AISEP Certificate Extension Program

Certificate Extension Report

Baltimore Technologies Ltd

UniCERT 3.1.2.A

Version	1.0
Date	May 03

Contents

1 Executive Summary

UniCERT 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.

UniCERT 3.1.2.A was evaluated in accordance with the rules of the Australasian Information Security Evaluation Program (AISEP). In November 2000, the Australasian Certification Authority (ACA) issued certificate number 2000/16 certifying that UniCERT 3.1.2.A had met the ITSEC Assurance Level E3.

This report describes the Australasian Certificate Extension (ACE) approved changes that have been made to the evaluated version of UniCERT (3.1.2.A), and lists the subsequent ACE approved versions of UniCERT. Relevant configuration and installation guidelines have also been included where appropriate.

For each change that is outlined in this report, ACE deliverables have been required to demonstrate that previous evaluation results remain valid. ACE approval signifies that the assurance gained from the most recent evaluation has been maintained.

This report concludes that UniCERT 3.1.2.B, 3.1.2.C, and 3.1.2.D have maintained the ITSEC E3 level of assurance.

2 Introduction

This report describes the AISEP Certificate Extension (ACE) approved changes that have been made to the evaluated version of UniCERT (3.1.2.A); and lists the subsequent ACE approved versions of UniCERT. The report is aimed at users of the certified product UniCERT 3.1.2.A. The report also outlines relevant configuration and installation guidelines that should be followed in order for the certified product to remain in an approved configuration. It is assumed that the reader is familiar with the UniCERT 3.1.2.A certification report.

2.1 ACE Program

The ACE program is aimed at assuring that a certified product will continue to meet its security target as changes are made to the certified product or its environment. Such changes include the discovery of new vulnerabilities, changes in user requirements, the correction of flaws found in the certified product and updates to functionality. For each change that is outlined in this report, ACE deliverables have been required to demonstrate that the results established during the original evaluation remain valid.

2.2 ACE Approval

It is important to note that those versions of UniCERT appearing as ACE approved in this report have not been evaluated and should not be referred to as such. ACE approval signifies that the assurance gained from the most recent evaluation has been maintained.

3 Identification

Table 3.1 below provides information about the certified Target of Evaluation (TOE).

	Details
TOE	UniCERT Version 3.1.2.A
Certificate Number	2000/16
Security Target	UniCERT Security Target, Version 3.10, Nov 2000
ITSEC Level	E3

Table 3.1 TOE Identification

4 Change Register

The changes shown in Table 4.1 below have been ACE approved.

	Version	Details
Change 1	3.1.2.B	Communications Change
Change 2	3.1.2.B	Support for NT SP6a
Change 3	3.1.2.C	Changes to Object Identifier (OID) generation for Customer Policy
Change 4	3.1.2.D	Retrieval of large Certificate Revocation Lists (CRLs) by the Certificate Authority (CA) and Certificate Authority Operator (CAO)
Change 5	3.1.2.D	CA handling multiple messages queued from the same Registration Authority (RA)

Table 4.1 Change Register

Baltimore Technologies Ltd has released the changes shown above as patches for UniCERT.

4.1 Patch B (UniCERT 3.1.2.B)

This patch fixes an intermittent communications problem which caused certain requests (such as certification requests) to be processed very slowly. The patch also provides support for Windows NT4 SP6a. ACE approval for Patch B was granted on 12 June 2002.

4.2 Patch C (UniCERT 3.1.2.C)

This patch prevents the CAO from crashing when a user attempts to add the Certification Policy extension to a policy after September 9 2001. With this patch applied, a user can successfully add the Certification Policy extension to a policy using the CAO's Security Policy Editor. ACE approval for Patch C was granted on 12 June 2002.

4.3 Patch D (UniCERT 3.1.2.D)

This patch fixes a problem with retrieval of large CRLs and also addressed a problem with the handling of multiple messages queued from the same RA. ACE approval for Patch D was granted on 22 April 2003.

4.3.1 Retrieval of Large CRLs

Previously, when a CRL exceeded 5.5 Megabytes in size the CA would shutdown while trying to generate the next CRL. Patch D has addressed this issue.

4.3.2 Multiple Messages

Any certification requests received during CRL generation are queued for handling. In some circumstances the CA would loop when reading these queued messages. Patch D addressed this issue.

5 Configuration

The following section provides installation guidance and relevant configuration advice for ACE approved updates to UniCERT 3.1.2.A. Also included is a list of elements that should be received as part of each update and specific information (such as directory listings) that should be checked as a means of ensuring integrity.

