KyberPASS

Virtual Private Network Version 4.1.1

with Hydra 3DES (CBC mode) encryption

Security Target

Version 1.5 (Sanitised)

Final

August 2000

Prepared for:

XCP Security Systems Pty Ltd
Level 2, 541 Blackburn Road
Mt. Waverley, VIC 3149

Prepared by:

90East (Asia Pacific) Pty Ltd
7-9 Geelong St
Fyshwick, ACT 2609

Table of Contents

List of Tables

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 2.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Security Target reader. The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment is indicated by showing the value in square brackets [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicised* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the CC an iteration number inside parenthesis, i.e., FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2).

All operations described above are used in this Security Target. *Italicised text* is used for both official document titles and text meant to be emphasised more than plain text.

Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following terms are a subset of those definitions. They are listed here to aid the user of the Security Target.

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Administrator - A role which users may be associated with to administer the security parameters of the TOE. Such users are not subject to any access control requirements once authenticated to the TOE and are therefore trusted to not compromise the security policy enforced by the TOE.

Application - Any IT product or system, untrusted or trusted, outside the TOE that interacts with the TOE.

Role - A predefined set of rules establishing the allowed interactions between a user and the TOE.

Identity - A representation (eg a string) uniquely identifying an authorised user, that can be either the full or abbreviated name of that user or a pseudonym.

Authentication data - Information used to verify the claimed identity of a user.

Document Organisation

Section 1 provides the introductory material for the Security Target.

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 has been sanitised by the sponsor of the evaluation and now documents PP conformance claims appropriate to the TOE

Section7 provides the mappings for objectives, threats, organisation security policies and assumptions appropriate for the TOE. Next section 7 maps the security functional requirements to the objectives and identifies dependencies.

Section 8 is a reference section that is provided to identify background material.

1 Introduction

This introductory section presents *security target (ST)* identification information and an overview of the ST structure. A brief discussion of the ST development methodology is also provided.

1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE). This ST targets an **Evaluation Assurance Level (EAL) 1** level of assurance.

ST Title:	KyberPASS Virtual Private Network Version 4.1.1 August 2000
TOE Identification:	KyberPASS Virtual Private Network Version 4.1.1
CC Version:	Common Criteria for Information Technology Security Evaluation, Version 2.1 Final
ST Evaluation:	Australasian Information Security Evaluation Program, Defence Signals Directorate, Australian Department of Defence
Author(s)	Rod Murn
Keywords:	Virtual private network, security target, encryption, public key technology

1.2 Security Target Overview

Note for readers: The KyberPASS product is built on the client / server model and comprises the KyberPASS Authentication Server (server) and KyberWIN (client). Where reference is made to KyberPASS functionality, it means that the function or capability is present in both the server and the client. Where specific reference is made to the server (KyberPASS Authentication Server), it means that the function is present in that component only. The same meaning applies correspondingly to the client (KyberWIN).

KyberPASS is a virtual Private Network (VPN) product that provides all the fundamental security services that are required to allow private, controlled access to sensitive computing resources. KyberPASS utilises industry-standard public/private key-based strong digital signature authentication (possession of a token, knowledge of a password, and third party public key infrastructure (PKI) authentication) for identifying and authenticating users attempting access to the private network. KyberPASS is PKI-enabled, connecting to any standard LDAP V3 PKI. KyberPASS supports private key tokens that can be stored on hard disks, diskettes, PCMCIA cards, and PKCS-11 compliant smart cards and biometrics scanners.

KyberPASS provides automatic session encryption using the Hydra 3DES product in Cipher Block Chaining (CBC) mode, with key exchange protected by public/private key encryption. Session keys and the session security policy are securely exchanged between the KyberWIN client workstation and the KyberPASS Authentication Server. The session keys are used only once.

KyberPASS Authentication Server checks the attributes of a user's X.509 digital certificate to control routing paths and check access permissions. Depending on the definitions set in the KyberPASS Authentication Server rules table, a user may be allowed, disallowed, or automatically routed to specific servers. KyberPASS uses MD5 Message Authentication Code hashing and digital signatures to verify and authenticate each data packet sent during a session.

KyberPASS Authentication Server audits all connection attempts, both successful and unsuccessful. It also records usage statistics and other relevant session information. KyberPASS Authentication Server is integrated with the Microsoft NT Server Event Logging and Alert Monitor such that automatic alarms and event messages can be generated when pre-defined thresholds have been reached. KyberPASS Authentication Server audit logs support non-repudiation. All user connections to the private network, including Microsoft Networking SMB sessions, are logged and signed with the user's PKI digital signature.

KyberPASS uses an industry standard RSA Public Key Cryptography engine and includes a simple Public Key repository on the KyberPASS Security server and a key management system to add and revoke Public Keys. KyberPASS Authentication Server is capable of retrieving Public Keys from any LDAP V3 X.509 directory.

1.3 Common Criteria Conformance

The TOE is conformant with Parts 2 and 3 of the CC, version 2.1.

2 TOE Description

This section provides context for the TOE evaluation by identifying the product type and describing the evaluated configuration.

2.1 Overview of the KyberPASS VPN System

This section presents an overview of the KyberPASS VPN version 4.1.1 to assist potential users in determining whether it meets their needs. The KyberPASS VPN, known as the TOE, consists of five distinct components:

- The **KyberPASS Authentication Server**, the inter-network security and policy management system that controls the flow traffic between network subjects and objects.
- The **KyberWIN security client**, the client system that interfaces with the security server to authenticate and protect user communications.
- The **Hydra** triple-DES symmetric (CBC mode) key encryption engine to protect user communications.
- The **NT Workstation**, by means of which administrators manage the security of the KyberPASS Authentication Server.
- The **Client Workstation**, by means of which users establish secure sessions with target hosts.

The KyberPASS Authentication Server is the heart of the KyberPASS product. It authenticates users and provides a secure data encryption/decryption transport between users and the network servers they access.

Public Key cryptography is used by the KyberPASS Security server, working with KyberWIN on each user's workstation, to verify a user's identity (authentication), and to verify that the user is permitted to access an organisation's secure systems.

KyberPASS can also be configured to encrypt the data being transferred between a workstation and a server to ensure privacy. In this case, a Hydra session key is created to encrypt the data.

KyberPASS supports TCP/IP compatible communications software products, such as terminal emulators (eg Telnet and TN3270), World Wide Web browsers (eg Netscape and Explorer), and file transfer programs, such as FTP.

The KyberPASS Authentication Client (KyberWIN) provides transparent access to KyberPASS. KyberWIN runs on the user's workstation and works with KyberPASS.

When access to a server protected by KyberPASS is attempted by any of the user's TCP/IP communications software products, KyberWIN will communicate with the user and with the KyberPASS Authentication Server to identify the user. The authentication and encryption process is transparent to the user and to the communications software products.

KyberPASS Control provides a control panel for starting and stopping all KyberPASS Authentication Server functions. It also provides automatic control of KyberPASS for unattended operations.

X.500 Directory Manager is used to define and maintain the definitions for X.500 directory access. It supports access to local X.500 directories using proprietary database software and an LDAP compliant server interface, and to remote third-party X.500 databases which are LDAP compliant. In addition, it supports the creation and management of a number of special purpose directories for use by the KyberPASS services and other KyberPASS products.

Configuration Manager is the management facility that allows the KyberPASS administrator to set the addresses and control parameters that define which public key repository the KyberPASS Authentication Server is to access, and which servers KyberPASS is to protect.

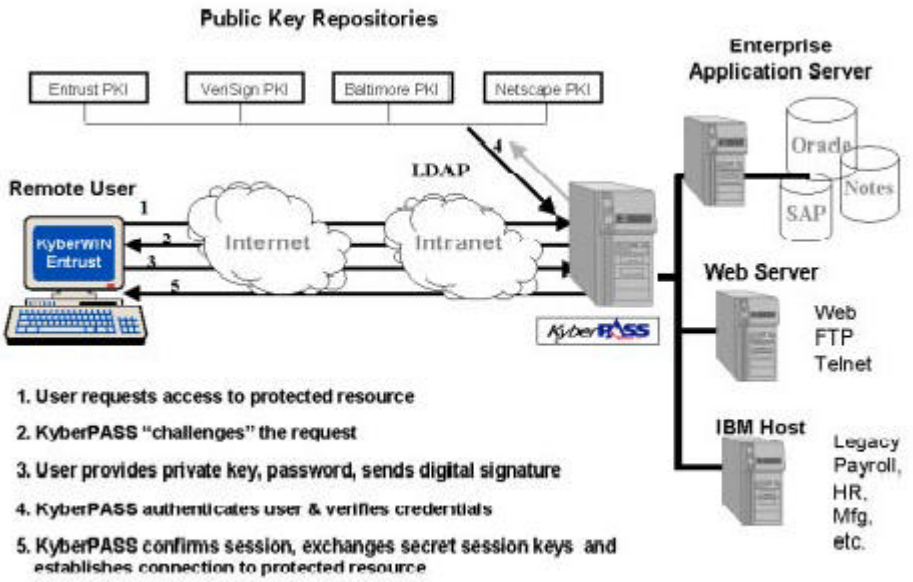
Display Manager is the KyberPASS administrator's tool to monitor traffic through the KyberPASS server. The administrator's interface is a multi-window display.

