Los Altos Technologies

Los Altos Technologies
UniShred Pro® Version 3.3.2
Security Target

Release Date: October 25, 2006, 2006

Version: 2.4 FINAL

Prepared By:

Arca CCTL
45901 Nokes Boulevard
Sterling, VA 20166

Prepared For:

Los Altos Technologies
111 Corning Road, Suite 100
Cary, NC 27511-9241

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 Identification

TOE Identification:	Los Altos Technologies UniShred Pro® Version 3.3.2
ST Identification:	Los Altos Technologies UniShred Pro® Version 3.3.2 Security Target
ST Version:	2.4 FINAL
ST Release Date:	October 25, 2006
ST Authors:	Alicia Squires, Arca CCTL

1.2 Overview

The TOE is the Los Altos Technologies UniShred Pro® Version 3.3.2, which is a software utility that overwrites data on electronic media in order to eliminate the threat of data compromise when computers are reassigned to different programs, departments, or people; when using portable computers; when computers are returned at end-of-lease; and when computers have reached end-of-life and are being donated. Without overwriting, simple computer data-recovery programs in widespread use could read, copy, or even undelete the original files. Los Altos Technologies UniShred Pro® Version 3.3.2 will hereafter also be referred to as UniShred Pro or the TOE.

1.3 CC Conformance Claim

The TOE is Common Criteria Version 2.2 (ISO/IEC 15408:2004) Part 2 extended and Part 3 conformant at EAL2. The TOE is also compliant with all International interpretations with effective dates on or before June 27, 2005.

The TOE does not conform to any Protection Profiles.

1.4 Organization

Section	Title	Description
1	Introduction	Provides an overview of the security target.
2	TOE Description	Defines the hardware and software that make up the TOE, and the physical and logical boundaries of the TOE.
3	TOE Security Environment	Contains the threats, assumptions and organizational security policies that affect the TOE.
4	Security Objectives	Contains the security objectives the TOE is attempting to meet.
5	IT Security Requirements	Contains the functional and assurance requirements for this TOE.
6	TOE Summary Specification	A description of the security functions and assurances that this TOE provides.

7	PP Claims	Protection Profile Conformance Claims.
8	Rationale	Contains pointers to the rationales contained throughout the document.

Table 1 – ST Organization and Description

1.5 Document Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify these operations.

Assignment: **indicated with bold text**

Selection: indicated with underlined text

Refinement: ***indicated with bold text and italics***

Iteration: indicated with typical CC requirement naming followed by a lower case letter for each iteration (e.g., FMT_MSA.1a)

Explicit Requirements: indicated with a "_EXP" as part of the SFR name.

1.6 Document Terminology

This section provides a list of acronyms used within the ST

CC: Common Criteria version 2.2 (ISO/IEC 15408:2004)

EAL: Evaluation Assurance Level

SFR: Security Functional Requirement(s)

SFP: Security Function Policy

SOF: Strength Of Function

ST: Security Target

TOE: Target Of Evaluation

TSF: TOE Security Function(s)

TSP: TOE security Policy

USP UniShred Pro ®

2 TOE Description

2.1 Overview

This section describes the Target of Evaluation (TOE) in terms of the class of product, the provided security functionality (logical boundaries), and the physical TOE boundaries.

2.2 Architecture Description

Los Altos Technologies UniShred Pro ® Version 3.3.2 is a software utility that can be operated from a hard disk, CD-ROM, other electronic media, or within a system's internal memory (RAM).

A term that often arises during discussions of magnetic media sanitization is "data remanence." Data remanence is the residual magnetic or electrical representation of data that has been in some way erased or overwritten. This residual information may allow data to be reconstructed typically using laborious, time-consuming methods. This usually is a concern only to those processing classified, financial, medical, and personally identifiable information, but can also be a significant concern for unclassified but sensitive information and a company's intellectual property.

UniShred Pro provides the capabilities to securely overwrite all existing information residing on either a portion of (based on partitions or a range of blocks), or an entire electronic media for complete non-recoverable elimination of data[1]. In addition, 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.[2]

To further ensure process reliability, UniShred Pro notifies users if any errors occur that could prevent the complete destruction of data. The TOE also provides capabilities for verifying the successful completion of overwriting any portion of electronic media, as well as, provides reports on the processes for all configurations. The reports that are generated are displayed on-screen and are archived to a file for viewing or printing at a later time.

UniShred Pro supports the following operating systems:

- Linux operating systems (OS')'s with kernels 2.2, 2.4, and 2.6[3]
- AIX 4.X and 5.X
- IRIX 6.5
- Solaris 2.3 – 10 (Sparc platforms)
- Solaris 8 – 10 (X86 platforms)[4]

---

[1] The terms "erasure" and "overwrite" although they can have different implications will be used interchangeably for this TOE. The TOE actually overwrites the existing data, which results in a virtual erasure of the data.

