Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

2012/80

23 Jul 2012

Version 1.0

Amendment Record

Version	Date	Description
1.0	23/07/2012	Public release.

Executive Summary

1 The Target of Evaluation (TOE), UniCERT 5.3.4.1 is a software product designed to provide the functionality required to implement and maintain a Public Key Infrastructure (PKI) system. The TOE was developed by Verizon Business.

2 This report describes the findings of the IT security evaluation of the TOE to the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.2. The report concludes that the product has met the target assurance level of EAL4 + ALC_FLR.2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed in May 2012.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Operate the TOE according to the administrator guidance (Ref [3]);

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved;

d) Plan PKI requirements prior to initial installation. UniCERT is complex and can be as expansive as your need requires. Initial planning can reduce setup time drastically;

e) Secure the Certificate Authority, Key Archive Server, Certificate Status Server and Registration Authority. These components are the heart of UniCERT. Compromising even one of those components can result in a complete collapse of the integrity of the PKI deployment;

f) Enable SSL on the web server. The WebRAO client requires encrypted logon in order to authenticate;

g) Patch Oracle as per requirements for the supporting environment. UniCERT has been tested on both versions 10g and 11g provided they have the relevant patches;

h) Ensure that any active directory requirements are documented, as this is the backbone of the AutoEnroll component;

i) Ensure that any Hardware Security Module requirements adhere to the supported product list, including supported firmware and software versions. Also ensure that any smart cards used are in the supported product list; and

j) As per the evaluated configuration, make sure that any entities that have left the organisation are removed from the PKI and their certificates revoked.

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 results of the IT security evaluation of the TOE, UniCERT 5.3.4.1, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.2, and

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.

10

Table 1: Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	UniCERT 5.3.4.1
Software Version	UniCERT 5.3.4.1
Security Target	Verizon UniCERT Security Target, Version 1.8, 29 March 2012
Evaluation Level	EAL4 + ALC_FLR.2
Evaluation Technical Report	Verizon UniCERT 5.3.4.1, Evaluation Technical Report, Version 1.0, 17 May 2012 (*EFS-T028-ETR*)
Criteria	Common Criteria for Information Technology Security Evaluation Parts 1, 2 & 3, July 2009 Version 3.1 Revision 3 Final

Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1 Revision 3, CCMB-2009-07-004
Conformance	Common Criteria Part 2 conformant Common Criteria Part 3 augmented (EAL4 + ALC_FLR.2)
Sponsor	Verizon Business 2-6 Pancras Way Camden London United Kingdom
Developer	Verizon Business (Ireland) Verizon House Lower Erne Street Dublin 2 Ireland
Evaluation Facility	stratsec lab – AISEF Suite 1/50 Geils Court Deakin ACT 2600 Australia

Chapter 2 - Target of Evaluation

2.1 Overview

11 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

12 The TOE is UniCERT 5.3.4.1 developed by Verizon Business. Its primary role is to issue and manage digital certificates that allow other IT systems to verify the identity of the holder.

13 UniCERT 5.3.4.1 is a software product that is designed to provide the functionality required to implement and maintain a Public Key Infrastructure (PKI) system. The TOE provides certificate registration, PKI management, a Certification Authority, and certificate lifecycle management functions. The TOE can be used to manage all the keys necessary for a system requiring security for end users, using either a centralised or distributed PKI.

14 As the TOE is a software product, the system must be hosted on a hardware platform that includes a Windows or Unix (Sun Solaris) operating system, a database management system (Oracle), a web server and a browser.

15 The TOE includes the following core components:

a) **Certification Authority (CA)**: Responsible for the generation and issuance (i.e. publication or distribution) of certificates and certificate revocation lists, and for the overall management of certificates and the PKI in general.

