AGD_ADM.1 AGD_USR.1 FIA_UAU.2 FIA_USB.1 FMT_MOF.1
O.Identify_Unusual_Act	FTA_TSE.1
O.Info_Flow_Control	

Security Objectives	***Requirement Components***
O.Integ_Sys_Data_Ext	
O.Integ_Sys_Data_Int	
O.Integrity_Data/SW	FDP_SDI.2
O.Integrity_Data_Rep	FPT_TRC.1
O.Integrity_Practice	FPT_AMT.1 FPT_TST.1
O.Lifecycle_Security	
O.Limit_Actions_Auth	FIA_UAU.2
O.Maintain_Sec_Domain	FPT_SEP.1
O.Maintenance_Access	FMT_MOF.1
O.Maintenance_Recover	FMT_SAE.1
O.Malicious_Code	FDP_ITC.1 FPT_AMT.1 FPT_TST.1
O.No_Residual_Info	FDP_RIP.2
O.No_Repudiate_Transact	
O.Obj_Attr_Integrity	FDP_ACC.1 FDP_ACF.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3
O.Priority_Of_Service	
O.Prvlg_IF_Status	FMT_MTD.1
O.Reference_Monitor	FPT_RVM.1
O.Robust_Encryption	FCS_CKM.1 FCS_CKM.2 FCS_CKM.3 FCS_COP.1
O.Screen_Lock	FTA_SSL.1 FTA_SSL.2
O.Secure_Configuration	AGD_ADM.1 FMT_MOF.1 FMT_MTD.1

Security Objectives	***Requirement Components***
O.Secure_State	FPT_FLS.1 FPT_RCV.2 FPT_RCV.4
O.Security_Attr_Mgt	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3
O.Security_Data_Mgt	FMT_MTD.1 FMT_MTD.3
O.Security_Func_Mgt	FMT_MOF.1
O.Security_Roles	FMT_SMR.2
O.Source_Code_Exam	ADV_LLD.1
O.Storage_Integrity	
O.Sys_Access_Banners	FTA_TAB.1
O.Sys_Assur_HW/SW/FW	FPT_TST.1
O.Sys_Backup_Procs	FPT_RCV.2
O.Sys_Backup_Restore	FMT_MOF.1 FMT_MTD.1
O.Sys_Backup_Storage	FMT_MOF.1 FMT_MTD.1
O.Sys_Backup_Verify	FPT_AMT.1 FPT_TST.1
O.Sys_Self_Protection	FPT_SEP.1
O.Tamper_ID	AGD_ADM.1 AGD_USR.1
O.Trusted_DS_Recov	FPT_RCV.2 FPT_RCV.4
O.Trusted_Recovery	FPT_RCV.2
O.Trusted_Recovery_Doc	AGD_ADM.1
O.User_Auth_Enhanced	FIA_UAU.3
O.User_Auth_Management	AGD_ADM.1 AGD_USR.1 FMT_MSA.1 FMT_REV.1 FMT_SAE.1

Security Objectives	***Requirement Components***
O.User_Auth_Multiple	FMT_MOF.1
O.User_Data_Integrity	
O.User_Data_Transfer	
O.User_Defined_AC	FDP_ACC.1 FDP_ACF.1
O.User_Guidance	AGD_USR.1

Table 12. Coverage of Security Objectives by Requirement Components

Requirement Components	***Security Objectives***
FAU_ARP.1	
FAU_GEN.1	O.Aud_Sys_Entry_Parms O.Audit_Account O.Audit_Generation
FAU_GEN.2	O.Audit_Account O.Audit_Gen_User
FAU_SAA.1	
FAU_SAR.1	O.Audit_Account
FAU_SAR.2	O.Audit_Account
FAU_SAR.3	O.Audit_Account
FAU_STG.2	O.Audit_Admin_Role O.Audit_Protect
FAU_STG.4	O.Audit_Loss_Respond
FCO_NRO.2	
FCS_CKM.1	O.Crypto_Key_Man O.Robust_Encryption
FCS_CKM.2	O.Crypto_Key_Man O.Robust_Encryption
FCS_CKM.3	O.Crypto_Key_Man O.Robust_Encryption
FCS_CKM.4	O.Crypto_Key_Man