[2] The conformance against the US Government regulations and requirements was not evaluated during this evaluation. Several military and government agencies have published guidelines and regulations pertaining to data removal that may have updated, superseded, or cancelled a regulation in this list. Los Altos Technologies recommends that one research the specific requirements.

[3] This includes both Sparc and X86 platforms.

- HPUX 10 and 11

When the customer orders the Linux version of the TOE, it can ship on a cd-rom with a stripped down version of Linux included. This allows the program to be booted from and run directly from the cd-rom. In all other modes of operation one of the operating systems listed above must be provided by the end-user to run the program.

2.3 Physical Boundaries

This section lists the software and hardware components of the product and denotes which are in the TOE and which are in the IT environment.

The TOE is the UniShred Pro software, version 3.3.2.

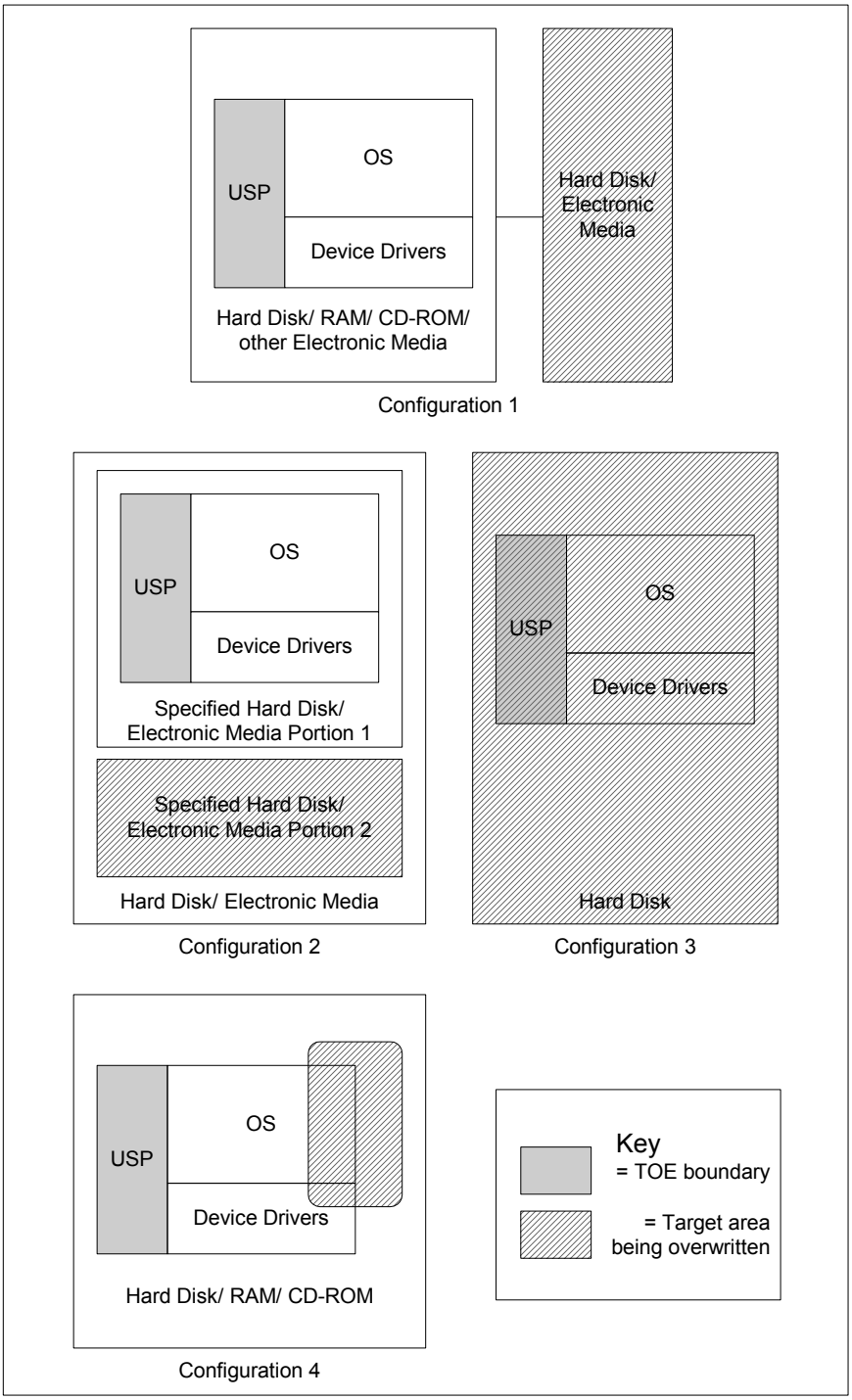
The operating systems, listed above, with which the TOE interoperates, are part of the IT environment. All underlying hardware upon which the TOE operates is not considered to be part of the TOE, but they compose the IT environment. The device drivers that are specific to the electronic media are also not part of the TOE, but they are within the IT environment.

The TOE is not a networked system and executes locally, therefore, a networking interface is not included as a physical TOE or NON-TOE component.

