AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAMME

Certification Report

Certificate Number: 2000/16

Baltimore Technologies Ltd

UniCERT
Version 3.1.2.A

Issue 1.1
November 2000

Issued by: -

Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

UniCERT (Version 3.1.2.A) is a software product developed by Baltimore Technologies Ltd. It provides the functionality to allow an organisation to create and maintain a Public Key Infrastructure (PKI). It provides facilities for creating and operating the PKI components and for issuing and revoking certificates both to the other PKI components, and to external users.

This report describes the evaluation findings of the UniCERT Version 3.1.2.A product to the ITSEC Assurance Level E3. It also includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product in order to meet the ITSEC E3 level of assurance. It concludes that the product has met the target Assurance Level of E3.

Originator ____________________

Matthew Earley
Certifier
Defence Signals Directorate

Approval ____________________

Sandra Ragg
Manager, Industry Engagement
Defence Signals Directorate

Authorisation ____________________

Stewart Skelt
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

CERTIFICATION STATEMENT ii
TABLE OF CONTENTS iii
Chapter 1 Introduction 1
Intended Audience 1
Identification of Target of Evaluation 1
Evaluation 1
General Points 2
Scope of the Evaluation 2
Chapter 2 Security Overview of UniCERT 3
Overview of the TOE 3
Documentation 5
Chapter 3 Evaluation Findings 6
Introduction 6
Assurance Results 6
Correctness – Construction 6
Correctness – Operation 8
Effectiveness – Construction 8
Effectiveness – Operation 9
Specific Functionality 10
Discussion of Unresolved Issues 10
General Observations 11
Chapter 4 Conclusions 12
Certification Result 12
Scope of the Certificate 12
Recommendations 12
Appendix A References 24
Appendix B Summary of the Security Target 27
Security Target 27
Product Rationale for the TOE 27
Security Objectives 27
Intended Method of Use and Intended Environment 27
Summary of Security Features of the TOE 28
Appendix C Contents of Distribution Package 31
Configuration for Evaluation 31
Software 31
Third Party Software 31
Procedures for Determining Version of TOE 32

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of UniCERT Version 3.1.2.A (hereafter referred to as UniCERT) developed by Baltimore Technologies Ltd. It is intended to assist potential Australian Government 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 UniCERT evaluated was Version 3.1.2.A.

1.3 UniCERT is a product that allows an organisation to create and maintain a Public Key Infrastructure (PKI). A typical UniCERT installation consists of at least one Certification Authority and one Registration Authority component. Microsoft Windows NT 4.0 with Service Pack 5 and Oracle 8.0.5 are required to support the operation of UniCERT.

1.4 UniCERT consists of two CD-ROMs. The first contains the UniCERT software, and the administration and user guidance. The second contains additional software required as part of the evaluated configuration. The version of UniCERT on the CD-ROMs should read **3.1.2** and **3.1.2.A** respectively**.**

1.5 For further details of the evaluated components of UniCERT, including details of how to identify the evaluated version, refer to Appendix C.

Evaluation

1.6 The evaluation was carried out in accordance with the rules of the Australasian Information Security Evaluation Programme (AISEP) which is described in Evaluation Memorandum 1 and Evaluation Memorandum 2 (refs [1,2] respectively).

1.7 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), UniCERT, in meeting its Security Target (ref [3]). The criteria against which the TOE is judged are expressed in the ITSEC (ref [4]). This describes how the degree of assurance is expressed in terms of the levels E1 to E6 and E0, where the latter indicates that the TOE has failed to meet its targeted level of assurance. The methodology used is described in ITSEM and Evaluation Memoranda 4 and 5 (refs [5,6,7]).

1.8 The evaluation was performed by CMG Admiral between September 1999 and July 2000, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). The evaluation of the cryptographic mechanisms was conducted by DSD in parallel with the AISEP evaluation with the Certification Group being advised of its completion in July 2000 (ref [23]). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [8]) describing the evaluation and its results was presented to the ACA. This Certification Report was then produced, based on the contents of the ETR, the Certification Group's knowledge of the evaluation, and the results of the cryptographic evaluation.

1.9 An additional activity was performed by the Certification Group in November 2000 to ensure that a potential low risk vulnerability in the product (that was outside the scope of the evaluation) was not exploitable in the TOE. This resulted in a supplement to the ETR (ref [24]) and an updated issue of the Certification Report. The results of this activity are discussed in paragraph 3.2.

1.10 The Security Target (ref [3]) claimed an assurance level for the product of E3 and minimum strength of mechanism of MEDIUM.

General Points

1.11 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.

1.12 The UniCERT product should only be used within the intended environment and in accordance with the method of use as explained in (ref [3]). In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

1.13 Ultimately, it is the responsibility of the user to ensure that the UniCERT 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 from the product vendor, and reads this Certification Report thoroughly prior to deciding whether to purchase the product.

Scope of the Evaluation

1.14 The scope of the evaluation is limited to those claims made in the Security Target (ref [3]). All security related claims in the Security Target were evaluated by CMG Admiral. A summary of the Security Target is provided in Annex B of this Certification Report. The cryptographic algorithms were evaluated by DSD for Australian Government use and found to be appropriate for the protection of material classified RESTRICTED, and non National Security classifications including IN-CONFIDENCE, PROTECTED and, in consultation with DSD, HIGHLY PROTECTED.

Chapter 2 Security Overview of UniCERT

2.1 Potential users are ***strongly*** recommended to read the Security Target (ref [3]). This explains the security functionality of the UniCERT 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 Baltimore Technologies Ltd.

Overview of the TOE

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

2.3 UniCERT is a product that provides registration, PKI management and certification authority functions that enable the establishment and functioning of a PKI. UniCERT can be used to manage all the certificates necessary for a system requiring security for end users, such as a secure messaging system, or security on web browsers.

2.4 UniCERT provides the ability to set up a centralised or a distributed architecture for organisations of various sizes, using a single level or multilevel certification authority to suit the structure, function and geography of the organisation and to manage this PKI centrally.

2.5 UniCERT is composed of a number of different software components. The main components are the Certification Authority (CA), Registration Authority (RA), CA Operators (CAO), RA Operators (RAO), Token Manager and the Gateway. These components can be placed on separate hardware systems, to allow the distribution of workload to corporate departments so that bottlenecks in processing within the PKI can be reduced.

2.6 UniCERT is used to generate X.509 certificates for end users and for the different components within the PKI. It can also revoke certificates and generate certificate revocation lists (CRLs). Both certificates and CRLs can be published on an X.500 directory using the Lightweight Directory Access Protocol (LDAP).

2.7 Apart from the CAO and RAO components, UniCERT runs as an unattended server on any machine hosting Microsoft Windows NT 4.0 with Service Pack 5. The CAO and RAO components require input from a user to fulfil their functions.

2.8 Audit information (in the form of operational errors and events) is generated securely by using the component's private key to sign the information. This information is then written to an Oracle database. In the case of database failure and/or user authentication failure to the UniCERT components, the audit information is sent to the Windows NT event log. However, these entries are not signed by UniCERT components.

2.9 The CA is the highest hierarchical component within a PKI system. UniCERT allows the CA component to operate both in the role of a root CA or as a subordinate CA within the hierarchy. Once installed and configured, the CA is intended to run as a Windows NT service. The primary function of the CA is to sign and issue certificates. Each CA requires its own CAO and at least one RA to operate.

2.10 The CAO component is the management interface to the UniCERT CA and the other components within the PKI. Through the CAO the various elements that make up the PKI can be defined. Additionally, the CAO is used to enter certificate details for the components of the PKI as well as setting up and distributing Customer Registration Policies for the RAOs.

2.11 The RA component provides a facility for forwarding certification and revocation requests from the RAO(s) to the CA. The RA is also able to forward certification and revocation requests from a Gateway to a CA. The RA also provides a facility for forwarding replies from the CA to the Gateway which in turn sends the reply to an end user. The RA is also responsible for tracking all events in the RA database, which can be accessed by the RAO as required.

2.12 The RAO component provides the interface through which requests for certification and revocation are received and processed. Requests can be received via email, WWW (remote requests through a Gateway) or in person (face to face). The RAO user must process these requests and perform whatever procedural steps are necessary to ensure that the end user's credentials are valid.

2.13 The Gateway component allows users to receive certificates via a Gateway either by email or web, as discussed above. The Token Manager component provides the means by which an operator can change the passphrase that protects the CAs, CAOs, RAs and RAOs private keys.

2.14 UniCERT provides five security objectives to create and maintain the confidentiality and integrity of the PKI components. In doing so, UniCERT implements nine Security Enforcing Functions (SEFs) in software. These are provided individually or in collaboration by one or more of the UniCERT components identified above. There is no hardware or firmware associated with the evaluated configuration of the product. In addition, the evaluation of UniCERT has not included end user PKI client software. Organisations looking for a complete PKI solution should refer to other products listed in the Evaluated Products List (ref [22]) that could be interoperable with a PKI managed by UniCERT.

2.15 More detailed information on the UniCERT SEFs can be found in the Security Target for the UniCERT product (ref [3]), and in Appendix B of this report.