Log Viewer provides a multi-window viewing and printing service for each of the KyberPASS activity and security audit logs.

The following is a typical sequence of events followed by KyberPASS and KyberWIN that illustrate the process of establishing and using a secure tunnel.

1. A user attempts to connect to a server using a TCP/IP client application, eg FTP.
2. KyberPASS Authentication Server accepts the connection and sends a challenge back to KyberWIN.
3. KyberWIN receives the challenge and prompts the user with a Windows panel to identify himself with a password and private key.
4. KyberWIN uses the private key to digitally sign a logon request.
5. KyberWIN sends the logon request to the KyberPASS Authentication Server.
6. The KyberPASS Authentication Server searches the X.500 directories and retrieves the user's public key from a LDAP compliant server, validates the digital signature, confirms access authority, and if the user is authenticated and authorised, sends a secure session ticket to KyberWIN.
7. Now that a secure session has been set up, the user continues working with the connection to the target server. The TCP/IP client application makes Winsock calls. KyberWIN intercepts the Winsock calls and adds a secure session ticket.
8. If data encryption is turned on, KyberWIN also encrypts/decrypts the data content as it passes back and forth between it and the KyberPASS Authentication Server.
9. KyberWIN passes the TCP/IP packet to Winsock, which then follows the normal network protocols and routing to the KyberPASS Authentication Server.
10. KyberPASS Authentication Server receives the TCP/IP data packet, validates the secure session ticket, and removes the ticket. If KyberWIN has encrypted the data content, then the KyberPASS Authentication Server decrypts the data.
11. Using pre-defined proxy connections, it hands the "clear" TCP/IP data packet from an inbound address to an outbound address within the KyberPASS Authentication Server, then on to the target server.
12. Traffic from a server to a user follows the same steps, in reverse.

The following diagram demonstrates the process of a KyberWIN/KyberPASS Authentication Server secure session:



KyberPASS provides an IP address proxy service for servers under its protection. The external network only sees KyberPASS' IP addresses. Only authenticated traffic gets through and only to IP addresses and TCP services defined in KyberPASS' proxy connections. A proxy connection can be defined for each TCP/IP service supported on each protected enterprise server. A proxy includes:

1. Proxy IP In - Address (ie Network Interface Card (NIC) attached to InterNet).
2. In Address - TCP Service/Port number, (ie service to be proxied).
3. Proxy IP Out - Address (ie NIC attached to EnterpriseNet).
4. Enterprise server address.
5. Enterprise server TCP Service/Port number.
6. Authentication policies for this proxy connection.

To protect multiple servers, the administrator can use Windows NT Server to configure several IP addresses on the inbound and outbound network access cards for each server connection. Proxy connections can be configured for multiple services on each enterprise server. Security policies are set for each proxy connection. An organisation defines a security policy for each application based on their corporate security requirements. Security policy options are:

Policies

- No authentication (pass thru)
- Logon Authentication (strong user authentication)
- Packet Authentication (data integrity plus logon authentication)
- Packet Encryption (data confidentiality, plus integrity, plus logon authentication)

Options

- Packet Compression

Authentication policies are held centrally by the KyberPASS server and transmitted to KyberWIN during session establishment.

The Server Workstation, an Intel Pentium-based PC with Microsoft Windows NT 4.0 operating system, provides system and security management, including management of the audit data.

The physical scope of the TOE includes the hardware and software elements identified in Table 1.

TOE Components	Hardware/Software Elements
KyberPASS Authentication Server	KyberPASS Authentication Server KyberPASS Control X.500 Directory Manager Configuration Manager Display Manager Log Viewer RSA Data Security Inc Bsafe library Hydra 3DES (CBC mode) crypto primitive
KyberWIN Client Workstation`	KyberWIN Client. RSA Data Security Inc Bsafe library Hydra 3DES (CBC mode) crypto primitive
Server Workstation (NT Workstation)	Intel Pentium with at least 64MB RAM PCI bus architecture CD-ROM for installing from CD-ROM media Hard disk drive with at least 1 GB storage Video board and monitor capable of running SVGA Two or more Network Access Cards WinNT 4.0 Server – including Service Pack 4 or later NT services used by the TOE: • File System • NT Security Sub-system • Event Log Services • NT Registry Services
Client Workstation	Intel 486 – 100MHz with at least 16MB RAM HDD with at least 1MB free disk space Windows '95 with Winsock 2.0 or DUN 1.3 upgrade, or Windows '98 or NT 4.0 with latest Service Pack

Table 1 - TOE Component Identification

2.2 Security Services

The TOE provides the following security features:

Feature	Description
Identification and Authentication	The KyberPASS Authentication Server and KyberWIN client require users and administrators to identify themselves before they can perform any action.
System Security Management	The Server workstation provides console access to the NT operating system for security administration of KyberPASS. The workstation also provides access to the management functions relating to the administration of privileged accounts.
Access Control	The KyberPASS Authentication Server restricts access to protected servers to those users defined in its access control lists.
System Architecture	The KyberPASS Server maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
Security Audit	The KyberPASS Authentication Server detects the occurrence of selected events and stores information relating to those events on the NT workstation. The NT workstation also detects the occurrence of certain events and records the related information.
TSF Data Import & Export	KyberPASS uses public key cryptography to protect the transfer of TSF data.
Secure Packet Transfer	KyberPASS uses a combination of asymmetric (public key) and symmetric (secret key) cryptography to protect the interchange of user data.
Key and Credential Management	The KyberPASS Authentication Server provides a limited number of functions (add, delete) for the management of user identity certificates.
Information Flow Control	The KyberPASS Authentication Server controls the flow of IP packets between any client and the application servers under its control.
Associations	KyberPASS provides a trusted information interchange channel between any client and the application servers under its control.

Table 2 - TOE Security Features

Software and hardware features outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- Cut-Through Proxies;
- The Alert Monitor
- Failover;
- Public Key pair and Certificate generation;
- Network Address Translation (NAT);
- Private-Link;
- Setup Wizard;
- TFTP Configuration Server;
- Remote Administration (Telnet interface);
- Acceptance of updates for internal data structures (e.g., routing tables) from authorised host; and
- Windows NT 4.0 features not used by the TOE.

2.3 Application Context

KyberPASS provides a virtual private network connection between selected, internal applications hosts and clients on an external network. As the external network may be an uncontrolled network such as the Internet, the KyberPASS Authentication Server must be protected from external attacks aimed at it by an assured firewall product and competent operational management procedures.

The KyberPASS Authentication Server workstation itself has no need to access resources on the external network nor resources in the applications host domain it protects. In this way, the workstation and the NT operating system and associated services can be considered as a trusted sub-system of the TOE.

3 TOE Security Environment

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any *assumptions* about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.
- Any known or assumed *threats* to the assets against which specific protection within the TOE or its environment is required.
- Any *organisational security policy* statements or rules with which the TOE must comply.

The TOE is intended to be used in Non-National Security environments where sensitive information up to the Protected level is processed or National Security environments where material up to Restricted is processed.

3.1 Secure Usage Assumptions

The following assumptions relating to the operation of the TOE are made.

Name	Description
A.ATTACK	The TOE will be used to protect attractive IT assets and possible attackers can be assumed to have a high level of expertise, resources and motivation.
A.PHYSICAL	As the server function of the TOE sits atop an NT workstation, logical access controls can be compromised if an attacker gets physical access to the console. Strong physical security countermeasures will therefore be in place.
A.FIREWALL	As the server function of the TOE sits atop the NT O/S, logical access controls can be compromised if an attacker gets online access to the NT workstation. Therefore, the server function of the TOE will be protected by an EAL-2 -assured or greater firewall product, operated in accordance with government best practice.
A.PLATFORM	The server function of the TOE depends on the NT operating system for security management functions. The TOE Operator will operate the server function of the TOE from an NT workstation in line with the TOE developer's recommendations, as contained in the Administrators and Secure Usage Guides.
A.SPILLAGE	The TOE provides optional encryption of packets between the server and the client. In situations where encryption of user data is not the default, an explicit user judgement is required to decide whether to invoke the encryption facility when receiving data over insecure telecommunications path.
A.NOEVIL	As the security functions of the TOE can be readily compromised by authorised administrators, it is assumed that they will have successfully completed a security background check before being granted access to the TOE management functions and are assumed to be non-hostile and can be trusted to do their duties correctly.
A.NO-USER-CODE	The operating environment provides no user-accessible code that allows modification of the KyberPASS security configuration by other than authorised administrators.

