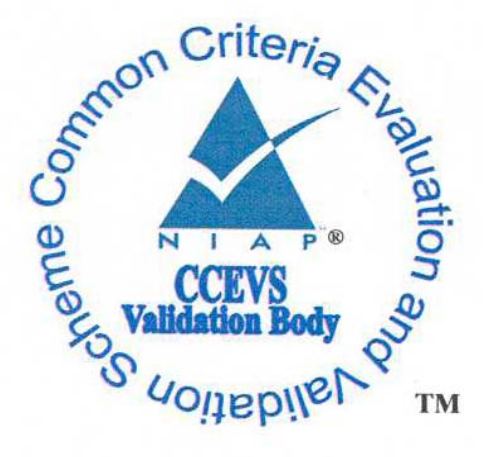
National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme
Validation Report

Los Altos Technologies
UniShred Pro® Version 3.3.2

Report Number: CCEVS-VR-06-0039
Dated: 22 November 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 Suite 6740
Fort George Meade, MD 20755-6740

Table of Contents

List of Figures

List of Tables

1 Executive Summary

The evaluation of the Los Altos Technologies UniShred Pro® Version 3.2.2 (hereafter referenced as the UniShred Pro®) was performed by the ARCA Common Criteria Testing Laboratory in the United States and was completed on 29 September 2006. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, version 2.2, Evaluation Assurance Level 2, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Part 2, Version 2.2.

The ARCA Common Criteria Testing Laboratory is an approved National Information Assurance Partnership (NIAP) Common Criteria Testing Laboratory (CCTL). The CCTL concluded that the Common Criteria assurance requirements for Evaluation Assurance Level 2 (EAL2) have been met and that the conclusions in its Evaluation Technical Report are consistent with the evidence produced.

This Validation Report is not an endorsement of the UniShred Pro®) by any agency of the US Government and no warranty of the product is either expressed or implied.

1.1 Los Altos Technologies UniShred Pro® Functionality

The Los Altos Technologies UniShred Pro® Version 3.3.2 is a software utility that renders unreadable the data previously contained on electronic storage media by overwriting the data with one or more specified patterns. While a user may have deleted or overwritten a file, directory, or disk partition, the original data can be easily recovered if new data are not written to all of the same area that the original data used.

The UniShred Pro® therefore eliminates the threat of compromising residual information when computers have been reassigned to different programs, departments, or people; returned at end-of-lease; or readied for disposal or donation.

The UniShred Pro® operates on several UNIX operating systems (AIX, HPUX, IRIX, Linux, and Solaris) and platforms (Sparc and X86). Table 2-1 in Section 2 identifies the UNIX operating systems and the types of storage media on which the UniShred Pro® operates.

The UniShred Pro has three major functions:

- Overwrite: Securely overwrite all existing information residing on an entire disk or on a partition or range of blocks and notify the user of any errors that could prevent the complete destruction of the data.

- Verify: Verify whether the overwriting of the media or portion(s) thereof was successful.

- Report: Provide on-screen reports of the progress of the overwrite and verify functions so that errors can be viewed and addressed. The reports can be saved to operating-system files.

1.2 Evaluation Details

Table 1-1 provides the required evaluation identification details.

Table 1-1. Evaluation Details

Item	Identification
Evaluation Scheme	US Common Criteria Evaluation and Validation Scheme (CCEVS)
Target of Evaluation	Los Altos Technologies UniShred Pro® Version 3.3.2
EAL	EAL2
Protection Profile	None
Security Target	Los Altos Technologies UniShred Pro® Version 3.3.2 Security Target, Version 2.4, 25 October 2006
Developer	Los Altos Technologies 111 Corning Road, Suite 100 Cary, North Carolina 27511-9241
Evaluators	Rick West and Ken Dill ARCA CCTL 45901 Nokes Boulevard Sterling, VA 20166
Validator	Elizabeth A. Foreman, The MITRE Corporation, McLean, VA
Dates of Evaluation	27 June 2005 to 29 September 2006
Conformance Result	Part 2 extended, Part 3 conformant, and EAL2 conformant
Common Criteria (CC) Version	CC, version 2.2, January 2004, and all applicable International Interpretations thereto effective on 27 June 2005
Common Evaluation Methodology (CEM) Version	CEM [Part 1, Introduction and General Model, Version 0.6, January 1997, and Part 2, Evaluation Methodology, Version 2.2, January 2004] and all applicable International Interpretations thereto effective on 27 June 2005
Evaluation Technical Report	
Key Words	

1.3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM effective on 27 June 2005 (the official starting date of the evaluation). The Validator determined that the Evaluation Team correctly applied the CCIMB interpretations listed in Table 1.2.

Table 1-2. CCIMB Interpretations Applied to the Evaluation

Interp #	Interpretation Title
003	Unique Identification of Configuration Items in the Configuration List
008	Augmented and Conformant Overlap
009	Definition of Counter
016	Objective for ADO_DEL
027	Events and Actions
031	Obvious Vulnerabilities

Interp #	Interpretation Title
032	Strength of Function Analysis in ASE_TSS
037	ACM on Product or TOE?
043	Meaning of "Clearly Stated" in APE/ASE_OBJ.1
049	Threats Met by Environment
051	Use of Documentation Without C & P Elements
058	Confusion Over Refinement
064	Apparent Higher Standard for Explicitly Stated Requirements
067	Application Notes Missing
075	Duplicate Informative Text for Different Work Units
084	Aspects of Objectives in TOE and Environment
085	SOF claims Additional to the Overall Claim
086	Role of Sponsor
098	Limitation of Refinement
116	Indistinguishable Work Units for ADO_DEL
127	[ASE_TSS.1-6]Work Unit Not at the Right Place
128	Coverage of the Delivery Procedures
138	Iteration and Narrowing of Scope
140	Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
146	C&P Elements Include Characteristics
150	A Completely Evaluated ST is Not Required When TOE Evaluation Starts
192	Sequencing of Sub-activities
202	Selecting One or More Items in a Selection Operation and Using "None" in an Assignment
222	Meaning and Use of "Normative" and "Informative"
243	Must Test Setup And Cleanup Code Run Unprivileged?
254	Applicability of ISO/IEC Standards

The Evaluation Team also complied with the CCEVS Precedents identified in Table 1.3.