Documentation

2.16 Before using the product, administrators should ensure that they are aware of and fully understand the relevant operational documentation. Administrators should ensure that they read Chapter 4 of this document, and the associated administration and user manuals contained on the CD-ROMs (refs [9]-[20]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of UniCERT followed a course consistent with the generic evaluation work programme described in the ITSEM (ref [5]), with work packages structured around the evaluator actions described in the ITSEC (ref [4]). The results of this work are reported in the ETR (ref [8]) under the ITSEC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ref [3]).

3.2 In November 2000, the developer had raised concerns of a potential vulnerability in the product that was outside the scope of the evaluation. While this potential vulnerability was outside the scope of the evaluation and was assessed as low risk, the ACA determined that it was in the interest of the Commonwealth to ensure this issue had been appropriately corrected (in a software patch) and therefore eliminated from the product. This resulted in an additional activity performed by the Certification Group in November 2000 (ref [24]). The results of this activity were consistent with the findings of the ETR (ref [8]) and recommended that the TOE maintain its ITSEC E3 level of assurance.

Assurance Results

Correctness – Construction

3.3 This aspect of the evaluation examined both the development process (including the Security Target, the Architectural and Detailed Designs, and the Implementation) and the development environment where the development took place.

Requirements

3.4 The final version of the Security Target (ref [3]) described the Security Enforcing Functions (SEF) and mechanisms provided by the TOE, and contained a product rationale that included the intended method of use, the intended environment and the assumptions about physical, personnel and procedural security. The Security Target also described how the functionality of the TOE was sufficient to counter the assumed threats.

3.5 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Security Target.

Architectural Design

3.6 The final version of the formal Architectural Design correctly described the general structure of the TOE and the external interfaces. The Architectural Design described how the SEFs from the Security Target are provided. The Architectural Design described that the TOE was structured and separated into two security enforcing components (the Certification Authority and Registration Authority).

3.7 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Architectural Design.

Detailed Design

3.8 The final set of Detailed Design documents properly identified all of the security mechanisms, described the realisation of the SEFs, and provided a mapping of the SEFs and their associated security enforcing mechanisms down to the basic components of the Detailed Design, and adequately documented the interfaces.

3.9 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Detailed Design.

Implementation

3.10 The evaluators were able to determine that the implementation described the correspondence between the source code and the basic components of the Detailed Design. The test documentation described how the developer's tests covered the implementation of the TOE SEFs, and were assessed to be of a standard that allowed for the tests to be repeatable and reproducible.

3.11 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Implementation.

Development Environment

3.12 The evaluators were able to determine that tool-based configuration control systems, appropriate quality practices and procedures, and appropriate levels of physical and procedural security supported the development environment, ensuring the confidentiality and integrity of the TOE and its associated documents during development.

3.13 As the TOE contains software, the evaluators performed an assessment of programming languages and compilers. The evaluators were able to determine that a well-defined programming language was used in the implementation of the TOE, and that appropriate coding standards and guidelines were applied to the development of the TOE.

3.14 The above results have enabled the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Development Environment.

Correctness – Operation

3.15 This aspect of the evaluation looked at how the delivery and configuration procedures maintain the security of the TOE, and how operational procedures ensure secure start-up and operation.

3.16 The evaluators determined that the operational documentation (refs [9]-[20]) described the operation of the SEFs relevant to the administrator of the TOE and described how to operate the TOE in a secure manner.

3.17 The evaluators determined that the startup and operation documentation (refs [9]-[20]) described the procedures for secure startup and operation of the TOE.

3.18 The evaluators determined that the manufacturing and delivery documentation (ref [21]) described the delivery arrangements from the development environment to the customer site, and that the generation of the TOE for delivery was described. Further recommendations relating to the secure delivery and authentication of UniCERT are provided in Appendix C of this Report.

3.19 The above results allowed the certifiers to conclude that the TOE met the requirements for ITSEC E3 in regard to its Operational Documentation and Environment.

Effectiveness – Construction

3.20 This aspect of the evaluation dealt with:

(i) the suitability of the TOE's security enforcing functions to counter the threats identified in the Security Target;

(ii) the ability of the security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

(iii) the ability of the TOE's security mechanisms to withstand direct attack; and

(iv) the question of whether known security vulnerabilities in the construction of the TOE could, in practice, compromise its security.

Suitability Analysis

3.21 The evaluators determined that the developer’s Suitability Analysis demonstrated that all of the threats listed in the Security Target were adequately countered by the stated SEFs and/or by a combination of other physical, personnel or procedural security measures. These findings were confirmed against an independent Suitability Analysis performed by the evaluators.

3.22 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Suitability Analysis.

Binding Analysis

3.23 The Binding Analysis must analyse all the potential relationships between security enforcing functions and mechanisms to ensure that there is no way for any mechanism or function to conflict with, or contradict the intent of, other security enforcing functions or mechanisms. The evaluators found that the developer's Binding Analysis demonstrated that it was not possible for any binding element to conflict with or contradict the intent of any other binding element. These findings were confirmed against an independent Binding Analysis performed by the evaluators.

3.24 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Binding Analysis.

Strength of Mechanisms Analysis

3.25 The Strength of Mechanisms Analysis correctly identified the mechanisms of the TOE as cryptographic and critical to the security of the TOE. DSD has determined that the mechanisms used by the TOE are appropriate for Australian Government use (ref [23]).

3.26 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Strength of Mechanisms Analysis.

Construction Vulnerability Assessment

3.27 For this aspect of the evaluation, the evaluators examined the developer's Construction Vulnerability Assessment that claimed several known vulnerabilities in the construction of the TOE, and performed their own assessment to find potential vulnerabilities in the TOE. The assessments demonstrated that the vulnerabilities are not exploitable in the intended environment of the TOE, as they are adequately covered by other, uncompromised, external security measures. Further testing of the TOE by the evaluators did not reveal any exploitable vulnerabilities due to its construction.

3.28 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Construction Vulnerability Assessment.

Effectiveness – Operation

3.29 This aspect of the evaluation entailed checking how easy the TOE is to use in a secure manner, and making an assessment of the known vulnerabilities in its operation to determine whether they could, in practice, compromise its security.

Ease of Use Analysis

3.30 The evaluators found that the TOE could not be configured or used in a manner which was insecure but which an Administrator or end-user would believe to be secure. Further, the evaluators found that the TOE could be installed and used securely using only the User and Administration Manuals (refs [9]-[20]) as guidance, and that all possible failure modes were adequately documented, along with their effects.

3.31 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Ease of Use.

Operational Vulnerabilities Assessment

3.32 During this part of the evaluation, the evaluators assessed the known vulnerabilities in the operation of the TOE to determine whether they could, in practice, compromise the security of the TOE. The evaluators found that the developer's Operational Vulnerability Assessment correctly identified several vulnerabilities in the operation of the TOE, and performed their own assessment to find potential vulnerabilities in the TOE. The assessments demonstrated that the vulnerabilities are not exploitable in the intended environment of the TOE, as they are adequately covered by other, uncompromised, external security measures. Further testing of the TOE by the evaluators did not reveal any operational vulnerabilities that were exploitable in practice.

3.33 As a result of the above determinations, the certifiers concluded that the TOE met the ITSEC E3 requirements for the Operational Vulnerability Assessment.

Specific Functionality

3.34 The Security Enforcing Functions (SEFs) provided by UniCERT are specified in section 3.0 of the Security Target (ref [3]) and summarised in Appendix B of this report.

3.35 The evaluators found that the product correctly and effectively provided the functionality specified in the Security Target (ref [3]).

Discussion of Unresolved Issues

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

General Observations

3.37 The certifiers would like to acknowledge the invaluable assistance provided by Baltimore 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.

3.38 Further, the certifiers would like to acknowledge the efforts of CMG Admiral 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 (refs [8], [24]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that UniCERT has met the requirements of the ITSEC E3 Assurance level.

Scope of the Certificate

4.2 This certificate applies only to version 3.1.2.A of the product. This certificate is only valid when the UniCERT product correctly comprises the designated components. These components are identified in Appendix C and there is an accompanying description explaining how the administrator can verify this version information on delivery.

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 UniCERT should only be used in accordance with the intended environment described in section 3.4 of the Security Target (ref [3]), including consideration of all physical, personnel and procedural security measures. Further, it is recommended that the UniCERT installation be accredited by an appropriate security authority to ensure that the intended environment described in the Security Target (ref [3]), together with the recommendations provided below, exists or has been implemented.

Functionality excluded from the Evaluation

4.5 The UniCERT software package is delivered with several other applications that can be used to support the operation of UniCERT. Not all of these applications have been included in this evaluation. The evaluated configuration has been specified in Appendix C of this Report. **The functionality that has been excluded from this evaluation of UniCERT is as follows:**

1. Archive Server: The CA provides an interface to an Archive Server to support archiving of end-user private keys. This interface must be disabled in the PKI editor.

2. PKCS#11 hardware tokens: UniCERT allows interoperability with other token based technologies (e.g. smartcards). These type of tokens have been excluded from the evaluated configuration.

