Los Altos Technologies

Security Target

for

Los Altos Technologies UniShred Pro ® Version 3.3.1

Release Date: December 13, 2002

Version: **2.0**

Status: **Final**

Prepared By:

CORSEC Security, Inc.
10340 Democracy Lane
Suite 201
Fairfax, VA 22030
Phone: 703.267.6050

Prepared For:

Los Altos Technologies, Inc.
1381 Kildaire Farm Road,
Suite 415
Cary, NC 27511
Phone: 919.233.9889

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 Security Target Identification

ST Title: Security Target for Los Altos Technologies UniShred Pro ® Version 3.3.1

ST Version: 2.0: Final

ST Date: December 13, 2002

TOE: Los Altos Technologies UniShred Pro ® Version 3.3.1

Assurance level: EAL1

Common Criteria: Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999 (aligned with ISO/IEC 15408:1999).

Interpretations: Interpretations are identified within section 9.2.

Keywords: Secure Delete, UniShred, Remanence Security

1.2 TOE Reference

The TOE is uniquely identified as Los Altos Technologies UniShred Pro version 3.3.1.

Further reference to the TOE is provided within table 12 of section 8.3.2 of this Security Target.

1.3 CC Conformance Claims

This TOE is CC Version 2.1 Part 2 extended, and CC Version 2.1 Part 3 conformant.

1.4 Security Target Overview

The TOE overwrites data on hard disks in order to eliminate the threat of data compromise when computers are reassigned to different programs, departments, or people; when using portable computers; and when computers are in poorly secured areas. Without the TOE, simple computer programs in widespread use could read, copy, or even undelete the original files. The TOE uses disk specific features to provide nondestructive removal of magnetic remanence.

The Los Altos Technologies UniShred Pro ® Version 3.3.1 ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to mitigate the defined threats:

- **ST Introduction** – Provides identification information for the Security Target to uniquely identify the Security Target itself, the authors of the Security Target, the TOEs identified within the Security Target, the assurance level the TOE is claiming, and identification of the CC standard along with a conformance claim to the CC standard.
- **TOE Description** – Provides an overview of the TOE security functions and describes the physical and logical boundaries for the TOE.
- **TOE Security Environment** – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.
- **Security Objectives** – Identifies the security objectives that are satisfied by the TOE and the TOE environment.
- **IT Security Requirements** – Presents the Security Functional Requirements (SFRs) met by the TOE and its environment. In addition, the Security Assurance Requirements (SARs) met by the TOE are presented.
- **TOE Summary Specification** – Describes the security functions provided by the TOE to satisfy the security requirements and objectives.
- **Protection Profile Claims** – Presents the rationale concerning compliance of the ST with CC Version 2.1.
- **Rationale** – Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.
- **References** – Presents a set of acronyms and interpretations of requirements that apply to this ST.

1.5 Document Conventions

There are several font variations within this ST. The text below provides an explanation of the font conventions used to show operations, as defined in Common Criteria, performed on the requirements.

Assignment	*Requirement text will appear in Italics and underlined*
Iteration	Typical CC requirement naming will be followed by a lower case letter for each new iteration. (Ex. FMT_MOF.1.1a)
Selection	**Requirement text will appear in bold and underlined**
Refinement	***Requirement text will appear in bold italics***

2 TOE Description

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

2.1 Los Altos Technologies UniShred Pro ® Version 3.3.1 Overview

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 information, but can also be a significant concern for unclassified but sensitive information and for potentially embarrassing comments, which can be unknowingly retained in a file after deletion when using some modern software applications. Often, utility overwrite programs contain an option to overwrite the location of the file to ensure that the chance of recovery of the information from data remanence is very remote.

As well, when users delete files from their computers, they do not often realize that instead of deleting the contents of these files, all that they have deleted is the links, or directory entries, to the files. The information that was contained in the file is not removed from the system until other information is saved that overwrites the same area of the computer disk. This typical method of file deletion enables disk editor products to recover information that has supposedly been "deleted".

