Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2006/39

25 October 2006

Version 1.0

Amendment Record

Version	Date	Description
1.0	25/10/2006	Public release.

Executive Summary

1 UniCERT 5.2.1 is a product that is designed to provide all the functionality needed to implement a Public Key Infrastructure (PKI) system. UniCERT 5.2.1 (including patch 5.2.1.900) is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Cybertrust's UniCERT 5.2.1, to the Common Criteria (CC) evaluation assurance level EAL4+. The report concludes that the product has met the target assurance level of EAL4+ and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by LogicaCMG and was completed in July 2006.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users:

a) Implement appropriate key and certificate generation and management policies;

b) Ensure any external cryptographic hardware used with the TOE is evaluated to an appropriate assurance level; and

c) Ensure strong pass-phrases are used in the protection of keys and certificates.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1], and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the TOE, UniCERT 5.2.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

b) Provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	UniCERT 5.2.1
Software Version	5.2.1 including patch 5.2.1.900
Security Target	Cybertrust UniCERT 5 Security Target-5.0.ab
Evaluation Level	EAL4+ (Augmented with ALC_FLR.2)
Evaluation Technical Report	Cybertrust UniCERT 5.2.1 Evaluation Technical Report, Issue 1.0, July 2006
Criteria	CC Version 2.1, August 1999, with interpretations as of 19 June 2003.
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 19 June 2003.

Conformance	CC Part 2 Conformant Part 3 Augmented with ALC_FLR.2 (Flaw Remediation)
Developer	Cybertrust
Evaluation Facility	LogicaCMG

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is called UniCERT 5.2.1 and is developed by Cybertrust. It provides all the functionality needed to implement a Public Key Infrastructure (PKI) system.

12 A PKI is composed of hardware and software products and combined with policies and procedures to implement and operate the system. It should consist of:

a) **Security Policy:** An organisational document that describes how to handle keys and valuable information.

b) **Certification Practices Statement (CPS):** An operational procedure document detailing how the Security Policy will be enforced and supported.

c) **Certificate Authority (CA):** The trust basis of a PKI, as it manages public key certificates for their whole life cycle. This includes activities such as: issuing certificates to entities; schedule expiration of certificates; revoke certificates if required; and publishing Certificate Revocation Lists (CRLs).

d) **Registration Authority (RA):** The interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The TOE is designed to accommodate a wide variety of CPSs. In particular, the registration process may involve the acquisition and verification of a variety of data from users, directly in face-to-face requests or indirectly via remote requests.

e) **Certificate Distribution System:** A mechanism for delivering end-user certificates and their status to the parties that rely upon them. The TOE can issue certificates in a wide variety of formats and deliver them using a number of mechanisms including distributing certificates in software or on cryptographic hardware.

f) **PKI-enabled applications:** Applications that utilise the PKI framework to provide end-to-end security such as email and Virtual Private Networks (VPNs).

2.3 Security Policy

13 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

Name	Description
SPM_TOE_CONFIDENTIALITY	Private key material is encrypted for the receiver by using key exchange using the receiver's public key certificate.
SPM_USER_CONFIDENTIALITY	Private key material is encrypted for the receiver by using key exchange using the receiver's public key certificate.
SPM_TOE_INTEGRITY	Security relevant TOE data is protected from modification by use of digital signatures.
SPM_USER_INTEGRITY	Security relevant user data is protected from modification by use of digital signatures.
SPM_SIGNATURE_VALIDITY	In relation to authenticating signed data against a given identity as well detecting Inter TOE Security Functions (TSF) modification of data, the signature is determined to be valid if: a) The entity certificate is in the PKI (for PKI entities). b) The signature is verified. c) Optionally checking for an appropriate extension. d) The certificate has not expired nor has been revoked or suspended.

