AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2000/15

XCP Security Systems Pty Ltd

KyberPASS Virtual Private Network Version 4.1.1 with Hydra 3DES (CBC mode) encryption

Issue 1.0
January 2001

Issued by: -

Defence Signals Directorate - Australasian Certification Authority


Common Criteria

CERTIFICATION STATEMENT

KyberPASS Virtual Private Network (VPN) version 4.1.1 is a product developed by Kyberpass Corporation that provides security services that are required to allow private, controlled access to sensitive computing resources. KyberPASS utilises industry-standard public/private key-based 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.

This report describes the evaluation findings of KyberPASS Virtual Private Network Version 4.1.1 with Hydra 3DES (CBC mode) encryption product to the Common Criteria Evaluation Assurance Level (EAL) 1, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its CC EAL1 level of assurance. It concludes that the product has met the target Assurance Level of CC EAL1.

Originator

Matthew Earley
Certifier
Defence Signals Directorate

Approval

Jane Holzapfel
Assistant Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation

Stewart Skelt
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the KyberPASS Virtual Private Network Version 4.1.1 with Hydra 3DES (CBC mode) encryption (hereafter referred to as KyberPASS). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner. Other users intending to use this product should seek advice from their National Security Advisory Authority to determine its suitability in meeting their particular requirements.

Identification of Target of Evaluation

1.2 The version of KyberPASS evaluated was Version 4.1.1, developed by Kyberpass Corporation.

1.3 KyberPASS is a software product. There are no hardware components associated with the product.

1.4 KyberPASS consists of:

a) The KyberPASS Authentication Server;

b) The KyberWIN security client;

c) The Hydra triple-DES symmetric (CBC mode) key encryption engine;

d) The Server Workstation (Windows NT 4.0 Server with Service Pack 6a)

e) The Client Workstation (Windows NT 4.0 Workstation with Service Pack 4)

1.5 KyberPASS consists of one CD-ROM. The CD-ROM contains the KyberPASS software, and the administration and user guidance. The version of KyberPASS on the CD-ROM should read **4.1.1** and should include **Hydra 168 bit 3DES** in its label**.**

1.6 For further details of the evaluated components of the KyberPASS VPN product, including details of how to identify the evaluated version, refer to Appendix C.

Evaluation

1.7 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1,2] respectively). In addition, the conditions outlined in the Common Criteria Mutual Recognition Agreement (ref [17]) were also upheld during the evaluation and certification of this product.

1.8 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), the KyberPASS product, in meeting its Security Target (ref [9]). The criteria against which the TOE is judged are expressed in the Common Criteria Part 3 (ref [5]). This describes how the degree of assurance can be expressed in terms of the levels EAL1 to EAL7. The methodology used is described in the Common Evaluation Methodology (CEM) and Evaluation Memoranda 4 and 5 (refs [6,7,8]).

1.9 The sponsor of the evaluation was Australian based company XCP Security Systems. The developer of the KyberPASS product was Canadian based company Kyberpass Corporation. A complete listing of the documentation used during the evaluation of this product is included in Appendix A of this Report.

1.10 The evaluation was performed by Computer Sciences Corporation between February 2000 and October 2000, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [10]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR and the Certification Group's knowledge of the evaluation.

1.11 The Security Target (ref [9]) claimed an assurance level for the product of CC EAL1.

General Points

1.12 Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher evaluation levels) that exploitable vulnerabilities remain undiscovered.

1.13 EAL1 provides a basic level of assurance by an analysis of the security functions using a functional and interface specification and guidance documentation, to understand the security behaviour. The analysis is supported by independent testing of the TOE security functions. This EAL provides a

meaningful increase in assurance over an unevaluated IT product or system.

1.14 KyberPASS should only be used within the defined TOE security environment in accordance with the secure usage assumptions and the organisational security policies, as explained in sections 3.1 and 3.3 of the ST (ref [9]). Also, the security requirements on the IT and non-IT environment must be fully understood in order to determine the suitability of the product in its assumed operational environment, as explained in sections 5.3 and 5.4 of (ref [9]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.15 Ultimately, it is the responsibility of the user to ensure that the KyberPASS product meets their requirements. For this reason, it is ***strongly*** recommended that a prospective user of the product obtains a copy of the Security Target (ref [9]) from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.16 The scope of the evaluation is limited to those claims made in the Security Target (ref [9]). All security related claims in the Security Target were evaluated by Computer Sciences Corporation. A summary of the Security Target is provided in Annex B of this Certification Report.

1.17 At CC EAL1, the evaluation of the implementation of the cryptographic algorithms is not required. However, the algorithms incorporated within the evaluated product have been assessed by DSD to be acceptable for Australian Government use for the protection of UNCLASSIFIED information.

1.18 This Report makes no claims about the use of KyberPASS in classified environments. Potential Commonwealth Government users are encouraged to contact DSD for further advice on the suitability of this product when used in conjunction with other evaluated products to protect national security and non-national security information.

Chapter 2 Security Overview of KyberPASS

2.1 Potential users are strongly recommended to read the Security Target (ref [9]). This explains the security functionality of the KyberPASS product in greater detail, as well as the intended environment and method of use for the product. A summary of the Security Target can be found in Appendix B. A full copy of the Security Target can be obtained from the sponsor of the evaluation - XCP Security Systems.

Overview of the TOE

2.2 This section provides a summary of the operational role of the TOE together with the security functions it is designed to perform.

2.3 KyberPASS is a Virtual Private Network (VPN) product providing a virtual private network connection between selected, internal application hosts and clients on an external, untrusted network like the Internet. The TOE consists of the KyberPASS Authentication Server, KyberWIN security client, and the Hydra 3DES encryption engine, running on either the Windows NT Server or Workstation operating systems. The role of these components is briefly described in the following paragraphs.

