AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report
Certificate Number: 2002/23

Tumbleweed Communications Inc.
Tumbleweed Messaging Management System (MMS)
Release 4.6

Issue 1.0
March 2002

Issued by: -
Defence Signals Directorate - Australasian Certification Authority

CERTIFICATION STATEMENT

Tumbleweed Message Management System (MMS) Release 4.6 is a product developed by Tumbleweed Communications Inc. that allows administrators and policy-makers to define and enforce security policies to ensure the safe, appropriate and efficient use of corporate e-mail systems.

This report describes the evaluation findings of the Tumbleweed MMS product to the Common Criteria (CC) Evaluation Assurance Level (EAL) 2, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product to meet its CC EAL 2 level of assurance. It concludes that the product has met the target Assurance Level of CC EAL 2.

Originator

Katrina Johnson
Certifier
Defence Signals Directorate

Approval

Douglas Stuart
Manager, Australasian Information Security Evaluation Program
Defence Signals Directorate

Authorisation

Lynwen Connick
Australasian Certification Authority
Defence Signals Directorate

TABLE OF CONTENTS

Chapter 1 Introduction

Intended Audience

1.1 This certification report states the outcome of the IT security evaluation of the Tumbleweed Messaging Management System (MMS) Version 4.6 developed by Tumbleweed Communications Inc. (hereafter referred to as Tumbleweed MMS). It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to advise security administrators on ensuring the product is used in a secure manner.

Identification of Target of Evaluation

1.2 The version of Tumbleweed MMS evaluated was **version 4.6**, developed by Tumbleweed Communications Inc.

1.3 The security functionality offered by Tumbleweed MMS is implemented entirely in software.

1.4 The evaluated component of Tumbleweed MMS **excludes** the following:

- Support for, interaction with, and interfaces to the Tumbleweed Integrated Messaging Exchange (IME) product
- The Secure Messaging Redirect Edition of MMS
- Conversion of messages from MIME to UUENCODE and from UUENCODE to MIME
- Any client-side applications including S/MIME clients
- The functionality of the McAfee anti-virus software supplied with the TOE
- Any encryption functionality not explicitly included in the TOE Security Functions, in particular excluding unapproved algorithms such as RC4
- Remote administration of the TOE by other than separately encrypted communication channels
- Operating system services not used by the TOE
- All hardware services provided by the defined hardware platforms

1.5 For further details of the evaluated components of Tumbleweed MMS, 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 Program (AISEP) which is described in AISEP Publication No. 1 and AISEP Publication No. 2 (refs [1], [2] respectively). In addition, the conditions outlined in the Common Criteria Recognition Arrangement (ref [15]) were also upheld during the evaluation and certification of this product.

1.7 The purpose of the evaluation was to provide assurance about the effectiveness of the Target of Evaluation (TOE), Tumbleweed MMS version 4.6, in meeting its Security Target (ST) (ref [9]). The criteria against which the TOE is evaluated are expressed in the Common Criteria Part 3 (ref [5]). This describes how the degree of assurance can be expressed in terms of the levels EAL1 to EAL7. The methodology used is described in the Common Evaluation Methodology (CEM) and Evaluation Memoranda 4 and 5 (refs [6][7][8]).

1.8 The evaluation was performed by CMG, between October 2000 and March 2002, and was monitored by the Certification Group on behalf of the Australasian Certification Authority (ACA). At the end of the evaluation, an Evaluation Technical Report (ETR) (ref [10]) describing the evaluation and its results was presented to the ACA. The Certification Report was then produced, based on the contents of the ETR (ref [10]) and the Certification Group's knowledge of the evaluation.

1.9 The Security Target (ref [9]) claimed an assurance level for the product of CC EAL2.

General Points

1.10 Certification is not a guarantee of freedom from security vulnerabilities; there remains a probability (less at the higher evaluation levels) that exploitable vulnerabilities remain undiscovered.

1.11 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

1.12 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis (if applicable), and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

1.13 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

1.14 Tumbleweed MMS should only be used within the defined TOE security environment in accordance with the secure usage assumptions and the organisational security policies, as

explained in section 3 of the Security Target (ref [9]). Also, the security requirements on the IT and non-IT environment must be fully understood in order to determine the suitability of the product in its assumed operational environment, as explained in section 5 of ref [9]. In addition, users should be aware of the certifiers' recommendations as given in Chapter 4 of this report.

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

Scope of the Evaluation

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

1.17 This Report makes no claims about the use of Tumbleweed MMS in classified environments. Potential users are encouraged to contact their National Information Security Authority for further advice on the suitability of this product when used in conjunction with other evaluated products to protect national and non-national security information.

Chapter 2 Security Overview of Tumbleweed MMS

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

Functionality of the TOE

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

2.3 The TOE is designed to enforce security policies to ensure the safe, appropriate and efficient use of corporate e-mail systems. The TOE enables organisations to apply virus scanning, content control, access control, encryption, and digital signature policies on incoming and outgoing SMTP e-mail.