3. The following restrictions apply for defining Customer Registration Policies:
   i) End User "Certificate Rollover" support cannot be included in any policy.
   ii) Key sizes of 512 bits for RSA and DSA have been excluded.
   iii) ECDSA (Elliptic Curve DSA) has been excluded.
   iv) Cisco SCEP has been excluded.
   v) Multiple RAO authorisation has been excluded.

Please refer to Appendix A of the Security Target (ref [3]) for further information on the constraints placed on the evaluated configuration.

Key Pair Generation for Australian Government Use

4.6 The asymmetric algorithms supported by UniCERT are RSA, DSA, and elliptic curve DSA. As mentioned above, elliptic curve DSA (ECDSA) has not been evaluated by DSD and is therefore not appropriate for Australian Government use.

4.7 For Australian Government use both RSA and DSA are acceptable (although DSA cannot be used for encryption). To be adequately secure all asymmetric key lengths must be at least 1024 bits, for both RSA and DSA. In the case of RSA it is recommended that a key length of 2048 bits be used for the CA.

4.8 UniCERT provides the option of generating multiple key pairs for CAs and end users. **For Australian Government use at least two key pairs should be generated in all cases, with separate keys used for signing and encryption.**

Authentication for Australian Government Use

4.9 Messages between UniCERT PKI entities are hashed using either the SHA-1 or MD5 hashing algorithms as part of the authentication process. The message authentication used in UniCERT is appropriate for Australian Government use.

Password Protection for Australian Government Use

4.10 Private keys for PKI entities are stored in UniCERT using Baltimore Personal Secure Environment (pse) files. The use of Personal Secure Environment files to protect PKI-entity private keys is suitable for Australian Government use, **provided a sufficiently strong password is used.**

4.11 The PKCS#12 format is suitable for Australian Government use provided triple-DES is used as the encryption algorithm. **This can be ensured by disabling weak encryption in the CAO component.**

Digital Signatures for Australian Government Use

4.12 Certificates generated by the CA are hashed using either SHA-1 or MD5, and signed using the CA non-repudiation key. Audit log and revocation list signatures use the CA digital signature and CRL signing keys, respectively. In each case the same hashing algorithm that was used to sign the CA certificate is used.

4.13 Both the SHA-1 and MD5 based signatures are appropriate for Australian Government use.

Pre-installation considerations for UniCERT components

4.14 Administrators should ensure that, prior to installing any UniCERT component, the hardware has been appropriately sanitised and contains no software other than the required Windows NT and Oracle database components. **Furthermore, to avoid the introduction of malicious software and viruses on UniCERT enabled servers, it is recommended that the hard drive of each UniCERT server be re-formatted prior to an installation of the operating system.** Australian Government users should also ensure that no other software is resident on UniCERT enabled servers.

4.15 Potential purchasers of UniCERT 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 UniCERT components. Organisations considering undertaking CA or RA responsibilities need to have a thorough understanding of the technical issues involved in establishing and maintaining a PKI. **Commonwealth Government agencies wishing to implement a PKI are strongly encouraged to contact DSD for further assistance.**

4.16 Operational documentation is delivered with the installation CD-ROMs. They can be viewed in both HTML and PDF format. Each UniCERT component has its own documentation. Prior to installation, administrators need to familiarise themselves with the content of all of these documents (refs [9]-[20]). **Furthermore, administrators are encouraged to contact the Baltimore help desk (Phone: +61 2 9409 6385 / Email: globalsupport@baltimore.com) if any technical problems are encountered with the installation or configuration of UniCERT.**

Considerations for Oracle and Windows NT

4.17 All entries within the Oracle audit log are digitally signed by the relevant entity (CA, CAO, RA or RAO) which created the entry. Access to these audit entries is controlled by Oracle's access control security mechanisms, which were not examined by the evaluators during the evaluation. While the digital signing of each audit entry prevents unauthorised modification of the audit log, there are no security mechanisms offered by the TOE to prevent the audit entries from being deleted. Therefore, **administrators must ensure that access to the Oracle database is restricted to authorised users of the PKI component. Administrators should also ensure that**

appropriate Oracle password policies are being enforced on UniCERT enabled systems.

4.18 Under certain circumstances, the TOE will write events to the Windows NT event log. One such situation arises when the TOE cannot establish communication with the Oracle database. While this situation would cause a failure and render the TOE inoperable, there are no security mechanisms offered by the TOE to prevent the 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 PKI component. Administrators should also ensure that appropriate Windows NT password policies are being enforced on UniCERT enabled systems.**

4.19 The Certification Group recommends that any security patches to Oracle 8.0.5 and the latest Service Pack for Windows NT 4.0 (currently Service Pack 6a) be evaluated under the AISEP Certificate Extension (ACE) Program and applied to future versions of the TOE.

Operational considerations

4.20 Administrators need to ensure that the communications link to and from the CA is adequately protected. A failure of a communications link with the CA could cause a delay for end users or applications in requesting UniCERT services, either from the CA or RA components. Please note that the Environmental and Method of Use Assumptions outlined in the Security Target (ref [3]) stipulate that appropriate measures must be taken to reduce the likelihood of these types of failure from occurring.

4.21 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 Oracle and Windows NT audit logs. **Administrators must ensure that there is an adequate amount of available disk space left on system disks, as specified by Appendix A of the Security Target (ref [3]). In the case of Windows NT, administrators should ensure that events in the event log are not automatically overwritten, unless their security policy has deemed it appropriate.**

Verification of End Users

4.22 UniCERT does not provide a mechanism to validate the credentials supplied to the RAO component while processing a new certificate request, an issue common to other PKI implementations. **Staff undertaking PKI administrator duties should ensure that appropriate procedural measures are in place to verify the identity of an end user when the need arises.**

Importance of a Certificate Practice Statement in a Hierarchical PKI

4.23 The Certificate Practice Statement must define the policy and procedures for users of the PKI to regularly confirm the authenticity of the other components in the PKI hierarchy. This is particularly important when a subordinate CA has been revoked, and end users of the subordinate CA need to confirm whether their CA can still be trusted. **It is the responsibility of PKI administrators to ensure that Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs) are made available in a timely manner, to end users and applications that are using certificates issued by Certificate Authorities in the PKI hierarchy, in accordance with a Certificate Practice Statement.**

Availability considerations for UniCERT

4.24 Administrators should note that the evaluation of UniCERT did not consider any threats to the availability of the CA, RA, CAO, RAO and Gateway components. Since the Gateway component allows users to receive certificates via a Gateway either by email or web, 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 UniCERT servers and their networks from denial of service or other types of availability attacks. Furthermore, Australian Government users should contact DSD for assistance on implementing appropriate countermeasures to protect their networks from attack.**

Protection of the Root CA

4.25 In a hierarchical PKI, it is imperative that the root CA is adequately protected. This may be accomplished by operating the root CA offline for certain periods, depending on the demand for CA services from other components in the PKI (such as subordinate CAs). Offline operation will reduce the likelihood of network based attacks against the root CA. Furthermore, it is recommended that appropriate physical measures are in place to prevent unauthorised access to the CAs private key(s).

Verification of CA certificates

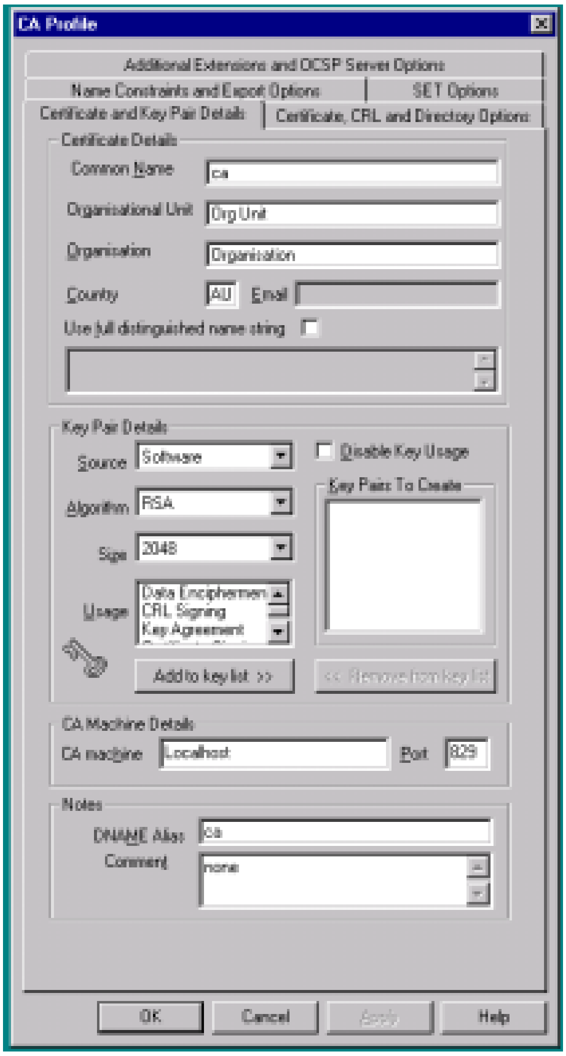
4.26 **It is the responsibility of PKI end-users to ensure their certificate is from a trustworthy source, by comparing the fingerprint of the CA that signed their certificate with the fingerprint of that CA's certificate obtained by another means**. Organisations undertaking CA responsibilities should ensure that appropriate mechanisms are in place for users to retrieve the CA fingerprint either by phone, fax, or letter. In the case of hierarchial CAs, these organisations should ensure that users have the option to verify the certificate up to the root CA so that complete trust can be established in the PKI.