Requirement Components	Security Objectives
FCS_COP.1	O.Robust_Encryption
FDP_ACC.1	O.AC_Admin_Limit O.Crypto_Key_Man O.Obj_Attr_Integrity O.User_Defined_AC
FDP_ACF.1	O.AC_Admin_Limit O.Crypto_Key_Man O.Obj_Attr_Integrity O.User_Defined_AC
FDP_ITC.1	O.Crypto_Import_Export O.Crypto_Key_Man O.Malicious_Code
FDP_RIP.2	O.No_Residual_Info
FDP_SDI.2	O.Integrity_Data/SW
FDP_UIT.1	O.Code_Signing
FIA_AFL.1	
FIA_ATD.1	O.I&A_Domain
FIA_UAU.2	O.I&A_Domain O.I&A_User_Action O.Limit_Actions_Auth
FIA_UAU.3	O.User_Auth_Enhanced
FIA_UAU.7	O.I&A_Domain
FIA_USB.1	O.I&A_Domain O.I&A_User_Action
FMT_MOF.1	O.Audit_Account O.Config_Management O.I&A_User_Action O.Maintenance_Access O.Secure_Configuration O.Security_Func_Mgt O.Sys_Backup_Restore O.Sys_Backup_Storage O.User_Auth_Multiple
FMT_MSA.1	O.Crypto_Key_Man O.Obj_Attr_Integrity O.Security_Attr_Mgt O.User_Auth_Management
FMT_MSA.2	O.Obj_Attr_Integrity O.Security_Attr_Mgt
FMT_MSA.3	O.Obj_Attr_Integrity O.Security_Attr_Mgt

Requirement Components	***Security Objectives***
FMT_MTD.1	O.Aud_Sys_Entry_Parms O.Audit_Admin_Role O.Config_Management O.Crypto_Key_Man O.Prvlg_IF_Status O.Secure_Configuration O.Security_Data_Mgt O.Sys_Backup_Restore O.Sys_Backup_Storage
FMT_MTD.3	O.Aud_Sys_Entry_Parms O.Security_Data_Mgt
FMT_REV.1	O.User_Auth_Management
FMT_SAE.1	O.Maintenance_Recover O.User_Auth_Management
FMT_SMR.2	O.Audit_Admin_Role O.Security_Roles
FPT_AMT.1	O.Integrity_Practice O.Malicious_Code O.Sys_Backup_Verify
FPT_FLS.1	O.Fail_Secure O.Secure_State
FPT_ITT.2	
FPT_ITT.3	
FPT_PHP.3	
FPT_RCV.2	O.Secure_State O.Sys_Backup_Procs O.Trusted_DS_Recov O.Trusted_Recovery
FPT_RCV.4	O.Atomic_Functions O.Secure_State O.Trusted_DS_Recov
FPT_RPL.1	
FPT_RVM.1	O.Reference_Monitor
FPT_SEP.1	O.Crypto_Key_Man O.Maintain_Sec_Domain O.Sys_Self_Protection
FPT_STM.1	
FPT_TRC.1	O.Integrity_Data_Rep

Requirement Components	***Security Objectives***
FPT_TST.1	O.Correct_Operation O.General_Integ_Checks O.Integrity_Practice O.Malicious_Code O.Sys_Assur_HW/SW/FW O.Sys_Backup_Verify
FRU_FLT.2	O.Fault_Tolerance
FTA_SSL.1	O.Screen_Lock
FTA_SSL.2	O.Screen_Lock
FTA_TAB.1	O.I&A_Domain O.Sys_Access_Banners
FTA_TSE.1	O.Identify_Unusual_Act
ACM_AUT.1	
ACM_CAP.4	
ACM_SCP.3	
ADO_DEL.2	
ADO_IGS.1	
ADV_FSP.3	
ADV_HLD.3	
ADV_IMP.2	
ADV_INT.1	O.Crypto_Data_Sep
ADV_LLD.1	O.Crypto_Dsgn_Impl O.Source_Code_Exam
ADV_SPM.3	
AGD_ADM.1	O.Admin_Guidance O.Audit_Admin_Role O.Crypto_Import_Export O.I&A_User_Action O.Secure_Configuration O.Tamper_ID O.Trusted_Recovery_Doc O.User_Auth_Management
AGD_USR.1	O.Crypto_Import_Export O.I&A_User_Action O.Tamper_ID O.User_Auth_Management O.User_Guidance