Table 1-3. CCEVS Precedents Applied to the Evaluation

Precedent	Precedent Title
0008	When Should Monitoring of the Public Domain for New 'Obvious Vulnerabilities' Cease? (23 August 2004)
0056	Exhaustiveness of ATE_IND Testing (23 August 2004)
0058	EAL2 Testing Requirements (23 August 2004)
0059	How Much Testing is Required at EAL2? (23 August 2004)
0062	What Must Be Tested for a [TOE] Running on Multiple Platforms? (23 August 2004)
0084	Evaluation of TOE Claiming Compatibility With Multiple IT Environments (23 August 2004)
0086	What SOF claim is Appropriate When There are No Probabilistic or Permutational Mechanisms? (1 December 2005)
0104	Testing All Claimed Platforms (23 August 2004)
0106	Situations Where AGD_USR May be Vacuously Satisfied (23 August 2004)

2. Identification of the TOE

The TOE consists of the UniShred Pro® software application and its guidance information.

The hardware and UNIX operating systems on which the TOE is installed are not considered part of the TOE. However, the UniShred Pro® depends on the operating system to do the following:

- Ensure that the user of the UniShred Pro® has UID 0 (i.e., the user is an administrator with the root privilege).
- Correctly retrieve and release the media that are being overwritten or verified.
- Provide a reliable date and time for the UniShred Pro®'s audit records.
- Control access to the UniShred Pro® software, the electronic media targeted for overwriting or verification, the configuration file, and any audit reports saved in operating system files.

Table 2-1 identifies the UNIX operating system variants and types of disk drives or media on which the UniShred Pro® operates (see the List of Acronyms for definitions of the media types).

Table 2-1. UniShred Pro Version 3.3.2 Supported OS/Media Combinations

Operating System (OS)	Media Types
AIX 4.X or 5.X	SCSI or SSA drive
HPUX 10 or 11	SCSI drive
IRIX 6.5	SCSI drive
Linux with kernels 2.2, 2.4, or 2.6 installed on Sparc or X86 platforms	SCSI, IDE (aka ATA), SATA, flash, solid state, SAN segments/slices, USB, Firewire, Fiber channel drives, SSA
Any of Solaris 2.3 - 10 on Sparc platform	SCSI drive, IDE (aka ATA) drive (as supported by Sun)
Any of Solaris 8-10 on X86 platform	SCSI drive

The Linux version of the TOE can be provided on a CD-ROM that includes a stripped-down version of Linux by which the TOE can be booted and executed directly from that CD-ROM. This mode of operation is not provided for the other operating systems listed in Table 2.1.

Figure 2-1 identifies the four media configurations in which the TOE can be operated:

- Configuration 1: UniShred Pro® overwrites an entire hard disk or other electronic media while running the application from separate media such as RAM, CD-ROM, or another hard disk.

- Configuration 2: UniShred Pro® overwrites a portion of a hard disk or other electronic media on an operating system different from the operating system on which the TOE is running.

- Configuration 3: UniShred Pro® overwrites the same (entire) disk upon which it resides. This configuration is only supported in the Solaris, IRIX, and HPUX operating system versions or kernels listed in Table 2.1.

- Configuration 4: UniShred Pro® overwrites a target area that overlaps the operating system but does not erase the entire disk or electronic media.