Table 3 - Table of Secure Usage Assumptions

3.2 Threats to Security

Threats may be addressed either by the TOE or by its intended environment (for example, using personnel, physical, or administrative safeguards). These two classes of threats are discussed separately.

Threats Addressed by the TOE

The TOE addresses the following treats.

Name	Description
T.ABUSE	An authorised user of the TOE (intentionally or otherwise) performing actions that individual is authorised to perform may compromise the TOE security function.
T.ACCESS	An authorised user of the TOE, however without permission from the person who owns or is responsible for cryptographic key material in use by the TOE, may intentionally or otherwise access that material.
T.ATTACK	An attacker (whether an insider or outsider) performing actions that bypass the TOE security functions may gain access to the protected applications hosts that it is meant to protect.
T.AUDIT-CONFIDENTIALITY	An unauthorised individual or process may gain access to the records of security-related events kept by the TOE.
T.AUDIT-CORRUPTED	An unauthorised individual or process may modify or destroy the records of security-related events kept by the TOE.
T.CAPTURE	An attacker may eavesdrop on, or otherwise capture, cryptographic key material or related user data being transferred across a network.
T.DENY	A user as either originator or recipient) may participate in the transfer of information and then deny having done so.
T.ERROR	An unauthorised individual or user of the TOE may, by inducing errors in the TOE, cause unauthorised disclosure or modification of cryptographic key material or related user data being transferred across a network.
T.IMPERSON	An attacker (an outsider or insider) may, by impersonation of an authorised user of the TOE, gain unauthorised access to cryptographic key material or related user data being transferred across a network.
T.INTEGRITY	User, hardware or transmission errors may compromise the integrity of information being transferred across a network.
T.MIX	A subject that is not the authorised recipient may, through the inadvertant mixing of plaintext and cyphertext on the same logical circuit, gain access to sensitive material.
T.MODIFY	An attacker may, through unauthorised modification or destruction, compromise the integrity of cryptographic key material or related user data being transferred across a network.
T.RECORD-EVENT	The TOE may not record in the audit trail the security-relevant events affecting the secure operation of the TOE.
T.RESOURCES	System error or non-malicious user action may exhaust the shared, internal resources of the TOE
T.TRACEABLE	The TOE may not be able to provide an auditable link between a security-relevant event and the user or system process that initiated it.

Table 4 - Table of Threats Addressed by the TOE

Threats Addressed by the Operating Environment

The TOE Operating Environment addresses the following threats.

Name	Description
TE.ADMIN-ERROR	The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.
TE.ENTRY-NON-TECHNICAL	An individual, either internally or externally, using non-technical means may gain access to cryptographic key material or related user data being transferred across a network.
TE.INSTALL	The TOE may be delivered or installed in a manner that undermines security.
TE.OPERATE	Improper operation of the TOE may cause a failure of the TOE security function.

Table 5 - Table of Threats Addressed by the Operational Environment

3.3 Organisational Security Policies

The table following describes the organisational security policies relevant to the operation of the TOE.

Name	Description
P.AUDIT	Details of user activity will be recorded in an audit trail that must be preserved in line with relevant organisational archive requirements.
P.CRYPTO	All cryptographically-relevant material is to be the subject of rigorous levels of physical and technical control as defined in ACSI 57.
P.NETWORK	The organisation's IT security policy will be maintained in the environment of distributed systems interconnected via insecure networking.
P.INFO-FLOW	The flow of information between IT components in a client-server architecture utilising insecure networks must be controlled and protected from disclosure.
P.USER-DUE-CARE	Users who have been issued authenticators that facilitate usage of IT systems will ensure that those authenticators are appropriately protected.

Table 6 - Table of Organisational Security Policies

4 Security Objectives

The security objectives are a concise statement of the intended response to the security problem. These objectives indicate, at a high level, how the security problem, as characterised in the "Security Environment" section of the ST, is to be addressed. Just as some threats are to be addressed by the TOE and others by its intended environment, so some security objectives are for the TOE and others are for its environment. These two classes of security objectives are discussed separately.

4.1 Security Objectives for the TOE

The security objectives for the TOE are as described in the following table.

Name	Description
O.I&A	The TOE must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE facilities.
O.DAC	The TOE must provide its operator with the means of controlling and limiting access to the objects and resources it owns or is responsible for.
O.AUDIT	The TOE must provide the means for recording security-relevant events in sufficient detail to help an administrator of the TOE to: (a) Detect attempted security violations; and (b) Hold individual users accountable for any actions they perform that are relevant to the security of the TOE.
O.ADMIN	The TOE, in conjunction with the underlying operating system where necessary, must provide functions to enable an authorised administrator to effectively manage the TOE and its security functions, and ensuring that only authorised administrators can access such functionality.
O.INTEGRITY	The TOE must provide the means for detecting loss of integrity of TSF data.
O.BYPASS	The TOE must prevent users or processes from bypassing or circumventing TOE security policy enforcement.
O.MESSAGE-INTEGRITY	The TOE must provide a means of detecting the loss of integrity of messages transferred between users across the telecommunications network.
O.DATA-CONFIDENTIALITY	The TOE must provide the means of protecting the confidentiality of user information when it is transferred across an insecure telecommunications network.
O.INFO-FLOW	The TOE must ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.
O.KEY-CONFIDENTIALITY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are transferred across an insecure telecommunications network and when kept in short and long-term storage.
O.NETWORK	The TOE must be able to meet its security objectives in a distributed environment. This may be either as a distributed TOE and as a TOE networked with other IT resources.
O.NOREPUD	The TOE must provide a means for generating evidence that can be used to prevent an originator of data from successfully denying ever having sent that data, and evidence that can be used to prevent a recipient of data from successfully denying ever having received that data.
O.RBAC	The TOE must prevent users from gaining access to and performing operations on its resources for which their role is not explicitly authorised.
O.SEPARATION	The TOE must provide a security domain for its own execution that protects it from compromise by unauthorised subjects.
O.RESOURCES	The TOE must protect itself from user or system errors that result in shared resource exhaustion.

Table 7 - Security Objectives for the TOE

4.2 Security Objectives for the Environment

The security objectives for the TOE environment are those specified in the table below.

Name	Description
OE.INSTALL	Those responsible for the operation of the TOE must ensure that: (a) The TOE is delivered, installed and operated in a manner that preserves IT security. (b) The underlying operating system and / or network services are installed and operated in accordance with the operational documentation for the relevant products.
OE.PHYSICAL	Those responsible for the operation of the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack that might compromise TOE security functions.
OE.FIREWALL	Those responsible for the operation of the TOE must ensure that the TOE is protected from network-based attacks that might compromise TOE security functions.
OE.CRYPTOMANAGE	Those responsible for the TOE must ensure that procedures and / or mechanisms are in place to ensure that storage and handling of cryptographic-related IT assets is conducted in accordance with the rules defined by the P.CRYPTO policy.
OE.TRUST	Those responsible for the TOE must ensure that only highly trusted users are given privileges that enable them to: (a) Set or alter the audit trail configuration. (b) Create or modify user roles. (c) Load or modify crypto-variables.
OE.ENTRY-NON-TECHNICAL	The TOE environment must provide sufficient protection against non-technical attacks, such as social engineering attacks.
OE.TRAINING	Those responsible for the TOE must ensure that all personnel given administrator privileges or who are to perform crypto-custodian duties are given training sufficient to enable them to fulfill their duties securely.
OE.SPILLAGE	TOE administrators must ensure that the system is configured to encrypt user connections as the default. If for operational reasons 'no-encryption' is required as the default operating mode, the TOE administrators must ensure that users are aware of this fact and do not send or request any sensitive material.
OE.NO-USER-CODE	TOE administrators must ensure that the TOE environment is such that there are no user-accessible code that could be used to bypass TOE security functions.
OE.PLATFORM	TOE administrators must ensure that they follow the developer's instructions and use the NT User Manager to establish the proper environment for controlling the configuration of the TOE.

Table 8 - Security Objectives for the Environment

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section contains the functional requirements for the TOE. The functional requirements are listed in summary form in Table 9, below.