2.4 The KyberPASS Authentication Server is the inter-network security and policy management system that controls the flow of traffic between the network subjects and objects. The KyberPASS Authentication Server forms the majority of the TOE. It authenticates users and provides a secure data encryption/decryption transport between users and the network servers they access. The NT workstation is used by the administrators to manage the security of the KyberPASS Security Server.

2.5 Public Key cryptography is used by the KyberPASS Security Server, working with KyberWIN on each user's workstation, to verify a users identity (authentication), and to verify that the user is permitted to access an organisation's secure systems. The TOE can also be configured to encrypt the data being transferred between a workstation and a server to ensure confidentiality by utilising the Hydra 3DES encryption engine to produce a session key to encrypt the data.

2.6 KyberPASS supports TCP/IP compatible communications software products, such as terminal

emulators, World Wide Web browsers, and file transfer programs.

2.7 The KyberPASS Authentication Client (KyberWIN) provides transparent access to KyberPASS protected servers. The KyberWIN security client interfaces with the security server to authenticate and protect end user communications from their workstation(s).

2.8 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 server. The authentication and encryption process is transparent to the user and to the communications software products.

2.9 KyberPASS can also be 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 Lightweight Directory Access Protocol (LDAP) compliant server interface, and to remote third-party X.500 databases which are LDAP compliant.

2.10 In order to achieve its security objectives, the KyberPASS product is dependent on a number of security services provided by the underlying operating system. Windows NT server utilities are used in conjunction with the KyberPASS product to facilitate secure and efficient administration of the overall system.

2.11 KyberPASS provides fifteen security objectives for the TOE to create and maintain the confidentiality and integrity of the protected IT assets, including the protected data transported via the VPN. Availability concerns are also addressed from within the protected network. These security objectives for the TOE have been satisfied by ten categories of technical (IT) countermeasures implemented by the TOE (i.e. TOE Security Functions) in software. These are provided individually or in collaboration with one or more of the KyberPASS components identified above.

2.12 In addition, KyberPASS provides ten security objectives for the environment. These security objectives for the environment have been satisfied by a collaboration of technical measures implemented by the IT environment, and by the enforcement of non-IT (eg. procedural) measures.

2.13 There is no hardware or firmware associated with the evaluated configuration of the product.

2.14 While it is possible to use the KyberPASS product in a Public Key Infrastructure (PKI), the KyberPASS product does not include the mandatory components needed to establish an operational PKI, such as a Certification Authority or a Registration Authority. Rather, the

KyberPASS product is intended to be incorporated into an existing PKI, particularly for cryptographic public key pair and certificate generation. Organisations looking for a complete PKI solution are recommended to refer to other products listed in the Evaluated Products List that could be interoperable with KyberPASS. Commonwealth Government users should ensure that the product is being used in accordance with Gatekeeper requirements.

2.15 More detailed information on the KyberPASS product can be found in the Security Target (ref [9]), and in Appendix B of this report

Security Policy

2.16 The following security policies are enforced by the KyberPASS product:

- The TOE shall not allow a user to establish a proxy (a secure connection) to a protected applications host until that user has been properly identified and authenticated.
- The TOE shall provide a mechanism for authorised roles to manage the TSF data and to provide accountability for the actions of users in those roles.
- The TOE shall provide a mechanism to ensure that a proxy is established only when the proxy request conforms with a number of preset rules, as delimited by the administrator in the TSF data.
- The TOE shall ensure that its internal architecture is such as to prevent its compromise by unauthorised subjects.
- The TOE shall provide a mechanism to ensure that sufficient details of the actions of subjects are recorded to ensure the accountability of the related human user.
- The TOE shall ensure that the import and export of cryptographic keys into and out of the TOE is controlled by operating site policy, that is based on guidance provided by the KyberPASS usage notes and DSD's ACSI 57 (ref [16]).
- The TOE shall provide a mechanism to ensure that all data packets passing between a client application and a protected applications server host are protected from unauthorised disclosure or change.
- The TOE shall provide a mechanism to ensure that the cryptographic keys used are

protected from unauthorised disclosure or change.

- The TOE shall provide a mechanism to ensure that the flow of information from protected applications hosts to external clients is limited to authorised proxies only.
- The TOE shall provide a mechanism to ensure that a trusted association (proxy) can be established between a remote user and a protected applications host.

2.17 In order for the TOE to comply with the remainder of the security policy, the KyberPASS product should only be used within the defined TOE security environment in accordance with the secure usage assumptions and the organisational security policies, as explained in sections 3.1 and 3.3 of the ST (ref [9]).

Documentation

2.18 Before using the product, administrators and security managers should ensure that they are aware of and fully understand the relevant operational documentation. In addition, they should ensure that they read Chapter 4 of this document, and the associated administration and user manuals contained on the product CD-ROM (refs [11]-[14]).

Chapter 3 Evaluation Findings

Introduction

3.1. The evaluation of KyberPASS followed a course consistent with the generic evaluation work programme described in the ITSEM (ref [15]) and the CEM (ref [6]), with work packages structured around the evaluator actions described in the Common Criteria (CC) Part 3 (ref [5]). The results of this work are reported in the ETR (ref [10]) under the CC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [9]).

Security Target Evaluation

3.2. The purpose of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

TOE Description (ASE_DES.1)

3.3. The TOE Description adequately described the product type, and the scope and boundaries of the TOE in general terms both in a physical and a logical way.

3.4. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Description, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Environment (ASE_ENV.1)

3.5. The statement of the TOE security environment adequately identified and explained the assumptions about the intended usage of the TOE (and its environment), the known threats to the protected assets of the TOE (and its environment), and the organisational security policies with which the TOE mandated.