Los Altos Technologies UniShred Pro ® Version 3.3.1 provides the capabilities to securely overwrite all existing information residing on either a partition, or entire disk. In addition, the overwrite methods provided conform to various United States Government regulations.

Los Altos Technologies UniShred Pro ® Version 3.3.1 also provides capabilities for verifying the successful completion of overwriting a partition or disk, as well as, provides reports on the processes. The reports that are generated, are displayed on-screen, can be archived to a file, and also printed at a later time.

Los Altos Technologies UniShred Pro ® Version 3.3.1 operates on the following operating systems:

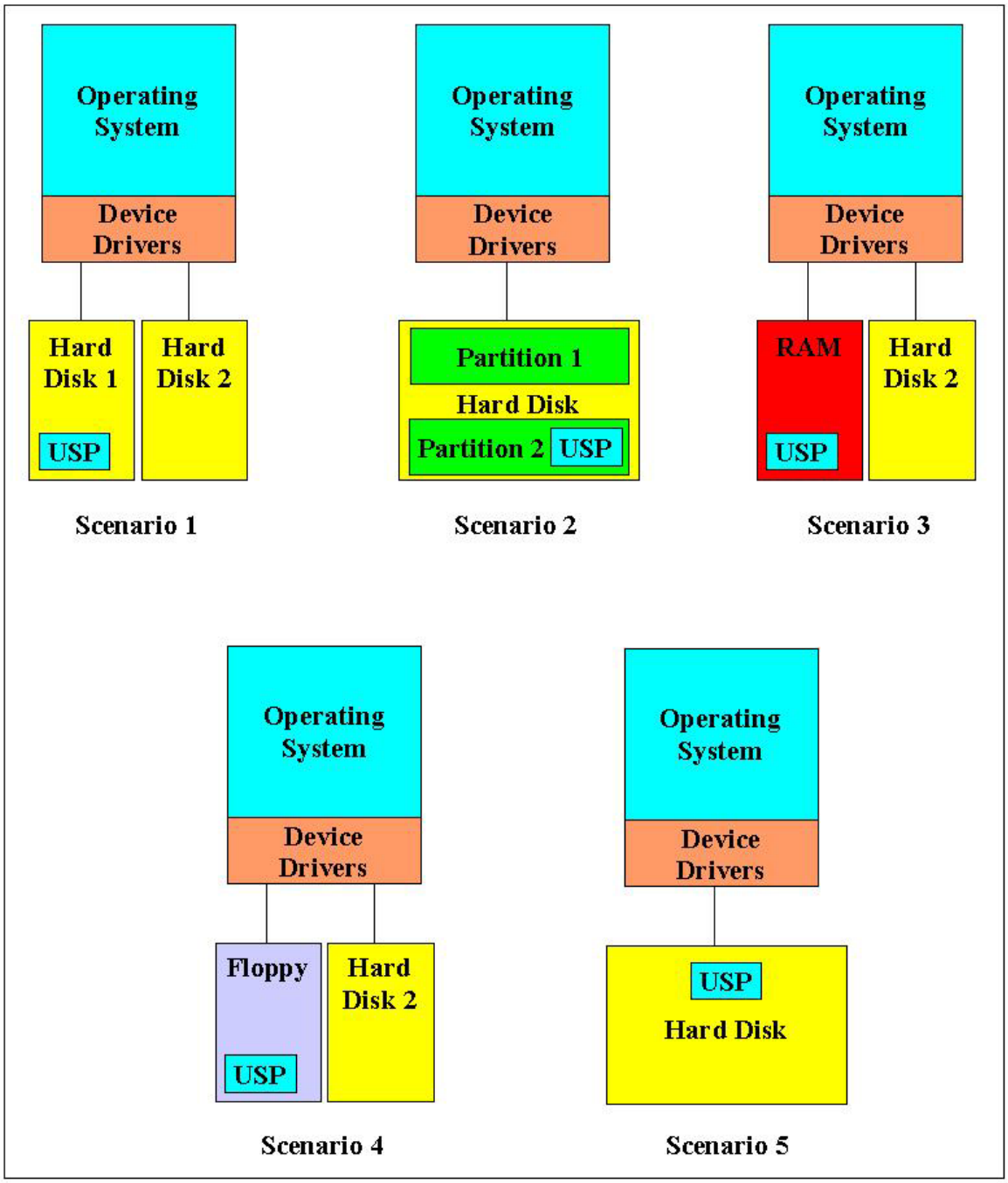
- HP HP/UX 9 - 11
- IBM AIX 4.x
- GNU Linux w/ kernel 2.x
- SGI IRIX 6.5.x
- and Sun Solaris 2.x, 7.x, 8.x, and 9.x