Requirement Components	***Security Objectives***
ALC_TAT.2	O.Crypto_Dsgn_Impl
ATE_COV.2	
ATE_DPT.2	
ATE_IND.2	
AVA_CCA.1	
AVA_MSU.2	
AVA_SOF.1	
AVA_VLA.3	

Table 13Coverage of Requirement Components by Security Objectives

6.4. Dependency Rationale

Requirement Component	***Dependencies***
Functional Requirements	
FAU_ARP.1	none
FAU_GEN.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FAU_SAA.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_STG.2	FAU_GEN.1
FAU_STG.4	FAU_STG.1
FCO_NRO.2	FIA_UID.2

Requirement Component	**Dependencies**
FCS_CKM.1	FCS_CKM.2, FCS_COP.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.2	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.3	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FCS_CKM.4	FDP_ITC.1, FCS_CKM.1, FMT_MSA.2
FCS_COP.1	FDP_ITC.1, FCS_CKM.1, FCS_CKM.4, FMT_MSA.2
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
FDP_ITC.1	FDP_ACC.1, FMT_MSA.3
FDP_RIP.2	none
FDP_SDI.2	none
FDP_UIT.1	FDP_ACC.1, FDP_IFC.1, FTP_ITC.1, FTP_TRP.1
FIA_AFL.1	FIA_UAU.2
FIA_ATD.1	none
FIA_UAU.2	FIA_UID.1
FIA_UAU.3	none
FIA_UAU.7	FIA_UAU.2
FIA_USB.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1, FDP_IFC.1, FMT_SMR.1
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1, FDP_IFC.1, FMT_MSA.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1

Requirement Component	***Dependencies***
FMT_MTD.3	ADV_SPM.1, FMT_MTD.1
FMT_REV.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1, FPT_STM.1
FMT_SMR.2	FIA_UID.2
FPT_AMT.1	none
FPT_FLS.1	ADV_SPM.1
FPT_ITT.2	none
FPT_ITT.3	FPT_ITT.2
FPT_PHP.3	none
FPT_RCV.2	FPT_TST.1, AGD_ADM.1, ADV_SPM.1
FPT_RCV.4	ADV_SPM.1
FPT_RPL.1	none
FPT_RVM.1	none
FPT_SEP.1	none
FPT_STM.1	none
FPT_TRC.1	FPT_ITT.2
FPT_TST.1	FPT_AMT.1
FRU_FLT.2	FPT_FLS.1
FTA_SSL.1	FIA_UAU.1
FTA_SSL.2	FIA_UAU.1
FTA_TAB.1	none
FTA_TSE.1	none

Requirement Component	***Dependencies***
Assurance Requirements	
ACM_AUT.1	ACM_CAP.3
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1
ACM_SCP.3	ACM_CAP.3
ADO_DEL.2	ACM_CAP.3
ADO_IGS.1	AGD_ADM.1
ADV_FSP.3	ADV_RCR.1
ADV_HLD.3	ADV_FSP.3, ADV_RCR.2
ADV_IMP.2	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1
ADV_INT.1	ADV_IMP.1, ADV_LLD.1
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1
ADV_SPM.3	ADV_FSP.1
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ALC_TAT.2	ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1
ATE_DPT.2	ADV_HLD.2, ADV_LLD.1, ATE_FUN.1
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1
AVA_CCA.1	ADV_FSP.2, ADV_IMP.2, AGD_ADM.1, AGD_USR.1
AVA_MSU.2	ADO_IGS.1, ADV_FSP.1, AGD_ADM.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.3	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1

Table 14. Functional and Assurance Requirement Components Dependencies

6.5. Rationale for Extensions

7. Glossary

CC specific terms:

Term	***Definition***
CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

TIS specific terms:

Term	***Definition***
administrator	One of the TIS roles for managing a TIS outlined in table .
alarms	
audit records	
authenticate	Confirm the claimed identity of an individual.
authentication	The confirmation of the claimed identity of an individual.
authentication certificate	An electronic document used to authenticate an individual.
authorization certificate	An electronic document containing the identity of an individual and the privileges he/she have for accessing resources.