The following figure shows the four configurations in which the TOE can be operated. The TOE is represented in each diagram by the shaded USP box.

[4] The Solaris OS's, going forward, will be referred to as either Sparc or X86 where applicable. Neither platform is mentioned when applicable to both.

Figure 1: Physical TOE Configurations



The first configuration provides the ability for USP to overwrite an entire hard disk or other electronic media, while running the application from separate media, such as RAM, CD-ROM, or another hard disk.

The second configuration provides the ability for USP to overwrite a portion of a hard disk or other electronic media that is different than from where the OS and TOE are running.

The third configuration provides the ability for USP to overwrite the same (entire) disk , upon which USP

resides. However, this configuration is only provided within the Solaris, IRIX, and HPUX operating systems.

The fourth configuration provides the ability for USP to overwrite a target area that overlaps the OS but doesn't erase the entire disk or electronic media.

Hardware and operating system components not considered part of the TOE, yet at the minimum are required for TOE operation include one of the following combinations of operating systems and drives:

Operating System	**Media Types**
Linux OS's with kernels 2.2, 2.4, or 2.6	SCSI, IDE (aka ATA), SATA, flash, solid state, SAN segments/ slices, USB, Firewire, or Fiber channel drives, SSA
AIX 4.X or 5.X	SCSI or SSA drive
IRIX 6.5	SCSI drive
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
HPUX 10 or 11	SCSI drive

2.4 Logical Boundaries

This section outlines the boundaries of the security functionality of the TOE.

2.4.1 Overwrite

The main purpose of the TOE is to provide the overwrite function, in which the contents of the sensitive media or specified portion thereof are made unrecoverable by overwrites of the data with various data patterns.

2.4.2 Verify

The TOE is capable of fully verifying an overwrite operation, which is done essentially the same way as the final read pass in a normal overwrite. The verify function analyzes the first couple of blocks on the electronic media to determine what pattern they seem to contain. The verify function then checks each remaining block to ensure that it has the correct value for the identified pattern. If all blocks contain the pattern, then an appropriate message is printed. If there are blocks that do not contain the pattern, these blocks are listed on the screen.

2.4.3 Report Generation

The TOE displays the progress of the overwriting operation on the screen so that errors can be viewed and addressed. Optionally, the on-screen overwriting progress output that is displayed to the user interactively is also placed in a flat file (an operating system text file). The on-screen report creates a record of the information on the overwriting session.

3 TOE Security Environment

The TOE environment is considered to be secure in that physically controlled access to the TOE is provided. The environment of the TOE is considered to be a low-risk environment.

3.1 Assumptions

The assumptions are ordered into three groups: personnel, physical environment, and operational assumptions.

3.1.1 Personnel Assumptions

A.ADMIN_CRED The Administrator (UID 0) of the TOE is assumed not to disclose their authentication credentials.

A.NOEVIL The Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.1.2 Physical Environment Assumptions

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.PHYSICAL Any individual with physical access to the processing platform on which the TOE resides is assumed to have full access to data on the platform.

3.1.3 Operational Assumptions

There are no operational assumptions for this TOE.

3.2 Threats

The TOE or IT environment addresses the threats identified in the following sections.

3.2.1 Threats Addressed by the TOE

The TOE addresses the threats discussed below.

The threat agents are either unauthorized persons or external IT entities not authorized to use the TOE itself.

T.DATA_ACCESS An unauthorized person attempts to access sensitive data stored on electronic media that has 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 has been deleted from electronic media that has been redeployed, transferred out of the organization's control, or discarded.

T.DATA_FORMAT An unauthorized person attempts to recover sensitive data remaining after formatting of electronic media that has 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.

3.2.2 Threats Addressed by the IT Environment

The IT Environment is not required to explicitly address any threats, although the IT Environment is constrained by the assumptions made above in Section 3.1.

3.3 Organizational Security Policies

This section describes the organizational security policies relevant to the operation of the TOE.

P.DISPOSAL An organization using the TOE must define an appropriate policy for the identification, disposal, sanitization, and verification of sanitization of electronic media.

4 Security Objectives

This chapter describes the security objectives for the TOE and the IT Environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the IT Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

O.NOTIFY The TOE shall provide a means of notifying authorized users of the success and/or failure to sanitize electronic media that is to be redeployed, transferred out of the organization's control, or discarded.

O.REPORT_GEN The TOE must provide the ability to generate the outcomes of the overwrite and verify operations in the form of an audit report.

O.SANITIZE The TOE must overwrite all information within an electronic device or specified portion thereof rendering the information unrecoverable by any information recovery program to prevent unauthorized access to data stored on electronic media that is to be redeployed, transferred out of the organization's control, or discarded.

O.VERIFY The TOE must provide the capability to verify that an electronic device or specified portion thereof was successfully overwritten.

4.2 Security Objectives For The IT Environment

This section defines the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

OE.ACCESS The IT environment must provide restricted access to the electronic media, TOE configuration file, and audit reports generated by the TOE and control access to the time mechanism.