In addition to these defined operating systems, Los Altos Technologies UniShred Pro ® Version 3.3.1 also can be operated from a self-bootable floppy disk using a stripped down version of GNU Linux from any Intel platform PC.

Los Altos Technologies UniShred Pro ® Version 3.3.1 is a software utility that can be operated from a floppy disk, hard disk, or within a system’s internal memory (RAM).

2.2 Physical Boundaries

Figure 1: TOE Physical Diagram



As shown in the above figure, the operating system and Los Altos Technologies UniShred Pro ® Version 3.3.1 (USP) are both displayed in a light blue coloration and therefore indicating these two components to be the TOE.

All underlying hardware in which the TOE operates on is not considered to be part of the TOE.

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.

Hardware components not considered part of the TOE, yet at the minimum are required for TOE operation are the following:

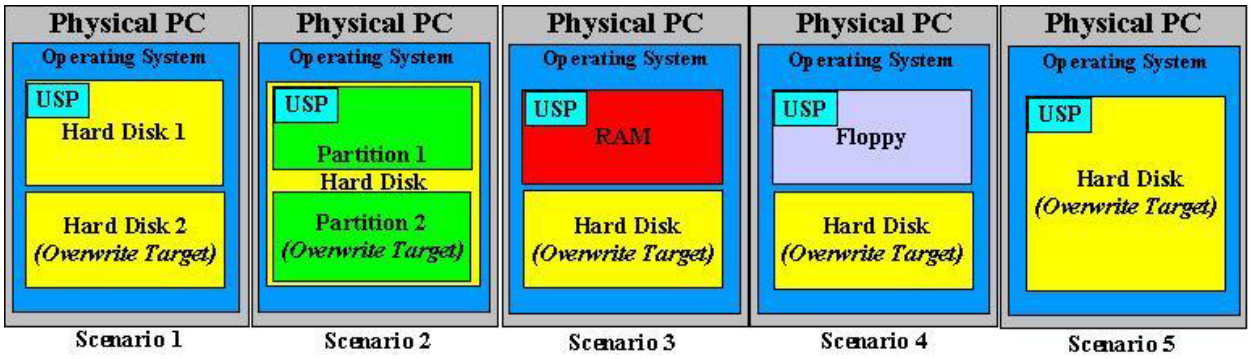
1. **HP HP/UX 9 – 11 Operating Systems**
   - RAM –24 MB minimum
   - Hard Drive Space – 2 MB minimum
2. **IBM AIX 4.x Operating Systems**
   - RAM – 32 MB minimum
   - Hard Drive Space – 1 MB minimum
3. **GNU Linux w/ kernel 2.x Operating Systems**
   - RAM – 32 MB minimum
   - Hard Drive Space – 2 MB minimum
4. **SGI IRIX 6.5.x Operating Systems**
   - RAM –24 MB minimum
   - Hard Drive Space – 2 MB minimum
5. **SUN Solaris 2.x, 7.x, 8.x, 9.x Operating Systems**
   - RAM – 24 MB minimum
   - Hard Drive Space – 2 MB minimum

Software components considered to be part of the TOE are the following operating systems:

1. **HP HP/UX 9 – 11 Operating Systems**
2. **IBM AIX 4.x Operating Systems**
3. **GNU Linux w/ kernel 2.x Operating Systems**
4. **SGI IRIX 6.5.x Operating Systems**
5. **SUN Solaris 2.x, 7.x, 8.x, 9.x Operating Systems**