3.6. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Environment, and consider it suitable to be used (in part) as a basis for the evaluation.

ST introduction (ASE_INT.1)

3.7. The ST introduction identified and adequately described the ST and the TOE. It contained an ST overview in narrative form, and contained a CC conformance claim to meet the predefined assurance level of EAL1.

3.8. The above results have enabled the certifiers to conclude that the ST has met the requirements for the ST introduction, and consider it suitable to be used (in part) as a basis for the evaluation.

Security Objectives (ASE_OBJ.1)

3.9. The statement of the TOE and environmental security objectives were adequately defined, and were clearly traceable back to the identified threats countered by the TOE, organisational security policies and assumptions on the TOE and its environment. The security objectives rationale demonstrated that the security objectives were suitable to counter the identified threats and cover the identified organisational security policies and assumptions.

3.10. The above results have enabled the certifiers to conclude that the ST has met the requirements for the Security Objectives, and consider it suitable to be used (in part) as a basis for the evaluation.

Protection Profile (PP) Claims (ASE_PPC.1)

3.11. The ST did not claim conformance to any PPs.

IT Security Requirements (ASE_REQ.1)

3.12. The statement of the TOE Security Functional Requirements (SFRs) correctly identified the SFRs drawn from CC Part 2 (ref [4]), and the TOE Security Assurance Requirements (SARs) for EAL1 from CC Part 3 (ref [5]). The justification for using the pre-defined EAL1 assurance package was sufficient.

3.13. Security requirements on the IT environment were identified. All operations on the IT security requirements were completed, and the relevant dependencies were satisfied. The security requirements rationale demonstrated that the IT security requirements were suitable to meet the security objectives. It also demonstrated that the set of IT security requirements together forms a mutually supportive and internally consistent whole.

3.14. The above results have enabled the certifiers to conclude that the ST has met the requirements for the IT Security Requirements, and consider it suitable to be used (in part) as a basis for the evaluation.

Explicitly stated IT Security Requirements (ASE_SRE.1)

3.15. The ST did not contain any explicitly stated IT security requirements.

TOE Summary Specification (ASE_TSS.1)

3.16. The TOE summary specification (TSS) adequately described the IT security functions and the assurance measures of the TOE. The TSS traced and clearly mapped all IT security functions to the TOE security functional requirements demonstrating that all TOE security functions contribute to the satisfaction of at least one TOE security functional requirement.

3.17. The IT security functions were informally specified to an appropriate level of detail. Security mechanisms were easily traced back to the relevant TOE security functions.

3.18. The TOE summary specification rationale demonstrated that the IT security functions were suitable to meet the TOE security functional requirements, and that the combination of IT security functions work together to also satisfy the TOE security functional requirements. The rationale also demonstrated, aided by a mapping, that the assurance measures met the assurance requirements for EAL1.

3.19. The TOE summary specification identified all IT security functions that are realised by a probabilistic or permutational mechanism. Common Criteria EAL1 evaluation does not require a strength of function (SOF) claim.

3.20. The above results have enabled the certifiers to conclude that the ST has met the requirements for the TOE Summary Specification, and consider it suitable to be used (in part) as a basis for the evaluation.

ST Evaluation Result

3.21. The certifiers consider that the above results have demonstrated that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the evaluation.

Common Criteria EAL1 Security Assurance Requirements

3.22. EAL1 provides a basic level of assurance by an analysis of the security functions using a functional and interface specification and guidance documentation, to enable the understanding of the security behaviour. The analysis is supported by independent testing of the TOE security functions.

3.23. EAL1 provides a meaningful increase in assurance over an unevaluated IT product or system. The results of this evaluation are discussed below.

Configuration Management (ACM)

3.24. Configuration management is one method or means for establishing that the functional requirements and specifications are realised in the implementation of the TOE. Configuration management meets these objectives by requiring discipline and control in the processes of refinement and modification of the TOE and the related information. Configuration management systems are put in place to ensure the integrity of the portions of the TOE that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorised.

Configuration Management Capabilities (ACM_CAP.1)

3.25. The TOE reference was assessed to be unique to each version of the TOE. In addition, the TOE was correctly labelled with its reference.

3.26. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Configuration Management assurance component for EAL1.

Delivery and Operation (ADO)

3.27. This aspect of the evaluation examines the requirements for the measures, procedures, and standards concerned with correct installation and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during installation, start-up and operation.

3.28. CC EAL1 does not require an examination of the delivery procedures.

Installation, Generation and Start-Up (ADO_IGS.1)

3.29. The operational documentation adequately described the steps necessary for secure installation, generation, and start-up of the TOE.

3.30. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Delivery and Operation assurance component for EAL1.

Development (ADV)

3.31. This aspect of the evaluation examines the requirements for the stepwise refinement of the TSF from the TOE summary specification in the ST down to the functional specification. Each of the resulting TSF representations provide information to help determine whether the functional requirements of the TOE have been satisfied.

Functional Specification (ADV_FSP.1)

3.32. The functional specification informally described the TSF and its external interfaces, including a description on the purpose and method of use of all external TSF interfaces, while also providing details of effects, exceptions and error messages.

3.33. The functional specification was found to be internally consistent and to completely represent the TSF.

3.34. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Specification assurance component for EAL1.

Representation Correspondence (ADV_RCR.1)

3.35. An analysis of the correspondence between the ST and the functional specification was provided. This analysis demonstrated that all relevant security functionality in the ST is correctly and completely refined in the functional specification.

3.36. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Representation Correspondence assurance component for EAL1.