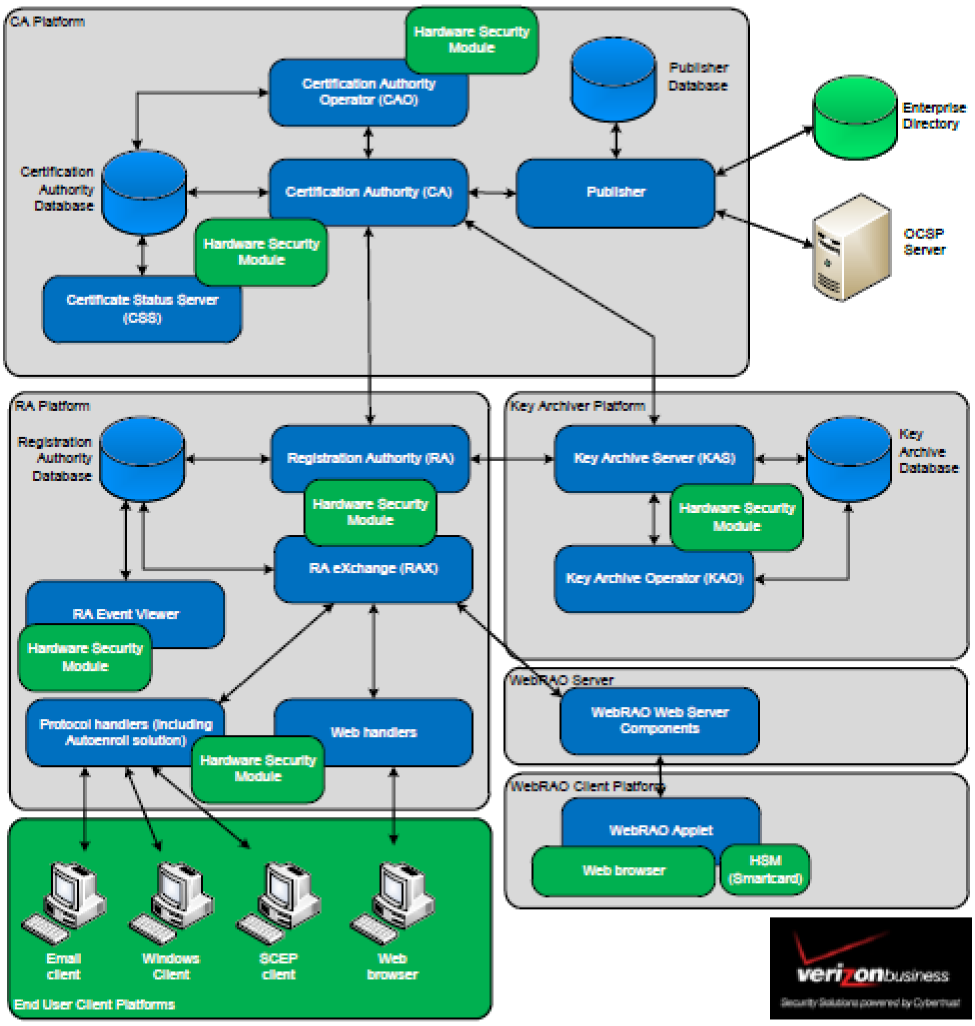
b) **Registration Authority (RA)**: Responsible for gathering registration information and revocation requests, authorising requests and handling renewals. The control over the functions the Registration Authority components are allowed to perform is provided by the Certification Authority Operator component.

16 In addition, the TOE may be configured with the following optional "advanced components":

a) **The Key Archiver (KAS)**: Provides the facility to archive and retrieve private keys.

b) **The AutoEnroll Solution**: Supports the automatic registration, generation and distribution of certificates (for use with computers in a Microsoft Windows domain).

17 An example UniCERT deployment is illustrated below. Those components shown in blue are included within the scope of the UniCERT evaluation, and those in green are external to the TOE.



2.3 Security Policy

18 The Security Target (Ref [1]) contains no explicit security policy statements.

2.4 TOE Architecture

19 The TOE consists of the following major architectural components:

a) **Certificate Authority Platform**;

b) **Registration Authority Platform**;

c) **Support Platform**; and

d) **Key Archiver Platform** (optional).

20 The Developer's Architectural Design identifies the following components of the TOE:

a) **Certificate Authority**: The CA core component generates certificates and Certificate Revocation Lists (CRLs) and as such is the nucleus of the PKI system.

b) **Certificate Authority Operator**: The CAO is a GUI application used to manage the CA system and register certificates for PKI components.

c) **Certificate Status Server**: The CSS subsystem responds to Online Certificate Status Protocol (OCSP) requests from other TOE components by providing real time certificate status information.

d) **Publisher**: The Publisher subsystem distributes and publishes certificates, CRLs and ARLs using a variety of distribution methods and directory formats.

e) **Registration Authority**: The RA core component provides a registration portal for the PKI system and an interface to the CA component. It receives, verifies and forwards requests to the CA and sends back the CA's response.

f) **WebRAO**: This subsystem is a web application used by an RAO/RRO/KRO to submit and authorise certificate registration, revocation, renewal and key recovery requests, as well as to perform key generation.

g) **RA Event Viewer**: This subsystem provides to the TOE the functionality for a trusted user to view logs at the RA database for auditing purposes.