No.	Component	Component Name
Class FAU: Audit		
1	FAU_GEN.1	Audit data generation
2	FAU_GEN.2	User identity association
3	FAU_STG.2	Guarantees of Audit Availability
Class FCS: Cryptographic Support		
4	FCS_CKM.1	Cryptographic key generation
5	FCS_CKM.2	Cryptographic key distribution
6	FCS_CKM.4	Cryptographic key destruction
7	FCS_COP.1	Cryptographic operation
Class FDP: User Data Protection		
8	FDP_ACC.2	Complete access control
9	FDP_ACF.1	Security Attribute Access control
10	FDP_IFC.1	Subset information flow control
11	FDP_IFF.1	Simple security attributes
12	FDP_ITC.1	Import of User Data Without Security Attributes
13	FDP_ITT.1	Basic internal transfer protection
14	FDP_ITT.3	Integrity monitoring
Class FIA: Identification and Authentication		
15	FIA_ATD.1	User attribute definition
16	FIA_UID.1	Timing of identification
17	FIA_UAU.1	Timing of authentication
18	FIA_UAU.6	Re-authenticating
Class FMT: Security Management		
19	FMT_MSA.1	Management of security attributes
20	FMT_MSA.2	Secure security attributes
21	FMT_MSA.3	Static attribute initialisation
22	FMT_MTD.1	Management of TSF data
23	FMT_SMR.1	Security roles
Class FPT: Protection of the TOE Security Functions		
24	FPT_ITT.2	TSF data transfer separation
25	FPT_ITT.3	TSF data integrity monitoring
26	FPT_RVM.1	Non-bypassability of the TSP
27	FPT_SEP.2	SFP domain separation
28	FPT_STM.1	Reliable time stamps

Table 9 - Functional Components

The following sections contain the functional components from the Common Criteria (CC) Part 2 with the operations completed. The standard CC text is in regular font; the text inserted by the Security Target (ST) author is in italic font enclosed in brackets.

5.1.1 Security audit (FAU)

Audit data generation (FAU_GEN.1)

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *detailed* level of audit; and

c) All auditable events as described in the [SA-1 security function].

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 ST, [SA-1 security function].

Dependencies: FPT_STM.1 Reliable time stamps

User identity association (FAU_GEN.2)

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

Guarantees of audit data availability (FAU_STG.2)

Hierarchical FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised 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 [all recorded] audit records will be maintained when the following conditions occur: *audit storage exhaustion*.

Dependencies FAU_GEN.1 Audit data generation

5.1.2 Cryptographic support (FCS)

Cryptographic key generation (FCS_CKM.1)

Hierarchical to: No other components.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Triple DES (3DES)] and specified cryptographic key sizes [168] that meet the following: [requirements for cryptographic key generation, as defined by the national COMSEC authority, DSD].

Dependencies FCS_COP.1 Cryptographic operation

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Cryptographic key distribution (FCS_CKM.2)

Hierarchical to: No other components.

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [Diffie-Hellman] that meets the following: [PKCS#3; and requirements for cryptographic key distribution as defined by the national COMSEC authority, DSD].

Dependencies FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

Cryptographic key destruction (FCS_CKM.4)

Hierarchical to: No other components.

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite] that meets the following: [requirements for cryptographic key destruction as defined by the national COMSEC authority, DSD].

Dependencies FCS_CKM.1 Cryptographic key generation
FMT_MSA.2 Secure security attributes

Cryptographic operation (FCS_COP.1)

Hierarchical to: No other components.

FCS_COP.1.1 The TSF shall perform [

a) cryptographic key generation;
b) data encryption and decryption;
c) cryptographic key encryption and decryption;
d) digital signature verification;
e) secure hash;
f) cryptographic key agreement]

in accordance with a specified cryptographic algorithm [

a) triple DES (3DES);
b) triple DES (3DES);
c) RSA;
d) RSA;
e) MD5;
f) Diffie-Hellman]

and cryptographic key sizes [

a) 168;
b) 168;
c) 1024,
d) 1024;
e) N/A;
f) 512]

.that meet the following: [requirements for cryptographic key management (generation, distribution & destruction) as defined by the national COMSEC authority, DSD and as re-iterated in the TOE Usage Notes].

Dependencies FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction
FMT_MSA.2 Secure security attributes

5.1.3 User data protection (FDP)

Complete access control (1) (FDP_ACC.2 (1))

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 (1) The TSF shall enforce the [Access Control (Proxy) SFP] on [

a) Subject: application client;
b) object: protected host applications data;
c) operation: access.]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (1) The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

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

Complete access control (2) (FDP_ACC.2 (2))

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 (2) The TSF shall enforce the [Access Control (Client) SFP] on [

a) subject: client application user;
b) object: user's private key;
c) operation: access]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (2) The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies FDP_ACF.1 (2) Security attribute based access control

Complete access control (3) (FDP_ACC.2 (3))

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 (3) The TSF shall enforce the [System Security Management SFP] on [

a) subject: authorised administrators
b) object: proxy configuration data, audit file data, X.500 directory data
c) operation: access and change]

and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 (3) The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies FDP_ACF.1 (3) Security attribute based access control

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

Hierarchical to: No other components.

FDP_ACF.1.1 (1) The TSF shall enforce the [Access Control (Proxy) SFP] to **target application hosts** based on [

a) source IP address;

b) user X.509 certificate attributes;

c) time of day].

FDP_ACF.1.2 (1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. Deny all access to protected applications hosts unless the requesting user's security attributes match those as defined for the requested proxy (host / service combination) and that access, based on such a match, is allowed.]

FDP_ACF.1.3 (1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (1) The TSF shall explicitly deny access of subjects to objects based on the rules: [none].

Dependencies FDP_ACC.2 (1) Complete access control (hierarchical to FDP_ACC.1)

FMT_MSA.3 (1) Static attribute initialisation

ITENV.1

ITENV.2

Security attribute based access control (2) (FDP_ACF.1 (2))

Hierarchical to: No other components.

FDP_ACF.1.1 (2) The TSF shall enforce the [Access Control (Client) SFP] on the **user private key** based on [user identity].

FDP_ACF.1.2 (2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. Deny all access to the container holding the user private key unless the user can provide the correct password.]

FDP_ACF.1.3 (2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (2) The TSF shall explicitly deny access of subjects to objects based on the rules: [none]

Dependencies FDP_ACC.2 (2) Complete access control (hierarchical to FDP_ACC.1)

ITENV.1

ITENV.2

Security attribute based access control (3) (FDP_ACF.1 (3))

Hierarchical to: No other components.

FDP_ACF.1.1 (3) The TSF shall enforce the [System Security Management SFP] on the [

a) proxy configuration data,

b) audit file data,

c) X.500 directory data]

based on [administrator identity].

FDP_ACF.1.2 (3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

1. Deny all access to the proxy configuration data, audit file data, X.500 directory data unless the administrator can provide the correct password
2. Deny all change to the proxy configuration data and X.500 directory definition data unless the administrator can provide the correct password.]

FDP_ACF.1.3 (3) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (3) The TSF shall explicitly deny access of subjects to objects based on the rules: [none].

Dependencies FDP_ACC.2 (3) Complete access control (hierarchical to FDP_ACC.1)

FMT_MSA.3 (1) Static attribute initialisation

ITENV.1

ITENV.2

Subset information flow control (1) (FDP_IFC.1 (1))

Hierarchical to: No other components.

FDP_IFC.1.1 (1) The TSF shall enforce the [Information Flow Control SFP] on [

a) Subject: KyberPASS-protected applications host;
b) object: IP packets;
c) operation: release from subject to user client application]

Dependencies FDP_IFF.1 (1) Simple security attributes

ITENV.2

Subset information flow control (2) (FDP_IFC.1 (2))

Hierarchical to: No other components.

FDP_IFC.1.1 (2) The TSF shall enforce the [TSF Data Import and Export SFP] on [

a) subject: KyberPASS Authentication server;
b) object: proxy session key;
c) operation: transfer to the KyberWIN client]

Dependencies FDP_IFF.1 (2) Simple security attributes

ITENV.2

Subset information flow control (3) (FDP_IFC.1 (3))

Hierarchical to: No other components.

FDP_IFC.1.1 (3) The TSF shall enforce the [Secure Packet Transfer SFP] on [

a) subjects: KyberPASS Authentication server and client application;
b) object: data packets;
c) operation: protection from disclosure or change].

Dependencies FDP_IFF.1 (3) Simple security attributes

ITENV.2

Simple security attributes (1) (FDP_IFF.1 (1))

Hierarchical to: No other components.

FDP_IFF.1.1 (1) The TSF shall enforce the [Information Flow Control SFP] based on the following types of subject and information security attributes: [

a) IP address of the connection requestor;
b) IP address of the target host;
c) type of service requested;
d) proxy allowed]

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

If proxy (secure connection between requestor and target host) established, release the IP packet.]

FDP_IFF.1.3 (1) The TSF shall enforce [no additional information flow control SFP rules].