OE.AUTHORIZATION The IT environment must authorize users attempting to access the TOE, and ensure that only users authorized as UID 0 are provided access to the TOE.

The non-IT security objectives listed below are to be satisfied without imposing technical requirements on the TOE or IT environment. Thus, they will be satisfied through application of procedural or administrative measures.

OE.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance. Any administrator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

OE.PHYSEC The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility.

4.3 Rationale For Security Objectives For The TOE

This section provides the rationale that all security objectives are traced back to aspects of the addressed threats and organizational security policies.

O.NOFITY O.NOTIFY ensures that a user is notified of the success and/or failure of the operation of the TOE. This counters the threat of an authorized user of the TOE being unaware of a failure to completely sanitize electronic media [T.INCOMP_OVER].

O.REPORT_GEN O.REPORT_GEN requires the ability to generate a report on the overwrite or verification operation, which contributes to mitigation of the threat that an authorized user would be unaware of a failure to completely sanitize electronic media [T.INCOMP_OVER] by providing a record of the event.

O.SANITIZE O.SANITIZE ensures that the data is not available for access due to sanitization, which counters the threat of an unauthorized person gaining access to sensitive data [T.DATA_ACCESS], attempting to recover data remaining after the data has been deleted [T.DATA_DELETED], or attempting to recover data remaining after formatting [T.DATA_FORMAT] of electronic media that is to be redeployed, transferred out of the organization's control, or discarded. P.DISPOSAL also applies by requiring end-users to outline and follow the policy for identification, disposal, sanitization, and verification of sanitization of electronic media.

O.VERIFY O.VERIFY requires the TOE to provide the capability to verify that an electronic device or specified portion thereof is successfully overwritten. This counters the threat of an overwrite operation being incompletely performed rendering data still recoverable [T.INCOMP_OVER]. P.DISPOSAL also applies by requiring end-users to outline and follow the policy for verification of sanitization of electronic media.

	T.DATA_ACCESS	T.DATA_DELETED	T.DATA_FORMAT	T.INCOMP_OVER	P.DISPOSAL
O.NOFITY				X	
O.REPORT_GEN				X	
O.SANITIZE	X	X	X		X

	T.DATA_ACCESS	T.DATA_DELETED	T.DATA_FORMAT	T.INCOMP_OVER	P.DISPOSAL
O.VERIFY				X	X

Table 2 – Threats & IT Security Objectives Mappings

4.4 Rationale For Security Objectives For The IT Environment

This section provides the rationale that all security objectives for the IT environment are traced back to aspects of the addressed threats or assumptions.

OE.ACCESS OE.ACCESS requires the IT environment to provide restricted access to the electronic media, TOE configuration file, and audit reports generated by the TOE, along with controlling access to the time mechanism, which are all supported by the assumption that the Administrator of the TOE is assumed not to disclose their authentication credentials so no unauthorized users should be able to access those files [A.ADMIN_CRED]. It is also supported by the assumption that any individual who does have physical access to the processing platform (or electronic media) is assumed to have full access to data on that platform [A.PHYSICAL].

OE.AUTHORIZATION OE.AUTHORIZATION requires the IT environment to authorize users attempting to access the TOE, and ensure that only users authorized as UID0 are provided access to the TOE, which is supported by the assumption that the Administrator of the TOE is assumed not to disclose their authentication credentials [A.ADMIN_CRED]. It is also supported by the assumption that any individual who does have physical access to the processing platform is assumed to have full access to data on that platform [A.PHYSICAL].

OE.NOEVIL OE.NOEVIL requires that any administrator of the TOE is trusted for access to the TOE, which is supported by the assumption that the Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation [A.NOEVIL]. It is also supported by the assumption that any individual who does have physical access to the processing platform is assumed to have full access to data on that platform [A.PHYSICAL].

OE.PHYSEC OE.PHYSEC requires that the facility surrounding the processing platform upon which the TOE resides provides a controlled means of access into the facility. This is supported by the assumption that 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 sensitive media is prevented [A.LOCATE]. It also supports the assumption that any individual who does have physical access to the processing platform is assumed to have full access to data on that platform [A.PHYSICAL].

	A.ADMIN_CRED	A.NOEVIL	A.LOCATE	A.PHYSICAL
OE.ACCESS	X			X
OE.AUTHORIZATION	X			X
OE.NOEVIL		X		X
OE.PHYSEC			X	X

Table 3 – Assumptions & IT Security Objectives Mappings for the IT Environment

5 IT Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table. These security requirements are defined in Sections 5.1 - 5.4.

TOE Security Functional Requirements	
None.	
Explicitly Stated TOE Security Functional Requirements	
FAU_GEN_EXP.1	Audit Data Generation
FDP_OOP_EXP.1	Overwrite Operation
FDP_VOP_EXP.1	Verify Operation
IT Environment Security Functional Requirements	
FIA_UID.1	Timing of identification
FPT_STM.1	Reliable time stamps

Table 4 – Functional Requirements

5.1 TOE Security Functional Requirements

The are no SFRs defined for this TOE that are taken directly from Part 2 of the CC.