Configuring UniCERT to reflect the Evaluated Version

4.27 Administrators installing the TOE components must use the Security Target [ref [3]) in conjunction with the operational documentation supplied on the CD-ROMs. **Specifically, Appendix A of the Security Target (ref [3]) must be fully understood before the installation and configuration is commenced.**

4.28 The following screenshots have been provided for each of the major components of the TOE to assist administrators in setting up the evaluated configuration. Not all of the options in the following screenshots are part of the evaluated configuration. Only the options specified in this Report and Appendix A of the Security Target represent the evaluated configuration. Please note that there are no configuration screens, or configuration options, for the Token Manager component.

Certification Authority (CA) Configuration Screens


CA Profile
Additional Extensions and OCSP Server Options
Name Constraints and Export Options
SET Options
Certificate and Key Pair Details
Certificate, CRL and Directory Options
Add to key list >>
<< Remove from key list
OK
Cancel
Apply
Help

Certificate Details

Common Name: ca

Organisational Unit: Org Unit

Organisation: Organisation

Country: AU Email:

Use full distinguished name string ☐

Key Pair Details

Source: Software

Algorithm: RSA

Size: 2048

Usage: Data Enciphermen, CRL Signing, Key Agreement

☐ Disable Key Usage

Key Pairs To Create

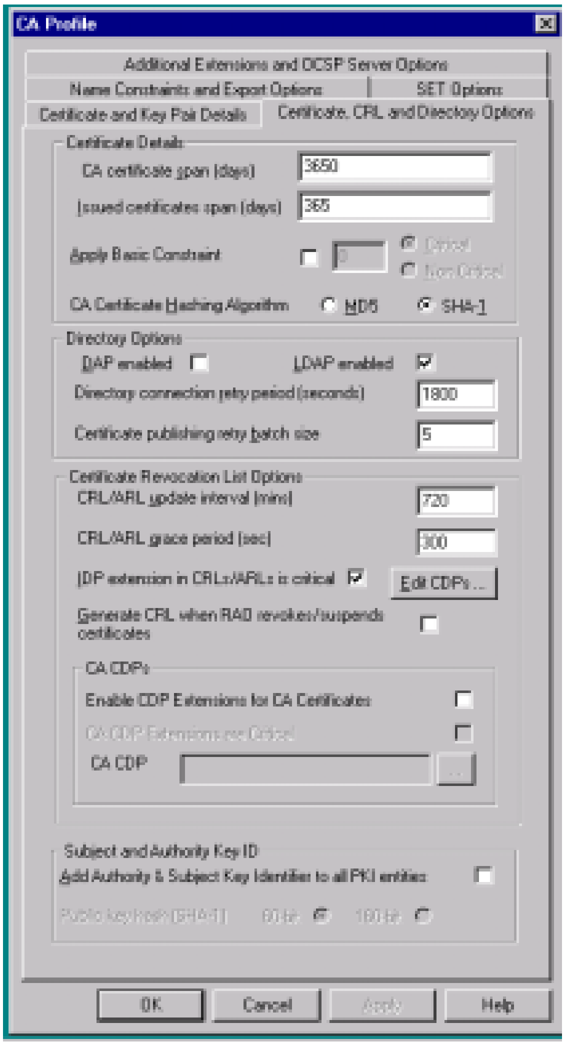
CA Machine Details

CA machine: Localhost Port: 829

Notes

DNAME Alias: ca

Comment: none


CA Profile
Additional Extensions and OCSP Server Options
Name Constraints and Export Options
SET Options
Certificate and Key Pair Details
Certificate, CRL and Directory Options
Edit CDPs ...
...
OK
Cancel
Apply
Help

Certificate Details

CA certificate span (days): 3650

Issued certificates span (days): 365

Apply Basic Constraint ☐ 0 ● Critical ○ Non Critical

CA Certificate Hashing Algorithm ○ MD5 ● SHA-1

Directory Options

DAP enabled ☐ LDAP enabled ☑

Directory connection retry period (seconds): 1800

Certificate publishing retry batch size: 5

Certificate Revocation List Options

CRL/ARL update interval (mins): 720

CRL/ARL grace period (sec): 300

IDP extension in CRLs/ARLs is critical ☑

Generate CRL when RAO revokes/suspends certificates ☐

CA CDPs

Enable CDP Extensions for CA Certificates ☐

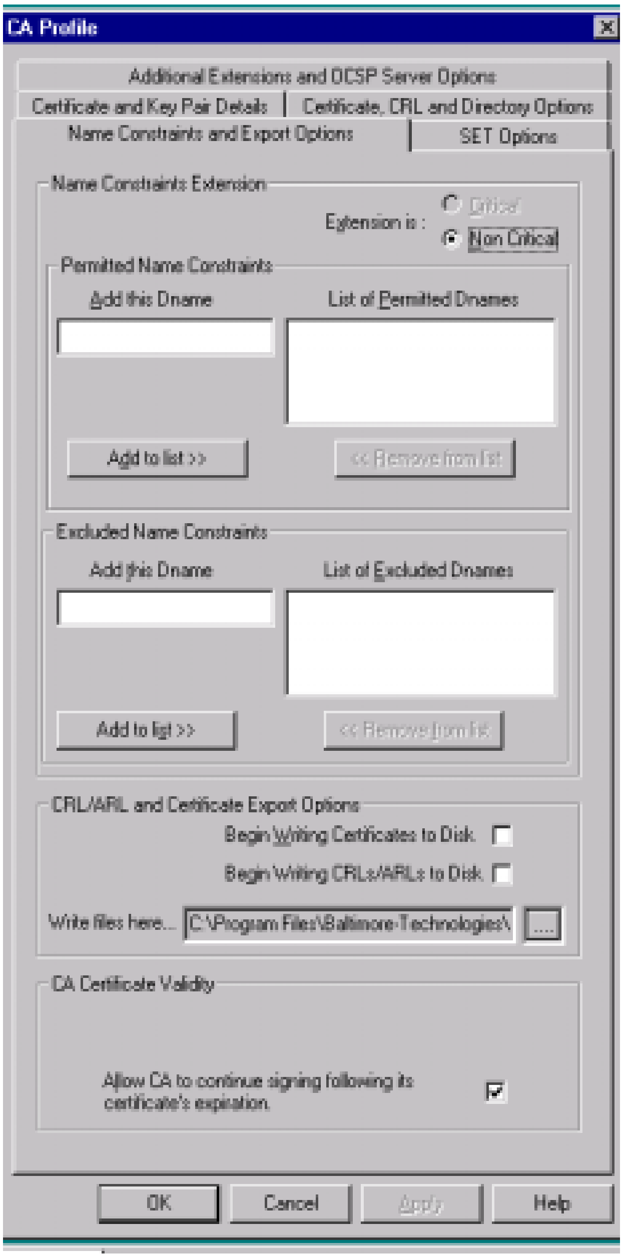
CA CDP Extensions are Critical ☐

CA CDP:

Subject and Authority Key ID

Add Authority & Subject Key Identifier to all PKI entities ☐

Public key hash (SHA-1) 60 bit ● 160 bit ○


CA Profile
Additional Extensions and OCSP Server Options
Certificate and Key Pair Details
Certificate, CRL and Directory Options
Name Constraints and Export Options
SET Options
Name Constraints Extension
Permitted Name Constraints
Add this Dname
List of Permitted Dnames
Add to list >>
<< Remove from list
Excluded Name Constraints
Add this Dname
List of Excluded Dnames
Add to list >>
<< Remove from list
CRL/ARL and Certificate Export Options
CA Certificate Validity
....
OK
Cancel
Apply
Help