FDP_IFF.1.4 (1) The TSF shall provide [no additional information flow control SFP capabilities].

FDP_IFF.1.5 (1) The TSF shall explicitly authorise an information flow based on the following rules:[no additional rules].

FDP_IFF.1.6 (1) The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies FDP_IFC.1 (1) Subset information flow control

FMT_MSA.3 (1) Static attribute initialisation

FMT_MSA.3 (2) Static attribute initialisation

ITENV.1

ITENV.2

Simple security attributes (2) (FDP_IFF.1 (2))

Hierarchical to: No other components.

FDP_IFF.1.1 (2) The TSF shall enforce the [TSF Data Import and Export SFP] based on [

a) the private authentication key belonging to the KyberPASS Authentication server
b) the private authentication key belonging to the KyberWIN client]

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

1. If the private authentication keys of the KyberWIN client and the KyberPASS Authentication server successfully exchanged, generate and exchange the Hydra session key using the Diffie-Hellman mechanism.]

FDP_IFF.1.3 (2) The TSF shall enforce [no additional information flow control SFP rules].

FDP_IFF.1.4 (2) The TSF shall provide [no additional information flow control SFP capabilities].

FDP_IFF.1.5 (2) The TSF shall explicitly authorise an information flow based on the following rules:[no additional rules].

FDP_IFF.1.6 (2) The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies FDP_IFC.1 (2) Subset information flow control

FMT_MSA.3 (1) Static attribute initialisation

FMT_MSA.3 (2) Static attribute initialisation

ITENV.1

ITENV.2

Simple security attributes (3) (FDP_IFF.1 (3))

Hierarchical to: No other components.

FDP_IFF.1.1 (3) The TSF shall enforce the [Secure Packet Transfer SFP] based on [the proxy establishment connection rules].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

1. If the KyberPASS Authentication server connection rules specify packet encryption, encrypt all packets with the Hydra session key.
2. If the KyberPASS Authentication server connection rules specify packet integrity, generate an MD5 digest for all packets exchanged and ensure that each packet is verified by its recipient, through reference to the digest.]

FDP_IFF.1.3 (3) The TSF shall enforce [no additional information flow control SFP rules].

FDP_IFF.1.4 (3) The TSF shall provide [no additional information flow control SFP capabilities].

FDP_IFF.1.5 (3) The TSF shall explicitly authorise an information flow based on the following rules:[no additional rules].

FDP_IFF.1.6 (3) The TSF shall explicitly deny an information flow based on the following rules: [none].

Dependencies FDP_IFC.1 (3) Subset information flow control

FMT_MSA.3 (1) Static attribute initialisation

ITENV.1

ITENV.2

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

Hierarchical to: No other components.

FDP_ITC.1.1 The TSF shall enforce the [TSF Data Import & Export SFP] when importing user data, controlled under the SFP, from outside of the TSC.

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:[None].

Dependencies FDP_IFC.1 (2) Subset information flow control

FMT_MSA.3 (2) Static attribute initialisation

Basic internal transfer protection (FDP_ITT.1)

Hierarchical to: No other components.

FDP_ITT.1.1 The TSF shall enforce the [Secure Packet Transfer SFP] to prevent the *disclosure* of user data when it is transmitted between physically-separated parts of the TOE.

Dependencies FDP_IFC.1 (3) Subset information flow control

Integrity monitoring (FDP_ITT.3)

Hierarchical to:	No other components.
FDP_ITT.3.1	The TSF shall enforce the [Secure Packet Transfer SFP] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [integrity errors].
FDP_ITT.3.2	Upon detection of a data integrity error, the TSF shall [request re-transmission of the packet].
Dependencies	FDP_IFC.1 (3) Subset information flow control FDP_ITT.1 Basic internal transfer protection

5.1.4 Identification and authentication (FIA)

User attribute definition (FIA_ATD.1)

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [a) X509 identity certificate; b) User private cryptographic key; c) User private key initiator password].
Dependencies	No dependencies

Timing of authentication (FIA_UAU.1)

Hierarchical to:	No other components.
FIA_UAU.1.1	The TSF shall allow [1. A user to attempt to connect to a **target application server** using a TCP/IP service. 2. The KyberPASS security server to accept the connection request and send a challenge back to the user. 3. KyberWIN to intercept the challenge and to prompt the user to identify and authenticate himself with a private key and password. 4. KyberWIN to use the private key to digitally sign a logon request and send it to the KyberPASS security server. 5. KyberPASS security server to search its X.500 directory and retrieve the user's public key, to validate the digital signature, confirm the user's access authority and to send a secure session ticket to KyberWIN] On behalf of the user to be performed before the user is authenticated **to the protected server**.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies	FIA_UID.1 Timing of identification

Re-authenticating (FIA_UAU.6)

Hierarchical to:	No other components.
FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions[1. 'logon renewal' - if the connection time exceeds the maximum time permitted since the user was last formally authenticated. 2. Logoff after inactivity period - if there has been no mouse or keyboard activity for a specified period of time].
Dependencies	No dependencies

Timing of identification (FIA_UID.1)

Hierarchical to:	No other components.
FIA_UID.1.1	The TSF shall allow [1. A user to attempt to connect to a protected server using a TCP/IP service. 2. The KyberPASS security server to accept the connection request and send a challenge back to the user. 3. KyberWIN to intercept the challenge and to prompt the user to identify himself with a private key and password.] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies	No dependencies

5.1.5 Security management (FMT)

Management of security attributes (1) (FMT_MSA.1 (1))

Hierarchical to:	No other components.
FMT_MSA.1.1 (1)	The TSF shall enforce the [Access Control (Proxy) SFP] to restrict the ability to *modify* [add, change or delete] the security attributes [Subject KyberPASS Authentication Server proxy attributes] to [authorised system administrators].
Dependencies	FDP_ACC.1 (1) Subset access control FMT_SMR.1 Security roles ITENV.1 ITENV.2

Management of security attributes (2) (FMT_MSA.1 (2))

Hierarchical to: No other components.

FMT_MSA.1.1 (2) The TSF shall enforce the [System Security Management SFP] to restrict the ability to *modify* [add, change or delete] the security attributes [

a) User attributes: (X.509 certificate);

b) Subject (KyberPASS Authentication Server) attributes: (those required to define the information flows]

to [authorised system administrators].

Dependencies FDP_ACC.1 (3) Subset access control

FMT_SMR.1 Security roles

ITENV.1

ITENV.2

Secure security attributes (FMT_MSA.2)

Hierarchical to: No other components.

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies ADV_SPM.1 Informal TOE security policy model

FDP_ACC.1 (1) Subset access control

FMT_MSA.1 (1) Management of security attributes

FMT_MSA.1 (2) Management of security attributes

FMT_SMR.1 Security roles

Static attribute initialisation (1) (FMT_MSA.3 (1))

Hierarchical to: No other components.

FMT_MSA.3.1 (1) The TSF shall enforce the [Access Control (Proxy) SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (1) The TSF shall allow the [authorised administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies FMT_MSA.1 (1) Management of security attributes

FMT_SMR.1 Security roles

Static attribute initialisation (2) (FMT_MSA.3 (2))

Hierarchical to: No other components.

FMT_MSA.3.1 (2) The TSF shall enforce the [Information Flow Control SFP] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (2) The TSF shall allow the [authorised administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies FMT_MSA.1 (2) Management of security attributes

FMT_SMR.1 Security roles

Management of TSF data (1) (FMT_MTD.1 (1))

Hierarchical to:	No other components.
FMT_MTD.1.1 (1)	The TSF shall restrict the ability to *modify* [change] the [a) system configuration b) TOE security attributes] to [authorised administrators].
Dependencies	FMT_SMR.1 Security roles ITENV.1 ITENV.2

Management of TSF data (2) (FMT_MTD.1 (2))

Hierarchical to:	No other components.
FMT_MTD.1.1 (2)	The TSF shall restrict the ability to *modify* [change] the [user private key initiator (password)] to [authorised users].
Dependencies	FMT_SMR.1 Security roles ITENV.1 ITENV.2

Security roles (FMT_SMR.1)

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [administrator and user].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies	FIA_UID.1 Timing of identification

5.1.6 Protection of the TOE Security Functions (FPT)

TSF data transfer separation (FPT_ITT.2)

Hierarchical to:	FPT_ITT.1
FPT_ITT.2.1	The TSF shall protect TSF data from *disclosure*, when it is transmitted between separate parts of the TOE.
FPT_ITT.2.2	The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE.
Dependencies	No dependencies

TSF data integrity monitoring (FPT_ITT.3)

Hierarchical to:	No other components.
FPT_ITT.3.1	The TSF shall be able to detect [modification of data] for TSF data transmitted between separate parts of the TOE.
FPT_ITT.3.2	Upon detection of a data integrity error, the TSF shall take the following actions: [a) Resend b) Session termination.]
Dependencies	FPT_ITT.1 Basic internal TSF data transfer protection

Non-bypassability of the TSP (FPT_RVM.1)

Hierarchical to:	No other components
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.
Dependencies	No dependencies

SFP domain separation (FPT_SEP.2)

Hierarchical to:	FPT_SEP.1
FPT_SEP.2.1	The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. **Note**: The TSF shall maintain its own security domain for the protection of: [the Authentication Server's private key and the temporary cryptographic keys established for a proxy, ie the Hydra session key and the secure session ticket.]
FPT_SEP.2.2	The TSF shall enforce separation between the security domains of subjects in the TSC.
FPT_SEP.2.3	The TSF shall maintain the part of the TSF related to the [Access Control SFP and the Information Flow SFP] in a security domain for their own execution that protects them from interference and tampering by the remainder of the TSF and by subjects untrusted with respect to those SFPs.
Dependencies	No dependencies

Reliable time stamps (FPT_STM.1)

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies	No dependencies

5.2 TOE Security Assurance Requirements

This section contains the assurance requirements for the TOE. The assurance requirements are listed in summary form in Table 10, below.