2.3 Logical Boundaries

Figure 2: TOE Logical Diagram



The TOE is defined to be the Los Altos Technologies UniShred Pro ® Version 3.3.1 application (USP) and the following operating systems: HP HP/UX 9, HP HP/UX 10, HP HP/UX 11, IBM AIX 4, GNU Linux /w kernel 2.x, SGI IRIX 6.5, SUN Solaris 2, SUN Solaris 7, SUN Solaris 8, and SUN Solaris 9. The identification and access control functionalities are considered to be the TOE portion of the operating system. Identification provides the capability for users identify themselves to the operating system. Access Control provides the capability for the operating system to control access to operating system resources.

The Physical PC, as shown in the above figure, is not considered part of the TOE. As shown in the above figure, there are five possible scenarios in which the application with any of the defined operating systems can run.

The first scenario provides the ability for USP to overwrite an entire hard disk, while running the application from a separate hard disk.

The second scenario provides the ability for USP to overwrite a partition within a hard disk, while running the application from a separate partition of that same hard disk.

The third scenario provides the ability for USP to overwrite an entire hard disk, while running the application from within the RAM of the residing PC.

The fourth scenario provides the ability for USP to boot from a floppy into a GNU Linux based operating system to provide the same capabilities of overwriting a hard disk.

The fifth scenario provides the ability for USP to overwrite the same disk and partition, in which USP resides in. In this case, the audit report would be written to the floppy. However, this scenario is only provided within the Solaris operating systems.

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

A.Admin_Credentials: Disclosure of Administrative Credentials

Administrators (UID 0) of the TOE are assumed not to disclose their authentication credentials to any individual that is not authorized for access to the TOE.

A.No_Evil_Admin: Trustworthy Administrator

The Administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.Facility_Access: Controlled Access to TOE Facility

The processing platform in which the TOE resides on is assumed to be located within a facility that provides controlled access, so that unauthorized access to the disk media is prevented.

3.2 Threats

T.Incomplete_Overwrite: Incomplete Overwrite Operation

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.

T.Unauthorized_Access: Unauthorized Access to the TOE

An unauthorized individual gains access to the TOE and its resources resulting in the disclosure, or unauthorized overwriting of the information within the disk media.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE or the security environment or both, therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the TOE IT Environment.

4.1 Security Objectives for the TOE

This section identifies and describes the security objectives satisfied by the TOE.

O.Access: Access Control

The TOE must provide restricted access to the TOE configuration file, and audit reports generated by the TOE.

O.Audit: Audit Report Management

The TOE must provide the ability to generate, display, store, and print all outcomes of the overwrite and verify operations in the form of an audit report.

O.Authorization: Authorization of a User

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

O.Overwrite: Overwrite Operation

The TOE must overwrite all information within a disk or partition rendering the information unrecoverable by any disk recovery program.

O.Verify: Verify Operation

The TOE must provide the capability to verify that a disk or partition was successfully overwritten.

4.2 Security Objectives for the Environment

The TOE Environment accomplishes the security objectives delineated within this section.

OE.Admin_Trust: Trustworthiness of the Administrator

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.TOE_Facilities: Access to TOE Facilities

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

5 IT Security Requirements

This section defines functional and assurance requirements for the TOE, and the Security requirements for the IT environment.

5.1 TOE Security Functional Requirements

The following table represents a summary of the functional requirements defined for this ST.

A justification to the TOE Security Functional requirements stated below is provided within section 8.2.4.

Table 1: TOE Security Functional Requirements

Functional Requirement:	Operations Performed:
Security Functional Requirements for the TOE	
FDP_ACC.1	Assignment
FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416	Assignment, Selection, Refinement
FIA_UID.1-NIAP-0405	Assignment
FMT_MOF.1	Assignment, Selection
FMT_MSA.1	Assignment, Selection
FMT_MSA.3	Assignment, Selection
FMT_SMR.1	Assignment
Explicitly Stated Security Functional Requirements for the TOE	
FAU_ARM.1	None Performed
FDP_OOP.1	None Performed
FDP_VOP.1	None Performed

5.1.1 User Data Protection (FDP)

5.1.1.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1

The TSF shall enforce the *Los Altos Access Control Policy* on *the Los Altos Technologies UniShred Pro version 3.3.1 product, the Los Altos Technologies UniShred Pro version 3.3.1 configuration file, and reports generated by Los Altos Technologies UniShred Pro version 3.3.1*.