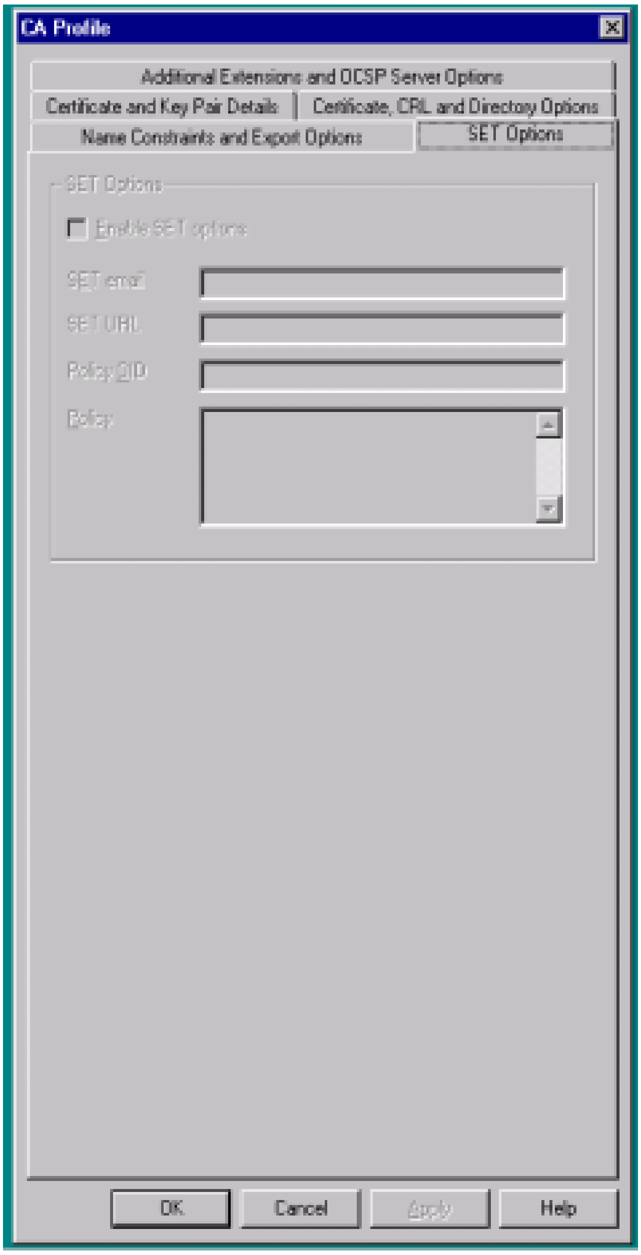
Extension is : ○ Critical ● Non Critical

Begin Writing Certificates to Disk ☐

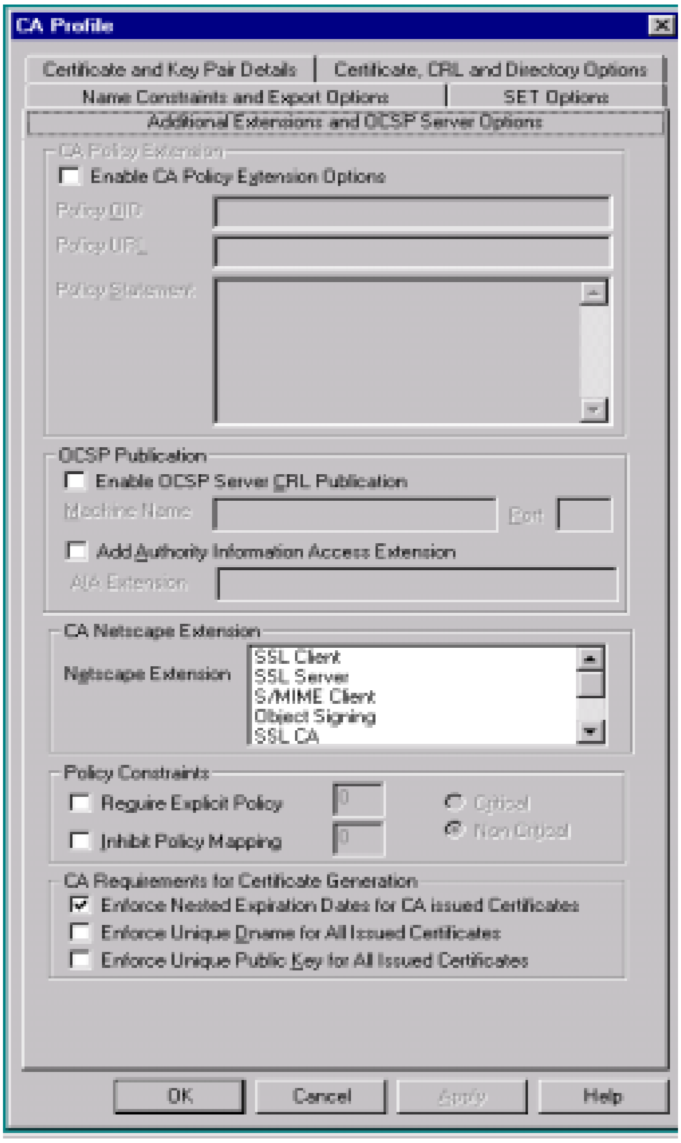
Begin Writing CRLs/ARLs to Disk ☐

Write files here... C:\Program Files\Baltimore-Technologies\

Allow CA to continue signing following its certificate's expiration. ☑


CA Profile
Additional Extensions and OCSP Server Options
Certificate and Key Pair Details
Certificate, CRL and Directory Options
Name Constraints and Export Options
SET Options
SET Options
SET email
SET URL
Policy OID
Policy
OK
Cancel
Apply
Help

☐ Enable SET options



CA Profile

Certificate and Key Pair Details
Certificate, CRL and Directory Options
Name Constraints and Export Options
SET Options
Additional Extensions and OCSP Server Options

CA Policy Extension

□ Enable CA Policy Extension Options

Policy OID:

Policy URL

Policy Statement:

OCSP Publication

□ Enable OCSP Server CRL Publication

Machine Name

Port

□ Add Authority Information Access Extension

AIA Extension

CA Netscape Extension

Netscape Extension: SSL Client, SSL Server, S/MIME Client, Object Signing, SSL CA

Policy Constraints

□ Require Explicit Policy 0

□ Inhibit Policy Mapping 0

○ Critical

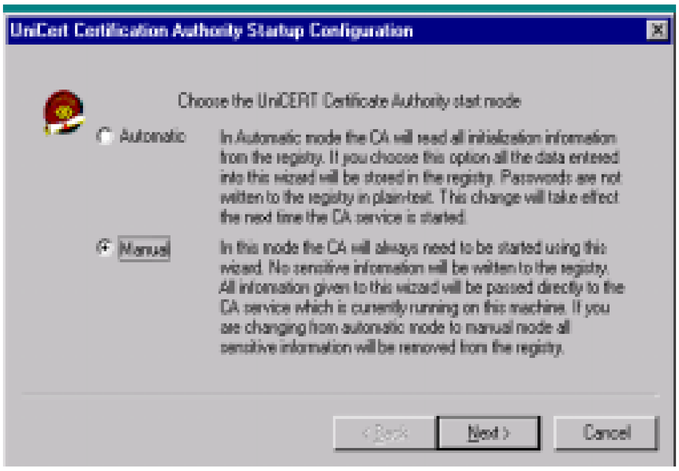
● Non Critical

CA Requirements for Certificate Generation

☑ Enforce Nested Expiration Dates for CA issued Certificates

□ Enforce Unique Dname for All Issued Certificates

□ Enforce Unique Public Key for All Issued Certificates



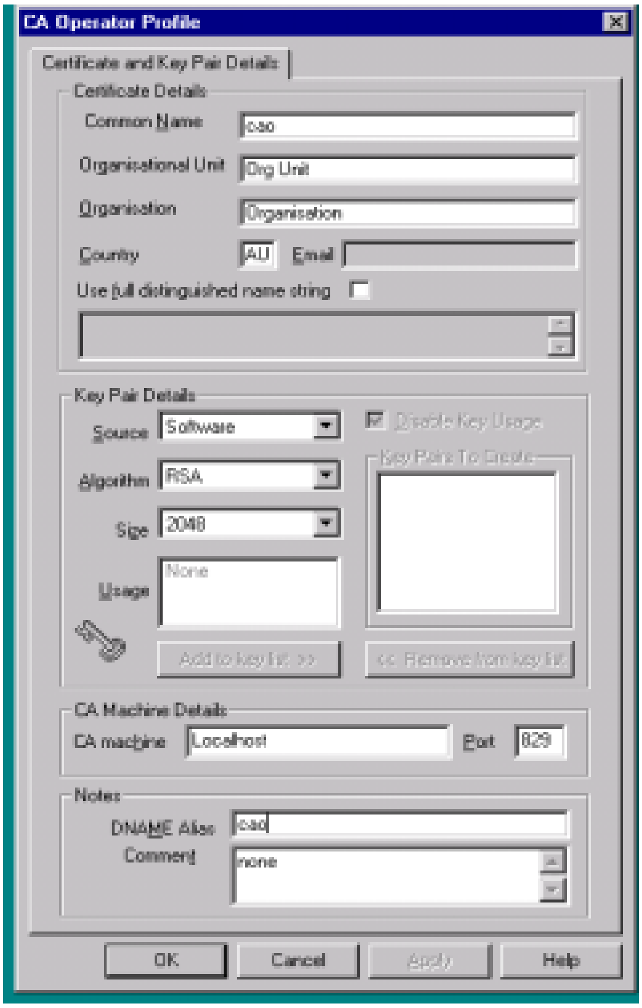
UniCert Certification Authority Startup Configuration

Choose the UniCERT Certificate Authority start mode

○ Automatic — In Automatic mode the CA will read all initialization information from the registry. If you choose this option all the data entered into this wizard will be stored in the registry. Passwords are not written to the registry in plain-text. This change will take effect the next time the CA service is started.

● Manual — In this mode the CA will always need to be started using this wizard. No sensitive information will be written to the registry. All information given to this wizard will be passed directly to the CA service which is currently running on this machine. If you are changing from automatic mode to manual mode all sensitive information will be removed from the registry.