5.2 Explicitly Stated TOE Security Functional Requirements

The SFRs defined in this section are explicitly stated and are derived from similar requirements and families in Part 2 of the CC.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN_EXP.1 Audit Data Generation

FAU_GEN_EXP.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) attempts to overwrite electronic media or specified portions within, attempts to verify electronic media or specified portions within;

b) no other events.

FAU_GEN_EXP.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event (time only for verify), and the type of event; and

b) For each audit event type, based on the auditable event definitions of the functional components

included in the ST,
start time;
finish time;
device name;
vendor (who made the device);
product (the commercial name of the device);
serial number (if available);
device type;
total number of blocks on the device;
total number of blocks being sanitized or range of blocks to be verified;
total number of defects (only for SCSI and if available);
any errors encountered;
pattern(s) used; and
success or failure of the overwrite process or whether the expected pattern was found in the verify.

5.2.2 User Data Protection (FDP)

5.2.2.1 Overwrite Operation (FDP_OOP_EXP.1)

FDP_OOP_EXP.1.1 The TSF shall overwrite electronic media and specified portions thereof.

5.2.2.2 Verify Operation (FDP_VOP_EXP.1)

FDP_VOP_EXP.1.1 The TSF shall verify the successful overwrite of electronic media or specified portions thereof.

5.3 IT Environment Security Requirements

The SFRs defined in this section are taken from Part 2 of the CC.

5.3.1.1 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The ***IT Environment*** shall allow **initiation of the logon process for multi-user mode or physical access to the TOE and verification of UID0 for single-user mode** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The ***IT Environment*** shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.1.2 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The ***IT Environment*** shall be able to provide reliable time stamps for its own use.

5.4 TOE Strength of Function Claim

No strength of function claim is made for this TOE.

5.5 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) as defined by the CC. The assurance components are summarized in the following table.

Assurance Class	Assurance Components	
ACM: Configuration management	ACM_CAP.2	Configuration items
ADO: Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5 – Assurance Requirements: EAL2

5.5.1 ACM_CAP.2 Configuration items

Developer action elements:

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.2.5C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.6C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.7C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.2 ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.3 ADO_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.5.4 ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages,

as appropriate.

ADV_FSP.1.4C - The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E - The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security requirements.

5.5.5 ADV_HLD.1 Descriptive high-level design

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security requirements.

5.5.6 ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF

representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.7 AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.8 AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.9 ATE_COV.1 Evidence of coverage

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.10 ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each

tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.5.11 ATE_IND.2 Independent testing - sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.5.12 AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

5.5.13 AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Content and presentation of evidence elements:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

5.6 Rationale For TOE Security Requirements

5.6.1 TOE Security Functional Requirements

	O.NOTIFY	O.REPORT_GEN	O.SANITIZE	O.VERIFY
FAU_GEN_EXP.1	X	X		
FDP_OOP_EXP.1			X	
FDP_VOP_EXP.1				X

Table 6 – SFR and Security Objectives Mapping

O.NOTIFY The TOE shall provide a means of notifying authorized users of the success and/or failure to sanitize electronic media that is to be redeployed, transferred out of the organization's control, or discarded.

The TOE must be able to generate an audit report during TOE execution that includes within it the success or failure of the overwrite or verification operation. [FAU_GEN_EXP.1].

O.REPORT_GEN The TOE must provide the ability to generate the outcomes of the overwrite and verify operations in the form of an audit report.

The TOE must be able to generate an audit report during TOE execution that includes within it the success or failure of the overwrite or verification operation. [FAU_GEN_EXP.1].

O.SANITIZE The TOE must overwrite all information within electronic media or specified portion thereof rendering the information unrecoverable by any information recovery program to prevent unauthorized access to data stored on electronic media that is to be redeployed, transferred out of the organization's control, or discarded.

The TOE must be able to overwrite electronic media and specified portions thereof. [FDP_OOP_EXP.1]. By overwriting media the TOE must ensure that the previous information content of electronic media or specified portion thereof is rendered inaccessible to the OS.

O.VERIFY The TOE must provide the capability to verify that electronic media or specified portion thereof was successfully overwritten.

The TOE must be able to verify the overwrite electronic media and specified portions thereof. [FDP_VOP_EXP.1]. By ensuring the successful overwriting of media the TOE ensures that the previous information content of electronic media or specified portion thereof is rendered inaccessible to the OS.

5.6.2 TOE Security Assurance Requirements

EAL2 was chosen to provide a low to moderate level of independently assured security. The chosen assurance level is consistent with the threat environment. Specifically, that the threat of malicious attacks is not greater than moderate and the product will have undergone a search for obvious flaws.

