National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Tumbleweed Valicert Validation Authority Version 4.8

Report Number: CCEVS-VR-06-0028
Dated: June 8, 2006
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 1

2 IDENTIFICATION 3

3 SECURITY POLICY 3

4 ASSUMPTIONS AND CLARIFICATION OF SCOPE 7

4.1 USAGE ASSUMPTIONS 7
4.2 ENVIRONMENTAL ASSUMPTIONS 7
4.3 CLARIFICATION OF SCOPE 8

5 ARCHITECTURAL INFORMATION 9

6 DOCUMENTATION 11

7 IT PRODUCT TESTING 11

8 EVALUATED CONFIGURATION 13

9 RESULTS OF THE EVALUATION 13

10 VALIDATOR COMMENTS/RECOMMENDATIONS 14

11 SECURITY TARGET 15

12 GLOSSARY 16

13 BIBLIOGRAPHY 17

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) validator's assessment of the evaluation of the Tumbleweed ValiCert Validation Authority Version 4.8, a product of Tumbleweed Communications Corp., Redwood City, CA. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by the SAIC Common Criteria Testing Laboratory (CCTL), and was completed during April 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC CCTL. The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 3. The product is conformant with Certificate Issuing and Management Components (CIMC) Security Level 1 Protection Profile (PP), Version 1.0, October 31, 2001.

Tumbleweed ValiCert Validation Authority Version 4.8 (hereafter Tumbleweed VA) provides a universal clearing house for establishing the validity of digital certificates. The Target of Evaluation (TOE) was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.2, Revision 256, January 2004 [CCV2.2], and the *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Revision 256, Evaluation Methodology, January 2004 [CEMV2.2]. The evaluation and validation were consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for Tumbleweed VA is contained within the document *Tumbleweed ValiCert Validation Authority Security Target Version 1.0,* dated April, 2006 [ST]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of [CCV2.2].

The Tumbleweed VA is an all-software TOE. It consists of two components:

- Validation Authority (VA): Provides online certificate revocation status information using Online Certificate validation Protocol (OCSP) and Certificate Revocation Lists (CRLs). The Tumbleweed VA can also operate in a distributed architecture providing pre-signed responses to other VAs.

- Publisher: Obtains revocation data from a Certificate Authority (CA) or a directory server supporting Lightweight Directory Access Protocol (LDAP), Secure LDAP (LDAPS), Hyper-text Transfer Protocol (HTTP), and Secure HTTP (HTTPS) and publishes it to the VA component.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with the IT environment:

- Identification and authentication
- Access Control
- Security Audit
- Backup and Recovery
- Key Management
- Profile Management
- Remote Data Entry and Export

The following are explicitly excluded from the TOE configuration, but are included in its environment:

- FIPS 140-1 approved cryptographic module
- Server operating system and hardware
- Administrator client operating system and hardware
- Networking with firewall boundary protection

It is assumed that the environment will counter the threats of unauthorized access to the physical components of the TOE - server and client platforms. It is also assumed that excluded software (e.g. Microsoft Windows 2003 Server and its services; and firewall software) will operate correctly and securely.

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

All copyrights and trademarks are acknowledged.

2 Identification

TOE: Tumbleweed ValiCert Validation Authority Version 4.8, Build 388

Evaluated Software: Tumbleweed ValiCert Validation Authority Version 4.8, Build 388

Developer: Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

CCTL: SAIC Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046.

Validation Body: NIAP Common Criteria Evaluation and Validation Scheme

CC Identification: *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004 [CCV2.2].

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2].

Interpretations: None

Protection Profile: Certificate Issuing and Management Components (CIMC) Security Level 1 Protection Profile (PP), Version 1.0, October 31, 2001.

3 Security Policy

The Tumbleweed VA security policy is reflected in the security functional requirements (SFRs) for the TOE described in section 5.2 of the ST and for the IT environment described in sections 5.1 of the ST. A summary of the principle security policies is as follows:

- **Remote Data Entry and Export**: The TOE is responsible for importing and exporting certificates, certificate revocation lists (CRL), and certificate status. The TOE sends signed messages to ensure the authenticity and integrity of the certificate status information.

- **Identification and authentication:** The TOE in conjunction with the IT environment requires users to be identified and authenticated before being allowed access to the system. The VA supports two types of identification and authentication. For Auditor and Operator, the VA identifies users using certificates. For Administrators, the VA uses user name/password authentication into the administrative console.

- **Role Based Access Control:** There are three roles in the VA as Administrator, Auditor, and Operator. Each role has a specific set of actions it is permitted to perform. The set of access controls each role is permitted to perform is specified in Table 8 of the ST. The functions that are restricted by role are specified in Table 9 of the ST.