h) **RA eXchange**: This subsystem provides a communication link whereby messages passed through the subsystem are put into a format that allows the RAX to query the RA database and return appropriate messages.

i) **Protocol Handler**: This subsystem provides the capability to handle AutoEnroll, Simple Certificate Enrolment Protocol (SCEP), email and web requests.

j) **Support Platform**: Provides a suite of utilities and key tools to support the platforms of the TOE.

k) **Key Archive Operator**: The KAO is a GUI application used to manage the KAS system and recover keys archived by the KAS.

l) **Key Archive Server**: This securely archives private keys received via the RA and KAO components in a KAS database.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

22 The TOE provides the following evaluated security functionality:

a) Audit;

b) Communication;

c) Cryptographic support;

d) User data protection;

e) Identification and authentication;

f) Security management; and

g) Protection of the TOE Security Functions.

2.5.2 Non-evaluated Functionality and Services

23 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 Security Manual (ISM) (Ref [1]) 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).

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

a) **DB Upgrade Utility**: Similar to the Database Wizard, the Database Upgrade Utility exists solely to set up the database that supports the operation of the TOE. The Database Upgrade Utility is used specifically to create new, or change existing database tables as required for the TOE. The Database Upgrade Utility exists as a stand-alone application that does not enforce or support any DB Wizard. The Database Upgrade Utility communicates solely with the Oracle database server which is also outside of the TOE Security

Function (TSF) boundary and as such, does not utilise any of the TSF Interfaces (TSFIs).

b) **Publisher Configuration Utility**: The Publisher Configuration Utility allows for an administrator to setup and configure the operation of either the Publisher or the AutoEnroll Publisher components. As the Publisher Configuration Utility communicates only with the database (outside the TSF) and does not enforce or support any security functional requirements; it is considered outside of the TSF and hence does utilise any of the TSFIs.

2.6 Usage

2.6.1 Evaluated Configuration

25 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 this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [1]) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

26 The TOE is comprised of the following software components:

a) **Certification Authority (CA)**;

b) **Registration Authority (RA)**;

c) **Key Archiver** – optional component;

d) **Autoenroll solution** – optional component; and

e) **Support utilities**.

27 The TOE relies on general server grade hardware with the following minimal requirements:

a) Pentium IV or higher with clock speed at least 1.8 GHz;

b) RAM of 1024 MB, or 2048 MB if you are installing Oracle Server;

c) Hard drive space of 450 MB for the UniCERT components and documentation (plus 5.5 GB for the Oracle Server); and

d) A CD-ROM drive for installation.

28 While the TOE provides a range of standard cryptographic methods, the TOE may also be securely integrated with dedicated HSM devices and smartcards (another form of HSM) that are PKCS#11 compliant devices.

29 The evaluated configuration is based on default installation of the TOE with the following additional configurations:

a) Start services manually using the UniCERT Service Manager. Do not configure services such as the CA, RA, RA eXchange and CSS to start in automatic mode. Using automatic mode means that the passwords and PINs used to open the private keys of these entities are stored on the computer where the Service Manager is installed.

b) Ensure authorisation groups are assigned in RPs; do not enable the **No Authorisation** option. For example, set up authorisation for the RPs used by the protocol handlers so any requests they pass to the RA are authorised by the WebRAO Client user. Authorisation is an important mechanism for you to ensure third party approval for certificate requests.

c) Use a HSM or smart card providing tamper detection, in conjunction with UniCERT, for storing root keys.

d) The UniCERT components ARM, CMP handler and UPI have **not** been evaluated as part of the UniCERT v5.3.4.1 evaluation; however, they could be included in an evaluated configuration of UniCERT, provided a separate evaluation of each such component (when installed in the PKI environment) is successfully performed.

e) Define an audit policy for the PKI that assures the independence of the appointed auditor and clearly states the frequency of the audit process, as well as how security-related event logs are dealt with and reported.

f) Promptly dispose of all authentication data for an administrator whose access rights have been removed. Revoke the certificate and destroy the data using the key destruction functions of UniCERT and the HSM or smart card where keys are stored. Remove the associated entity from the PKI.

g) Set the clocks on the computers in your PKI from a trusted, accurate and reliable time source to ensure that an accurate time source is used to timestamp audit records.

h) Implement security-related patches as soon as you receive them.

2.6.2 Delivery procedures

30 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct version of the TOE.

31 Orders sent to customers are transported via DHL couriers and stored in a tamper–evident bag. The purpose of this container is that any attempt to open the bag at the opening will tear the bag, immediately revealing to the recipient that something or someone attempted to tamper with the product.