Certification Authority Operator (CAO) Configuration Screen



Common Name: cao

Organisational Unit: Org Unit

Organisation: Organisation

Country: AU

Email:

Use full distinguished name string □

Source: Software

Algorithm: RSA

Size: 2048

Usage: None

☑ Disable Key Usage

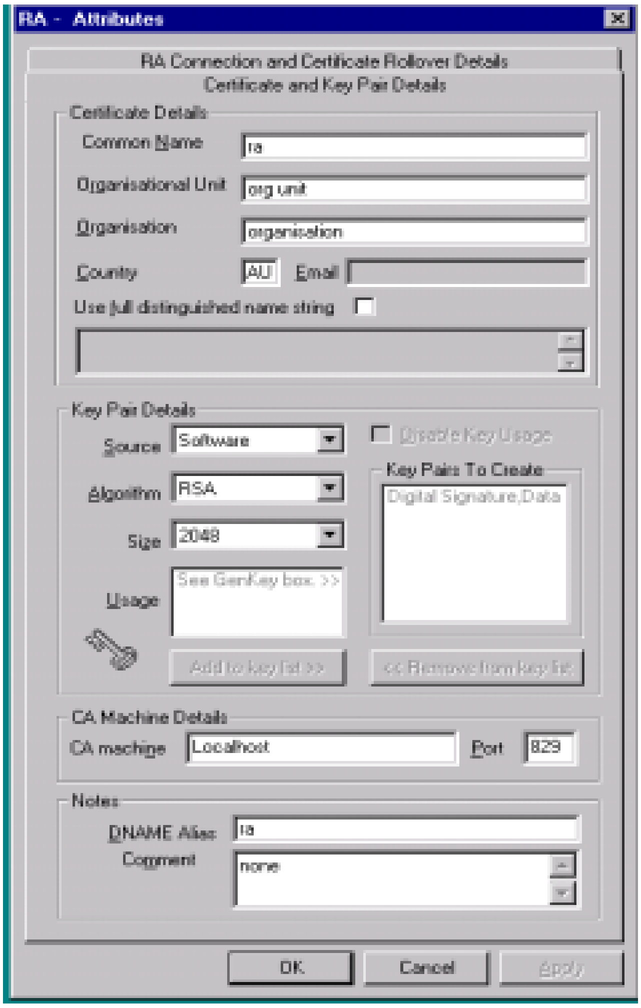
CA machine: Localhost

Port: 829

DNAME Alias: cao

Comment: none

Registration Authority (RA) Configuration Screens


RA - Attributes
RA Connection and Certificate Rollover Details
Certificate and Key Pair Details
Add to key list >>
<< Remove from key list
OK
Cancel
Apply

Certificate Details

Common Name: ra

Organisational Unit: org unit

Organisation: organisation

Country: AU Email:

Use full distinguished name string □

Key Pair Details

Source: Software

Algorithm: RSA

Size: 2048

Usage: See GenKey box >>

□ Disable Key Usage

Key Pairs To Create: Digital Signature,Data

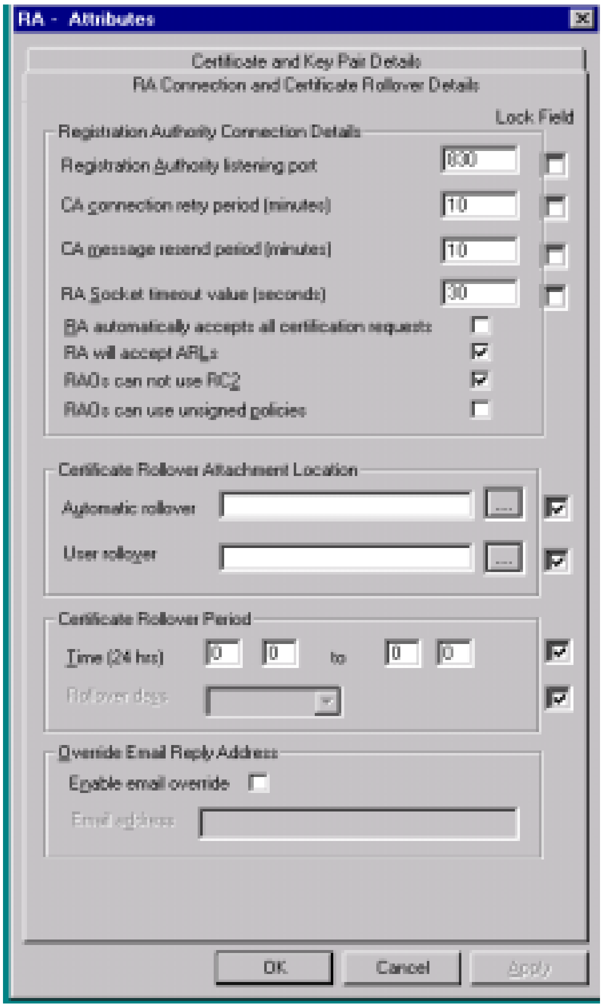
CA Machine Details

CA machine: Localhost Port: 829

Notes

DNAME Alias: ra

Comment: none


RA - Attributes
Certificate and Key Pair Details
RA Connection and Certificate Rollover Details
OK
Cancel
Apply