5.1 Identify Running Version

The UniCERT program directory should be examined in order to identify the running version of UniCERT. As each patch is applied, certain files within the subdirectories of UniCERT will be replaced with updated versions. This information relates only to UniCERT 3.1.2A and subsequent ACE approved releases.

The UniCERT program directory used as an example is c:\Program Files\Baltimore-Technologies\UNICERT.

The subdirectories and files that should be examined are the following:

- c:\Program Files\Baltimore-Technologies\UNICERT\CAO
  - cao.exe
- c:\Program Files\Baltimore-Technologies\UNICERT\CA
  - UniCA_Service.exe

Table 5.1 below provides the details of the above files and the corresponding UniCERT version.

Version	File Name	Details		
UniCERT 3.1.2.A	cao.exe	5,068,800	08-11-00	6:09p
	UniCA_Service.exe	4,429,824	08-11-00	5:58p
UniCERT 3.1.2.B	cao.exe	5,068,800	08-11-00	6:09p
	UniCA_Service.exe	4,419,072	08-05-01	5:31p
UniCERT 3.1.2.C	cao.exe	5,053,440	18-09-01	2:54p
	UniCA_Service.exe	4,419,072	08-05-01	5:31p
UniCERT 3.1.2.D	cao.exe	5,059,584	26-02-02	10:25a
	UniCA_Service.exe	4,445,184	26-02-02	10:25a

Table 5.1 Version Identification

To identify the current version of UniCERT, obtain a directory listing of the CAO and CA subdirectories. The details of cao.exe and UniCA_Service.exe should then be compared to Table 5.1.

5.2 UniCERT v3.1.2.B

1 x CD_ROM consisting of two files:

- UniCA_Service.exe
- UniCERT_V3_1_2_B_Readme.htm

The Readme file describes how to load this patch.

The Volume is labelled **UNICERT_312B**. It contains the following directory listing:

08/05/2001	17:31	4,419,072	UNICA SERVICE.EXE
14/05/2001	11:45	3,632	UNICERT_V3_1_2_B_README.HTM

5.2.1 Installation

UniCERT v3.1.2.B is a patch for UniCERT 3.1.2.A. Only apply v3.1.2.B to UniCERT 3.1.2.A. You cannot use this patch in conjunction with UniCERT 3.1.2 Patch 1 or later.

Follow the instructions from UniCERT_V3_1_2_B_Readme.htm to install the patch.

5.3 UniCERT v3.1.2.C

1 x CD_ROM consisting of two files:

- cao.exe
- UniCERT_3.1.2.C_Readme.html

The Readme file describes how to load this patch.

The Volume is labelled **UNICERT_312C**. It contains the following directory listing:

18/09/2001	14:54	5,053,440	CAO.EXE
27/09/2001	11:26	3,319	UNICERT_3.1.2.C_README.HTML

5.3.1 Installation

UniCERT v3.1.2.C is a patch for UniCERT 3.1.2.B, the ACE approved version. Only apply v3.1.2.C to UniCERT 3.1.2.B. Do not use this patch with UniCERT v3.1.2 patch 1 or later patches.

Follow the instructions from UniCERT_3.1.2.C_readme.html to install the patch.

5.4 UniCERT v3.1.2.D

1 x CD_ROM consisting of three files:

- cao.exe
- UniCA_Service.exe
- UniCERT_3.1.2.D_Readme.html

The Readme file describes how to load this patch.

The Volume is labelled **UNICERT_312D**. It contains the following directory listing:

26/02/2002	10:25	5,059,584	CAO.EXE
26/02/2002	10:25	4,445,184	UNICA_SERVICE.exe
26/02/2002	10:26	14,110	UNICERT_3.1.2.D_README.HTML

5.4.1 Installation

UniCERT 3.1.2.D contains the CA and CAO. This patch can be applied to UniCERT 3.1.2 (RoW), UniCERT 3.1.2.A, UniCERT 3.1.2.B or UniCERT 3.1.2.C.

Follow the instructions from UniCERT_3.1.2.D_readme.html to install the patch.

6 Conclusion

The Australasian Certification Authority has determined that the changes made to UniCERT 3.1.2.A and identified as ACE approved in this report have met the requirements for the ACE program.

These ACE approved versions of UniCERT should only be used in accordance with all recommendations and guidelines as set out in this report and the UniCERT 3.1.2.A Certification Report.

7 Document History

Version	Details	Author	Date
draft	Patch B & C	Lachlan Turner	June 02
1.0	Patch D	Lachlan Turner	May 03