Term	Definition
biometric	A measurable, physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual.
biometric scan	Data representing a biometric characteristic of an individual as captured by a biometric scanner device.
biometric scanner	A device which can scan and capture an individual's biometric.
biometric template	A subset of information extracted from biometric scan(s) during enrollment. Such a template is used to authenticate that future biometric scans came from the same person.
biometric subsystem	The subsystem consisting of a biometric scanner and biometric verifier.
biometric verifier	A component which compares a biometric scan with a biometric template to determine if there is a match or not.
enclave	A physically secured area where entry to or egress from can be made only through a portal. An enclave could be an enclosed area in a building or one or more buildings themselves.
enrollment	The process of creating an authentication certificate for an individual and placing it on his/her token.
entry station	The set of TIS devices on the entry side of a portal used to authenticate an individual requesting entry into the enclave.
exit station	The set of TIS devices on the exit side of a portal used to log when an individual leaves the enclave and retrieve and remove their authorization certificates from their token.
FAR	False Acceptance Rate
FRR	False Rejection Rate
PCMCIA card	
PIN	Personal Identification Number - A 4- to 12-character alphanumeric code or password used to authenticate an identity.

Term	***Definition***
portal	An entry/egress point to an enclave. It could be a door or a turnstile. It is usually latched (locked) and only unlatched to allow an individual to enter or egress the enclave.
Portal Latch Interface (PLI)	An interface device through which a portal may be unlatched, latched and through which the state of the portal can be sensed (e.g., if the portal is open or not).
role certificate	An electronic document containing a list of TIS roles that an individual can assume after they are authenticated by the TIS.
smart card	A shaped piece of plastic or other carrier with a small computer chip embedded into it.
TIS	Token ID Station
token	A portable device (e.g., a smart card or PCMCIA card) that can be carried by an individual which can hold tokens.
token reader	A device used to retrieve and place tokens on a token carrier.

8. References

Citation	***Reference***
[BiometricPP2002]	Anne Kong, **Department of Defense & Federal Biometric System Protection Profile for Medium Robustness Environments**, Version 0.02, 3 March 2002.
[CC1999a]	**Common Criteria for Information Technology Security Evaluation User Guide**, a guide by Syntegra sponsored by CESG in the UK and NIST in the USA, October 1999
[CC1999b]	**Common Methodology for Information Technology Security Evaluation Part 2: Evaluation Methodology Supplement: ALC_FLR - Flaw Remediation,** CEM-2001/0015R, Version 1.1 February 2002 http://www.commoncriteria.org
[CC1999c]	**Common Methodology for Information Technology Security Evaluation Part 1: Introduction and general model,** August 1999 Version 2.1 CCIMB-99-031
[CCPKB2000]	Jim Williams and Allen Basey, **CC Profiling Knowledge Base User's Guide**, Version 1.0j,k, May 2000
[CCToolbox2000a]	**CCToolbox Reference Manual**, Version 6.0f, 2000
[CCToolbox2000b]	Gary Grainger, **Touring the CC Toolbox**, 13 September 2000
[DoD2000]	***X.509 Certificate Policy for the United States Department of Defense***, version 5.2, 13 November 2000.
[NIST2001]	National Institute of Standards and Technology (NIST)*,* **Security Requirements for Cryptographic Modules,** Federal Information Processing Standard Publication (FIPS-PUB) 140-2, *25* May 2001.
[Tokeneer1998a]	*Tokeneer System Design Description,* Build 1: Version 2.0, 1 June 1998.
[Tokeneer1998b]	*Tokeneer Operational Concept Description,* Build 1: Version 2.0, 1 June 1998.
[Tokeneer1998c]	*Tokeneer System/Subsystem Specification (Requirements Document),* Build 1: Version 2.0, 1 June 1998.
[TokenPP2002]	Tamara Cleveland, et. al, **Department of Defense Public Key Infrastructure Token Protection Profile**, Version 3.0, 22 March 2002.