2.4 The TOE provides a graphical user interface for Administrators to set policies that implement e-mail controls. These controls are applied to all SMTP-based messages that pass through a corporate firewall, protecting networks and information assets, and allowing organisations to monitor and archive all SMTP e-mail communications. Tumbleweed MMS provides centralised security features on top of SMTP-based e-mail systems and behind existing firewalls.

2.5 Specifically, the TOE provides the following security functions:

a) **Message Confidentiality** by encrypting messages;

b) **Message Integrity and Non-Repudiation** by digitally signing messages;

c) **Message Archiving** by automatically storing some or all ingoing and outgoing e-mail to meet organisational or regulatory requirements;

d) **Sender Privacy** by stripping out or rewriting message headers to remove information such as e-mail aliases, hostnames, and sub-domain information to help keep internal architectures private and protect details of individuals;

e) **Information Confidentiality** by dropping, quarantining or returning to sender outgoing messages based on the recipient's address or address domain, message content, or attachment type;

f) **Information and System Integrity** by dropping, quarantining or returning to sender incoming messages based on the sender's address or address domain,

content of message, or attachment type;

g) **Information and System Availability** by dropping, quarantining or deferring delivery of incoming messages based on sender's address or address domain, content of message, attachment type or size of message;

h) **Message Disclosure** by automatically adding recipients to certain messages in accordance with organisational requirements for monitoring, auditing and legal compliance;

i) **Disclaimer/Warning Annotation** by automatically annotating outgoing messages with appropriate warnings or disclaimers based on the recipient's address or address domain, sender's address, or content of message;

j) **Notification of Violations** by notifying the sender, recipient or other designated person of a policy violation; and

k) **System Security Management** by restricting access to the functions for configuring the security attributes and policies to only authorised administrators and all associated activities.

2.6 The TOE relies on security functionality provided by Windows NT 4.0 Service Pack 6a. Specifically, the TOE relies on the Windows NT 4.0 operating system to restrict access to its administration functions, record security-related events performed by the Administrator, and to protect the storage of security-related data and attributes.

Architecture of the TOE

2.7 This section provides a summary of the architectural design of the TOE together with the security functions it is designed to perform.

2.8 The Tumbleweed MMS product is a software application that is made up of a number of subsystems that provides SMTP e-mail security and policy services.

2.9 Tumbleweed MMS comprises the following main architectural components:

a) **MMS Server:** Provides the policy enforcement services for all messages passing through it; and

b) **MMS Administration Workstation:** Administrators can use it to manage and configure the policies and operation of the MMS Server.

2.10 Additionally, the Tumbleweed MMS product can be described through the following subsystems:

a) **Administration Subsystem:** Provides the functionality necessary to configure

and manage the TOE. This subsystem resides on the MMS Administration Workstation.

b) **Policy Subsystem:** Provides a single-point for access to all MMS policy engines. The various policy engines include: Policy Manager, Content Manager, Security Manager, Access Manager, Virus Manager, Format Manager, Message Monitor, and Archive. This subsystem resides on the MMS Server.

c) **Message Handling Subsystem:** Provides the functionality for handling messages and routing them through the system. This subsystem resides on the MMS Server.

Security Policy

2.11 The following security policies are enforced by Tumbleweed MMS:

a) Security audit policy, defining the audit generation and review capabilities of the TOE.

b) Communications policy, designed to assure the identification of parties participating in a data exchange.

c) Cryptographic support policy, defining the management aspects of cryptographic key generation, distribution, destruction, and operation.

d) User data protection policy, specifying requirements for the protection of data by the TSFs for both authenticated and unauthenticated services.

e) Identification and authentication policy, defining access rights and privileges to protect assets from loss or disclosure by specifying applicable rules for users and management.

f) Security management policy, defining the administrators role and interaction with the TOE.

g) Privacy policy, defining rules for user protection against discovery and misuse of identity by other users of the system.

h) Protection of the TSFs policy, defining the requirements that enable the resources being controlled by the TSF to be protected from alteration or tampering.

i) Resource utilization policy, defines the requirements for supporting the availability of required resources.

j) Trusted path/channels policy, defines requirements for a trusted communications path between users and the TSF.

2.12 In order for the TOE to comply with the security policy model, the Tumbleweed MMS

product should only be used within the defined TOE security environment in accordance with the secure usage assumptions, as explained in section 3 of the Security Target (ref [9]).

Documentation

2.13 Before using the product, administrators and security managers should ensure that they are aware of, and fully understand the relevant operational documentation. In addition, they should ensure they read Chapter 4 of this document, and associated administration manuals contained on the product CD-ROM (refs [11] and [12]).

Chapter 3 Evaluation Findings

Introduction

3.1 The evaluation of Tumbleweed MMS followed a course consistent with the generic evaluation work program described in the ITSEM (ref [14]) and the CEM (ref [6]), with work packages structured around the evaluator actions described in the Common Criteria (CC) Part 3 (ref [5]). The results of this work are reported in the ETR (ref [10]) under the CC headings. This report summarises the general results, followed by the findings in relation to the security functionality claimed in the Security Target (ST) (ref [9]).