Lock Field

Registration Authority Connection Details

Registration Authority listening port 830 □

CA connection retry period (minutes) 10 □

CA message resend period (minutes) 10 □

RA Socket timeout value (seconds) 30 □

RA automatically accepts all certification requests □

RA will accept ARLs ☑

RAOs can not use RC2 ☑

RAOs can use unsigned policies □

Certificate Rollover Attachment Location

Automatic rollover ... ☑

User rollover ... ☑

Certificate Rollover Period

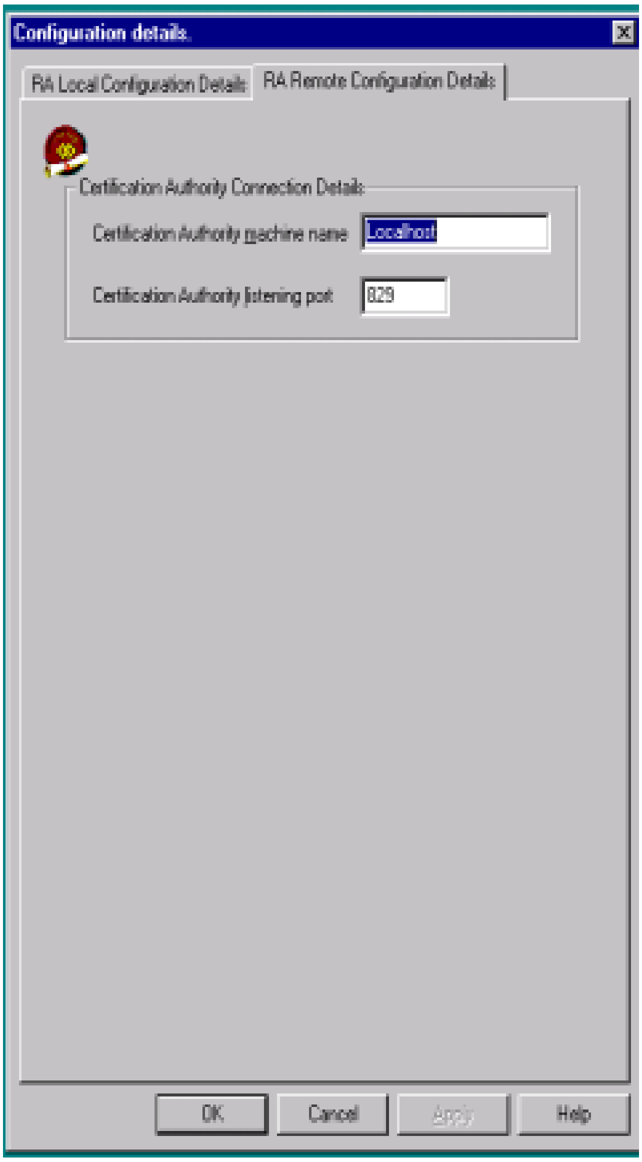
Time (24 hrs) 0 0 to 0 0 ☑

Roll over days ☑

Override Email Reply Address

Enable email override □

Email address

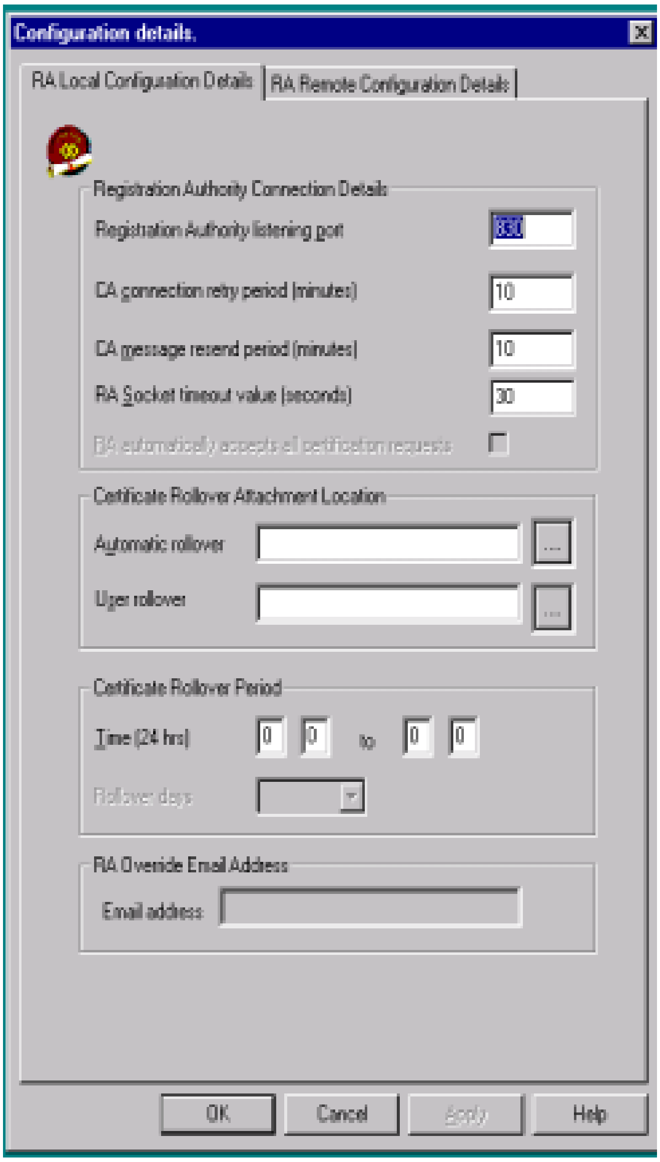


Configuration details.
RA Local Configuration Details
RA Remote Configuration Details
OK
Cancel
Apply
Help

Certification Authority Connection Details

Certification Authority machine name: Localhost

Certification Authority listening port: 829



Configuration details.
RA Local Configuration Details
RA Remote Configuration Details
OK
Cancel
Apply
Help

Registration Authority Connection Details

Registration Authority listening port: 830

CA connection retry period (minutes): 10

CA message resend period (minutes): 10

RA Socket timeout value (seconds): 30

RA automatically accepts all certification requests ☐

Certificate Rollover Attachment Location

Automatic rollover: ...

User rollover: ...

Certificate Rollover Period

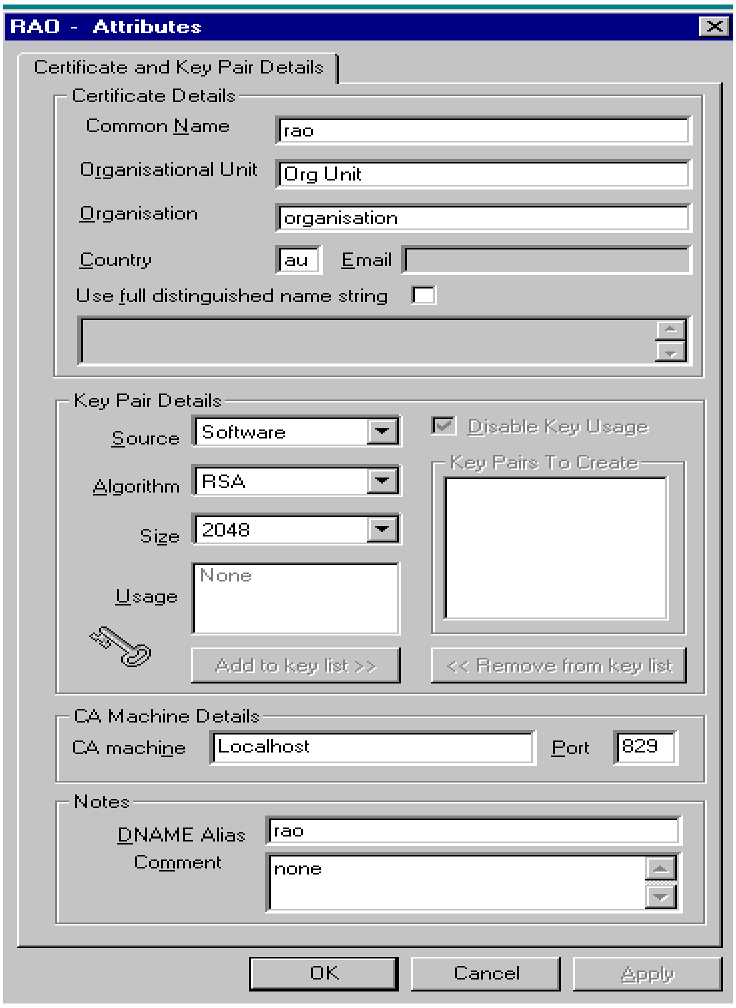
Time (24 hrs): 0 0 to 0 0

Rollover days:

RA Override Email Address

Email address:

Registration Authority Operator (RAO) Configuration Screens



Common Name: rao

Organisational Unit: Org Unit

Organisation: organisation

Country: au

Email:

Use full distinguished name string □

Source: Software

Algorithm: RSA

Size: 2048

Usage: None

☑ Disable Key Usage

Key Pairs To Create

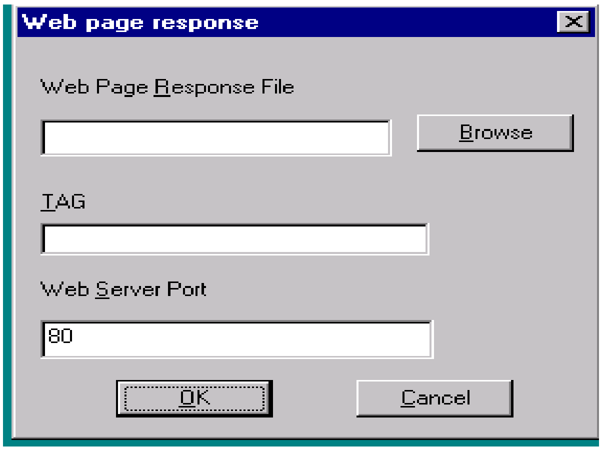
CA machine: Localhost

Port: 829

DNAME Alias: rao

Comment: none

Gateway Configuration Screen



Web Page Response File:

TAG:

Web Server Port: 80

Appendix A References

[1] Evaluation Memorandum No. 1 - Description of the AISEP
Defence Signals Directorate
EM 1, Issue 1.0, August 1994

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

[3] UniCERT Security Target
Baltimore Technologies Ltd
Version 3.10, 10th November 2000
(COMMERCIAL-IN-CONFIDENCE)

[4] Information Technology Security Evaluation Criteria (ITSEC)
Commission of the European Communities
CD-71-91-502-EN-C, Version 1.2, June 1991

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

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

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

[8] UniCERT Evaluation Technical Report
CMG Admiral
Issue 1.0, July 2000.
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[9] UniCERT Administrator's Guide: Certification Authority Operator
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[10] UniCERT Administrator's Guide: Certification Authority
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[11] UniCERT Administrator's Guide: Registration Authority Operator
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[12] UniCERT Administrator's Guide: Registration Authority
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[13] UniCERT Administrator's Guide: Gateway
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[14] UniCERT Administrator's Guide: Installation Notes
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[15] UniCERT Administrator's Guide: Migration Utility
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[16] UniCERT Administrator's Guide: Product Overview
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[17] UniCERT Administrator's Guide: Release Notes
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[18] UniCERT Administrator's Guide: Appendices
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[19] UniCERT Administrator's Guide: System Monitoring Guide
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[20] UniCERT Administrator's Guide: Token Manager
Published on CD with UniCERT v3.1.2
Baltimore Technologies Ltd

[21] Baltimore Software Shipping Procedures
Baltimore Technologies Ltd
Release 1.0, June 2000
(COMMERCIAL-IN-CONFIDENCE)

[22] Evaluated Products List (Section VIII)
Defence Signals Directorate
April 2000

[23] Cryptographic Evaluation Report for Baltimore UniCERT
Defence Signals Directorate
July 2000
[COMMERCIAL-IN-CONFIDENCE]

[24] UniCERT Evaluation Technical Report (supplement)
Defence Signals Directorate
Issue 1.0, November 2000.
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

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 security enforcing functions meet the requirements of their security policy.

Product Rationale for the TOE

Security Objectives

B.2 UniCERT has the following IT security objectives:

a) **Provide trusted certificates**. The TOE will provide trusted certificates to protect public keys of end users and UniCERT components.
b) **Provide authorised certificates.** The TOE will ensure that all certification and revocation requests are made through the authorised channels and according to an authorised Customer Registration Policy.
c) **Keep private keys confidential.** The TOE will ensure the confidentiality of private keys for use within the TOE and, optionally, for end users.
d) **Create end user private keys.** The TOE will provide the facility to generate private authentication and/or confidentiality keys for end users.
e) **Generate audit log events and archive.** The TOE will generate an audit log of security related events and an archive of certificates, CRLs, ARLs and requests.