Guidance Documents (AGD)

3.37. This aspect of the evaluation examines the requirements directed at the understandability, coverage and completeness of the operational documentation provided by the developer. This documentation, which provides two categories of information, for users and administrators, is an important factor in the secure operation of the TOE.

Administrator Guidance (AGD_ADM.1)

3.38. The administrator guidance clearly described the administrative functions and interfaces, instructions on how to administer the TOE securely, all assumptions regarding user behaviour that are relevant to the secure operation of the TOE, all security parameters under the control of the administrator, and each type of security-relevant event relative to the administrative functions being performed, including changing the security characteristics of entities under control of the TSF.

3.39. The guidance also contained appropriate warnings about functions and privileges that need to be controlled in a secure environment, and indicated secure values if applicable.

3.40. The administrator guidance described all security requirements for the IT environment that were relevant to an administrator, and was consistent with all other documentation supplied for the evaluation.

3.41. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Administrator Guidance assurance component for EAL1.

User Guidance (AGD_USR.1)

3.42. The user guidance clearly described the functions and interfaces available to the non-administrative users of the TOE, and the use of user-accessible security functions provided by the TOE. Appropriate warnings about user-accessible security functions and privileges that should be controlled in a secure processing environment were also described.

3.43. All user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of the TOE security environment, were clearly presented.

3.44. The user guidance described all security requirements for the IT environment that were relevant

to a user, and was consistent with all other documentation supplied for the evaluation.

3.45. As a result of the above determinations, the certifiers conclude that the TOE fully meets the User Guidance assurance component for EAL1.

Tests (ATE)

3.46. Testing helps to establish that the TOE security functional requirements are met. Independent testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified.

Independent Testing (ATE_IND.1)

3.47. Independent testing was conducted to confirm that the TOE operates as specified in the documentation supplied for the evaluation. The configuration of the TOE (and its environment) used during testing was consistent with the evaluated configuration, as stipulated in the ST (ref [9]) and the operational guidance (ref [14]).

3.48. The evaluators conducted testing on all of the TOE Security Functions specified in the ST. As all TOE Security Functions were tested, no sampling was performed on the selection of the test subset. All tests were sufficiently documented to enable the tests (and their results) to be reproducible.

3.49. Developer testing is not required at CC EAL1.

3.50. The testing demonstrated that the security functions performed as specified in ST.

3.51. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Independent Testing assurance component for EAL1.

Specific Functionality

3.52. The TOE Security Functional Requirements and the TOE Security Functions provided by KyberPASS are specified in sections 5.1 and 6.1 of the Security Target (ref [9]) and summarised in Appendix B of this report.

3.53. The evaluators found that the product provided the TOE security functionality and satisfied the

TOE Security Functional Requirements, as specified in the Security Target (ref [9]).

Discussion of Unresolved Issues

3.54. At the conclusion of the evaluation there were no unresolved issues requiring the consideration of the certifiers.

General Observations

3.55. The certifiers would like to acknowledge the invaluable assistance provided by XCP Security Systems staff during the evaluation. Without the due attention to problems found, and their technical assistance, the process could not have succeeded in the same time frame.

3.56. Further, the certifiers would like to acknowledge the efforts of Computer Sciences Corporation in ensuring prompt delivery of the Evaluation Technical Report for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the Evaluation Technical Report (ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that KyberPASS has met the requirements of the Common Criteria EAL1 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 4.1.1 of the product. This certificate is only valid when the KyberPASS product correctly comprises the designated components. These components are identified in Appendix C and should be verified on receipt of the delivered product.

Recommendations

4.3 The following recommendations involve information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the Certification Group.

4.4 KyberPASS should only be used in accordance with the intended environment described in sections 3.1 (Secure Usage Assumptions), 3.3 (Organisational Security Policies), and 5.3 (IT Environment Requirements), including consideration of all physical, personnel and procedural security measures contained in section 5.4 (non-IT Environment Requirements) of the Security Target (ref [9]).

Functionality not part of the Evaluated Configuration

4.5 The KyberPASS software package is delivered with several other applications that are used to support the operation of KyberPASS. Not all of these applications have been included in this evaluation. The evaluated configuration has been specified in Appendix C of this Report. In particular, **the KyberWIN 32-bit client (operating on the Windows 95 or 98 platforms) has not been included in the evaluated configuration and is therefore not to be used for**

Australian Government use. Other functionality and/or components that have not been included in this evaluation of KyberPASS are as follows:

1. Cut-Through Proxies;
2. The Alert Monitor (Windows component);
3. Failover;
4. Public Key Pair and Certificate generation;
5. Network Address Translation (NAT);
6. Private-Link;
7. Setup Wizard;
8. TFTP Configuration Server;
9. Remote Administration (Telnet Interface);
10. Acceptance of updates for internal data structures (e.g. routing tables) from authorised host; and
11. Windows NT 4.0 features NOT used by the TOE (refer to Appendix C of this Report)

Cryptographic Requirements for Australian Government Use

4.6 The following cryptographic constraints have been placed on the evaluated configuration with respect to the use of cryptographic algorithms:

i) 168 bit 3DES (CBC mode) for cryptographic key generation, and for data encryption and decryption;

ii) 1024 bit RSA for cyptographic key encryption and decryption, and for digital signature verification;

iii) MD5 for secure hashing; and

iv) 512 bit Diffie-Hellman for cryptographic key agreement.

Administrators of the TOE should be aware of these restrictions, and ensure the correct versions have been supplied with the evaluated product, and that the configurations of any cryptographic parameters are in line with the above requirements.