Security Target Evaluation

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

TOE Description (ASE_DES.1)

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

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

Security Environment (ASE_ENV.1)

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

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

ST introduction (ASE_INT.1)

3.7. The ST introduction identified and adequately described the ST and the TOE. It contained an ST overview in narrative form, and contained a CC conformance claim to meet the predefined assurance level of EAL2.

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

Security Objectives (ASE_OBJ.1)

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

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

Protection Profile (PP) Claims (ASE_PPC.1)

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

IT Security Requirements (ASE_REQ.1)

3.12. The statement of the TOE Security Functional Requirements (SFRs) correctly identified the SFRs drawn from CC Part 2 (ref [4]), and the TOE Security Assurance Requirements (SARs) for EAL2 from CC Part 3 (ref [5]). The justification for using the pre-defined EAL2 assurance package was sufficient.

3.13. The ST did not identify any security requirements for the IT environment.

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

Explicitly stated IT Security Requirements (ASE_SRE.1)

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

TOE Summary Specification (ASE_TSS.1)

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

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

3.18. The TOE summary specification rationale demonstrated that the IT security functions were suitable to meet the TOE security functional requirements, and that the combination of IT security functions work together to also satisfy the TOE security functional requirements. The rationale also demonstrated, aided by a mapping, that the assurance measures met the assurance requirements for EAL2.

3.19. The TOE Summary Specification stated that there were no IT security functions that are realised by a probabilistic or permutational mechanism that were not cryptographic

in nature.

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

ST Evaluation Result

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

Common Criteria EAL2 Security Assurance Requirements

3.22. EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

3.23. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

3.24. EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

Configuration Management (ACM)

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

Configuration Management (CM) Capabilities (ACM_CAP.2)

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

3.27. The CM documentation included a configuration list, and the configuration list described the configuration items that comprise the TOE.

3.28. The CM documentation described the method used to uniquely identify the configuration items and the CM system uniquely identified all configuration items.

3.29. As a result of the above determinations, the certifiers conclude that the TOE fully

meets the Configuration Management Capabilities assurance component for EAL2.

Delivery and Operation (ADO)

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

Delivery (ADO_DEL.1)

3.31. The delivery documentation adequately described all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

3.32. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Delivery and Operation assurance component for EAL2.

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

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

3.34. The evaluators confirmed that the installation and generation of the TOE was achieved through the application of the documented procedures.

3.35. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Installation, Generation and Start-Up assurance component for EAL2.

Development (ADV)

3.36. This aspect of the evaluation examines the requirements for the stepwise refinement of the TSF from the TOE Summary Specification in the ST, down to the high-level design. Each of the resulting TSF representations provides information to help determine whether the functional requirements of the TOE have been satisfied.

Functional Specification (ADV_FSP.1)

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

3.38. The Functional Specification was found to be internally consistent and to completely represent the TSF.

3.39. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Specification assurance component for EAL2.

High-Level Design (ADV_HLD.1)

3.40. The presentation of the High-Level Design was informal and found to be internally consistent. It adequately described the structure of the TOE in terms of sub-systems, and the security functionality provided by each sub-system of the TSF.

3.41. The High-Level Design identified all underlying hardware, firmware and software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware or software.

3.42. The High-Level Design identified all interfaces to the sub-systems of the TSF, together with an identification of the interfaces that are externally visible.

3.43. As a result of the above determinations, the certifiers conclude that the TOE fully meets the High-Level Design assurance component for EAL2.

Representation Correspondence (ADV_RCR.1)

3.44. An analysis of the correspondence between all adjacent pairs of the TSF representation was provided. This analysis demonstrated that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation, which was the high-level design.

3.45. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Representation Correspondence assurance component for EAL2.

Guidance Documents (AGD)

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

Administrator Guidance (AGD_ADM.1)

3.47. The administrator guidance clearly described the administrative functions and interfaces, instructions on how to administer the TOE securely, however, not all assumptions regarding user behaviour relevant to the secure operation of the TOE where identified. This issue was addressed during the certification process, and has been documented in Section 4 of this Certification Report, with the identification and recommendation of secure usage operational requirements for the TOE.

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

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

3.50. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Administrator Guidance assurance component for EAL2.

User Guidance (AGD_USR.1)

3.51. The user guidance clearly described the functions and interfaces available to the non-administrative users of the TOE, and the use of user-accessible security functions provided by the TOE. There were no appropriate warnings about user -accessible security functions and privileges that should be controlled in a secure processing environment that needed to be described.

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

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

3.54. It was noted that user interaction with the TOE was minimal, only requiring an understanding of the proxy-user authentication process. However, all of the above requirements were upheld.

3.55. As a result of the above determinations, the certifiers conclude that the TOE fully meets the User Guidance assurance component for EAL2.

Tests (ATE)

3.56. Testing helps to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements, although it cannot establish that the TOE does no more than what was specified. Testing at this level of assurance is also directed towards the internal structure of the TSF, such as the testing of subsystems (identified in the High-Level Design) against their specification.