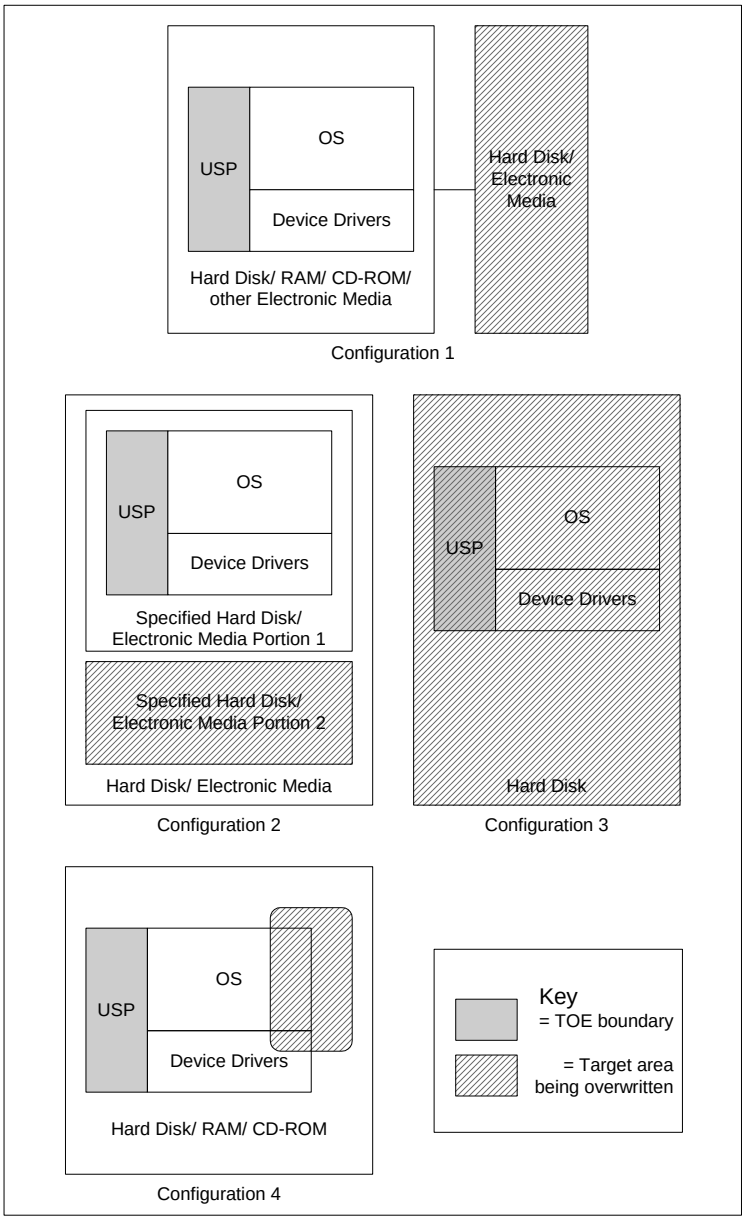


Figure 2-1. UniShred Pro® Version 3.3.2 Supported Media Configurations

3. Security Policy

The UniShred Pro® provides the following security functions:

- Overwriting of electronic media or specified portions thereof
- Verification of the overwriting operation
- Auditing the overwrite and verify operations

In addition, the UniShred Pro® verifies that the user who invokes these security functions is a UNIX root user (Section 3.4).

3.1 Overwriting Electronic Media or Portions Thereof

The UniShred Pro®'s primary function is to overwrite sensitive electronic media. The overwrite function executes read, write, and read/write passes over all of the blocks of a device based on the pattern and number of overwrite passes specified by the user in either the configuration file or within the command syntax of his request. The user may specify a custom overwriting pattern or choose from 17 pre-defined patterns for which the number of passes is predefined. If the user does not specify a pattern, an error is returned.

The target of the overwrite operation may be an entire disk (or other electronic media), a partition, or a range of blocks. For a complete overwrite, the UniShred Pro® overwrites all addressable blocks on the disk; this includes all active data files, deleted data files, file directories, disk allocation tables, the boot area, the disk label, and unallocated disk space. While specifying a range is available for all disks, the partition specification is available only on disks with a recognized partition table.

For SCSI disks, if the disk is capable of address translation and there are new defects on the disk, the defective areas are made accessible and the defective blocks are overwritten with the same set of patterns as used for the full disk. Once the latter activity is complete, the defective areas are again made inaccessible and the full disk is again overwritten.

The default mode for the UniShred Pro® program is to overwrite defects but the user can override this default.

Before the overwrite operation is actually started, the UniShred Pro® presents disk information to the user and requests that the user verify that the operation is desired. During the overwrite operation, the UniShred Pro® displays progress statements to the user.[1]

3.2 Verifying the Overwrite Operation

The verify operation is used to fully verify that the complete disk or portion thereof that the user specified in the overwrite operation was actually overwritten.

---

[1] UniShred Pro® Version 3.3 Disk Overwriting Software User's Manual, Document No: USP-DOC-01-07, April 3, 2006, Sections 1.3 and 3.5.6.

The UniShred Pro® checks the contents of the first set of blocks on the device or specified portion thereof to determine the overwrite pattern. Then it checks each of the remaining blocks of the device, range of blocks, or partition to determine whether the blocks have the correct value for the identified pattern. If all relevant blocks contain the pattern, an appropriate message is displayed. If any of the blocks on the device or specified portion thereof do not contain the appropriate pattern, an error is indicated and the blocks are listed on the screen.

In those cases in which both the entire disk and the operating system have been overwritten, which is supported on the HPUX, IRIX, and Solaris operating systems (see Media Configuration 3 in Section 2), the verify operation will require connecting the media to another HPUX, IRIX, or Solaris system in which the UniShred Pro® has also been installed and running the verify operation options against the media that were overwritten.

3.3 Auditing the Overwrite and Verify Operations

While the UniShred Pro® is performing the overwrite and verify operations, it displays the progress of those operations so that errors that occur can be brought to the attention of the user and promptly addressed. These displays comprise the audit report which the user has the option of saving (as indicated in the configuration file or in the command syntax) to an operating system file on a drive or specified portion thereof other than the one being overwritten or verified. If the self-overwriting option (see Media Configuration 3 in Section 2) is invoked, no report file is written to an operating system file and none can be specified.

The report can be saved to a newly-named file or to an existing file. In the latter case, the same report file name can be specified for multiple reports because each new report will be appended to the file. If no output file is specified, the report is saved to the default file name and directory location.

3.4 Verifying UNIX Root User

The TOE depends on the underlying operating system to identify and authenticate users and to control access to the UniShred Pro® executables, configuration file, and saved audit reports. However, before the UniShred Pro® executes the operations that the user requests, it invokes a system call to the underlying operating system to ensure that the user who is requesting a TOE operation has UNIX root privileges with which to access the root account – the User Identification (UID) of which is 0 (zero). If the user's UID is not 0, the UniShred Pro® returns an error and does not execute.

4. Assumptions and Clarification of Scope

This section describes the security aspects of the environment in which the UniShred Pro® is expected to operate.

4.1 Usage Assumptions

The assumptions listed below are not addressed by any IT requirements but instead rely on the procedural or administrative measures applies to the operating environment.