4.7 As stated in the Security Target (ref [9]), **Commonwealth Government users must ensure that key pairs and certificates are issued by a Gatekeeper compliant product operated by an GPKA-endorsed Certification Authority. Further advice can be obtained by contacting DSD.**

4.8 Also stated in the Security Target (ref [9]), **all cryptographic-relevant material is to be the subject of rigorous levels of physical and technical control as defined in ACSI 57 (ref [16]),** such as an appropriate key management plan**.** Commonwealth Government users are encouraged to contact DSD for further assistance in this area.

4.9 A major user and administrator responsibility is ensuring the privacy of their security profile (digital certificate) password. **Commonwealth Government agencies are advised to have appropriate password policies in place for the protection of private keys, profiles and certificates.**

4.10 The user and administrator password and their associated certificate (including the private key) can either be stored on the individual's workstation hard drive, on a diskette, on a smartcard, or on an appropriate token (such as a PCMCIA card). These storage technologies have not been considered as part of the evaluation. **Commonwealth Government agencies wishing to interoperate the product with an appropriate storage device are strongly encouraged to contact DSD for further assistance.**

Pre-installation considerations for KyberPASS components

4.11 Administrators should ensure that, prior to installing any KyberPASS server component, the hardware has been appropriately sanitised and contains no software other than the required components specified in Appendix C of this Report. **Furthermore, to avoid the introduction of malicious software and viruses on KyberPASS enabled servers, it is recommended that the hard drive of each KyberPASS server be re-formatted prior to an installation of the operating system.**

4.12 Similarly, to prevent the infection of a KyberWIN enabled host with a malicious virus, installers of the client software are recommended to install an appropriate virus scanner to prevent infected files from spreading into a KyberPASS protected server.

4.13 Potential purchasers of KyberPASS need to be aware that the operational documentation is aimed at the administrator level. Therefore, only appropriately qualified staff should install, configure and maintain the KyberPASS server components.

4.14 Operational documentation is delivered with the installation CD-ROM. Each major KyberPASS component has its own documentation. Prior to installation, administrators need to familiarise themselves with the content of all of these documents (refs [11]-[14]). In particular, the operational documentation contains a guidance document specific to the secure use of the evaluated version of the product. **Commonwealth Government users are strongly encouraged to follow the installation and configuration guidelines contained in this document (ref [14]).**

Configuring KyberPASS to reflect the Evaluated Version

4.15 Administrators installing the TOE components must use the Security Target [ref [9]) in conjunction with the operational documentation supplied on the CD-ROM. **Specifically, the KyberPASS Usage Guide - A Guide for the secure use of EAL1 assured version of KyberPASS 4.1.1 with Hydra 3DES (CBC mode) encryption (ref [14]) must be fully understood before the installation and configuration is commenced.** This guide is intended to assist government agencies in the secure installation and operation of the assured version of the KyberPASS Authentication Server and the KyberWIN Authentication Client.

Considerations for Windows NT

4.16 The TOE relies on various Windows NT 4.0 server utilities to securely manage and configure the TOE. These utilities include, but are not limited to, the Alert Monitor, Log Viewer, Event Viewer, and the User Manager. Therefore, **Commonwealth Government users are strongly encouraged to implement the latest secure configuration guidelines for Windows NT 4.0, which can be obtained by contacting their relevant security authority.**

4.17 TOE specific events are stored under the KyberPASS installation directory, as denoted by the .KYB file extension. Potential purchasers are advised that once access has been granted to the host computer, there are no security mechanisms offered by the TOE to prevent the signed audit entries from being deleted, other than the operating system security offered by Windows NT. Therefore, **administrators must ensure that administrative privilege is restricted to authorised users of the KyberPASS component. Administrators should also ensure that appropriate Windows NT password policies are being enforced on KyberPASS enabled systems.**

Operational considerations

4.18 Administrators need to ensure that the communications link to and from the KyberPASS Authentication Server (within the protected network) is adequately protected. A failure of a communications link with the Authentication Server could cause a delay for end users or applications in requesting KyberPASS services. Please note that the Secure Use Assumptions outlined in the Security Target (ref [9]) stipulate that appropriate measures must be taken to reduce the likelihood of these types of failure from occurring.

4.19 An exhaustion of disk space may produce unexpected behaviour from the TOE. Importantly, this situation may cause the TOE to cease recording security related information in the Windows NT system audit logs or the KyberPASS specific audit files (as described in 4.16 above). **Administrators must ensure that there is an adequate amount of available disk space left on system disks, as specified by the operational guidance (ref [11]). Administrators should ensure that events in the event log are not automatically overwritten, unless their security policy has deemed it appropriate.**

Availability considerations for KyberPASS

4.20 Administrators should note that the KyberPASS product does not counter any external threats to the availability of the TOE components. Since the functionality of the TOE allows users to interoperate with a wide variety of applications and technologies, it may be possible for an external party to launch a denial of service attack against the TOE. While this type of threat does not invalidate the security objectives of the TOE, **administrators should ensure that adequate measures are in place to protect KyberPASS servers and their networks from denial of service or other types of availability attacks coming from outside the protected network. Furthermore, Australian Government users should contact DSD for assistance on implementing appropriate countermeasures to protect their networks from such attack.**

4.21 Further to the recommendation discussed above, the Security Target (ref [9]) assumes that an EAL2 assured firewall is correctly positioned to protect the KyberPASS servers from external attack. **Australian Government users are strongly encouraged to protect the TOE from external attack by connecting the public network interface of the KyberPASS Security Server to the external (untrusted) network via an appropriately assured firewall.**

Proxy Considerations

4.22 KyberPASS allows the administrator to minimise the number of ports opened by the firewall protecting the KyberPASS Security Server. This feature can be utilised by tunneling all proxies through a single port on the firewall, and should be considered when installing the KyberPASS server components.