Coverage (ATE_COV.1)

3.57. The test coverage analysis adequately demonstrated the correspondence between the tests identified in the test documentation and the TSF described in the functional specification, and that the coverage was complete.

3.58. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Coverage assurance component for EAL2.

Functional Testing (ATE_FUN.1)

3.59. The provided test documentation consisted of test plans, test procedure descriptions, expected test results and actual test results. The documentation identified the security functions that were tested and the goals of each test. The test procedure descriptions

described the scenarios for testing each security function. The scenarios did not require that the tests be ordered in any way.

3.60. The expected test results showed the anticipated outputs from the successful execution of these tests, and the test results demonstrated that all identified security functions behaved as specified.

3.61. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Functional Testing assurance component for EAL2.

Independent Testing (ATE_IND.1)

3.62. Independent testing was conducted to confirm that the TOE operates as specified in the documentation supplied for the evaluation. The configuration of the TOE (and its environment) used during testing was consistent with the evaluated configuration, as stipulated in the ST (ref [9]) and the operational guidance (refs [11][12]). In addition, an equivalent set of resources was used that were utilised during the developer functional testing of the TSF.

3.63. The evaluation team repeated all developer tests to verify the developer's test results. All tests executed by the evaluators produced the expected results, consistent with the results produced by the developer's own functional testing.

3.64. The evaluators based their own independent testing on the sample identified above, and extended their testing to investigate the core security functionality of the TOE. Adhoc testing was also performed where appropriate. All tests were sufficiently documented to enable the tests (and their results) to be reproducible.

3.65. The overall outcome of the evaluator testing effort showed that the TOE security functions have been implemented correctly in the TOE. A summary of the evaluator testing effort for this component can be found in the ETR (ref [10]).

3.66. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Independent Testing assurance component for EAL2.

Vulnerability Assessment (AVA)

3.67. This aspect of the evaluation examines the requirements directed at the identification of exploitable vulnerabilities. Specifically, it addresses those vulnerabilities introduced in the construction, operation, misuse, or incorrect configuration of the TOE.

Strength of Function (AVA_SOF.1)

3.68. The Security Target (ref [9]) did not make a strength of function claim.

3.69. As a result of the above determination, the certifiers conclude that the TOE fully meets the Strength of Function component for EAL2.

Vulnerability Analysis (AVA_VLA.1)

3.70. The developer provided a vulnerability analysis searching for ways in which a user can violate the TOE Security Policy (TSP). The documentation showed that none of the identified vulnerabilities were exploitable in the intended environment for the TOE. It also justified that the TOE is resistant to obvious penetration attacks.

3.71. Additional testing did not identify any vulnerabilities that were not considered by the developer. The overall outcome of the evaluator penetration testing effort showed that there are no exploitable vulnerabilities of the TOE in its intended environment.

3.72. Finally, the evaluators determined that the TOE is resistant to penetration attacks performed by an attacker possessing a low attack potential. A summary of the evaluator testing effort for this component can be found in the ETR (ref [10]).

3.73. As a result of the above determinations, the certifiers conclude that the TOE fully meets the Vulnerability Analysis assurance component for EAL2.

Specific Functionality

3.74. The TOE Security Functional Requirements and the TOE Security Functions provided by Tumbleweed MMS are specified in sections 5 and 6 of the Security Target (ref [9]) and summarised in Appendix B of this report.

3.75. The evaluators found that the product correctly and effectively provided the functionality specified in the Security Target (ref [9]).

Discussion of Certification Issues

3.76. During the certification process, one issue identified by the evaluation team remained unresolved. The evaluators observed that not all assumptions regarding user behaviour that are relevant to the secure operation of the TOE had been documented within the administrator guidance. This issue has been addressed in Section 4 of this Certification Report, with the identification and recommendation of several secure usage operational requirements. As a result, there are no remaining unresolved issues following certification of Tumbleweed MMS.

General Observations

3.77. The certifiers would like to acknowledge the invaluable assistance provided by staff from Tumbleweed Communications Inc. 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.

3.78. Further, the certifiers would like to acknowledge the efforts of CMG in ensuring

prompt delivery of the ETR (ref [10]) for certification.

Chapter 4 Conclusions

Certification Result

4.1 After due consideration of the Evaluation Technical Report (ref [10]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Tumbleweed MMS has met the requirements of the Common Criteria EAL 2.

Scope of the Certificate

4.2 The certificate applies only to version 4.6 of the product. This certificate is only valid when the Tumbleweed MMS product is installed and configured in its evaluated configuration. The evaluated configuration of Tumbleweed MMS product is described in Appendix C and should be verified on receipt of the delivered product.

Recommendations

4.3 The following recommendations include 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 Tumbleweed MMS should only be used in accordance with the intended environment described in section 3 (Assumptions) of the Security Target (ref [9]) and the TOE's operational documentation (refs [11]-[12]). Importantly, the evaluated configuration does not include the full functionality offered by the Tumbleweed MMS product.