A.ADMIN_CRED	The Administrator (UID 0) of the TOE is assumed not to disclose his or her authentication credentials.
A.LOCATE	The processing platform on which the TOE resides is assumed to be located within a facility that provides controlled access so that unauthorized access to the electronic media is prevented.
A.NOEVIL	The Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PHYSICAL	Any individual with physical access to the processing platform on which the TOE resides is assumed to have full access to the data on the platform.

4.2 Environmental Threats

The TOE addresses the threats described below.

T.DATA_ACCESS	An unauthorized person attempts to access sensitive data stored on electronic media that have been redeployed, transferred out of the organization's control, or discarded.
T.DATA_DELETED	An unauthorized person attempts to recover sensitive data remaining after the data have been deleted from electronic media that have been redeployed, transferred out of the organization's control, or discarded.
T.DATA_FORMAT	An unauthorized person attempts to recover sensitive data remaining after the formatting of electronic media that have been redeployed, transferred out of the organization's control, or discarded.
T.INCOMP_OVER	An overwrite operation is incompletely performed rendering data still recoverable and the user performing the overwrite operation has no knowledge of the operation being performed incompletely.

4.3 Other

The organization that uses the TOE is expected to define an appropriate policy for the identification, disposal, sanitization, and verification of sanitization of electronic media [P.DISPOSAL].

5. Architectural Information

The UniShred Pro® has ten subsystems – four of which enforce or support the TOE's security functions:

1. USP 3.2.2: This subsystem performs all of the controlling operations for the TOE. However, before doing so, it invokes a system call to the underlying operating system to verify that the user executing the program has UID 0; if the user does not have UID 0, the subsystem returns an error and prevents TOE execution. Otherwise, this subsystem receives the commands entered by the administrator, parses them, and sends the information to the appropriate subsystem for further processing.

2. Scrub Disk: This subsystem performs the write, read/write, and read passes over all the specified blocks of a device based on the parameters received from the USP 3.3.2 subsystem regarding the specified pattern to use, how to handle errors, whether to preserve the disk label, and what portion of the device to overwrite. This subsystem also generates an on-screen display of the progress of the overwrite function – including, for example, the start and finish times of the overwrite, the properties of the device that is being overwritten, the total number of blocks being overwritten, the patterns being used, any errors encountered, and where the results are being saved.

3. Verify Overwrite: This subsystem reads all of the specified blocks of the device to verify that a specified pattern has been placed on the device and that no residual information can be accessed. This subsystem also generates an on-screen display of the progress of the verify function.

4. Error Processing: This subsystem provides the error processing capability for the TOE. It receives the details of any errors found, receives administrator inputs on whether to retry, abort, or proceed, and relays that information to the Scrub Disk and Verify Overwrite subsystems, as appropriate.

Table 5-1 lists each of the 10 subsystems and indicates whether the subsystem enforces, supports, or has no security relevance to the operation of the three TOE Security Functions (TSF).

Table 5-1. Mapping of UniShred Pro® Subsystems to TOE Security Functions

Subsystem	TOE Security Functions		
	Overwrite	**Verify**	**Audit/Report**
USP 3.3.2	TSF-supporting	TSF-supporting	TSF-supporting
Scrub Disk	TSF-enforcing	No relevance	TSF-enforcing
Verify Overwrite	No relevance	TSF-enforcing	TSF-enforcing
Error Processing	TSF-supporting	TSF-supporting	No relevance
Help	No relevance	No relevance	No relevance
List Defects	No relevance	No relevance	No relevance
List Devices	No relevance	No relevance	No relevance
Show Device	No relevance	No relevance	No relevance

Information			
Show Disk Blocks	No relevance	No relevance	No relevance
Show Partition Data	No relevance	No relevance	No relevance

Figure 5-1 shows the subsystems' interactions.