4.23 Administrators should note that changes to the proxy definitions in the KyberPASS Server component do not take effect until the KyberPASS service is stopped and restarted. **Therefore, administrators must ensure this procedure is followed and is incorporated into their System Security Policy (SSP) when a change occurs to the proxy settings, in accordance with the operational documentation.**

Considerations for the X.500 Directory Server

4.24 The TOE incorporates an X.500 Directory Manager to define and maintain the definitions for X.500 directory access. One of the supported features includes the caching of Certificate Revocation Lists (CRLs) and another feature to specify the refresh rate of the cache. More importantly, it is possible to specify a "zero" refresh rate, implying that the cached copy of the CRL would never refresh. Therefore, **administrators of the TOE are strongly recommended not to assign a zero refresh value to the CRL cache. Furthermore, organisations should ensure that the appropriate X.500 directory access policy is in place in accordance with their operational requirements.**

Appendix A References

[1] Evaluation Memorandum No. 1 - Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.1, March 1997

[2] Evaluation Memorandum No. 2 - The Licensing of AISEFs
Defence Signals Directorate
EM 2, Issue 1.0, August 1994

[3] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model (CC)
CCIMB-99-031, Version 2.1, August 1999

[4] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements
CCIMB-99-032, Version 2.1, August 1999

[5] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements
CCIMB-99-033, Version 2.1, August 1999

[6] Common Methodology for Information Technology Security Evaluation (CEM)
CEM-99/045, Version 1.0, August 1999

[7] Manual of Computer Security Evaluation Part I - Evaluation Procedures
Defence Signals Directorate
EM 4, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[8] Manual of Computer Security Evaluation Part II - Evaluation Techniques and Tools
Defence Signals Directorate
EM 5, Issue 1.0, April 1995
(EVALUATION-IN-CONFIDENCE)

[9] KyberPASS 4.1.1 Security Target
XCP Security Pty Ltd.
Version 1.6, August 2000
(COMMERCIAL-IN-CONFIDENCE)

[10] KyberPASS 4.1.1 Evaluation Technical Report

Computer Sciences Corporation
Issue 2.0, 30 October 2000.
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[11] KyberPASS Security Software Suite Administrators Guide
XCP Security Pty Ltd.
Version 4.1.1, 9th February 2000

[12] KyberPASS Authentication Client - KyberWIN User Guide (UG)
XCP Security Pty Ltd.
Version 4.1.1, 24th January 2000

[13] KyberPASS Authentication Client - KyberWIN User Guide (UG-K2)
PKCS12K2-4.1.1
XCP Security Pty Ltd.
Version 4.1.1, 24th January 2000

[14] KyberPASS Usage Guide - A Guide for the secure use of EAL1 assured version of KyberPASS 4.1.1 with Hydra 3DES (CBC mode) encryption
XCP Security Pty Ltd.
Version 4.1.1, 24th January 2000

[15] Information Technology Security Evaluation Methodology (ITSEM)
Commission of the European Communities
Version 1.0, 10 September 1993

[16] Australian Communications-Electronic Security Instructions (ACSI) 57 (B),
Guidelines for the Use of Cryptographic Systems listed in section VIII of the Defence Signals Directorate Evaluated Products List (EPL)
Bravo Edition, Defence Signals Directorate

[17] Arrangement on the Recognition of Common Criteria Certificates (in the field Information Technology Security)
Available from: http://www.commoncriteria.org/registry/ccra-final.html
May 2000

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target is given below. Potential purchasers should attempt to obtain a copy of the full Security Target to ensure that the TOE security functionality satisfies the requirements of their security policy.

Security Objectives for the TOE

B.2 KyberPASS has the following IT security objectives:

a) **Identification and Authentication**. The TOE must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE facilities.

b) **Discretionary Access Control**: 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.

c) **Auditing:** The TOE must provide the means for recording security-relevant events in sufficient to help an administrator of the TOE to: detect attempted security violations; and hold individual users accountable for any actions they perform that are relevant to the security of the TOE.

d) **Administration:** 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.

e) **Integrity:** The TOE must provide the means for detecting loss of integrity of TSF.

f) **Bypassability**: The TOE must prevent users of processes from bypassing or circumventing TOE security policy enforcement.

g) **Message Integrity:** The TOE must provide a means of detecting the loss of integrity of messages transferred between users across the telecommunications network.

h) **Data Confidentiality:** The TOE must provide the means of protecting the confidentiality of user information when it is transferred across an insecure telecommunications network.

i) **Information Flow:** The TOE must ensure that any information flow control policies are

enforced - (1) between TOE components and (2) at the TOE external interfaces.

j) **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.

k) **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.

l) **Non Repudiation:** 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 every having received that data.

m) **Role Enforcement:** The TOE must prevent users from gaining access to and performing operations on its resources for which their role is not explicitly authorised.

n) **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.

Security Objectives for the Environment

B.3 KyberPASS has the following environmental objectives:

a) **Installation:** Those responsible for the operation of the TOE must ensure that: the TOE is delivered, installed and operated in a secure manner; the underlying operating system and/or network services are installed and operated in accordance with the operational documentation for the relevant products.

b) **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.

c) **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.

d) **Crypto Management:** 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.

e) **Trust:** Those responsible for the TOE must ensure that only highly trusted users are given privileges that enable them to: set or alter the audit trail configuration; create or modify user roles; load or modify crypto-variables.

f) **Non-technical Entry:** The TOE environment must provide sufficient protection against non-technical attacks, such as social engineering attacks.

g) **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 then to fulfil their duties securely.

h) **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.

i) **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.

j) **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.