SPM_SECURE_HASH	Security relevant messages and data are hashed, and signed, for integrity checking. The receiver can verify that the message or data is unmodified by checking the hash of the message with the hash encrypted in the signature.
SPM_PASSWORD_METRIC	Enforced when Personal Secure Environment (PSE) or Public Key Cryptography Standard (PKCS)#12 information is generated by TOE components.
SPM_REVOKE_CERTIFICATE	An entity can request a revocation of their certificate, but only an authorised entity can authorise the revocation.
SPM_REMOVE_PKI	The CA Operator (CAO) with PKI management attributes can remove an entity from the PKI directly.
SPM_CHANGE_WEBRAO_GROUP	A Web RA Operator (WebRAO) user may only authorise requests for certificates which have been requested using a registration policy to which they have been granted access.
SPM_CHANGE_CAO_ATTRIBUTE	The operations that a CAO can perform are controlled by their privileges.
SFP_SIGNED_MESSAGES	Several of the components sign messages to other components within the TOE and to users external to the TOE.
SFP_SIGNED_DATA	Certain TOE data and certain user data is signed when being saved to the database.
SFP_AUDITOR	The audit functions can only be accessed by the roles with auditor attributes.

2.4 TOE Architecture

14 The TOE consists of the following major architectural components:

a) CA components.

b) RA components.

c) Utilities.

2.4.1 Certificate Authority Components

15 The CA Components are responsible for the generation and publication of certificates and certificate revocation lists, and for the overall management of the PKI. The components are:

a) **CA service:** The CA service's primary purpose is to sign and issue digital certificates.

b) **CAO:** The CAO module provides a GUI for the administrator to manage the PKI.

c) **Publisher (not part of the TOE):** The Publisher handles all of the publishing requirements of the CA, including the ability to publish to a wide range of different directories (including Microsoft's Active Directory), multiple directories, and Online Certificate Status Protocol (OCSP) responders. However, the Publisher may be used in conjunction with the TOE as it does not contain any security functionality relied upon by the TOE.

d) **Certificate Status Server (CSS):** The CSS provides real-time certificate status information to the other TOE components. It also acts as a responder to OCSP requests.

2.4.2 Registration Authority Components

16 The Registration Authority components are responsible for gathering registration information and revocation requests, authorising requests, and handling renewals. The components are:

a) **RA service:** This component acts as a router between the RA Operators (WebRAOs), Protocol Handlers, and the CA.

b) **The RA Event Viewer:** This component provides a GUI for retrieving and performing limited actions on the audit events from the RA database.

c) **RA eXchange (RAX):** The RAX provides a communication link between the RA and the Protocol Handlers, WebRAOs and the WebHandler. It also acts as an entry point in the TOEs RA database. It receives requests, retrieves or inserts data in the database according to the requests, and determines the appropriate response.

d) **Protocol Handlers:** The Protocol Handlers handle certification requests using such protocols such as web, email, and Cisco Simple Certificate Enrollment Protocol (SCEP). Note that the Public Key Infrastructure X.509 Certificate Management Protocol (PKIX CMP) Handler does not form part of the TOE.

e) **WebRAO:** The WebRAO enables its users to authorise certification and revocation requests. These requests will have been sent from the Protocol Handlers, or from other WebRAO users. It can also handle face-to-face registrations.

2.4.3 TOE Utilities

17 The TOE contains a number of utilities for handling functions such as token management, key generation, database setup, and service management:

a) **Token Manager Utility:** The Token Manager allows an administrator to manage the various PSEs used in PKIs including smart card and Hardware Security Module (HSM) PSEs.

b) **Service Manager Utility:** The Service Manager provides an interface that allows an administrator to start and stop all of the server components.

c) **Database Wizard Utility (DBW):** The DBW is used to initially create the Oracle tables, and to create database user accounts for the TOE users.

d) **Key Generator Utility (KGU):** The main purpose of this utility is to perform key generation for the TOE components. The Key Generator supports both hardware based cryptographic devices (HSMs, smart cards), as well as software.