- **Audit:** The TOE in conjunction with the IT environment provides an auditing capability. Auditable events for the VA are identified in tables 2 and 6 of the ST. The administrator is able to include or exclude auditable events from the set of audited events based on the event type. The TOE protects the stored audit records from unauthorized deletion. The TOE is able to detect unauthorized modifications to the audit records in the audit trail.

The TOE also provides support for other significant objectives as described in the following paragraphs:

- **Key Management (or Cryptographic Support):** The TOE in conjunction with the IT environment implements FIPS 140-1 validated cryptographic algorithms for key generation, storage and destruction techniques, encryption/decryption, authentication, and signature generation/verification.

- **Backup and Recovery**: The TOE includes a backup and restore utility. The utility is invoked from within the TOE. The utility can be used on demand and is capable of restoring TOE configuration using only the applicable backup files and applicable encryption keys.

.

The security functional requirements for the TOE and the IT environment are documented in section 5 of the ST. A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SEL.1	Selective Audit
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of Audit Data Loss
Class FCO: Communication	
FCO_NRO_CIMC.3	Enforced Proof of Origin and Verification of Origin
Class FCS: Cryptographic Support	
FCS_CKM_CIMC.5	CIMC Private and Secret Key Zeroization
Class FDP: User Data Protection	
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute based Access Control
FDP_ACF_CIMC.2	User Private Key Confidentiality Protection
FDP_CIMC_BKP.1	CIMC Backup and Recovery
FDP_CIMC_CER.1	Certificate Generation
FDP_CIMC_CRL.1	Certificate Revocation
FDP_CIMC_CSE.1	Certificate Status Export
FDP_CIMC_OCSP.1	Basic Response Validation
FDP_ITT.1	Basic Internal Transfer Protection
FDP_UCT.1	Basic Data Exchange Confidentiality
Class FIA: Identification and Authentication	
FIA_ATD.1	User Attribute Definition
FIA_UAU.1	Timing of Authentication
FIA_UID.1	Timing of Identification
FIA_USB.1	User-subject Binding
Class FMT: Security Management	
FMT_MOF.1	Management of Security Functions Behavior
FMT_MOF_CIMC.2	Certificate Profile Management
FMT_MOF_CIMC.4	Certificate Revocation List Profile Management
FMT_MOF_CIMC.6	OCSP Profile Management
FMT_MSA.1	Management of Security Attributes
FMT_MTD_CIMC.4	TSF Private Key Confidentiality Protection
FMT_SMR.2	Restrictions on Security Roles
Class FPT: Protection of the TSF	
FPT_ITC.1	Inter-TSF Confidentiality during Transmission

FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM.1	Non-bypassability of the TSP

IT Environment Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective Audit
Class FCS: Cryptographic Operation	
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1	Cryptographic Operation
FCS_CKM.1	Cryptographic Key Generation
Class FDP: User Data Protection	
FDP_ACC.1	Subset Access Control
FDP_ACF.1	Security Attribute Based Access Control
FDP_ITT.1	Basic Internal Transfer Protection
FDP_UCT.1	Basic Data Exchange Confidentiality
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of Authentication
FIA_UID.1	Timing of Identification
FIA_USB.1	User-subject Binding
Class FMT: Security Management	
FMT_MOF.1	Management of Security Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static Attribute Initialization
FMT_MTD.1	Management of TSF Data
FMT_SMR.2	Restrictions on security roles
Class FPT: Protection of the TSF	
FPT_AMT.1	Abstract Machine Testing
FPT_ITC.1	Inter-TSF Confidentiality during Transmission
FPT_ITT.1	Basic Internal TSF Data Transfer Protection
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF Domain Separation
FPT_STM.1	Reliable Time Stamps
FPT_TST_CIMC.2	Software/Firmware Integrity Test
FPT_TST_CIMC.3	Software/Firmware Load Test

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL3 assurance requirements.

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

4.2 Environmental Assumptions

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

Environmental Assumptions

Assumption	Description
A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators, Operators, Officers and Auditors	Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.CPS	All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility)
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity

A.Notify Authorities of Security Issues	Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Social Engineering Training	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
A.Social Engineering Training	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.
A.No Abusive Administrators, Operators, Officers and Auditors	Administrators, Operators, Officers and Auditors are trusted not to abuse their authority.
A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.
A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the Security Level 1 as identified in CIMC PP.

4.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation.

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL3 in this case).