32 In conjunction with this, the delivery note contains the same tracking number as on the tamper-evident bag. This means that if the product has been stolen from the bag, there is an accurate representation of what was taken. This is also mapped to the couriers tracking email, so the customer will immediately know if the package was tampered with in transit.

33 The customer is able to confirm the exact location of the package via DHL's tracking website. When the package arrives, it needs to be signed for in order to receive the package. This information gets added to the sales, distribution and finance spreadsheet.

2.6.3 Determining the Evaluated Configuration

34 To establish the integrity of the TOE, it must be installed and configured in a particular manner. The evaluated configuration is attained by following the steps outlined in section 2.6.1 above.

35 The TOE version number is printed on the disc and can be verified during the installation process. Once installed, the version number may be checked by querying the properties on executables and DLLs under Windows.

2.6.4 Documentation

36 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available upon request from the developer:

a) UniCERT 5.3.4 Installation Guidance for Windows

b) UniCERT 5.3.4 Installation Guidance for Solaris

c) UniCERT 5.3.4 Configuration Guide for Windows

d) UniCERT 5.3.4 Configuration Guide for Solaris

e) UniCERT 5.3.4 Administrators Guide, 03 May 2011

f) UniCERT 5.3.4 Autoenroll Guide, 03 May 2011

g) UniCERT 5.3.4 Database Administrators Guide, 03 May 2011

h) UniCERT 5.3.4 Elliptic Curve Cryptographic Guide, 03 May 2011

i) UniCERT 5.3.4 Extensions Guide, 03 May 2011

j) UniCERT 5.3.4 KeyArchiver Guide, 03 May 2011

k) UniCERT 5.3.4 Publisher Guide, 03 May 2011

l) UniCERT 5.3.4 Web Components Guide, 03 May 2011

m) UniCERT 5.3.4 WebRAO Guide, 03 May 2011

n) UniCERT 5.3.4 Additional CC Guidance

2.6.5 Secure Usage

37 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.

38 The following assumptions were made:

Identifier	Assumption Statements
A.AUTH_DATA_DISPOSAL	Authentication data and associated privileges are properly disposed of and/or removed as appropriate when no longer required within the PKI system. This includes both removal (secure deletion) of data from the PKI system, and the revocation of certificates. (For example, if a CAO user leaves the organisation that runs the PKI system, then their certificate should be revoked and their private key securely destroyed. Similarly, if it is suspected that a private key has been compromised, then the associated certificate should be promptly suspended or revoked.)
A.AUDIT_REVIEW	Authorised auditor(s) regularly review audit records produced by the TOE, respond promptly to any indication of an attempted or actual security breach, and ensure that audit records are regularly archived to prevent audit data storage exhaustion.
A.COMPETENT_USERS	All (human) TOE users and those users managing the operational environment are competent, either by training or experience, to manage, operate and use the PKI system, and to maintain the security and privacy of the data it handles.

Identifier	Assumption Statements
A.TRUSTED_USERS	All (human) TOE users and those users managing the operational environment are trusted, as far as is reasonably possible, not to abuse the PKI system facilities that they are authorised to use; in particular, they are trusted to not install or execute malicious software within the PKI system.
A.SECURE_INSTALL	The (human) TOE users and those users managing the operational environment install, configure and maintain the PKI system securely, i.e. in accordance with all relevant guidance documentation.
A.COMMS_PROTECTION	There is adequate logical and physical protection on the communication channels used by the TOE. The protection extends to the boundary of the PKI system, and includes the use of firewall(s) to prevent unauthorised access to the PKI system via a communication channel.
A.PHYSICAL_PROTECTION	The PKI system has adequate physical protection against, in particular, unauthorised physical access by potential attackers.
A.TIME_SOURCE	There is a trusted, accurate, and reliable time source within the PKI system that may be used to timestamp TOE audit records.
A.ACCOUNTABILITY	The PKI system is configured and operated such that individual administrators or users can be held accountable for their actions.
A.ROLE_SEPARATION	The PKI system is configured and operated such that any separation of roles (as recommended in guidance documentation) is maintained.

Identifier	Assumption Statements
A.HSM	Any HSM that will be integrated with the TOE is PKCS#11 compliant and that the following security features are suitably assured: • Cryptographic key management (generation/destruction); • Cryptographic operations (digital signature generation); • Identification, authentication and access control; • Physical protection; and • Secure data exchange between the TOE and the HSM.

39 There are no organisational security policies defined for the TOE.

Chapter 3 - Evaluation

3.1 Overview

40 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

41 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8] and [10]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

3.3 Functional Testing

42 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 in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

43 The developer performed a 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. This analysis included a search for possible vulnerability sources in publicly available information.