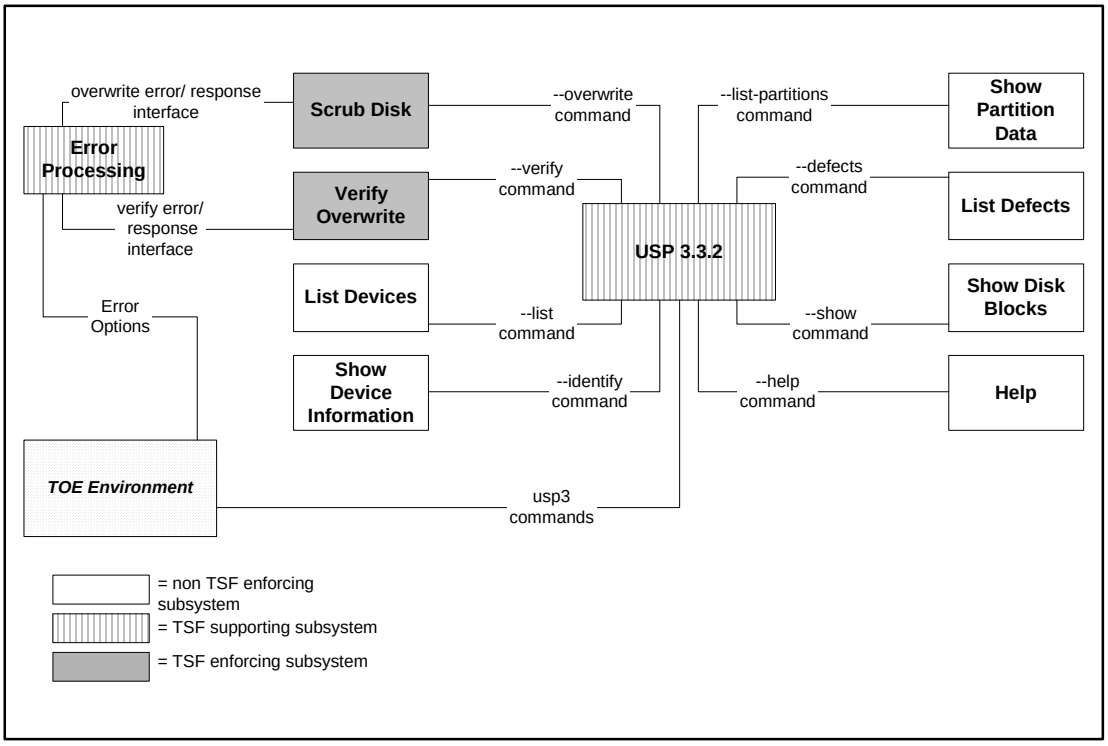


Figure 5-1. Interaction of UniShred Pro® Subsystems

6. Documentation

Los Altos Technologies provides the following documentation with the Los Altos Technologies UniShred Pro® Version 3.3.2 to consumers – depending on the particular UNIX operating system variant and platform:

- For all UNIX operating systems:
  - *UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual*, Document No: USP-DOC-01-07, April 3, 2006
- For AIX 4.X or 5.X operating systems:
  - *UniShred Pro® Version 3.3.2 Installation Guide for AIX Operating Systems*, Document No: USP3-DOC-17-05, April 3, 2006
- For HP-UX Release 10 or 11 operating systems:
  - *UniShred Pro® Version 3.3.2 Installation Guide for HP-UX Release 10 and 11 Operating Systems*, Document No: USP3-DOC-09-07, April 3, 2006
- For IRIX Version 6.5 operating systems:
  - *UniShred Pro® Version 3.3.2 Installation Guide for IRIX Version 6.5 Operating System*, Document No: USP3-DOC-06-07, April 3, 2006
- For Linux operating systems with kernels 2.2, 2.4, or 2.6 installed on X86 platforms:
  - *UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems*, Document No: USP3-DOC-18-05, April 3, 2006
- For Linux operating systems with kernels 2.2, 2.4, or 2.6 installed on Sparc™ platforms:
  - *UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems on Sparc™ Platforms*, Document No: USP3-DOC-19-01, April 3, 2006
- For Solaris 2.3 to 10 operating systems installed on Sparc™ platforms:
  - *UniShred Pro® Version 3.3.2 Installation Guide for Solaris Operating Systems Sparc Platform Edition*, Document No: USP3-DOC-02-08, April 3, 2006
- For Solaris 8 to 10 operating systems installed on X86 platforms:
  - *UniShred Pro® Version 3.3.2 Installation Guide for Solaris Operating Systems X86 Platform Edition*, Document No: USP3-DOC-16--03, April 3, 2006

7. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The developer provided test plans, procedures, test results, and a test coverage analysis. The Plan identified the test configurations and the specific test operating systems and hardware platforms that were used for the tests.

The Evaluation Team determined that the developer's approach and effort were appropriate for this EAL2 evaluation.

The test environment resembled the standard Government or corporate environment in which the TOE would be used. Neither the TOE nor the TOE environment required or used a networked system. All test execution was local to the operating system and hardware platform on which the TOE was installed. The TOE's command-line interface, usp3, and applicable parameters were used to conduct the tests.

The developer's test team developed a perl script, `uspverify.prl`, that it chose to run on the HPUX platform during testing to provide an independent verification (that is, one not using the TOE's verify function) that the TOE had overwritten the intended portion(s) of the disk that were the objects of the overwrite operation. The script can actually be used with any of the UNIX variants that accept perl scripts.

Table 7-1 summarizes the hardware, software, and media configurations utilized for testing. There were a total of seven testing scenarios, which covered three of the four media configurations (see Figure 2-1) and five of the six UNIX variants on which the TOE may operate.

The developer did the following for each scenario:

- Installed the TOE in accordance with the installation instructions applicable to the UNIX operating system on which the TOE was being tested
- Ensured that each of the devices or media to be overwritten contained data prior to testing
- Logged on to the UNIX operating system as root (UID 0)
- Executed all three TOE security functions:
  - Executed the overwrite function on the target media or portions thereof
  - Verified that the overwrite function was successful with the verify function and/or the perl script
  - Verified that the audit reports generated for the overwrite and verify functions were generated and contained correct information

All developer tests were successful; actual results were consistent with expected results.

Table 7-1. Developer Testing Scenarios and Their Configurations

SCENARIO NAME	USAGE SUMMARY	APPLICABLE MEDIA CONFIG	MEDIA TYPE	UNIX OS	SYSTEM DESC
Scenario 1	Wipe a range of a secondary media from main media	Configuration 2	SATA	Fedora v3 (w/ 2.6.3 kernel)	Intel-based PC Type: SATA 512 MB memory 120 GB disk space Secondary SATS
Scenario 2	Wipe a secondary media from CD-ROM	Configuration 1	Flash Drive	Linux kernel v2.6.5	Intel-based PC Type: IDE 512 MB memory 120 GB disk space 256 MB removable flash drive, USB port on system
Scenario 3	Wipe primary media (self-destruct)	Configuration 3	IDE	Solaris v8 (for Sparc)	Sun Ultra 5 Type: IDE 128 MB memory 20.576 GB disk space 3.5” floppy drive, 3.5” floppy disk
Scenario 4	Specify media blocks for wipe	Configuration 2	SSA	AIX v4.3.3	IBM PowerPC Type: SSA 32 MB memory 18.223 MB disk space External SSA Array
Scenario 5	Specify media partition for wipe	Configuration 2	SCSI	IRIX v5.3	Silicon Graphics Type: SCSI 128 MB memory 2255 MB disk space
Scenario 6	Wipe entire secondary drive	Configuration 1	SCSI	HPUX v10.20	HP Apollo 715-50 Type: SCSI 32 MB memory 2.1 GB disk space Secondary SCSI drive
Scenario 7	Wipe a secondary media from CD-ROM	Configuration 2	IDE	Linux kernel v2.6.5	Intel-based PC Type: IDE 64 MB memory 4325 MB disk space Secondary IDE drive