5.7 Rationale for IT Environment Security Requirements

5.7.1 IT Environment Security Functional Requirements

	OE.ACCESS	OE.AUTHORIZATION
FIA_UID.1		X
FPT_STM.1	X	

Table 7 – IT Environment SFR and Environmental IT Security Objectives Mapping

OE.ACCESS The IT environment must provide restricted access to the electronic media, TOE configuration file, and audit reports generated by the TOE and control access to the time mechanism.

The TOE environment is assumed to restrict physical access to the TOE and electronic media, including protection of the ability to maintain accurate time [FPT_STM.1].

OE.AUTHORIZATION The IT Environment must authorize users attempting to access the TOE, and ensure that only users authorized as UID 0 are provided access to the TOE.

The IT Environment must verify users attempting access to the IT environment as UID0 [FIA_UID.1].

5.8 Rationale for Explicitly Stated Security Requirements

Table 8 presents the rationale for the inclusion of the explicit requirements found in this Security Target.

Explicit Requirement	Identifier	Rationale
FAU_GEN_EXP.1	Audit Data Generation	This requirement is necessary because the CC version of the FAU_GEN.1 requirement requires an identification of the subject responsible for the audit event. This TOE does not record data on subjects as UID0 was verified.
FDP_OOP_EXP.1	Overwrite Operation	This requirement is necessary because no requirements within the user data protection functionality class (FDP) appropriately define the intended functionality of an overwrite operation. The user data protection functionality class was chosen for this requirement because the functionality provided by the overwrite operation is intended for protecting data through securely overwriting the data and making it unrecoverable. This type of data protection is useful for systems containing information that is not to be disclosed, but destroyed.
FDP_VOP_EXP.1	Verify Operation	This requirement is necessary because no requirements within the user data protection functionality class (FDP) appropriately define the intended functionality to provide a verification of the above defined overwrite operation. The user data protection functionality class was also chosen for this requirement since it provides a verification of the successful completion of the overwrite operation. Without a method to verify the successful completion of the overwrite operation, it would be possible to have an incomplete overwrite operation. This would leave user data recoverable by an attacker who gained control of the machine.

Table 8 – Explicitly Stated SFR Rationale

5.9 Rationale For IT Security Requirement Dependencies

Although all of the requirements are explicitly stated, some of the Part 2 requirements upon which they

were based have dependencies. Those dependencies are listed below.

Functional Component	Dependency	Included?
FAU_GEN_EXP.1	FPT_STM.1	Yes

5.10 Rationale For Internal Consistency and Mutually Supportive

The selected requirements are internally consistent, which was shown by mapping them to the TOE and IT environmental objectives without having conflicts.

The selected requirements together form a mutually supportive whole by:

- satisfying all dependencies as demonstrated in Section 5.10
- tracing security functional requirements to security objectives and justifying that tracing as demonstrated in Section 5.6.1

5.11 Rationale For Strength of Function Claim

No strength of function claim is made for this TOE.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Overwrite Function

The primary goal of UniShred Pro® is to overwrite sensitive electronic media. The overwrite function consists of a number of write, read/write, and read passes[5] over all the blocks of a device based on the pattern specified by the user in either the configuration file or within the command syntax. If no pattern is specified in either of these places an error is returned. The target of the overwrite can be an entire disk (or other electronic media), a partition, or a range of blocks. For SCSI disks, if the disk is capable of address translation, and there are new defects, the defect areas are made accessible, and the defect blocks are overwritten with the same set of patterns as the full disk. Once that is complete the defect areas are again made inaccessible and the full disk is again overwritten. [FDP_OOP_EXP.1]

The TOE also does self-checking (a system call) to ensure that the user executing the program is UID 0. If they are not the TOE returns an error and will not execute.

In order to be able to execute the overwrite function, the TOE relies on the low level OS device drivers to make electronic media available. The TSF gets 'full control' of the disk in terms of its ability to write to it, but all disk input/output is handled through existing OS device drivers in the IT environment. At the conclusion of the overwrite operation, the operating system is able to de-allocate the media. In cases where the entire disk, including the OS, has been overwritten, the operating system does not formally de-allocate the media from the application, however the application is removed as well so access is removed by default.

By performing the overwrite function, the TOE ensures that data is made inaccessible so that the electronic media may be disposed of or put to other uses without the risk of revealing residual information.

6.1.2 Verify Function

In order to gain assurance that the overwrite function has been successful in removing traces of information from electronic media or specified portion thereof the TOE provides the verify function. This functionality checks the contents of the first set of blocks on the device or specified portion thereof and determines the pattern that exists. Then by checking each of the remaining blocks of the device, the TOE is able to determine whether the pattern was repeated across the entire device. If any of the blocks on the device or specified portion thereof do not contain the appropriate pattern, then an error is indicated, and the blocks are listed on the screen. In cases where the entire disk, including the OS, has been overwritten the verify operation involves connecting the media to another Solaris, IRIX, or HPUX system with the TOE installed, and running the verify command options against the media that was overwritten. [FDP_VOP_EXP.1]

The TOE also does self-checking (a system call) to ensure that the user executing the program is UID 0. If they are not the TOE returns an error and will not execute.