5.1.1.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1-NIAP-0405-NIAP-0407-NIAP-0416

The TSF shall enforce the *Los Altos Access Control Policy* to objects based on ***the following:*** *users and roles of users of the operating system*.

FDP_ACF.1.2-NIAP-0405-NIAP-0407-NIAP-0416

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *the user or the role of the user of the operating system attempting to access Los Altos Technologies UniShred Pro version 3.3.1 is UID 0 or included within the administrators role*.

FDP_ACF.1.3-NIAP-0405-NIAP-0407-NIAP-0416

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **no additional rules**.

FDP_ACF.1.4-NIAP-0405-NIAP-0407-NIAP-0416

The TSF shall explicitly deny access of subjects to objects based on the ***following rules:*** *the user or role of the user of the operating system attempting to access Los Altos Technologies UniShred Pro version 3.3.1 is not UID 0 or within the administrators group*, **no additional explicit denial rules**.

5.1.2 Identification and authentication (FIA)

5.1.2.1 Timing of identification (FIA_UID.1)

FIA_UID.1.1-NIAP-0405

The TSF shall allow *initiation of the logon process* on behalf of the user to be performed before the user is identified.

FIA_UID.1.2-NIAP-0405

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

5.1.3 Security Management (FMT)

5.1.3.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1

The TSF shall restrict the ability to **enable** the functions *overwrite and verify* to *UID 0 or to a user of the administrators group*.

5.1.3.2 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1

The TSF shall enforce the *Los Altos Access Control Policy* to restrict the ability to **modify** the security attributes *for the TOE configuration file and generated audit reports* to *UID 0 or to a user of the administrators group*.

5.1.3.3 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the *Los Altos Access Control Policy* to provide **restrictive** default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2

The TSF shall allow the *user account UID 0 or a user of the administrators group* to specify alternative initial values to override the default values when an object or information is created.

5.1.3.4 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles *Administrators*.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

5.2 Explicitly Stated TOE Security Functional Requirements

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Report Management (FAU_ARM.1)

FAU_ARM.1.1

The TSF shall generate audit reports upon completion of an overwrite or verification operation that has been performed.

FAU_ARM.1.2

The TSF shall provide capabilities to display and store the audit reports that are generated.

5.2.2 User Data Protection (FDP)

5.2.2.1 Overwrite Operation (FDP_OOP.1)

FDP_OOP.1.1

The TSF shall overwrite disks and partitions.

5.2.2.2 Verify Operation (FDP_VOP.1)

FDP_VOP.1.1

The TSF shall verify the successful overwrite of a disk or partition.

5.3 TOE Security Assurance Requirements

The assurance requirements for this Security Target are taken from Part 3 of the CC and comprise the EAL1 level of assurance. The assurance components are summarized in the following table.

Table 2: Assurance Components (EAL1)

Assurance Class	Assurance Components	
Class ACM: Configuration Management	ACM_CAP.1	Version numbers
Class ADO: Delivery and Operation	ADO_IGS.1	Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal correspondence demonstration
Class AGD: Guidance Documents	AGR_ADM.1	Administrator guidance
	ARG_USR.1	User guidance
Class ATE: Tests	ATE_IND.1	Independent testing - conformance

5.3.1 ACM: Configuration Management

5.3.1.1 ACM_CAP.1: Version Numbers

A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated. Labeling the TOE with its reference ensures that users of the TOE can be aware of which instance of the TOE they are using.

Developer action elements:

ACM_CAP.1.1D The developer shall provide a reference for the TOE.

Content and presentation of evidence elements:

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.1.2C The TOE shall be labeled with its reference.