Functionality not part of the evaluated configuration

4.5 Potential users of the TOE are advised that the evaluated version of Tumbleweed MMS does not include the following:

- Support for, interaction with, and interfaces to the Tumbleweed Integrated Messaging Exchange (IME) product,
- The Secure Messaging Redirect Edition of MMS,
- Conversion of messages from MIME to UUENCODE and from UUENCODE to MIME,
- Any client-side applications including S/MIME clients,
- The functionality of the McAfee anti-virus software supplied with the TOE,

- Any encryption functionality not explicitly included in the TSFs, in particular excluding unapproved algorithms such as RC4,
- Remote administration of the TOE by other than separately encrypted communication channels,
- Operating system services not used by the TOE,
- All hardware services provided by the defined hardware platforms.

Importance of the Administrator Guidance and Release Notes

4.6 Potential purchasers of the TOE are strongly recommended to request the *"evaluated version of Tumbleweed MMS"* when ordering the TOE from Tumbleweed Communications Inc. The evaluated configuration of the TOE will include important operational documentation such as the administrator guide and product release notes (refs [11]-[12]). These documents contain necessary guidance for an administrator to install and configure the TOE in its evaluated configuration.

Qualifications of Administrators

4.7 To ensure the competent administration of the TOE, Administrators of the TOE should be trained in Windows NT 4.0 administration and have a sound knowledge of Internet protocols and messaging technologies.

4.8 It is important that TOE Administrators follow all policies and procedures described in the TOE operational documentation (refs [11]-[12]) to ensure secure administration of the TOE. Additionally, TOE administrators must be competent to carry out administration of the TOE, understand the consequences of their actions and the security policies in place.

Protection by an EAL2 Evaluated Firewall

4.9 Administrators of the TOE should be aware that for the TOE to operate as defined in the Security Target (ref [9]), it relies on network security protection. Therefore, administrators should ensure that Tumbleweed MMS is installed in a network environment that protects it from attack by an EAL2, or higher, assured firewall product.

Non-Bypassibility of the TOE

4.10 The Administrators should ensure that the TOE environment is divided into trusted and untrusted systems. All e-mail communication between trusted and untrusted systems should be mediated by the TOE—ensuring that users cannot bypass the security

mechanisms of the TOE.

Important Operational Considerations

4.11 The Administrators should note that the operating environment should not provide user-accessible code, either malicious or non-malicious, that allows modification of the MMS security configuration by other than authorised administrators.

4.12 The Administrators should ensure that the TOE and its environment have sufficient protections and controls in place to protect the availability of the TOE from natural disasters such as fire or flood, as well as catastrophic failures of power supply and communications.

Storage of Private Keys

4.13 Potential users of the TOE are advised that the MMS Server stores public/private key pairs unencrypted on the system. The TOE is relying on physical and network security measures to protect the keys from compromise. Therefore, it is recommended that strong physical security countermeasures be implemented to protect the TOE. Additionally, the TOE should be protected from network-based attacks by implementing appropriate perimeter security measures.

Tumbleweed MMS Digital Certificates

4.14 Potential users of the TOE are advised that the TOE does not check validity dates on MMS Server certificates. As a result, expired certificates can be used by the TOE to continue providing confidentially and integrity services. Certificates are self-generated by the TOE and are created with a validity period of ten-years. It is recommended that TOE Administrators implement procedures to regenerate MMS Server certificates within a one-year period.

MMS Patch sapassword.exe

4.15 Potential users of the TOE are advised that the vendor has released a software patch to correct a known vulnerability relating to a default administration password for the TOE. This software patch, ***sapassword.exe***, is supplied separately to the base software. It is recommended that TOE Administrators request the software patch from the vendor when purchasing the product and apply the patch following the provided procedures.

Appendix A References

[1] AISEP Publication No.1- Description of the AISEP
Defence Signals Directorate
AP 1, Version 2.0, February 2001

[2] AISEP Publication No.2 - The Licensing of the AISEFs
Defence Signals Directorate
AP 2, Version 2.1, February 2001

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

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

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

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

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

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

[9] Tumbleweed Messaging Management System Version 4.6 Security Target 90 East (Prepared for Tumbleweed Communications
Version 2.3, March 2002
(COMMERCIAL-IN-CONFIDENCE)

[10] Tumbleweed MMS Release 4.6 Evaluation Technical Report
CMG
Issue 1.1, February 2001
(EVALUATION-IN-CONFIDENCE, COMMERCIAL-IN-CONFIDENCE)

[11] Administrator's Guide for MMS Release 4.6
Tumbleweed Communications Inc.

[12] MMS Release 4.6 Release Notes
Tumbleweed Communications Inc.

[13] Tumbleweed MMS Customer Registration Card
Tumbleweed Communications Inc.
Issue 010-1010-00, For Release 4.6

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

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

Appendix B Summary of the Security Target

Security Target

B.1 A brief summary of the Security Target (ref [9]) 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.