In order to be able to execute the verify function, the TOE relies on the IT environment, specifically the low level OS device drivers to, to make the electronic media available. At the conclusion of the verify operation, the operating system is able to de-allocate the media.

---

[5] . If using a pre-defined pattern, the number of passes is pre-determined, otherwise the number of passes is configurable and can be defined within the execution command.

By performing the verify function, the TOE ensures that the data has been made inaccessible has actually been replaced by the random pattern, so that the electronic media may be disposed of or put to other uses without the risk of revealing residual information.

6.1.3 Report Generation Function

During the overwrite function and the verification function the TOE displays the progress of the overwriting and verification operations on the screen so that errors can be viewed and addressed. This on-screen progress represents the audit report, and it can optionally be saved to a flat file (an operating system text file) on a drive or specified portion thereof other than the one being overwritten. Using a parameter on the usp3 command activates the export to a flat file (an operating system text file). If a specified file already exists, the report for the current overwrite operation is appended to that file. These files become part of the IT environment after they are generated, as they are controlled by the operating system.

The on-screen overwrite report contains several fields, and a sample is shown in the UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual Section 3.6.6. The start-up and shutdown of the audit functions are exhibited by the "Disk overwrite starting" and "Disk overwrite completed" fields. The following fields are also included: start time, finish time, device name, vendor, product, serial number (if possible), device type, total number of blocks on the device, total number of blocks being sanitized, total number of defects (only for SCSI and if available), any errors encountered, pattern(s) used, and success or failure of the overwrite process. [FAU_GEN_EXP.1]

The on-screen verify report contains the same fields as the overwrite report, and a sample is shown in the UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual Section 3.6.9. The differences from the overwrite report are that no date is given (only time), instead of displaying the total number of blocks being sanitized it displays the range of blocks to be verified, and instead of showing numerous passes over the device with different patterns, it shows the single pass over the device to check for the expected pattern [FAU_GEN_EXP.1].

6.2 Security Assurance Measures

Assurance Requirement	Assurance Components
ACM_CAP.2	The description of the configuration items is provided in Configuration Management for Los Altos Technologies UniShred Pro ® Version 3.3.2.
ADO_DEL.1	The description of the delivery procedures is provided in Delivery Documentation for Los Altos Technologies UniShred Pro ® Version 3.3.2
ADO_IGS.1	The installation, generation, and start-up procedures are provided in UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual; UniShred Pro® Version 3.3.2 Installation Guide for AIX Operating Systems; UniShred Pro® Version 3.3.2 Installation Guide for HP-UX Release 10 and 11 Operating Systems; UniShred Pro® Version 3.3.2 Installation Guide for IRIX Version 6.5 Operating System; UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems; UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems on Sparc™ Platforms; UniShred Pro®

	Version 3.3.2 Installation Guide for Solaris Operating Systems Sparc Platform Edition; UniShred Pro® Version 3.3.2 Installation Guide for Solaris Operating Systems X86 Platform Edition.
ADV_FSP.1	The informal functional specification is provided in Informal Functional Specification for Los Altos Technologies UniShred Pro ® Version 3.3.2.
ADV_HLD.1	The descriptive high-level design is provided in High Level Design for Los Altos Technologies UniShred Pro ® Version 3.3.2.
ADV_RCR.1	The informal correspondence demonstration is provided in Informal Functional Specification for Los Altos Technologies UniShred Pro ® Version 3.3.2 and High Level Design for Los Altos Technologies UniShred Pro ® Version 3.3.2.
AGD_ADM.1	The administrator guidance is provided in the following documents: UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual
AGD_USR.1	Not applicable. No user guidance is provided for this product as there are no non-administrative users (PD-0106).
ATE_COV.1	The evidence of coverage is provided in Test Plan and Coverage Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2.
ATE_FUN.1	The functional testing description is provided in Test Plan and Coverage Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2.
ATE_IND.2	The TOE, testing documentation, and test resources that were equivalent to those used in the developer's functional testing were made available to the CC testing laboratory for independent testing.
AVA_SOF.1	The strength of function analysis performed is provided in Strength of Function and Vulnerability Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2.
AVA_VLA.1	The vulnerability analysis performed is provided in Strength of Function and Vulnerability Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2.

Table 9 – Assurance Requirements: EAL2

6.3 Rationale for TOE Security Functions

This section contains a table that relates the security functional requirements to the TOE security functions. The rationale that the security functions cover the security functional requirements is in Sections 6.1.1, 6.1.2, and 6.1.3.

	Overwrite Function	Verify Function	Report Generation
FDP_OOP_EXP.1	X		
FDP_VOP_EXP.1		X	
FAU_GEN_EXP.1			X

Table 10 – TSF to SFR Mapping

6.4 Appropriate Strength of Function Claim

There are no probabilistic or permutational mechanisms for this TOE; therefore there is no SOF claim for the TOE.