2.5 Clarification of Scope

18 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

19 The TOE provides the following evaluated security functionality:

a) **Security Audit:** The TOE is capable of generating audit records of security events in the following components: CA; CAO; RA; RA Event Viewer; and RAX. The TOE can provide a select group of users the capability of reading all, or a defined selection of, audit records. The TOE protects audit records from unauthorised deletion and is capable of detecting modifications of records.

b) **Communication:** The TOE generates evidence of origin for transmitted: PKI Certificates; PKI Entity interactions; PKCS#11 Interactions; End user certificates; Certificate Revocation Lists; and Group Lists. The TOE can verify the evidence of origin information if it has access to the originators public key certificate and its certificate status.

c) **Cryptographic Support:**

i) **Key Generation:** The TOE can generate Triple Data Encryption Standard (3DES) (168 bits), Digital Signature Algorithm (DSA) (1024, 1536 bits) and Rivest Shamir Adleman (RSA) (1024, 2048, 4096 bits) cryptographic keys.

ii) **Public Key Distribution:** Cryptographic keys can be distributed as X.509 public key certificates in Privacy Enhanced Mail (PEM), Distinguished Encoding Rules (DER) and PKCS#7 certificates-only formats.

iii) **Private Key Distribution:** Private cryptographic keys can be distributed using PKCS#11 and PKCS#12 standards by the WebRAO component.

iv) **Key Access:** The TOE can use cryptographic keys from a PKCS#12 or PKCS#11 device.

v) **Key Destruction:** The TOE overwrites all cryptographic keys in memory before deallocation.

vi) **Digital Signature creation and verification:** The TOE can create and verify the following digital signatures: RSA signature with Secure Hash Algorithm #1 (SHA-1) or Message-Digest #5 (MD5) hashing; and DSA signature with SHA-1 hashing.

vii) **Hash Functions:** The TOE can perform SHA-1 (160 bits) and MD5 (128 bit) hashing functions.

viii) **Symmetric Encryption and decryption:** The TOE can perform symmetric encryption and decryption using the 3DES algorithm.

d) **User Data Protection:**

i) **Access Control:** The TOE only allows a user to undertake an operation among controlled subjects and objects if the user has the required attributes for the role.

ii) **Information Flow Control:** The TOE enforces the Security Policy Model.

iii) **Internal Transfer Protection:** The TSF prevents the modification of user data when it is transmitted between physically separated parts of the TOE. If the digital signature is not verified, the data is assumed to be corrupt or from an untrusted source.

e) **Identification and Authentication:** The TOE maintains a list of security attributes of users including: a X.500 Distinguished Name;

user role and group; registered entity; authentication method and any associated access information. The CAO and WebRAO components require that a user successfully authenticate before any other actions can be performed on behalf of that user. The TOE also enforces a minimum password complexity.

f) **Security Management:** The TOE restricts certain management functions based upon the subject requesting the action and the object it is applied to. The TOE can associate users to these roles. Specialised security management functions within the TOE include revocation and time-limited authorization.

g) **Protection of the TOE Security Functions:** The TOE protects the integrity of all TSF data transmitted between the TOE and trusted remote IT products. The TOE can protect the confidentiality and integrity of TSF data transmitted between itself and other parts of the TOE. If requested, the TOE can provide an acknowledgement of the unmodified receipt of TSF data.

20 Section 5 of the Security Target (Ref [1]) provides further details on the security functions provided by the TOE.

2.5.2 Non-evaluated Functionality

21 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The functions and services that have not been included as part of the evaluation are provided below:

a) **Unicert Publisher:** The Publisher may be used in conjunction with the TOE as it does not contain any security functionality relied upon by the TOE.

b) **PKIX CMP Protocol Handler:** Protocol handler whose purpose is to handle PKIX CMP certificate requests. This functionality may not be used in the evaluated configuration.

c) **Advanced Registration Module:** This functionality may not be used with the TOE in its evaluated configuration.

d) **UniCERT Programmatic Interface:** This functionality may not be used with the TOE in its evaluated configuration.

e) **Data Base Wizard Utility:** The Database Wizard is used to initially create the Oracle tables, and to create database user accounts for the UniCERT users. It does not contain security functionality, and does not handle security relevant data, but only exists to assist an administrator begin working with the TOE.

f) **Key Archive Server:** The Key Archive Server may be used in conjunction with the TOE to support the archive and recovery of user private keys. The TOE provides an evaluated interface to the Key Archive Server.