Security Objectives for the TOE

B.2 Tumbleweed MMS has the following IT Security objectives:

a) The TOE must provide the means for recording and archiving messages passing through MMS based on an administrator-defined P.AUDIT Policy.

b) The TOE must provide a means for generating evidence that can be used to prevent an originator of data from successfully denying ever having sent that data, and evidence that can be used to prevent a recipient of data from successfully denying ever having received that data.

c) The TOE must provide a means of detecting the loss of integrity of messages transferred between users across the telecommunications network.

d) The TOE must provide the means of protecting the confidentiality of user information when it is transferred across an insecure telecommunications network.

e) The TOE must ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.

f) The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are transferred across an insecure telecommunications network.

g) The TOE must enable the identifying details of users to be protected according to a defined privacy policy.

h) The TOE must prevent users or processes from bypassing or circumventing TOE security policy enforcement.

i) The TOE must provide a security domain for its own execution that protects it from compromise by unauthorised subjects.

j) The TOE must provide cryptographic service using the strongest possible

algorithms and key lengths whilst still maintaining efficiencies.

k) The TOE must protect itself from user or system errors that result in shared resource exhaustion.

Security Objectives for the Environment

B.3 Tumbleweed MMS has the following environmental objectives:

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

b) Those responsible for the operation of the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack that might compromise TOE security functions.

c) Those responsible for the operation of the TOE must ensure that the TOE is protected from network-based attacks that might compromise TOE security functions.

d) Those responsible for the TOE must ensure that procedures and / or mechanisms are in place to ensure that storage and handling of cryptographic-related IT assets is conducted in accordance with the rules defined by the P.CRYPTO policy.

e) Those responsible for the TOE must ensure that only highly trusted users are given privileges that enable them to modify the security configurations of the TOE.

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

g) Those responsible for the TOE must ensure that all personnel given administrator privileges or who are to perform crypto-custodian duties are given training sufficient to enable them to fulfill their duties securely.

h) TOE administrators must ensure that the TOE environment is such that there is no user-accessible code that could be used to bypass TOE security functions.

i) TOE administrators must ensure that they follow the developer's instructions and use the NT User Manager to establish the proper environment for controlling the configuration of the TOE.

j) The TOE Operating System must uniquely identify all users, and must authenticate the claimed identity before granting a user access to the TOE

facilities.

k) The TOE Operating System must provide the means for recording security-relevant events in sufficient detail to help an administrator of the TOE to: (a) Detect attempted security violations; and (b) Hold individual users accountable for any actions they perform that are relevant to the security of the TOE.

l) The TOE, in conjunction with the underlying operating system where necessary, must provide functions to enable an authorised administrator to effectively manage the TOE and its security functions, and ensuring that only authorised administrators can access such functionality.

Secure Usage Assumptions

B.4 Tumbleweed MMS has the following secure usage assumptions:

a) TOE Administrators will follow all policies and procedures described in the TOE system documentation to ensure secure administration of the TOE.

b) TOE administrators are competent to carry out administration of the TOE, understand the consequences of their actions and the security policies in place.

c) As the security functions of the TOE can be readily compromised by authorised administrators, it is assumed that they will have successfully completed a security background check before being granted access to the TOE management functions and are assumed to be non-hostile and can be trusted to do their duties correctly.

d) The TOE environment is divided into trusted and untrusted systems. All communication between trusted and untrusted systems is mediated by the TOE. Thus, users cannot bypass the security mechanisms of the TOE.

e) The TOE and its environment have sufficient protections and controls in place to protect the availability of the TOE from natural disasters such as fire or flood, as well as catastrophic failures of power supply and communications.

f) The TOE will be used to protect attractive IT assets and possible attackers can be assumed to have a medium level of expertise, resources and motivation.

g) As the TOE operates on an NT platform, logical access controls can be compromised if an attacker gets physical access to the console. Strong physical security countermeasures will therefore be in place.

h) As the TOE operates on an NT platform, logical access controls can be compromised if an attacker gets online access to the NT computer. Therefore, the TOE will be protected by an EAL-2 -assured or greater firewall product, operated in accordance with government best practice.

i) The TOE depends on the underlying operating system for security management functions, such as logical access control and auditing for the administration client. The TOE Administrator will operate the TOE from an NT workstation in line with the TOE developer's recommendations, as contained in the Administrators Guide.

j) The TOE relies on an IT system software environment, and TOE users cannot unintentionally overwrite any system programs, logs, or data.

k) The operating environment provides no user-accessible code, either malicious or non-malicious, that allows modification of the MMS security configuration by other than authorised administrators.