2. This evaluation covers Tumbleweed VA version 4.8, and not any earlier or later versions released or in process. These evaluation results do not automatically apply to other versions.

3. As with all EAL3 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or vulnerabilities in the IT environment or to objectives not claimed in the ST.

The ST provides additional information on the assumptions made and the threats countered.

The evaluation of this TOE is not directly tied to possible evaluations of any of those other components in an electronic messaging application. In particular, the evaluation of this TOE does not imply that all of the properties required of the Tumbleweed VA for the evaluation of those other products have been included in this evaluation. This is not necessarily a limitation upon the capabilities of this product or those other components of the messaging environment, but rather it is a statement of the limitations on the scope of the analysis that was performed for this evaluation.

5 Architectural Information

The TOE, as evaluated, consists of the Validation Authority (VA) and the accompanying publisher

1. Tumbleweed VA – Validates revocation status of digital certificates and has option to communicate over an HTTPS interface.
2. Tumbleweed Publisher – Collects revocation data from a CA or a directory server supporting LDAP, LDAPS, HTTP, or HTTPS and publishes it to a VA.

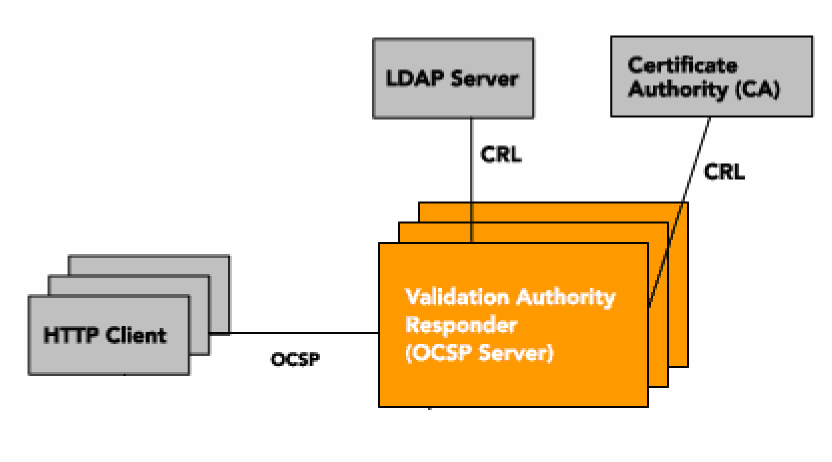
LDAP Server
Certificate Authority (CA)
CRL
CRL
HTTP Client
OCSP
Validation Authority Responder (OCSP Server)

Figure 1 TOE architecture – traditional OCSP

In the distributed OCSP architecture, the TOE is deployed in the traditional and distributed mode as shown in the following figure.

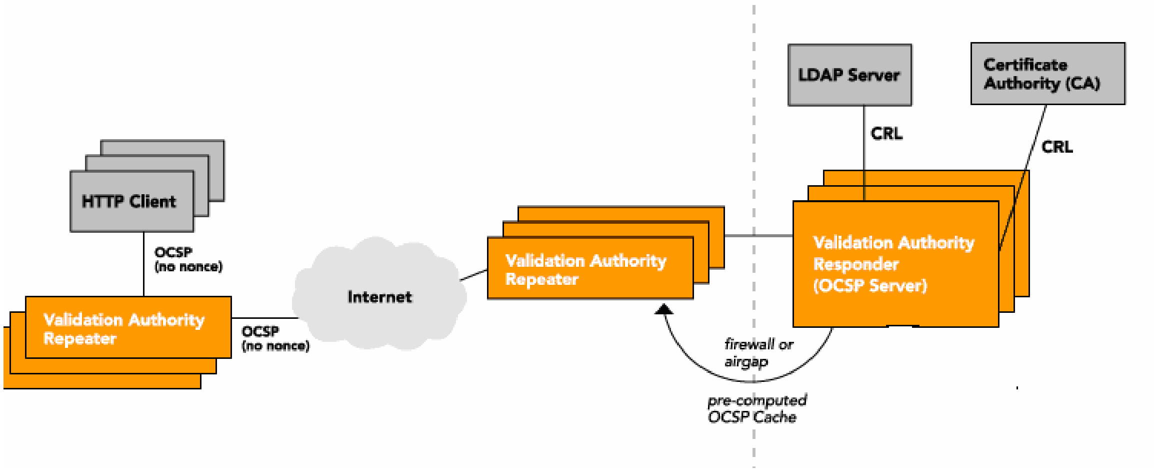
LDAP Server
Certificate Authority (CA)
CRL
CRL
HTTP Client
OCSP (no nonce)
Validation Authority Repeater
OCSP (no nonce)
Internet
Validation Authority Repeater
Validation Authority Responder (OCSP Server)
firewall or airgap
pre-computed OCSP Cache

Figure 1 Distributed Architecture

In addition to the above two architectures, the certificate validation depends on the trust agreement between the VA and the clients. Three trust models are identified followed by a brief description.