Secure Usage Assumptions

B.4 The following assumptions relate to the operation of the TOE:

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.

b) **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.

c) **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 EAL2 assured or greater firewall product, operated in accordance with government best practice.

d) **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 developer's recommendations.

e) **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 telecommunication path.

f) **No Evil:** 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.

g) **No User Code:** The operating environment provides no user-accessible code that allows modification of the KyberPASS security configuration by other than authorised administrators.

Threats addressed by the TOE

B.5 The following threats are addressed by the TOE:

a) **Abuse:** An authorised user of the TOE (intentionally or otherwise) performing actions that individual is authorised to perform may compromise the TOE security function.

b) **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 the material.

c) **Attack:** An attacker (whether 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.

d) **Audit Confidentiality:** An unauthorised individual or process may gain access to the records of security-related events kept by the TOE.

e) **Audit Corruption:** An unauthorised individual or process may modify or destroy the records of security-related events kept by the TOE.

f) **Capture:** An attacker may eavesdrop on, or otherwise capture, cryptographic key material or related user data being transferred across a network.

g) **Deny:** A user as either originator or recipient may participate in the transfer of information

and then deny having done so.

h) **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

i) **Impersonate:** 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.

j) **Integrity:** User, hardware or transmission errors may compromise the integrity of information being transferred across a network.

k) **Mixing:** A subject that is not the authorised recipient may, through the inadvertent mixing of plaintext and cyphertext on the same logical circuit, gain access to sensitive material.

l) **Modification:** An attacker may, through unauthorised modification or destruction, compromise the integrity of cryptographic key material or related user data being transferred across a network.

m) **Record Event:** The TOE may not record in the audit trail the security-relevant events affecting the secure operation of the TOE.

n) **Resources:** System error or non-malicious user action may exhaust the shared, internal resources of the TOE.

o) **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.

Threats addressed by the TOE Environment

B.6 The following threats are addressed by the TOE Environment:

a) **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.

b) **Non Technical Entry:** 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.

c) **Installation:** The TOE may be delivered or installed in a manner that undermines security.

d) **Operation:** Improper operation of the TOE may cause a failure of the TOE security function.

Organisational Security Policies

B.7 The following organisational security policies are relevant to the operation of the TOE:

a) **Audit:** Details of user activity will be recorded in an audit trail that must be preserved in line with relevant organisational archive requirements.

b) **Crypto:** All cryptographic-relevant material is to be the subject of rigorous levels of physical and technical control as defined in ACSI 57.

c) **Network:** The organisation's IT security policy will be maintained in the environment of distributed systems interconnected via insecure networking.

d) **Information Flow:** The flow of information between IT components in a client -server architecture utilising insecure networks must be controlled and protected from disclosure.

e) **User Due Care:** Users who have been issues authenticators that facilitate usage of IT systems will ensure that those authenticators are appropriately protected.

Summary of TOE Security Functional Requirements

The TOE security functional requirements (SFRs) are tabulated below. Full description and explanation of these SFRs can be found in section 5.1 of the Security Target (ref [9]).

Class FAU: Audit

FAU_GEN.1 Audit data generation

FAU_GEN.2 User identity association

FAU_STG.2 Guarantees of audit availability

Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic access control

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Class FDP: User Data Protection

FDP_ACC.2 Complete access control

FDP_ACF.1 Security attribute access control

FDP_IFC.1 Subset information flow control

FDP_IFF.1 Simple security attributes

FDP_ITC.1 Import of user data without security attributes

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.3 Integrity monitoring

Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_UID.1 Timing of identification

FIA_UAU.1 Timing of authentication

FIA_UAU.6 Re-authentication

Class FMT: Security Management

FMT_MSA.1 Management of security attributes

FMT_MSA.2 Secure security attributes

FMT_MSA.3 Static attribute initialisation

FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

Class FPT: Protection of the TOE Security Functions

FPT_ITT.2	TSF data transfer separation
FPT_ITT.3	TSF data integrity monitoring
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.2	SFP domain separation
FPT_STM.1	Reliable time stamps

Security Requirements for the IT Environment

B.8 The Security Requirements for the IT Environment are briefly listed below. Full description and explanation of these security requirements can be found in section 5.3 of the Security Target (ref [9]).

a) **ITENV.1:** KyberPASS relies on the Configuration Manager to configure the system by setting user attributes. In doing so, the TOE also relies on the Windows NT operating system to provide this capability.

b) **ITENV.2:** KyberPASS relies on the Configuration Manager to establish and control the TSF data. In doing so, the TOE also relies on the Windows NT operating system to provide this capability.

Security Requirements for the Non-IT Environment

B.9 The Security Requirements for the Non-IT Environment are briefly listed below. Full description and explanation of these security requirements can be found in section 5.4 of the Security Target (ref [9]).

a) **NONITENV.1:** The KyberPASS server must be protected from unauthorised modification by external threat by a firewall of at least EAL2 level of assurance or equivalent.

b) **NONITENV.2:** The KyberPASS server must be located within a controlled access facility that will prevent unauthorised physical access.

c) **NONITENV.3:** Access to the KyberPASS server and the console must be restricted to administrators only.

d) **NONITENV.**4: The TOE environment must provide sufficient protection against non-technical attacks, such as social engineering attacks.

e) **NONITENV.**5: 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.

f) **NONITENV.6:** The TOE environment must provide a mechanism that ensures that the likelihood of administration staff perform illegal actions is minimised.

g) **NONITENV.**7: The TOE environment must ensure that at any time no user-accessible code that may modify TOE security functions exists on the KyberPASS server.

h) **NONITENV.**8: The KyberPASS server must be installed and configured in accordance with the developer guidance.

i) **NONITENV.**9: The TOE environment must ensure that at all times cryptographic keys are protected against unauthorised access, loss or destruction.

j) **NONITENV.**10: The TOE environment must ensure that administrators are well trained and motivated to make the right choices when providing administrative support to the TOE.

k) **NONITENV.**11: KyberPASS relies on a GATEKEEPER compliant CA product to meet the SOF requirement for the public/private key cryptographic services that it uses.