7.2 Evaluation Team Independent Testing

Instead of testing a sample of the developer's tests, the Evaluation Team chose to re-run the developer's entire functional test set during its independent testing. Due to the limited number of TOE Security Functional Interfaces (TSFIs) to stimulate the TOE's three security functions, the Evaluation Team's approach was to execute as many tests as possible across as many media configurations on which the TOE can operate (see Table 2-1) using different supported hardware platforms. Although the Evaluation Team observed slight differences between the expected and actual results of its tests, it determined that they were due to the slight variances in the different hardware that they used for its tests.

The Evaluation Team then ran a set of functional tests that would augment the developer's testing and that would focus on consumers' normal and typical uses of the TOE. This strategy concentrated on media configurations 1 and 2 (Figure 2-1) and using the most popular operating systems – Solaris and Linux. In addition, the Evaluation Team chose to verify the overwrite function by utilizing operating system utilities to confirm that the previous data were unrecoverable.

Table 7-2 summarizes the hardware, software, and media configurations that the Evaluation Team employed for the tests that augmented the developer's tests. Note that Test 6 is a penetration test that is discussed in Section 7.3

Table 7-2. Evaluation Team Tests and Their Configurations

TEST NO	USAGE Summary	APPLICABLE MEDIA CONFIG	MEDIA TYPE	UNIX OS	SYSTEM DESC
1	Securely erase a range of blocks on a non-mounted (inactive) USB thumb drive	Configuration 2	IDE	Linux	Dell Latitude Csx 512 MB memory 12 GB FUJITSU primary disk 512 MB USB SanDisk thumb drive
2	Securely erase entire non-mounted (inactive) secondary disk	Configuration 1	SCSI	Solaris 2.8 default install	Sun Ultra 5 640 MB memory 9 GB FUJITSU primary disk 9 GB IBM secondary disk
3	Securely erase entire mounted (active) secondary disk, NOT including OS	Configuration 1	SCSI	Solaris 2.8 default install	Sun Ultra 5 128 MB memory 2 GB Seagate primary disk 2 GB Seagate secondary disk
4	Securely erase entire non-mounted (inactive) primary disk	Configuration 1	IDE	Red Hat Linux 8.0	Dell 256 MB memory 2 GB Seagate primary disk 2 GB Seagate secondary disk
5	Securely erase range of blocks on non-mounted secondary disk	Configuration 2	SCSI	Red Hat Linux 8	Gateway E-5200 1.2 GB memory 9 GB IBM primary disk 36 GB Quantum secondary disk 36 GB Quantum tertiary disk

TEST NO	USAGE Summary	APPLICABLE MEDIA CONFIG	MEDIA TYPE	UNIX OS	SYSTEM DESC
6	Attempt to run TOE software with non-root account	Configuration 1	SCSI	Solaris 2.8 default install	Sun Ultra 5 640 MB memory 9 GB FUJITSU primary disk 9 GB IBM secondary disk

The Evaluation Team did the following for its tests:

- Developed a test plan
- Assigned tests to hardware configurations different from the developer's assignments to verify that the tests could successfully complete on different operating systems and hardware platforms
- Installed the TOE in accordance with the installation instructions applicable to the UNIX operating system on which the TOE was being tested in accordance with the ADO_IGS.1.2E requirement to determine whether the installation, generation, and start-up procedures result in a secure configuration; all such installations succeeded and provided no issues or errors
- Ensured that each of the devices or media to be overwritten contained data prior to testing
- Ensured that partitions that needed to be unmounted for testing were unmounted
- Ensured that no test suites were running concurrently
- Ensured that no other activities that could change system configurations were performed during testing
- Executed all three TOE security functions:
  - Executed the overwrite function on the target media or portions thereof
  - Verified that the overwrite function was successful with the verify function
  - Verified that the audit reports generated for the overwrite and verify functions were generated and contained correct information
- Verified that the overwrite function was successful with operating system utilities

All Evaluation Team tests and installations were successful; actual results were consistent with expected results.

7.3 Evaluation Team Penetration Testing

Since the TOE is a non-networked system, the Evaluation Team determined that the testing of typical vulnerabilities such as denial-of-service or privilege-escalation attacks were not applicable. Therefore, the Evaluation Team performed a test (Test 6 in Table 7-2) to verify that an operating system user with a UID other than 0 would be prevented from operating the TOE. In fact, the TOE commands that the Evaluation Team entered – one to list the disks on the platform and one to overwrite a disk – both failed.

8. Evaluated Configuration

The TOE was evaluated on the operating-system, hardware, and media configurations listed in Table 8.1.