- Direct Trust
- VA Delegated Trust
- CA Delegated Trust

The Tumbleweed VA only issues certificates and CRLs in the VA delegated trust model. The directly trusted VA has a self-issued digital certificate that it uses to issue a digital certificate to a subordinate VA. The subordinate VA uses the certificate to sign client OCSP responses only. The directly trusted VA issues X509 certificates. The directly delegated VA issues standard X509 CRLs to the subordinate VAs. In the VA-delegated model, TOE issues two types of CRLs, full and delta CRLs. The full CRLs are a mirror of the CRLs received from the CAs or a delta CRL that include the serial numbers of the revoked and invalid certificates issued by the directly trusted VA.

The IT environment includes the following software:

- Microsoft Internet Explorer 5.5 or 6.0, or Netscape 6.2. (JavaScript enabled)
- Operating System
    - Windows 2000 or Server 2003
    - Solaris 2.7, 2.8, 2.9 or 2.10

  - Red Hat Enterprise Linux 7, 8 or 9

6 Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- Certificate Issuing and Management Components Family of Protection Profiles Version 1.0
- Tumbleweed VA Version 4.8 Security Target
- Secure Installation, Generation, and Startup Procedures / Administrator Supplement Guide for Tumbleweed Validation Authority Version 4.8, version 1.6, October 31, 2005
- Tumbleweed Valicert Validation Authority Operator's Guide, Release 4.8, Rev02

7 IT Product Testing

7.1 Developer Testing

The vendor testing covered all of the security functions identified in Section 6.1 of the ST. These security functions were: Security Audit, Backup and Recovery, Access Control, Identification and Authentication, Remote Data Entry and Export, Key Management, and Profile Management. At EAL3, vendor testing must demonstrate correspondence between the tests and the design documentation and in accordance with the TOE security functional requirements specified in the ST. This is accomplished by determining that the developer has tested the TSF against its functional specification and high-level design, gaining confidence in those test results by performing a sample of the developer's tests, and by independently testing a subset of the TSF.

The developer testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures were designed to be exercised manually, using the web client interfaces and command-line interfaces of the TOE as well as the command-line and file systems interfaces of the IT environment and the use of some custom testing tools designed for use on the hosting operating system. The test suite was executed on three representative operating system configurations: Windows 2000 SP4, Solaris 2.9, and Red Hat Linux 9. Tumbleweed's "ValiCert Security Module" was used as the FIPS 140-1 validated crypto modules (certificate #288).

7.2 Evaluator Independent Testing

At EAL 3, the stated purpose of the evaluator's independent testing activity "The goal of this activity is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." As part of devising their test cases, the evaluator considers a number of factors (see [CEMV2.2] section 7.9.5). The IT environment for testing included the following:

- Dell Precision 370 workstations
- Windows XP Professional (SP2)
- Internet Explorer 6
- Tumbleweed "ValiCert Security Module" (FIPS 140-1 certificate #288)

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran all of the provided developer test procedures for the Windows platform and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality. Test results, which are contained in proprietary reports, were satisfactory to both the evaluation and the validation teams.

7.3 Strength of Function

The TOE depends on the strength of the passwords used to access the Tumbleweed VA server. For this mechanism a qualification of its security behavior was made using the results of a quantitative or statistical analysis of the security behavior of the mechanism and the effort required to overcome the mechanism. A strength-of-function (SOF) claim of SOF-basic was made for accounts on the Tumbleweed VA server. The basis of the claim of SOF-basic is the enforcement of the policy that passwords must contain a minimum of 8 characters with at least 1 numeric character and 1 alphabetic character and that account access is locked out after 3 failed attempts. The SOF analysis used these password requirements to justify a ranking of SOF-basic which effectively requires resistance to password guessing attacks of greater than one day.