Summary of TOE Security Functionality

B.10 The KyberPASS TOE Security Functions (TSFs) are briefly listed below. Full description and explanation of these TSFs can be found in section 6.1 of the Security Target (ref [9]). The Security Function Policy is stated in full to facilitate the readers understanding of each of the TOE Security Function groupings.

B.11 Identification and Authentication

The TOE shall not allow a user to establish a proxy (a secure connection) to a protected applications host until that user has been properly identified and authenticated.

This Security Function Policy is achieved by the following functions:

I&A-1 User Identity Certificate

I&A-2	TOE Logical Access
I&A-3	User authentication
I&A-4	Source authentication
I&A-5	Private key password

B.12 System Security Management

The TOE shall provide a mechanism for authorised roles to manage the TSF data and to provide accountability for the actions of users in those roles.

This Security Function Policy is achieved by the following functions:

SSM-1	Administration system
SSM-2	Audit log-file management
SSM-3	Management of TSF data
SSM-4	Directory Administration
SSM-5	Role definition
SSM-6	User access rights definition
SSM-7	Administrator guidance

B.13 Access Control

The TOE shall provide a mechanism to ensure that a proxy is established only when the proxy request conforms with a number of preset rules, as delimited by the administrator in the TSF data.

This Security Function Policy is achieved by the following functions:

ACTRL-1	Discretionary access controls
ACTRL-2	Proxy services
ACTRL-3	Time & Location constraints
ACTRL-4	Timed reauthentication

ACTRL-5 Logoff after inactivity period

B.14 System Architecture

The TOE shall ensure that its internal architecture is such as to prevent its compromise by unauthorised subjects.

This Security Function Policy is achieved by the following functions:

SIA-1 TSF domain separation

SIA-2 Inter-TSF data consistency

B.15 Security Audit

The TOE shall provide a mechanism to ensure that sufficient details of the actions of subjects are recorded to ensure the accountability of the related human user.

This Security Function Policy is achieved by the following functions:

SA-1 Audit data generation

SA-2 Audit data signing and storage

SA-3 Audit reporting

B.16 TSF Data Import & Export

The TOE shall ensure that the import and export of cryptographic keys into and out of the TOE is controlled by operating site policy, that is based on guidance provided by the KyberPASS usage notes and DSD's ACSI 57.

This Security Function Policy is achieved by the following functions:

TSF-DI&E-1 Private key import controls

TSF-DI&E-2 Certificate import controls

TSF-DI&E-3 TSF Data encryption

B.17 Secure Packet Transfer

The TOE shall provide a mechanism to ensure that all data packets passing between a client application and a protected applications server host are protected from unauthorised disclosure or change.

This Security Function Policy is achieved by the following functions:

SPT-1 Packet encryption

SPT-2 Packet integrity

SPT-3 Packet source authentication

SPT-4 Connection non-repudiation

B.18 Key and Credential Management

The TOE shall provide a mechanism to ensure that the cryptographic keys used are protected from unauthorised disclosure or change.

This Security Function Policy is achieved by the following functions:

K&CM-1 Key Management

K&CM-2 Certificate management

B.19 Information Flow Control

The TOE shall provide a mechanism to ensure that the flow of information from protected applications hosts to external clients is limited to authorised proxies only.

This Security Function Policy is achieved by the following functions:

IFC-1 Packet flow control

IFC-2 Single port tunneling

B.20 Associations

The TOE shall provide a mechanism to ensure that a trusted association (proxy) can be established between a remote user and a protected applications host.

This Security Function Policy is achieved by the following functions:

ASSOC-1 Signed association request

ASSOC-2 Diffie-Hellman key exchange

ASSOC-3 Trusted channel

Appendix C Contents of Distribution Package

Configuration for Evaluation

C.1 The evaluation was conducted on the KyberPASS VPN product, Version 4.1.1. The software components of KyberPASS have been identified below. KyberPASS does not consist of any hardware.

Software

C.2 The software elements of KyberPASS are as follows:

a) 1 x CDROM containing the **KyberPASS Software, Version 4.1.1 (Hydra 168 bit 3DES)**.

b) The evaluated components of the KyberPASS Security Server are:

i) KyberPASS Security Server

ii) KyberPASS Authentication Server

iii) KyberPASS Control

iv) X.500 Directory Manager

v) Configuration Manager

vi) Display Manager

vii) Log Viewer

viii) RSA Data Security Inc Bsafe library (Version Pending)

ix) Hydra 3DES crypto primitive (XCP32.4_0)

c) The evaluated components of the KyberPASS client workstation are:

i) KyberWIN Client K2 version 4.1.1

ii) RSA Data Security Inc Bsafe library (Version Pending)

iii) Hydra 3DES crypto primitive (XCP32.4_0)

Third Party Software

C.3 The third party software required to operate KyberPASS is as follows:

a) For the server workstation:

i) Windows NT 4.0 Server - with Service Pack 6a

ii) The following NT services are also required: NT File System (NTFS), NT Security subsystem, Event Log Services, and NT Registry Services.

b) For the client workstation:

iii) Windows NT 4.0 Workstation - with Service Pack 4.

C.4 This evaluation is only valid for the above mentioned version of KyberPASS running on the Microsoft Windows NT 4.0 Workstation and Server products, with the specified Service Packs applied. No other versions, operating systems or third party software are part of the evaluated configuration.