2.6 Usage

2.6.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration(s). Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that configuration(s) meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

24 The TOE is implemented entirely in software.

25 A number of configuration options of the product must be set as specified by the administrator for the product to be in its evaluated configuration, as follows:

a) Automatic startup of the TOE services must not be used. All TOE services must be set to manual startup so that the passphrases or PINs used to open the PKI keys are not stored anywhere on the machines running the TOE.

b) Elliptic Curve Digital Signature Algorithm key algorithm must not be used in registration policies. It does not form part of the evaluated product.

c) Registration policies can provide an option to allow *No Authorisation*. This feature must not be used in the evaluated configuration.

26 There are multiple valid evaluated configurations for the TOE:

a) **Root CA Configuration:** CA, CAO, database and optionally Publisher installed on one system, optionally using an HSM for the CA, and a smart card for the CAO.

b) **Single CA/RA Configuration:** all the components resident on one system, with cryptographic functionality implemented in software. Alternatively, the databases may be installed on a separate system, and cryptographic functions supplied by HSMs and smart cards.

c) **Separate CA and RAs:** CA and RA are implemented on separate systems. Cryptographic functionality can be implemented in software or supplied by HSMs and smart cards.

27 Sections 2.4 and 2.5 of the Security Target (Ref [1]) provide further details on valid evaluated configurations of the TOE.

2.6.2 Delivery procedures

28 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

29 Upon an order being processed and verified, the developer's distribution team copy the appropriate Master CDs, label them and send via courier in a tamper-evident bag to the purchaser, along with the following documentation:

a) Delivery Note (detailing customer contact details, quantity and description of shipment, method of dispatch, date of despatch and Courier Air Way Bill Tracking number).

b) Export Licence (if required).

c) Pro Forma (if outside EU, containing Air Way Bill Number, Customer Details, Licence Number, declaration that software is dual use goods and value of software).

d) Courier (DHL) Air Way Bill.

30 If supplied with the purchaser's email address, the distribution team provides the purchaser with the shipping details so the package may be tracked in transit.

31 Once the order has been received, the purchaser should:

a) Check the integrity of the tamper-evident seals on the packaging. If the packaging does show any signs of tampering, the purchaser should contact the supplier.

b) Check the product description on the delivery note.

c) Check the label on the installation disks identify the product as UniCERT 5.2.1, including the patch disk UniCERT 5.2.1 Patch 900.

d) Return the proof of delivery sheet to Cybertrust.

32 Appendix A of the Security Target (Ref [1]) provides a full list of the contents of the CDs.

2.6.3 Product Installation

33 Guidance on installing the product in the evaluated configuration is provided in the following documentation:

a) Security Target (Ref [1]).

b) Additional Guidance for Users and Administrators of the Common Criteria Evaluated version of Cybertrust UniCERT 5 (Ref [3]).

c) UniCERT Version 5.2.1 Installation Guide for Windows, Betrusted 2004 (Ref [4]).

d) UniCERT Version 5.2.1 Administrator's Guide for Solaris, Betrusted 2004. (Ref [5]).

2.6.4 Documentation

34 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage.

35 The documentation that is provided varies depending on which variation of the TOE is purchased. The following documentation is provided with the Windows version of UniCERT Version 5.2.1:

a) UniCERT Version 5.2.1 Release Notes for Windows, Betrusted 2004.

b) UniCERT Version 5.2.1 Installation Guide for Windows, Betrusted 2004.

c) UniCERT Version 5.2.1 Product Overview, Betrusted 2004.

d) UniCERT Version 5.2.1 Database Administrator's Guide, Betrusted 2004.

e) UniCERT Version 5.2.1 Administrator's Guide for Windows, Betrusted 2004.

f) UniCERT Version 5.2.1 Configuration Guide, Betrusted 2004.

g) UniCERT Publisher Version 5.2.1 Administrator's Guide for Windows, Betrusted 2004.

h) UniCERT Version 5.2.1 Extensions Guide, Betrusted 2004.

i) UniCERT WebRAO Version 5.2.1 Client User's Guide, Betrusted 2004.

j) UniCERT Core v5.2.1 known issues "Readme.html" file for Windows.

k) Error Message Listing "Remarks.htm".

l) Copyright and License Agreement Information.