No.	Component	Component Name
Class ACM: Configuration management		
1	ACM_CAP.1	CM capabilities
Class ADV: Development		
2	ADV_RCR.1	Representation correspondence
3	ADV_FSP.1	Functional specification
Class ADO: Delivery and operation		
4	ADO_IGS.1	Installation, generation and start-up
Class ATE: Tests		
5	ATE_IND.1	Independent testing
Class AGD: Guidance documents		
6	AGD_ADM.1	Administrator guidance
7	AGD_USR.1	User guidance

Table 10 - TOE Assurance Requirements

5.2.1 Configuration management (ACM)

Version numbers (ACM_CAP.1)

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.1.1D The developer shall provide a reference for the TOE.

ACM_CAP.1.2C The TOE shall be labeled with its reference.

5.2.2 Delivery and operation (ADO)

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)

Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.

Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1C	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.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.2.4 Guidance documents (AGD)

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 behaviour 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.

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 behaviour 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 Tests (ATE)

Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1C	The TOE shall be suitable for testing.
ATE_IND.1.1D	The developer shall provide the TOE for testing.

5.3 Security Requirements for the IT Environment

The TOE has the following security requirements allocated to its IT and Non-IT environment.

ITENV.1 KyberPASS Configuration Manager for Setting User Attributes

KyberPASS relies on the Configuration Manager to configure the system by setting user attributes. Configuration Manager relies, in turn, on the Windows NT operating system to provide this capability. The KyberPASS Administrator Guide suggests the creation of two NT accounts (administrator and a local operator) through the User Manager mechanism of the NT Security Subsystem.

ITENV.2 KyberPASS Configuration Manager for Modifying TSF Data

KyberPASS relies on the Configuration Manager to protect the system by establishing the TSF data and controlling changes to it. Configuration Manager relies, in turn, on the Windows NT operating system to provide this capability via the NT Security Subsystem.

5.4 Security Requirements for the Non-IT Environment

NONITENV.1 KyberPASS Server protected by Firewall.

The KyberPASS Server must be protected from unauthorised modification by potentially hostile outsiders by a firewall of at least EAL-2 level of assurance, or equivalent.

NONITENV.2 KyberPASS Server is to be Physically Protected.

The KyberPASS Server must be located within a controlled access facility that will prevent unauthorised physical access.

NONITENV.3 Access to the KyberPASS Server is restricted to administrators only.

The KyberPASS Server and associated directly-attached console must be physically secure and available to authorised administrators only.

NONITENV.4 Protection against non-technical attacks.

The TOE environment must provide sufficient protection against non-technical attacks, such as social-engineering attacks.

NONITENV.5 Protection against spillage of sensitive data.

The TOE environment must provide the ability to warn users that session encryption has been defaulted to 'off' and to use their judgement over what material is to be sent over the communications line.

NONITENV.6 KyberPASS Server administrators are trusted.

The TOE environment must provide a mechanism that ensures that the likelihood of administration staff perform illegal actions is minimised.

NONITENV.7 KyberPASS Server has no user-accessible code.

The TOE environment must ensure that at any time no user-accessible code that may modify TOE security functions exists on the KyberPASS Server.

NONITENV.8 KyberPASS Server is installed and configured according to developer guidance.

The KyberPASS Server must be installed and configured in line with the developer's guidance and administrators must ensure that the configuration remains in step with developer's ongoing guidance.

NONITENV.9 Protection against unauthorised access to / loss of cryptographic keys.

The TOE environment must ensure that at all times cryptographic keys are protected against unauthorised access, loss or destruction.

NONITENV.10 KyberPASS Server administrators are well-trained.

The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

NONITENV.11 Cryptographic Services Strength of Function (SOF) Requirement

KyberPASS relies on a GATEKEEPER-compliant CA product to meet the SOF requirement for the public / private key cryptographic services that it uses.

6 PP Claims

The KyberPASS with Hydra 3DES encryption Security Target was not written to address any existing Protection Profile.

7 Rationale

7.1 Security Objectives Rationale

The purpose of this rationale is to demonstrate that the identified security objectives are *suitable*, that is they are *sufficient* to address the security needs, and that they are *necessary*, ie, there are no redundant security objectives.

7.1.1 All Assumptions, Policies and Threats Addressed

The need to demonstrate that there are no redundant security objectives is satisfied as follows:

- The first section (tables 11-13) shows that all of the secure usage assumptions, organisational security policies, and threats to security have been addressed.
- The second section shows that each IT security objective and each Non-IT security objective counters at least one assumption, policy, or threat.

Threat Label	Threat Short Description	Associated Security Objective
T.ABUSE	Abuse of privilege	O.AUDIT O.DAC OE.TRUST
T.ACCESS	Unauthorised access to the TOE	O.SEPARATION O.DAC O.RBAC OE.CRYPTOMANAGE
T.ATTACK	Unauthorised action.	O.DAC O.BYPASS O.I&A OE.PHYSICAL OE.FIREWALL OE.NO-USER-CODE
T.AUDIT-CONFIDENTIALITY	Disclosure of audit record.	O.RBAC
T.AUDIT-CORRUPTED	Unauthorised modification of audit records.	O.INTEGRITY
T.CAPTURE	Eavesdrop on information transfer.	O.DATA-CONFIDENTIALITY O.KEY-CONFIDENTIALITY OE.SPILLAGE OE.CRYPTOMANAGE
T.DENY	Repudiation of information transfer.	O.AUDIT O.NOREPUD
T.ERROR	Unauthorised disclosure.	O.SEPARATION OE.CRYPTOMANAGE
T.IMPERSON	Impersonation of an authorised user.	O.I&A OE.CRYPTOMANAGE
T.INTEGRITY	Compromise of information integrity	O.MESSAGE-INTEGRITY
T.MIX	Mixing of plaintext and cyphertext.	O.DATA-CONFIDENTIALITY O.INFO-FLOW
T.MODIFY	Unauthorised information modification or destruction	O.INTEGRITY O.ADMIN
T.RECORD-EVENT	Security-relevant events may not be recorded.	O.AUDIT
T.RESOURCES	Exhaustion of internal system resources.	O.RESOURCES
T.TRACEABLE	Security-relevant events may not be traceable.	O.AUDIT
TE.ADMIN-ERROR	Compromise due to administration errors and omissions.	OE.TRAINING
TE.ENTRY-NON-TECHNICAL	Compromise through non-technical means.	OE.ENTRY-NON-TECHNICAL
TE.INSTALL	Incorrect delivery or installation.	OE.TRAINING OE.INSTALL
TE.OPERATE	Compromise due to improper operation	OE.TRAINING OE.PLATFORM

Table 11 - All Threats to Security Addressed by Objectives

Policy Label	Policy Short Description	Associated Security Objective
P.AUDIT	IT usage must be recorded and preserved.	O.AUDIT
P.CRYPTO	Cryptographic material must be subject to rigorous control.	O.KEY-CONFIDENTIALITY O.ADMIN
P.NETWORK	IT security policy must be maintained in a distributed environment.	O.NETWORK
P.INFO-FLOW	Information flow controlled and protected from disclosure.	O.INFO-FLOW
P.USER-DUE-CARE	Users must protect their authenticators.	OE.PHYSICAL OE.ENTRY-NON-TECHNICAL

Table 12 - All Organisational Policies met by Objectives

Assumption Label	Assumption Short Description	Associated Security Objective
A.ATTACK	Attackers have high levels of skill.	OE.INSTALL OE.PHYSICAL OE.FIREWALL
A.FIREWALL	Approved firewall to protect facility.	OE.FIREWALL
A.PHYSICAL	NT workstation protected by strong physical safeguards	OE.PHYSICAL
A.PLATFORM	TOE depends on the NT operating system for security management functions	O.ADMIN O.DAC OE.PLATFORM
A.SPILLAGE	User judgement required when encryption function not invoked	O.DATA-CONFIDENTIALITY O.ADMIN OE.SPILLAGE
A.NO-USER-CODE	No user-accessible code in TOE	O.DAC O.RBAC OE.NO-USER-CODE
A.NOEVIL	Administrators are non-hostile.	O.KEY-CONFIDENTIALITY OE.TRUST

Table 13 - All Secure Usage Assumptions met by Objectives

Table 14 shows that there are no unnecessary IT security objectives.