In the evaluated configuration, the TOE is designed so that its cryptographic functions are performed using following approved algorithms: DES and triple-DES (FIPS 46-3); RSA (FIPS 186-2) ; and SHA-1 (FIPS 180-2). The TOE performs these functions by invoking a FIPS 140-1 validated cryptographic module in the IT environment. Requirements involving digital signatures rely on SHA-1 hashing and RSA public/private key pairs. All user and TSF private RSA keys accessed by the TOE are stored encrypted in the IT environment using triple-DES (FDP_ACF_CIMC.2 and FMT_MTD_CIMC.4). The TOE is configured so that SSL connections are restricted to use of the following crypto algorithms and parameters: triple-DES for encryption, SHA-1 for hashing, and RSA for key exchange and authentication. Furthermore, only SSL sessions using the TLS version 1.0 protocol are allowed which ensures use of the SHA-1 as the effective hashing algorithm. Audit logs are signed using a SHA-1 hash and the TOE's RSA private key (FAU_STG.1). The RSA key length in all cases is 1024 bits. For triple-DES the key length is 168 bits.

7.4 Vulnerability Analysis

The vendor searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of Tumbleweed VA were found, although some vulnerabilities related to the previous versions were discovered. The following public sources were searched using the keyword "Validation Authority" to find known TOE vulnerabilities:

- Carnegie Mellon CERT Coordination Center (www.cert.org)
- CERIAS Cassandra (cassandra.cerias.purdue.edu)
- Common Vulnerabilities and Exposures (www.cve.mitre.org)
- ICAT Metabase (icat.nist.gov)
- SecurityFocus Vulnerability Database (www.securityfocus.com)
- SysAdmin, Audit, Network, Security Institute (www.sans.org)

The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

8 Evaluated Configuration

The evaluated version of the Tumbleweed VA product is version 4.8 Hot Fix 3 (Build 388)

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon the CC, Version 2.2 [CCV2.2]; and CEM, Version 2.2 [CEMV2.2].

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 assurance component. For Fail or Inconclusive work unit verdicts, the

Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The evaluation determined that the product is both **Common Criteria Part 2 extended and Part 3 conformant**, and meets the assurance requirements of EAL 3. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.3	Authorisation Controls
ACM_SCP.1	TOE CM coverage
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.2	Security enforcing high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ALC_DVS.1	Identification of Security Measures
ATE_COV.2	Analysis of Coverage
ATE_DPT.1	Testing: High-level Design
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_MSU.1	Examination of Guidance
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

The Validation Team agreed with the conclusion of the SAIC CCTL Evaluation Team, and recommended to CCEVS Management that an EAL3 certificate rating be issued for Tumbleweed VA.

10 Validator Comments/Recommendations

The Tumbleweed VA product is bundled with 2 significant third party components that are not directly maintained by Tumbleweed. Publicly available patches to or newer versions of these components that might mitigate obvious vulnerabilities cannot be installed independently by the end-users of Tumbleweed VA. Tumbleweed should be contacted to obtain security critical patches related to these components:

- OpenSSL, version 0.9.7e
- Apache Web server, version 1.3.33

For the TOE to satisfy objectives derived from the CIMC PP, the IT environment must include a FIPS 140-1 validated crypto module which implements the following FIPS approved algorithms: DES and triple-DES (FIPS 46-3), RSA (FIPS 186-2) , and SHA-1 (FIPS 180-2). Tumbleweed's "ValiCert Security Module" (FIPS 140-1 certificate number 288), which is the default crypto module, was used for testing. While the required cryptographic algorithms are listed on its certificate, the FIPS evaluation only considered the Windows and Solaris configurations. As a result, the "ValiCert Security Module" cannot be considered to be FIPS 140-1 validated on a Linux platform. While Tumbleweed has stated its intention to add a Linux-based platform to the "ValiCert Security Module" FIPS 140 series evaluations in the future, currently no alternative FIPS 140-1 validated crypto modules have been identified for the Linux platform that implements all of the required algorithms.

11 Security Target

The Security Target for Tumbleweed VA is contained within the document *Tumbleweed ValiCert Validation Authority Security Target Version 1.0,* dated April, 2006. [ST]. The ST is compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of the CC [CCV2.1].

12 Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CA	Certificate Authority
CC	Common Criteria for Information Technology Security
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CIMC	Certificate Issuing and Management Components
CRL	Certificate Revocation List
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification and Authentication
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OCSP	Online Certificate validation Protocol
PP	Protection Profile
SFR	Security Function Requirement
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
VA	Validation Authority

13 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).

- NIST's Cryptographic Module Validation Program: (http://csrc.nist.gov/cryptval/)

- SAIC CCTL, (http://www.saic.com).

- Tumbleweed Corporation (http://www.tumbleweed.com).

CCEVS Documents

[CCV2.2] *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004.

[CEMV2.2] *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, August 2004.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[ST] *Tumbleweed ValiCert Validation Authority Security Target Version 1.0,* April 3, 2006