44 The evaluators performed penetration testing based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description, implementation representation as well as publicly available information.

45 During the penetration testing, the evaluators found an exploitable vulnerability that could allow an attacker to assume a user's identity without needing to authenticate as that user. Verizon responded to this vulnerability by releasing a security patch which expanded the

authentication mechanism. The functionality added to the TOE required a change of version, bringing the TOE to 5.3.4.1.

46 Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Chapter 4 - Certification

4.1 Overview

47 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

48 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [1]), the Australasian Certification Authority certifies the evaluation of UniCERT 5.3.4.1 performed by the Australasian Information Security Evaluation Facility, stratsec.

49 stratsec has found that UniCERT 5.3.4.1 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.2.

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

4.3 Assurance Level Information

51 EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

52 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

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

54 This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

4.4 Recommendations

55 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 ISM (Ref [1]) and New Zealand Government users should consult the GCSB.

56 The ACA recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;

b) Operate the TOE according to the administrator guidance (Ref [3]);

c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved;

d) Plan PKI requirements prior to initial installation. UniCERT is complex and can be as expansive as your need requires. Initial planning can reduce setup time drastically;

e) Secure the Certificate Authority, Key Archive Server, Certificate Status Server and Registration Authority. These components are the heart of UniCERT. Compromising even one of those components can result in a complete collapse of the integrity of the PKI deployment;

f) Enable SSL on the web server. The WebRAO client requires encrypted logon in order to authenticate;

g) Patch Oracle as per requirements for the supporting environment. UniCERT has been tested on both versions 10g and 11g provided they have the relevant patches;

h) Ensure that any active directory requirements are documented, as this is the backbone of the AutoEnroll component;

i) Ensure that any Hardware Security Module requirements adhere to the supported product list, including supported firmware and software versions. Also ensure that any smart cards used are in the supported product list; and

j) As per the evaluated configuration, make sure that any entities that have left the organisation are removed from the PKI and their certificates revoked.

Annex A - References and Abbreviations

A.1 References

[1] Verizon UniCERT Security Target, Version 1.8, 29 March 2012

[2] 2012 Australian Government Information Security Manual (ISM), Defence Signals Directorate, (available at www.dsd.gov.au).

[3] UniCERT 5.4.3.1 User Documentation:

a) UniCERT 5.3.4 Installation Guidance for Windows

b) UniCERT 5.3.4 Installation Guidance for Solaris

c) UniCERT 5.3.4 Configuration Guide for Windows

d) UniCERT 5.3.4 Configuration Guide for Solaris

e) UniCERT 5.3.4 Administrators Guide, 03 May 2011

f) UniCERT 5.3.4 Autoenroll Guide, 03 May 2011

g) UniCERT 5.3.4 Database Administrators Guide, 03 May 2011

h) UniCERT 5.3.4 Elliptic Curve Cryptographic Guide, 03 May 2011

i) UniCERT 5.3.4 Extensions Guide, 03 May 2011

j) UniCERT 5.3.4 KeyArchiver Guide, 03 May 2011

k) UniCERT 5.3.4 Publisher Guide, 03 May 2011

l) UniCERT 5.3.4 Web Components Guide, 03 May 2011

m) UniCERT 5.3.4 WebRAO Guide, 03 May 2011

n) UniCERT 5.3.4 Additional CC Guidance

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001.

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002.

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[8] AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.

[9] AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.

[10] AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.

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

[12] Evaluation Technical Report for Verizon UniCERT 5.3.4.1, 17 May 2012.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ALC_FLR	Assurance component: Life Cycle, Flaw Remediation
ARL	Authority Revocation List
ARM	Advanced Registration Module
CA	Certification Authority
CAO	Certificate Authority Operator
CC	Common Criteria
CEM	Common Evaluation Methodology
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
CSS	Certificate Status Server
DB	Database
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
GUI	Graphical User Interface
HSM	Hardware Security Module
KAO	Key Archive Operator
KAS	Key Archive Server
KRO	Key Revocation Operator
OSCP	Online Certificate Status Protocol
OWASP	Open Web Application Security Project
PIN	Personal Identification Number
PKCS#11	Public Key Cryptographic Standard #11 (for cryptographic tokens)
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
RAO	Registration
RAX	Registration Authority eXchange
RRO	Registration Revocation Operator
SCEP	Simple Certificate Enrolment Protocol

SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
UPI	UniCERT Programmatic Interface
+	Augmented