36 The following documentation is provided with the Solaris version of UniCERT Version 5.2.1:

a) UniCERT Version 5.2.1 Release Notes for Solaris, Betrusted 2004.

b) UniCERT Version 5.2.1 Installation Guide for Solaris, Betrusted 2004.

c) UniCERT Version 5.2.1 Product Overview, Betrusted 2004.

d) UniCERT Version 5.2.1 Database Administrator's Guide, Betrusted 2004.

e) UniCERT Version 5.2.1 Administrator's Guide for Solaris, Betrusted 2004.

f) UniCERT Version 5.2.1 Configuration Guide, Betrusted 2004.

g) UniCERT Publisher Version 5.2.1 Administrator's Guide for Solaris, Betrusted 2004.

h) UniCERT Version 5.2.1 Extensions Guide, Betrusted 2004.

i) UniCERT WebRAO Version 5.2.1 Client User's Guide, Betrusted 2004.

j) UniCERT Core v5.2.1 known issues "Readme.html" file for Solaris.

k) Error Message Listing "Remarks.htm".

l) Copyright and License Agreement Information.

37 The following documentation is provided with the CD for Unicert v5.2.1 patch 900 for Windows:

a) UniCERT v5.2.1 Patch 900 Release Notes for Windows, Cybertrust 2005.

b) Additional Guidance for Users and Administrators of the Common Criteria Evaluated version of Cybertrust UniCERT 5, Version 5.0i, October 2005, Cybertrust 2005.

38 The following documentation is provided with the CD for Unicert v5.2.1 patch 900 for Solaris:

a) UniCERT v5.2.1 Patch 900 Release Notes for Solaris, Cybertrust 2005.

b) Additional Guidance for Users and Administrators of the Common Criteria Evaluated version of Cybertrust UniCERT 5, Version 5.0i, October 2005, Cybertrust 2005.

2.6.5 Secure Usage

39 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

a) A.DisposalofAuthenticationData: Authentication data is properly disposed of.

b) A.AuditReview: Authorised auditor(s) will regularly review audit records.

c) A.CPS: PKI users are familiar with and uphold the CP and CPS that the PKI operates.

d) A.CompetentPKIUsers: PKI users are competent.

e) A.MaliciousCodeNotExecuted: The TOE trusted users do not execute malicious code.

f) A.SecureInstallation: The system is set up and operated securely.

g) A.Guidance: The PKI administrators and users read and follow the guidance material.

h) A.CommunicationsProtection: Communications are protected both logically and physically.

i) A.PhysicalProtection: The physical boundary of the system is protected.

j) A.Timesource: There is a trusted, accurate and reliable time source.

40 In addition, the following organisational security policies must be in place:

a) P.Accountability: Individuals are accountable for their actions.

b) P.DisposalOfAuthenticationData: Authentication data and privileges are removed after access has been revoked.

c) P.Guidance: Installation and usage guidance is provided for the system.

d) P.QualifiedTOEUsers: The TOE users should be sufficiently qualified to perform their duties.

e) P.RoleSeparation: The TOE owners must ensure that there is independence in roles.

f) P.Cryptography: The TOE owners are responsible for insuring the TOE uses secure algorithms and parameters for all cryptographic functions.

g) P.HardwareCryptography: The TOE owners are responsible for ensuring if the TOE uses external cryptographic devices, then secure algorithms and parameters for all cryptographic functions are employed, and that there is sufficient protection of the keys.

h) P.ApplyFlawRemediation: The TOE owners are responsible for insuring the TOE security functionality is maintained by applying developer supplied flaw remediation.

41 Section 3 of the Security Target (Ref [1]) provides a full description of the assumptions and the organisational security policies.

Chapter 3 - Evaluation

3.1 Overview

42 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

43 The criteria against which the Target of Evaluation (TOE) has been evaluated are expressed in the Common Criteria for Information Technology Security Evaluation (Refs [6], [7], [8]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [9]). The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [10], [11], [12], [13]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [14]) were also upheld.

3.3 Functional Testing

44 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests (approximately 20%) in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

45 The developer performed an extensive vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

46 The evaluators augmented the developer's analysis by considering vulnerabilities in the TOE in the following categories:

a) Generic vulnerabilities.

b) Bypassing TOE security functionality.

c) Tampering.

d) Direct Attacks.

e) Misuse.