Threats addressed by the TOE

B.5 Tumbleweed MMS addresses the following threats:

a) An attacker (whether an insider or outsider) performing actions that bypass the TOE security functions may perform actions, including the unauthorised release of information that violate the security policies.

b) An attacker may eavesdrop on, or otherwise capture, user data or cryptographic key material being transferred across a network.

c) A user as either originator or recipient may participate in the transfer of information and then deny having done so.

d) An attacker (an outsider or insider) may, by impersonation of an authorised user of the TOE, gain unauthorised access to user data or cryptographic key material being transferred across a network.

e) An attacker (whether insider or outsider) may attempt to perform cryptanalysis of data in order to recover user data or cryptographic material.

f) An attacker may, through unauthorised modification or destruction, compromise the integrity of user data or cryptographic key material.

g) A user may either deliberately or accidentally attempt to transmit confidential information without appropriate protection measures in place.

h) A user may either deliberately or accidentally attempt to transmit information to unauthorised recipients.

i) An attacker may be able to determine identity details for authorised users in breach of a privacy policy.

j) An attacker (whether insider or outsider) could execute commands, send data, or

perform other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth and processor time.

k) Non-malicious user action may result in system resources such as bandwidth and processor time being unavailable.

l) Failure of one or more system components of the TOE results in the loss of system-critical functionality.

Threats addressed by the TOE Environment

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

a) The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.

b) An individual, either internally or externally, using non-technical means may gain access to cryptographic key material or related user data being transferred across a network.

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

d) Improper operation of the TOE may cause a failure of the TOE security functions.

e) A TOE Administrator may be able to perform security-relevant actions which cannot be traced or attributed to that person.

f) A person with authorised physical access to the TOE is able to gain unauthorised logical access to the TOE.

Organisational Security Policies

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

a) Details of user message transactions (including incoming and outgoing messages with details such as sender, recipients, subject, content, etc) will be recorded in an audit trail that must be preserved in line with relevant organisational archive requirements.

b) All cryptographically-relevant material is to be the subject of rigorous levels of physical and technical control in accordance with your organisational security policies.

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

d) The flow of information between IT components in a distributed architecture utilising insecure networks must be controlled and protected from disclosure.

e) All confidential, proprietary, or otherwise sensitive information shall be protected, in terms of confidentiality, integrity and authenticity, when transmitted over insecure networks in accordance with the organisational security policy.

f) The organisation shall provide procedures and features to assure that system recovery is done in a trusted and secure manner. Any circumstances that could result in an untrusted recovery shall be documented.

g) The integrity of organisational data will be protected through the identification and treatment of any message content or attachment that might pose a risk. An organisational policy should identify potential risk sources and appropriate actions.

h) Organisational bandwidth can be conserved through assigning priorities to messages based on size, content, sender or recipient.

i) An organisational privacy policy will determine the degree to which an individual's identity is transmitted out of the organisation, for example through e-mail aliases and sub-domain information.

Summary of the TOE Security Functional Requirements

B.8 The TOE security functional requirements (SFRs) are tabulated below. Full description and explanation of these SFRs can be found in Section 5 of the Security Target (ref [9]).

Class FAU: Audit

FAU_ARP.1 Security alarms

FAU_GEN.1 Audit data generation

FAU_GEN.2 User identity association

FAU_SAA.2 Profile based anomaly detection

FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

FAU_SEL.1 Security audit event selection

FAU_STG.2 Guarantees of audit data availability

Class FCO: Communication

FCO_NRO.1 Selective proof of origin

FCO_NRR.1 Selective proof or receipt

Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

FCS_CKM.2 Cryptographic key distribution

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1 Cryptographic operation

Class FDP: User Data Protection

FDP_ETC.2 Export of user data with security attributes

FDP_IFC.2 Complete information flow control

FDP_IFF.1 Simple security attributes

FDP_ITC.2 Import of user data with security attributes

FDP_UCT.1 Basic data exchange confidentiality

FDP_UIT.1 Data exchange integrity

Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

FIA_UID.2 User identification before any action

FIA_UAU.1 Timing of authentication

Class FMT: Security Management

FMT_MSA.1 Management of security attributes

FMT_MSA.2 Secure security attributes

FMT_MSA.3 Static attribute initialisation

FMT_MTD.1 Management of TSF data

FMT_SMR.1 Security roles

Class FPR: Privacy

FPR_PSE.1 Pseudonymity

Class FPT: Protection of the TOE Security Functions

FPT_RVM.1 Non-bypassability of the TSP

FPT_SEP.1 TSF domain separation

FPT_STM.1 Reliable time stamps

FPT_TDC.1 Inter-TSF basic TSF data consistency

Class: FRU: Resource Utilisation

FRU_PRS.2 Full priority of service

FRU_RSA.1 Maximum quotas

Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Security Requirements for the IT Environment

B.9 Tumbleweed MMS places no requirements on the IT environment.

Security Requirements for the Non-IT Environment

B.10 Tumbleweed MMS places the following requirements on the Non-IT Environment:

a) The TOE environment must provide sufficient protection from network-based attacks.

b) The MMS Server must be located within a controlled access facility that will prevent unauthorised physical access.

c) The MMS Server and associated directly-attached console must be physically secure and available to authorised administrators only.