Objective Label	Objective Short Description	Threat / Policy/ Assumption
O.ADMIN	Facilities provided to manage the TOE.	P.CRYPTO T.MODIFY A.PLATFORM A.SPILLAGE
O.AUDIT	Facilities to be provided to record activity on the TOE.	T.RECORD-EVENT T.TRACEABLE T.ABUSE T.DENY P.AUDIT
O.DAC	Facilities to be provided to control access to objects.	T.ATTACK T.ABUSE T.ACCESS A.PLATFORM A.NO-USER-CODE
O.DATA-CONFIDENTIALITY	Facilities to be provided to protect data in transit.	T.MIX T.CAPTURE A.SPILLAGE
O.I&A	Facilities to be provided to identify all users.	T.IMPERSON T.ATTACK
O.INFO-FLOW	Facilities to be provided to enforce flow policies.	T.MIX P.INFO-FLOW
O.INTEGRITY	Facilities to be provided to prevent loss of data integrity.	T.MODIFY T.AUDIT-CORRUPTED
O.KEY-CONFIDENTIALITY	Facilities to be provided to protect cryptographic keys.	P.CRYPTO T.CAPTURE A.NOEVIL

Objective Label	Objective Short Description	Threat / Policy/ Assumption
O.MESSAGE-INTEGRITY	Facilities to be provided to detect message integrity loss.	T.INTEGRITY
O.NETWORK	Security objectives to be met in a distributed environment.	P.NETWORK
O.NOREPUD	Facilities to be provided to prevent repudiation of data sent.	T.DENY
OE.TRAINING	Operators are given sufficient training to perform their duties	TE.INSTALL TE.OPERATE TE.ADMIN-ERROR
O.RBAC	Facilities to be provided to prevent unauthorised user activities.	T.ACCESS T.AUDIT-CONFIDENTIALITY A.NO-USER-CODE
O.BYPASS	No bypass of policy enforcement	T.ATTACK
O.SEPARATION	Maintenance of TOE security domain.	T.ERROR T.ACCESS
O.RESOURCES	Shared resource exhaustion.	T.RESOURCES
OE.PHYSICAL	Protected from physical attack.	T.ATTACK P.USER-DUE-CARE A.ATTACK A.PHYSICAL
OE.ENTRY-NON-TECHNICAL	Protection against non-technical attacks.	P.USER-DUE-CARE TE.ENTRY-NON-TECHNICAL
OE.INSTALL	TOE installed and operated properly	TE.INSTALL A.ATTACK
OE.FIREWALL	TOE protected from network attacks	T.ATTACK A.ATTACK A.FIREWALL
OE.CRYPTOMANAGE	Crypto assets managed properly	T.ACCESS T.CAPTURE T.ERROR T.IMPERSON
OE.TRUST	Administrators are highly trusted	T.ABUSE A.NOEVIL
OE.SPILLAGE	System is configured with session encryption as default	T.CAPTURE A.SPILLAGE
OE.NO-USER-CODE	No user-accessible code in the TOE operating environment	A.NO-USER-CODE T.ATTACK
OE.PLATFORM	Administrator will operate the server function in line with developer's guidance	TE.OPERATE A.PLATFORM

Table 14 - All Security Objectives Necessary

7.2 Security Requirements Rationale

7.2.1 Suitability of the Security Requirements

The purpose of this section is to show that the identified security requirements are *suitable* to meet the security objectives. Tables 15, 16 and 17 show that each security requirement (and SFRs in particular) is *necessary*, that is, each security objective is addressed by at least one security requirement and vice versa. Note that several objectives are partially satisfied by the TOE and partially satisfied by the IT environment. Security Objectives for the TOE are satisfied by Common Criteria functional components. Security Objectives for the Environment are satisfied by IT requirements for the environment (ITENV.n and NONITENV.x).

Objectives	Requirements
O.ADMIN	FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.2, FMT_MSA.3 (1), FMT_MSA.3 (2), FMT_MTD.1 (1), FMT_SMR.1, ITENV.1, ITENV.2
O.AUDIT	FAU_GEN.1, FAU_GEN.2, FAU_STG.2, ITENV.1
O.BYPASS	FPT_RVM.1
O.DAC	FDP_ACC.2 (1), FDP_ACC.2 (2), FDP_ACF.1 (1), FDP_ACF.1 (2), ITENV.1, ITENV.2
O.DATA-CONFIDENTIALITY	FCS_COP.1, FDP_IFC.1 (3), FDP_IFF.1 (3)
O.I&A	FIA_ATD.1, FIA_UAU.1, FIA_UAU.6, FIA_UID.1
O.INFO-FLOW	FDP_IFC.1 (1), FDP_IFC.1 (2), FDP_IFF.1 (1), FDP_IFF.1 (2), FDP_ITC.1, FPT_SEP.2
O.INTEGRITY	FDP_ITT.3
O.KEY-CONFIDENTIALITY	FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FDP_ITC.1, FMT_SMR.1, FDP_IFC.1 (2), FDP_IFF.1 (2), FMT_MTD.1 (2)
O.MESSAGE-INTEGRITY	FCS_COP.1, FDP_IFC.1 (3), FDP_IFF.1 (3)
O.NETWORK	FPT_ITT.2, FPT_ITT.3, FDP_ITT.1, FPT_SEP.2
O.NOREPUD	FAU_GEN.1, FAU_GEN.2, FPT_STM.1, FCS_COP.1, ITENV.1
O.RBAC	FDP_ACF.1 (3), FDP_ACC.2 (3), FIA_UID.1, FMT_SMR.1, ITENV.2, NONITENV.3
O.SEPARATION	FPT_SEP.2
O.RESOURCES	FAU_STG.2
OE.INSTALL	NONITENV.8
OE.PHYSICAL	NONITENV.2, NONITENV.3
OE.FIREWALL	NONITENV.1
OE.CRYPTOMANAGE	NONITENV.9, NONITENV.11
OE.TRUST	NONITENV.6
OE.ENTRY-NON-TECHNICAL	NONITENV.4
OE-TRAINING	NONITENV.10
OE.SPILLAGE	NONITENV.5
OE.NO-USER-CODE	NONITENV.7
OE.PLATFORM	ITENV.1, ITENV.2