47 One penetration test was devised to test the strength of the mechanism that protects the Personal Secure Environment (PSE) file. This test demonstrated that this security mechanism meets the Strength of Function (SOF) Basic level.

48 To supplement the penetration test, the evaluators examined a sample of the source code, for indication of buffer overflows and other memory allocation problems. No issues were identified.

Chapter 4 - Certification

4.1 Overview

49 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

50 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [15]), the Australasian Certification Authority (ACA) certifies the evaluation of UniCERT 5.2.1 performed by the Australasian Information Security Evaluation Facility, LogicaCMG.

51 LogicaCMG has found that UniCERT 5.2.1 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

52 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

53 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the Target of Evaluation (TOE), and a subset of the implementation, to understand the security behaviour.

Assurance is additionally gained though an informal model of the TOE security policy.

54 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, Strength of Function (SOF) analysis, evidence of a developer search for obvious vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

55 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

56 Augmentation is a term used in the CC to describe the addition of assurance components to a particular EAL that are not included in the defined EAL packages (each made up of multiple assurance components). Augmentation is denoted by a '+' symbol appended after the EAL (e.g. EAL4+).

57 The scope of this evaluation was augmented with the ALC_FLR.2 (Flaw reporting procedures) assurance component which requires that the developer has established flaw remediation procedures that can track and correct security flaws. Users must also be informed about these flaw remediation procedures.

4.4 Recommendations

58 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to Australian Government Information and Technology Security Manual (ACSI 33) (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

59 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance documentation is followed (Refs [1], [3], [4], [5] and Section 2.6.4 Documentation), the ACA also recommends that users:

a) Implement appropriate key and certificate generation and management policies;

b) Ensure any external cryptographic hardware used with the TOE is evaluated to an appropriate assurance level; and

c) Ensure strong pass-phrases are used in the protection of keys and certificates.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Cybertrust UniCERT 5, Version 5.0ab, January 2006, Cybertrust.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Additional Guidance for Users and Administrators of the Common Criteria Evaluated version of Cybertrust UniCERT 5, Version 5.0i, October 2005, Cybertrust.

[4] UniCERT Version 5.2.1 Installation Guide for Windows, 2004, Betrusted.

[5] UniCERT Version 5.2.1 Administrator's Guide for Solaris, 2004, Betrusted.

[6] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, Incorporated with interpretations as of 19 June 2003.

[7] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, Incorporated with interpretations as of 19 June 2003.

[8] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, Incorporated with interpretations as of 19 June 2003.

[9] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, Incorporated with interpretations as of 19 June 2003.

[10] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.0, 21 February 2006, Defence Signals Directorate.

[11] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.0, 21 February 2006, Defence Signals Directorate.

[12] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.0, 21 February 2006, Defence Signals Directorate.

[13] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.0, 21 February 2006, Defence Signals Directorate.

[14] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[15] EFA T028 Cybertrust UniCERT 5.2.1 Evaluation Technical Report, Issue 1.0, July 2006, LogicaCMG.

A.2 Abbreviations

3DES	Triple Data Encryption Standard
ACA	Australasian Certification Authority
ALC_FLR	Assurance in Life Cycle Flaw Remediation
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CA	Certificate Authority
CAO	Certificate Authority Operator
CC	Common Criteria
CEM	Common Evaluation Methodology
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSS	Certificate Status Server
DBW	Database Wizard Utility
DER	Distinguished Encoding Rules for ASN.1
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
HSM	Hardware Security Module
KGU	Key Generator Utility
MD5	Message-Digest #5
OCSP	Online Certificate Status Protocol
PEM	Privacy Enhanced Mail
PH	Protocol Handler
PKCS	Public Key Cryptography Standard (Published by RSA Security Inc.)
PKI	Public Key Infrastructure
PKIX CMP	Public Key Infrastructure X.509 Certificate Management Protocol
PP	Protection Profile
PSE	Personal Secure Environment
RA	Registration Authority
RAX	RA eXchange

RSA	Rivest Shamir Adleman
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm #1
SOF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network
WebRAO	Web Registration Authority Operator