Intended Method of Use and Intended Environment

B.3 The Intended Method of Use and Environmental Assumptions for UniCERT are:

a) Trusted system and database administrators are available to install and maintain the TOE in accordance with the configuration described in Appendix A of the Security Target (ref [3]).

b) The people responsible for running the CAO and RAO components can be trusted, within the boundaries of the functionality provided by these components.

c) Procedural measures are in place to verify the identity of an end user.

d) Physical access to the CA and CAO is restricted to CAO users and system / database administration staff.

e) Physical access to the RA is restricted to RAO users, RA administrators and system / database administration staff.

f) Logical access to the systems on which TOE components and database(s) are installed are restricted in accordance with a defined security policy which must define suitable countermeasures to mitigate any risk factors to an acceptable level.

g) Network links between the TOE components and database(s) are protected from eavesdropping in accordance with a defined security policy that defines suitable countermeasures to mitigate any risk factors to an acceptable level.

h) Operation of the TOE is performed according to organisational policies that specify sound information management procedures including disaster recovery of TOE components and data.

i) Procedural and physical measures will be established to ensure that the backup media is held securely, is accessible only to authorised administrators, and when no longer required is deleted or destroyed in a secure manner.

j) Operators will keep their passwords secret and change them at regular intervals.

k) Procedural measures are in place to ensure that CRLs and ARLs are made available in a timely manner, to end users and applications that are using certificates issued by CAs in the PKI hierarchy. Users are responsible for the correct use of such CRLs and ARLs, in accordance with policies and procedures issued by the operators of the TOE e.g. Certificate Practice Statement.

Summary of Security Features of the TOE

B.4 The following Security Enforcing Functions (SEFs) are provided by UniCERT:

B.5 SEF1:

Sign Certificates: The TOE shall create and sign X.509 certificates of end users and UniCERT components. On receipt of a valid request for a certificate to be created, the CA shall generate a certificate containing the public key of the end user or UniCERT component. The CA shall then sign this certificate using the certificate signing private key of the CA.

B.6 SEF2:

Sign/Verify Certification Requests: The TOE shall provide the functionality to sign and verify certification requests. All requests for a certificate shall be signed by an authorised component within the TOE and verified by the component that acts upon this request.

B.7 SEF3:

Sign CRL and ARL: The TOE shall create and sign a CRL and ARL using all the certificates listed in the certificate revocation table contained in the Oracle database. An X.509 v2 CRL and ARL shall be generated by the CA either on a periodic basis through the CA operational policy, manually by the CAO, or when a certificate has been revoked. The CRL shall contain a list of all end user certificates held in the certificate revocation table, along with their revocation details. The ARL shall contain the same but for PKI component certificates.

B.8 SEF4:

Sign/Verify Revocation Requests: The TOE shall provide functionality to sign and verify certificate revocation or certificate suspension/unsuspension requests. All requests for certificate revocation shall be signed by an authorised component within the TOE and verified by the component that acts upon this request. Either the CA or the CAO is able to revoke a certificate by adding that certificate to the certificates revocation table within the Oracle database. Component certificates will be directly revoked by the CAO.

B.9 SEF5:

Sign/Verify Customer Registration Policy: The TOE shall provide the functionality to sign and verify CRPs. Registration of users will be carried out by the RAO in accordance with a CRP defined by the CAO. The CRP is signed by the CA and transmitted to the RAO via the RA.

B.10 SEF6:

Access Control: The TOE shall provide the functionality to control access to the private keys within the TOE. Access to any of the private keys shall require the entry of the correct corresponding passphrase. Access to the private key is required prior to accessing the functionality of each component within the PKI.

B.11 SEF7:

Generate Key Pairs: The TOE shall provide the functionality to generate key pairs for components within the PKI and optionally for end users. The TOE allows the creation of RSA or DSA key pairs with a maximum length of 2048 and 1024 bits respectively.

B.12 SEF8:

Generate Archive and Audit Log: The TOE shall provide the functionality to log security related events and to archive certificates, CRLs, ARLs and certification/revocation requests. The TOE generates an audit log listing of security related events, which may then be used by the CA or RA administrator to identify attempts to attack the system. These events are written to an Oracle database or to the Windows NT event log.

B.13 SEF9:

Sign Audit Log Entries: The TOE shall provide the functionality to individually sign each audit event that is written to the UniCERT audit log. Each event is signed by the entity that writes the event to the [Oracle] database. This may then be verified by the CAO or RAO components.

Appendix C Contents of Distribution Package

Configuration for Evaluation

C.1 The evaluation was conducted on Baltimore's UniCERT product, Version 3.1.2.A. The software components of UniCERT have been identified below. UniCERT does not consist of any hardware.

Software

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

a) 1 x CDROM containing the **UniCERT Software, Version 3.1.2 (RoW)**. Please note that the letters **RoW** (Rest of the World) must follow the version number in parenthesis. Only the English version has been evaluated. The evaluated components are:

i) Certificate Authority
ii) Certificate Authority Operator
iii) Registration Authority
iv) Registration Authority Operator
v) Gateway
vi) Token Manager

b) 1 x CD-ROM containing additional **UniCERT Software, Version 3.1.2.A (Patch).** The evaluated components on this CD-ROM consist of three files:

i) cao.exe
ii) UniCA_Service.exe
iii) UniCERT_3.1.2.A_Readme.html

Third Party Software

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

a) Oracle version 8.0.5
b) Microsoft Windows NT 4.0 (with Service Pack 5)

C.4 This evaluation is only valid for the above mentioned version of UniCERT running on Microsoft Windows NT 4.0 with Service Pack 5. No other versions, operating systems or third party software are part of the evaluated configuration.

Procedures for Determining Version of TOE

C.5 In order that an administrator can determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

C.6 Once a copy of UniCERT has been received, the administrator should inspect the packaging for any signs of tamper. The plastic shrink wrap around the CD-ROMs should be intact on delivery. Any indication of tamper should be reported immediately to Baltimore and the product returned to the supplier.

C.7 The evaluated version of UniCERT can be verified by inspecting the contents of the delivered CD-ROMs. Additionally, each delivered instance of UniCERT can be uniquely determined by the serial number on the CD-ROMs. This serial number must be verified through Baltimore.

C.8 An example directory and file listing of the evaluated version has been provided below. UniCERT administrators should verify the contents of the CD-ROMs with these listings to determine the authenticity of their purchased version of UniCERT prior to installation. Please note that these listings are only partial, and do not reflect the entire contents of the installation CD-ROMs.

Directory Listing for UniCERT CD-ROM Version 3.1.2

```
Volume in drive D is UNICERT_V31
Volume Serial Number is 5439-9A9D

Directory of D:\

AUTORUN      INF      51           04-08-99 12:36p      AUTORUN.INF
MSVBVM50     DLL   1,347,344       12-22-98 10:46a      Msvbvm50.dll
SETUP        EXE     777,728       04-28-00  2:15p      Setup.exe
WIN32        <DIR>                 05-09-00 12:26p      Win32
      3 file(s)    2,125,123 bytes

Directory of D:\Win32

.            <DIR>                 05-09-00 12:26p      .
..           <DIR>                 05-09-00 12:26p      ..
ACROBAT      <DIR>                 05-09-00 12:26p      acrobat
BALTIM~8     ICO      1,078        04-19-99  4:08p      Baltimore.ico
DATA         TAG      113          05-09-00 12:08p      DATA.TAG
DATA1        CAB   30,569,281      05-09-00 12:09p      data1.cab
DATA1        HDR     193,667       05-09-00 12:08p      data1.hdr
DOCUME~7     <DIR>                 05-09-00 12:26p      Documentation
LANG         DAT      23,541       01-12-99 11:34a      lang.dat
LAYOUT       BIN      609          05-09-00 12:09p      layout.bin
MISC         <DIR>                 05-09-00 12:26p      Misc
OS           DAT      450          07-27-98  5:41p      os.dat
PLUGTOC      <DIR>                 05-09-00 12:26p      PlugTOC
```

```
SETUP          BMP    231,480        02-15-00  4:17p        setup.bmp
SETUP          INI    102            05-09-00 12:08p        SETUP.INI
SETUP          INS     79,028        05-08-00  3:06p        setup.ins
SETUP          LID    49             05-09-00 12:08p        setup.lid
UNICE~36       EXE    73,728         01-12-99 12:42p        UniCERT_Install.exe
_INST32I       EX_    296,674        02-23-99 11:45a        _inst32i.ex_
_ISDEL         EXE     27,648        10-27-98  1:06p        _ISDel.exe
_SETUP         DLL     34,816        09-29-98  4:34p        _Setup.dll
_SYS1          CAB    175,466        05-09-00 12:08p        _sys1.cab
_SYS1          HDR     3,999         05-09-00 12:08p        _sys1.hdr
_USER1         CAB     327,302       05-09-00 12:08p        _user1.cab
_USER1         HDR      4,990        05-09-00 12:08p        _user1.hdr
     19 file(s)    32,044,021 bytes
```

Directory Listing for the additional UniCERT CD-ROM Version 3.1.2.A

```
Volume in drive E is UNICERT_V312A
Volume Serial Number is D803-6F25

Directory of E:\

.              <DIR>                 10-11-00 11:12a     .
..             <DIR>                 10-11-00 11:12a     ..
CAO            EXE    5,068,800      08-11-00  6:09p    cao.exe
UNI_CA_Ser~    EXE    4,429,824      08-11-00  5:58p    UniCA_Service.exe
UNICERT_3.~    EXE    3,646          08-11-00  5:58p    UniCERT_3.1.2.A_Readme.html

5 file(s)     9,502,270 bytes
```