Table 15 - Security Objective to Functional Component Mapping

Component	Component Name	Objective
FAU_GEN.1	Audit data generation	O.AUDIT O.NOREPUD
FAU_GEN.2	User identity association	O.AUDIT O.NOREPUD
FAU_STG.2	Guarantees of Audit Availability	O.AUDIT O.RESOURCES
FDP_ITC.1	Import of User Data Without Security Attributes	O.INFO-FLOW O.KEY-CONFIDENTIALITY
FDP_ACC.2 (1)	Complete access control (1)	O.DAC
FDP_ACC.2 (2)	Complete access control (2)	O.DAC
FDP_ACC.2 (3)	Complete access control (3)	O.RBAC
FDP_ACF.1 (1)	Security Attribute Access control (1)	O.DAC
FDP_ACF.1 (2)	Security Attribute Access control (2)	O.DAC
FDP_ACF.1 (3)	Security Attribute Access control (3)	O.RBAC
FDP_IFC.1 (1)	Subset information flow control (1)	O.INFO-FLOW
FDP_IFC.1 (2)	Subset information flow control (2)	O.INFO-FLOW O.KEY-CONFIDENTIALITY
FDP_IFC.1 (3)	Subset information flow control (3)	O.MESSAGE-INTEGRITY O.DATA-CONFIDENTIALITY
FDP_IFF.1 (1)	Simple security attributes (1)	O.INFO-FLOW
FDP_IFF.1 (2)	Simple security attributes (2)	O.INFO-FLOW O.KEY-CONFIDENTIALITY
FDP_IFF.1 (3)	Simple security attributes (3)	O.MESSAGE-INTEGRITY O.DATA-CONFIDENTIALITY
FDP_ITT.1	Basic internal transfer protection	O.NETWORK
FDP_ITT.3	Integrity monitoring	O.INTEGRITY
FIA_UID.1	Timing of identification	O.RBAC O.I&A
FIA_UAU.1	Timing of authentication	O.I&A
FIA_UAU.6	Re-authenticating	O.I&A
FIA_ATD.1	User attribute definition	O.I&A
FMT_MSA.1 (1)	Management of security attributes (1)	O.ADMIN
FMT_MSA.1 (2)	Management of security attributes (2)	O.ADMIN
FMT_MSA.2	Secure security attributes	O.ADMIN
FMT_MSA.3 (1)	Static attribute initialisation (1)	O.ADMIN
FMT_MSA.3 (2)	Static attribute initialisation (2)	O.ADMIN
FMT_MTD.1 (1)	Management of TSF data (1)	O.ADMIN
FMT_MTD.1 (2)	Management of TSF data (2)	O.KEY-CONFIDENTIALITY
FMT_SMR.1	Security roles	O.KEY-CONFIDENTIALITY O.RBAC O.ADMIN
FCS_CKM.1	Cryptographic key generation	O.KEY-CONFIDENTIALITY
FCS_CKM.2	Cryptographic key distribution	O.KEY-CONFIDENTIALITY
FCS_CKM.4	Cryptographic key destruction	O.KEY-CONFIDENTIALITY
FCS_COP.1	Cryptographic operation	O.DATA -CONFIDENTIALITY O.MESSAGE-INTEGRITY O.NOREPUD
FPT_ITT.2	TSF data transfer separation	O.NETWORK
FPT_ITT.3	TSF data integrity monitoring	O.NETWORK
FPT_RVM.1	Non-bypassability of the TSP	O.BYPASS
FPT_SEP.2	SFP domain separation	O.INFO-FLOW O.NETWORK O.SEPARATION
FPT_STM.1	Reliable time stamps	O.NOREPUD

Table 16 - Mapping of Functional Requirements to Security Objectives

Requirement Label	Requirement Name	Objective
ITENV.1	KyberPASS Configuration Manager for Setting User Attributes	O.ADMIN O.AUDIT O.DAC O.NOREPUD OE.PLATFORM
ITENV.2	KyberPASS Configuration Manager for Modifying TSF Data	O.ADMIN O.DAC O.RBAC OE.PLATFORM
NONITENV.1	KyberPASS Server protected by Firewall.	OE.FIREWALL
NONITENV.2	KyberPASS Server is to be Physically Protected.	OE.PHYSICAL
NONITENV.3	Access to the KyberPASS Server is restricted to administrators only.	OE.PHYSICAL O.RBAC
NONITENV.4	Protection against non-technical attacks.	OE.ENTRY-NON-TECHNICAL
NONITENV.5	Protection against spillage of sensitive data.	OE.SPILLAGE
NONITENV.6	KyberPASS Server administrators are trusted.	OE.TRUST
NONITENV.7	KyberPASS Server has no user-accessible code.	OE.NO-USER-CODE
NONITENV.8	KyberPASS Server is installed and configured according to developer guidance.	OE.INSTALL
NONITENV.9	Protection against unauthorised access to / loss of cryptographic keys.	OE.CRYPTOMANAGE
NONITENV.10	KyberPASS Server administrators are well-trained.	OE.TRAINING
NONITENV.11	Cryptographic Services Strength of Function (SOF) Requirement	OE.CRYPTOMANAGE

Table 17 - Mapping of Environment Requirements to Security Objectives

7.2.2 Satisfaction of Dependencies

Table 18 shows the dependencies between the functional requirements. All of the dependencies are satisfied. (Note that (H) indicates the dependency is satisfied through the inclusion of a component that is hierarchical to the one required).

Component Reference	Requirement	Dependencies	Dependency Reference
Functional Requirements			
1	FAU_GEN.1	FPT_STM.1	28
2	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	1, 18
3	FAU_STG.2	FAU_GEN.1	1
4	FCS_CKM.1	FCS_CKM.4, FCS_COP.1, FMT_MSA.2	6, 7, 20
5	FCS_CKM.2	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	4, 6, 20
6	FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	4, 20
7	FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	4, 6, 20
8a	FDP_ACC.2 (1)	FDP_ACF.1 (1)	9a
8b	FDP_ACC.2 (2)	FDP_ACF.1 (2)	9b
8c	FDP_ACC.2 (3)	FDP_ACF.1 (3)	9c
9a	FDP_ACF.1 (1)	FDP_ACC.1 (1), FMT_MSA.3 (1), ITENV.1, ITENV.2	8a(H), 21a, 29, 30
9b	FDP_ACF.1 (2)	FDP_ACC.1 (2), ITENV.1, ITENV.2	8b(H), 29, 30
9c	FDP_ACF.1 (3)	FDP_ACC.1 (3), FMT_MSA.3 (1), ITENV.1, ITENV.2	8c(H), 21a, 29, 30
10a	FDP_IFC.1 (1)	FDP_IFF.1 (1), ITENV.2	11a, 30
10b	FDP_IFC.1 (2)	FDP_IFF.1 (2), ITENV.2	11b, 30
10c	FDP_IFC.1 (3)	FDP_IFF.1 (3), ITENV.2	11c, 30
11a	FDP_IFF.1 (1)	FDP_IFC.1 (1), FMT_MSA.3 (1), FMT_MSA.3 (2), ITENV.1, ITENV.2	10a, 21a, 21b, 29, 30
11b	FDP_IFF.1 (2)	FDP_IFC.1 (2), FMT_MSA.3 (1), FMT_MSA.3 (2), ITENV.1, ITENV.2	10b, 21a, 21b, 29, 30
11c	FDP_IFF.1 (3)	FDP_IFC.1 (3), FMT_MSA.3 (1), ITENV.1, ITENV.2	10c, 21a, 29, 30
12	FDP_ITC.1	FDP_IFC.1 (2), FMT_MSA.3 (2)	10b, 21b
13	FDP_ITT.1	FDP_IFC.1 (3)	10c
14	FDP_ITT.3	FDP_ITT.1, FDP_IFC.1 (3)	10c, 13
15	FIA_ATD.1	No dependencies	
16	FIA_UAU.1	FIA_UID.1	18
17	FIA_UAU.6	No dependencies	
18	FIA_UID.1	No dependencies	
19a	FMT_MSA.1 (1)	FMT_SMR.1, FDP_ACC.1 (1), ITENV.1, ITENV.2	10a, 23, 29, 30
19b	FMT_MSA.1 (2)	FMT_SMR.1, FDP_ACC.1 (3), ITENV.1, ITENV.2	10c, 23, 29, 30
20	FMT_MSA.2	ADV_SPM.1, FDP_IFC.1 (1), FMT_MSA.1 (1), FMT_MSA.2 (2), FMT_SMR.1	10a, 19a, 19b, 23
21a	FMT_MSA.3 (1)	FMT_MSA.1 (1), FMT_SMR.1	19a, 23
21b	FMT_MSA.3 (2)	FMT_MSA.1 (2), FMT_SMR.1	19b, 23
22a	FMT_MTD.1 (1)	FMT_SMR.1, ITENV.1, ITENV.2	23, 29, 30
22b	FMT_MTD.1 (2)	FMT_SMR.1, ITENV.1, ITENV.2	23, 29, 30
23	FMT_SMR.1	FIA_UID.1	18
24	FPT_ITT.2	No dependencies	
25	FPT_ITT.3	FPT_ITT.1	13
26	FPT_RVM.1	No dependencies	

Component Reference	Requirement	Dependencies	Dependency Reference
27	FPT_SEP.2	No dependencies	
28	FPT_STM.1	No dependencies	
29	ITENV.1	No dependencies	
30	ITENV.2	No dependencies	
31	ACM_CAP.1	No dependencies	
32	ADO_IGS.1	AGD_ADM.1	35
33	ADV_FSP.1	ADV_RCR.1	34
34	ADV_RCR.1	No dependencies	
35	AGD_ADM.1	ADV_FSP.1	33
36	AGD_USR.1	ADV_FSP.1	33
37	ATE_IND.1	AGD_USR.1, ADV_FSP.1, AGD_ADM.1	36, 31, 35

Table 18 - Functional and Assurance Requirements Dependencies

The following dependency is not satisfied in this Security Target because it is not considered relevant:

- ADV_SPM.1 is not an EAL1 assurance component and therefore this dependency has been omitted.

7.2.3 Strength of function claims

Consequent upon the factors just outlined above and the fact that the EAL-1 assurance level does not mandate the AVA_SOF SAR, the TOE makes no Strength of Function claims.

7.3 Rationale for Extensions

Not applicable.

7.4 PP Claims Rationale

Not applicable.

8 Appendix A - Acronyms

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