Table 8-1. Evaluated Configurations

UNIX OS	APPLICABLE MEDIA CONFIG	MEDIA TYPE	SYSTEM DESCRIPTION
AIX v4.3.3	Configuration 2	SSA	IBM PowerPC; Type: SSA; 32 MB memory; 18.223 MB disk space; External SSA Array
HPUX v10.20	Configuration 1	SCSI	HP Apollo 715-50; Type: SCSI; 32 MB memory; 2.1 GB disk space; Secondary SCSI drive
IRIX v5.3	Configuration 2	SCSI	Silicon Graphics; Type: SCSI; 128 MB memory; 2255 MB disk space
Linux	Configuration 1	IDE	Dell Latitude Csx; 512 MB memory; 12 GB FUJITSU primary disk; 512 MB USB SanDisk thumb drive
Linux kernel v2.6.5	Configuration 1	Flash Drive	Intel-based PC; Type: IDE; 512 MB memory; 120 GB disk space; 256 MB removable flash drive, USB port on system
Linux kernel v2.6.5	Configuration 2	IDE	Intel-based PC; Type: IDE; 64 MB memory; 4325 MB disk space; Secondary IDE drive
Fedora v3 (w/ 2.6.3 kernel)	Configuration 2	SATA	Intel-based PC; Type: SATA; 512 MB memory; 120 GB disk space; Secondary SATS
Red Hat Linux 8.0	Configuration 1	IDE	Dell; 256 MB memory; 2 GB Seagate primary disk; 2 GB Seagate secondary disk
Red Hat Linux 8	Configuration 2	SCSI	Gateway E-5200; 1.2 GB memory; 9 GB IBM primary disk; 36 GB Quantum secondary disk; 36 GB Quantum tertiary disk
Solaris 2.8 default install	Configuration 1	SCSI	Sun Ultra 5; 640 MB memory; 9 GB FUJITSU primary disk;; 9 GB IBM secondary disk
Solaris 2.8 default install	Configuration 1	SCSI	Sun Ultra 5; 128 MB memory; 2 GB Seagate primary disk; 2 GB Seagate secondary disk
Solaris 2.8 default install	Configuration 1	SCSI	Sun Ultra 5; 640 MB memory; 9 GB FUJITSU primary disk; 9 GB IBM secondary disk
Solaris v8 (for Sparc)	Configuration 3	IDE	Sun Ultra 5; Type: IDE; 128 MB memory; 20.576 GB disk space; 3.5” floppy drive, 3.5” floppy disk

9. Results of the Evaluation

The Los Altos Technologies UniShred Pro® satisfies all of the EAL2 assurance requirements against which it was evaluated. The EAL2 assurance requirements include the following:

Table 9-1. CC EAL 2 Security Assurance Requirements

EAL2 Component	EAL2 Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Information functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Information correspondence demonstration
AGD_ADM.1	Administer guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

The Security Target provides a detailed description of how the Los Altos Technologies UniShred Pro® meets each of the listed components.

10. Validation Comments/Recommendations

10.1 Validation Recommendation

The Validator determined that the evaluation and all of its activities were performed in accordance with the CC, the CEM and CCEVS practices.

The Validator agrees that the CCTL presented appropriate rationales to support the Evaluation Results presented in Section 4 of the ETR and the Conclusions and Recommendations presented in Section 7 of the ETR.

The Validator, therefore, concludes that the evaluation and the Pass results for the TOE identified below are complete and correct:

Los Altos Technologies UniShred Pro® Version 3.3.2

10.2 Validation Comments

This section provides validator comments regarding the usage of the UniShred Pro®.

10.2.1 Consumer and Environment Responsibilities

Consumers of the product are expected to do the following:

- Place the processing platform on which the Los Altos Technologies UniShred Pro® Version 3.3.2 is installed in a controlled access facility that mitigates unauthorized, physical access to that platform and to the electronic media stored therein.

- Protect other electronic media (e.g., thumb drive, CD ROM) on which sensitive information is stored from unauthorized access.

- Ensure that system operating requirements (e.g., acceptable UNIX variant; power, disk space, and RAM requirements) and installation requirements (e.g., applicable floppy, tape, or CD drive) are met.

- Define and follow a policy and procedures that meet the applicable regulations or requirements for disposing and sanitizing the consumer's electronic media and for verifying the sanitization effort.

- Ensure that administrators have been trained on the security policies and practices of the environment in which the product will operate.

- Ensure that administrators are knowledgeable of the UNIX commands required for the installation and operation of the product.

- Allow only trustworthy administrators with root (UID 0) privileges to execute the product and to access the configuration file and any saved audit reports (generated by the overwrite and verify functions) that have been stored on the processing platform.

Consumers should be aware that the Los Altos Technologies UniShred Pro® Version 3.3.2 is a software application that relies on the underlying UNIX operating system (see Table 2-1) to do the following:

- Identify and authenticate users.
- Control access to the product's executables, configuration file, and saved audit reports.
- Perform the read and write operations that the product's overwrite and verify functions request from the file system.
- Retrieve the disk information that the product provides in audit reports and in response to the *list* and *show* commands (see Table 5-1).
- Perform any available operating system auditing of the execution of the product.

10.2.2 Product Conformance With Government Regulations

Section 2.2, Architecture Description, in the *Los Altos Technologies UniShred Pro® Version 3.3.2 Security Target*, states, "the overwrite methods provided conform to various United States Government regulations and requirements, including AFSSI 5020, AR 380-19, DoD 5200.28-M, DoD 5220.22-M, NAVSOP-5239-26, NCSC-TG-025, OPNAVINST 5239.1A CH-1, and OPNAVINST 5510.1H CH-5."

Appendix D, Government Regulations, of the *Los Altos UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual*, dated 3 April 2006, provides the publication dates and titles of some of these regulations. Table 10-1 reports those dates and titles and the results of the Validator's research of the regulations in response to a Senior Validator's questions regarding whether overwriting disks was an acceptable DoD data purging method. Note that the product's conformance to the listed US Government regulations and requirements was not evaluated during this CC evaluation.