6.5 Rationale for Security Assurance

The assurance documentation listed below was developed to meet the developer action and content and presentation of evidence elements for each assurance requirement defined in the CC.

Assurance Requirement	Assurance Measures	Assurance Rationale
ACM_CAP.2	*Configuration Management for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 2.1 October 25, 2006*	The configuration management document defines the configuration items and contains the necessary information to demonstrate that a CM system is used and that there is a unique reference for the TOE.
ADO_DEL.1	*Delivery Documentation for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.2, October 5, 2005.*	The delivery document describes the steps performed to ensure consistent, dependable delivery of the TOE to the customer.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADO_IGS.1	*UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual, Document No: USP-DOC-01-07, April 3, 2006; UniShred Pro® Version 3.3.2 Installation Guide for AIX Operating Systems, Document No: USP3-DOC-17-05, April 3, 2006; 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; UniShred Pro® Version 3.3.2 Installation Guide for IRIX Version 6.5 Operating System, Document No: USP3-DOC-06-07, April 3, 2006; UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems, Document No: USP3-DOC-18-05, April 3, 2006; UniShred Pro® Version 3.3.2 Installation Guide for Linux Operating Systems on Sparc™ Platforms Document No: USP3-DOC-19-01, April 3, 2006; UniShred Pro® Version 3.3.2 Installation Guide for Solaris Operating Systems Sparc Platform Edition, Document No: USP3-DOC-02-08, April 3, 2006; UniShred Pro® Version 3.3.2 Installation Guide for Solaris Operating Systems X86 Platform Edition, Document No: USP3-DOC-16--03, April 3, 2006*	The installation documents describe the steps necessary for secure installation, generation and start-up of the TOE. There is an overall user/ administrator guide that covers basic installation, and there are operating system specific installation guides.
ADV_FSP.1	*Informal Functional Specification for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.6, September 21, 2006*	The informal functional specification document identifies the external interfaces that completely represent the TSF and describes the purpose and method of use of all external TSF interfaces. It also describes the effects, exceptions, and error messages for each of the external TSF interfaces.

Assurance Requirement	Assurance Measures	Assurance Rationale
ADV_HLD.1	*High Level Design for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.5, October 25, 2006*	The security enforcing high-level design describes the complete TSF in terms of subsystems. The security functions for each subsystem are described. The subsystem interfaces are defined and the externally visible interfaces are identified.
ADV_RCR.1	*Informal Functional Specification for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.6, September 21, 2006* *and* *High Level Design for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.5, October 25, 2006*	The informal correspondence document maps the security functionality as described in the FSP and ST and as described in the FSP and HLD.
AGD_ADM.1	*UniShred Pro® Version 3.3.2 Disk Overwriting Software User's Manual, Document No: USP-DOC-01-07, April 3, 2006*	Administrative guidance provides the TOE administrators with detailed, accurate information of how to administer the TOE in a secure manner.
AGD_USR.1	Not Applicable.	No user guidance is provided for this product as there are no non-administrative users (PD-0106).
ATE_COV.2	*Test Plan and Coverage Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.9 September 21, 2006*	The test coverage document provides a mapping of the test cases performed against the TSF.
ATE_FUN.1	*Test Plan and Coverage Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.9, September 21, 2006*	The functional testing document includes the test plans, test procedures, and associated test cases of the TOE functional testing effort.
ATE_IND.2	*Los Altos Technologies UniShred Pro® Version 3.3.2 Team Test Plan Version 3.0*	The TOE hardware, software, guidance, and testing documentation (including test procedures, actual, and expected results) were made available to the CC testing laboratory for independent testing.

Assurance Requirement	Assurance Measures	Assurance Rationale
AVA_SOF.1	*Strength of Function and Vulnerability Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.2, October 7, 2005*	The strength of function analysis document reiterates that there are no strength of function claims for this TOE.
AVA_VLA.1	*Strength of Function and Vulnerability Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.2, Version 1.2, October 7, 2005*	The vulnerability analysis document identifies and describes the process used to discover obvious vulnerabilities, the results of the vulnerability analysis, and the mitigation of each identified obvious vulnerability.

Table 11 – Assurance Measure Rationale: EAL2

7 Protection Profile Claims

This Security Target does not claim conformance to any Protection Profiles.

8 Rationale

8.1 Security Objectives Rationale

Sections 4.3 and 4.4 provide the security objectives rationale.

8.2 Security Requirements Rationale

Sections 5.6 to 5.10 provide the security requirements rationale.

8.3 TOE Summary Specification Rationale

Sections 6.3 - 6.5 provide the TOE summary specification rationale.

8.4 Protection Profile Claims Rationale

This Security Target does not claim conformance to any Protection Profiles

8.5 Rationale for Strength of Function Claim

Section 5.11 provides the SOF rationale for this ST.