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

e) The TOE environment must provide a mechanism that ensures that the likelihood of administration staff performing illegal actions is minimised.

f) The TOE environment must ensure that at any time no user-accessible code that may modify TOE security functions exists on the MMS Server.

g) The MMS Server must be installed and configured in line with the developer's guidance and administrators must ensure that the configuration remains in step

with developer's ongoing guidance.

h) The TOE environment must ensure that at all times cryptographic keys are protected against unauthorised access, loss or destruction.

i) The TOE environment must ensure that administrators are trained and motivated to make the right choices when providing administrative support to the TOE.

j) The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that access is limited to only authorised TOE Administrators. For examples, accounts on the TOE platform should only exist for authorised TOE Administrators.

k) The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that actions by the MMS Administrator including the modification of security attributes, the modification of MMS policies, and the configuration of the audit function itself are audited.

l) The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that the storage of TSF data and attributes including cryptographic material, policy configuration data, and message archives are appropriately protected.

m) The TOE environment shall provide procedures for installing, configuring and maintaining the underlying operating system for the MMS Server such that configuration of the security features through the creation, review and modification of policies and key word lists can be performed.

Summary of the TOE Security Functionality

B.11 The TOE's Security Functions (TSFs) are briefly listed below. Full description and explanation of these TSFs can be found in section 6 of the Security Target (ref [9]).

a) Message Confidentiality (MES_CON)

b) Message Integrity (MES_INT)

c) Message Non-repudiation (MES_NOR)

d) Message Archive (MES_ARC)

e) Sender Privacy (SEN_PRI)

f) Information Confidentiality (INF_CON)

g) Information and System Integrity (INF_INT)

h) Information and System Availability (INF_AVA)

i) Message Disclosure (MES_DIS)

j) Disclaimer/Warning Annotation (DIS_ANN)

k) Notification of Violations (NOT_VIO)

l) System Security Management (SYS_MAN)

Appendix C Identification of the TOE

Configuration for Evaluation

C.1 The evaluation was conducted on Tumbleweed Version 4.6. The evaluated software components of the TOE have been identified below.

Software

C.2 The software elements of Tumbleweed MMS are as follows:

a) 1 x CD-ROM containing the Tumbleweed MMS Software, Version 4.6; and

b) MMS Patch sapassword.exe.

C.3 As stated in Chapter 4, the evaluated configuration of Tumbleweed MMS excludes the following:

a) Support for, interaction with, and interfaces to the Tumbleweed Integrated Messaging Exchange (IME) product

b) The Secure Messaging Redirect Edition of MMS

c) Conversion of messages from MIME to UUENCODE and from UUENCODE to MIME

d) Any client-side applications including S/MIME clients

e) The functionality of the McAfee anti-virus software supplied with the TOE

f) Any encryption functionality not explicitly included in the TSFs, in particular excluding unapproved algorithms such as RC4

g) Remote administration of the TOE by other than separately encrypted communication channels

h) Operating system services not used by the TOE

i) All hardware services provided by the defined hardware platforms

Third Party Software

C.4 The third party software required to operate Tumbleweed MMS is as follows:

a) For the MMS Server:

- Microsoft Windows NT 4.0 Server with Service Pack 6.0a

The following applications are also required:

- Microsoft Internet Explorer 5.0 or later
- Microsoft Internet Information Server 4.0 or later

b) For the MMS Administration Workstation:

- Microsoft Windows NT 4.0 Workstation with Service Pack 6.0a.

C.5 This evaluation is only valid for the above mentioned version of Tumbleweed MMS running on the identified third party software. No other versions, operating systems or third party software are part of the evaluated configuration.

Hardware

C.6 The minimum hardware configuration of the TOE, both MMS Server and MMS Administration Workstation, is as follows:

- Pentium II 333 MHz
- CD-ROM Drive
- 8 GB hard drive
- 256 MB of memory
- Colour monitor
- An Ethernet or Token Ring interface card

C.7 Please note that none of the hardware identified above implements any of the security functionality offered by the TOE. The minimum recommended hardware configurations for the above hardware platforms are located in section 2.2 of the Security Target (ref [9]).

Procedures for determining the evaluated version of the TOE

C.8 In order for an administrator to determine if a delivered product is in fact the evaluated product, the following procedures can be followed in making that determination.

C.9 When administrators are placing an order for the product, they should request for the evaluated version of Tumbleweed MMS. Once a copy of Tumbleweed MMS has been received, the administrator should inspect the shrink-wrap packaging for any signs of tamper. Any indication of tamper should be reported immediately to Tumbleweed Communications Inc. and the product returned.

C.10 Operational documentation (refs [11]-[12]) is delivered in soft copy with Tumbleweed MMS on CD-ROM. Additionally, a Customer Registration Card (ref [13]) will arrive

with the TOE. Upon receiving the delivered TOE, Administrators should seek to verify its authenticity by activating the software.

C.11 The Administrator should use the License Key contained on the Customer Registration Card (ref [13]) to obtain an Activation Code for the software. The Activation Code is obtained by accessing the Technical Support pages on the Tumbleweed Communications Inc. web site. The Administrator should go to http://www.tumbleweed.com and navigate to Support and then Technical Support, select Tumbleweed MMS and then MMS Activation Code. Procedures for activating the software can be found in the TOE's operational documentation (refs [11]- [12]).