Table 10-1. Policies/Regulations Cited in ST

Policy/Regulation	Date	Title	Status
AFSSI 5020	15 April 2003	Remanence Security	Document not retrievable
AR 25-2	14 November 2003	Information Assurance	Supersedes AR 380-19
AR 380-19	1 August 1990	Information Systems Security	New version 27 Feb 1998 Superseded by AR-25-2
DoD 5200.28-M	January 1973	ADP Security Manual	Superseded and cancelled by DODD 8500.1
DoD 5220.22-M	January 1995	National Industrial Security Program Operating Manual	Reissued and cancelled by DoD 5220.22-M, 28 Feb 2006

Policy/Regulation	Date	Title	Status
		(NISPOM)	
NAVSOP-5239-26	Not listed in the Appendix	Not listed in the Appendix	Document reference should be NAVSO P-5239-26; date is September 1993; title is Remanence Security Guidebook
NCSC-TG-025	September 1991	A Guide to Understanding Data Remanence in Automated Information Systems	No change (part of "Rainbow Series" guidance)
OPNAVINST 5239.1A CH-1	1 April 1985	Department of the Navy Automatic Data Processing Security Program	Document not retrievable
OPNAVINST 5510.1H CH-5	20 January 1995	Department of the Navy Information and Personnel Security Program Regulation	Document not retrievable

The Appendix also presents two additional regulations (which were included after the Validator's research) excluded from the ST:

Policy/Regulation	Date	Title	Status
DoN IA Pub-5239-26	May 2000	Information Assurance Remanence Security Publication	Not examined
IA BBP 04-PE-O-0004	24 January 2004	Reuse of Army Computer Hard Drives Version 1.0	Not examined

The Validator observed the following:

- Except for NAVSO P-5239-26, which mentioned "SCSI," the sections of the regulations that the Validator examined did not explicitly refer to the media types identified in Section 2.2 of the Security Target.

- Some of the examined document sections were vague about what constitutes "properly destroyed" or "properly disposed" media or where "special handling" was described.

- The examined sections that mention electronic media types use terms (e.g., coercivity, bubble memory, Bernoulli) different from those identified in the Security Target (e.g., SCSI, SATA, IDE) and it is unclear whether and how such terms correspond to the disk technologies that UniShred Pro® supports.

- Most of the examined sections refer readers to various authorities for additional (or more situation-specific) guidance.

Therefore, the Validator recommends that consumers follow Los Altos Technologies' advice in Footnote 2 of the Security Target and in Appendix D of the *Los Altos UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual*:

Several military and government agencies have published guidelines and regulations pertaining to data removal. Los Altos Technologies recommends that one research the specific requirements. The Designated Approval Authority (DAA) can say what regulations apply to a given situation. Most of the cognizant government agencies will provide copies of relevant regulations at little or no cost.

11. Security Target

The Security Target is entitled, *Los Altos Technologies UniShred Pro® Version 3.3.2 Security Target*, Version 2.4, 25 October 2006.

12. List of Acronyms

AFSSI	Air Force System Security Instruction
aka	also known as
AR	Army Regulation
ATA	Advanced Technology Attachment
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratory
CD-ROM	Compact Disk – Read Only Memory
CEM	Common Evaluation Methodology
DAA	Designated Approving Authority
DoD	Department of Defense
DON	Department of the Navy
EAL	Evaluation assurance level
ETR	Evaluation Technical Report
GB	Gigabyte(s)
IA BBP	Information Assurance Best Business Practice(s)
IDE	Intelligent Drive Electronics or Integrated Drive Electronics
MB	Megabyte(s)
NAVSO P	Navy Staff Office Publication
NCSC	National Computer Security Center
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	OPNAV Instruction
PC	Personal Computer
RAM	Random Access memory
SAN	Storage Are Network
SATA	Serial ATA
SCSI	Small Computer System Interface
SSA	Serial Storage Architecture
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
UID	User Identification
USB	Universal Serial Bus
USP	UniShred Pro®

13. Bibliography

The following documents were used in compiling this Validation Report:

- CCEVS Precedent Database, http://niap.bahialab.com/cc-scheme/PD/index.html

- *CCEVS Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, February 2002, Appendix D.6, Validation Report (VR) Format

- CCIMB Interpretations Applicable to CC v2.1 and CC v2.2, http://www.commoncriteriaportal.org/public/expert/index.php?menu=4

- Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004:
  - Part 1: Introduction and General Model
  - Part 2: Security Functional Requirements
  - Part 3: Security Assurance Requirements

- Common Evaluation Methodology for Information Technology Security:
  - Part 1: Introduction and General Model, Version 0.6, 11 January 1997
  - Part 2: Evaluation Methodology, Version 2.2, January 2004

- Los Altos Technologies UniShred Pro® documentation:
  - Los Altos Technologies UniShred Pro Version 3.3.2 Security Target, Version 2.4, 25 October 2006.
  - UniShred Pro® Version 3.3.2 *Disk Overwriting Software User's Manual*, Document No: USP-DOC-01-06, 2 September 2002.
  - UniShred Pro® Version 3.3.2 *Disk Overwriting Software User's Manual*, Document No: USP-DOC-01-07, 3 April 2006.
  - *ATE_COV.1; ATE_FUN.1; ATE_IND.2: Evaluation Technical Report for Los Altos Technologies UniShred Pro Version 3.3.2*, Version 0.3, 28 September 2006.
  - *Los Altos Technologies UniShred Pro® Version 3.3.2 Team Test Actual Results*, Final, 28 August 2006.

- VID10105-0031-MR, [Validator] Review of the 8 Government Regulations Cited in the ST, Section 2.2, 18 August 2006.