Evaluator action elements:

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

5.3.2 ADO: Delivery and Operation

5.3.2.1 ADO_IGS.1: Installation generation and start-up procedures

Installation, generation, and start-up procedures are useful for ensuring that the TOE has been installed, generated, and started up in a secure manner as intended by the developer. The requirements for installation, generation and start-up call for a secure transition from the TOE's implementation representation being under configuration control to its initial operation in the user environment.

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 documentation shall describe 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.

5.3.3 ADV: Development

5.3.3.1 ADV_FSP.1: Informal functional specification

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is an instantiation of the TOE security functional requirements. The functional specification has to show that all the TOE security functional requirements are addressed.

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 functional requirements.

5.3.3.2 ADV_RCR.1: Informal correspondence demonstration

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

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.

5.3.4 AGD: Guidance Documents

5.3.4.1 AGD_ADM.1: Administrator Guidance

Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security. Because the secure operation of the TOE is dependent upon the correct performance of the TSF, persons responsible for performing these functions are trusted by the TSF. Administrator guidance is intended to help administrators understand the security functions provided by the TOE, including both those functions that require the administrator to perform security-critical actions and those functions that provide security-critical information.

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.

5.3.4.2 AGD_USR.1: User Guidance

User guidance refers to material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces. User guidance describes the security functions provided by the TSF and provides instructions and guidelines, including warnings, for its secure use.

The user guidance provides a basis for assumptions about the use of the TOE and a measure of confidence that non-malicious users, application providers and others exercising the external interfaces of the TOE will understand the secure operation of the TOE and will use it as intended.

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.

5.3.5 ATE: Tests

5.3.5.1 ATE_IND.1: Independent Testing - Conformance

This component does not address the use of developer test results. It is applicable where such results are not available, and also in cases where the developer's testing is accepted without validation. The evaluator is required to devise and conduct tests with the objective of confirming that the TOE security functional requirements are met. The approach is to gain confidence in correct operation through representative testing, rather than to conduct every possible test. The extent of testing to be planned for this purpose is a methodology issue, and needs to be considered in the context of a particular TOE and the balance of other evaluation activities.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.4 Strength of Function Claim

No strength of function claim is made for this TOE

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions implemented by the TOE and its environment to meet the security requirements stated within section 5.1. A mapping of the security functions identified and their related security requirements can be found within table 11, section 8.3.1.

6.1.1 Access Control Function

The access control function enforces access control on the TOE for access to modifying the Los Altos Technologies UniShred Pro ® Version 3.3.1 configuration file, generated audit reports, and executing Los Altos Technologies UniShred Pro ® Version 3.3.1. The access control function is enforced by checking the user identity of the authenticated user to ensure that the user is authenticated as UID 0 or belonging to the administrators group. The access control function is provided by the underlying operating system of Los Altos Technologies UniShred Pro ® Version 3.3.1 and enforces the Los Altos Access Control Policy.

6.1.2 Audit Report Management Function

The audit report management function provides the ability to generate audit reports upon completion of the overwrite and verification functions. The audit report management function also provides the ability to display and store the generated audit reports. For storage options, the Los Altos Technologies UniShred Pro ® Version 3.3.1 can be configured to store audit reports to a hard disk, floppy, or network device. The fifth scenario identified in section 2.3 specifically uses the floppy as an audit report storage option.

The underlying operating system of the Los Altos Technologies UniShred Pro ® Version 3.3.1 provides the capabilities to print the reports using the “lp” command. The underlying operating system also provides the capability to view the reports using a text editor such as vi.

When multiple audit reports are generated, they are appended to the same output file. This keeps previous audit data from being overwritten, and allows a user to view or print all audit reports simultaneously from within the same file.

When an overwrite operation is performed, the audit report displays the following information:

- License number, and expiration of license.
- For the target device, the name, size, vendor name, product number, revision number, serial number, disk type, number of blocks, disk speed, and disk mount status.
- Overwrite date and time, overwrite pattern, pattern used for each pass and number of passes within the overall pattern, and confirmation of the output report file.
- Confirmation of each sub-operation being performed for the overall overwrite operation with the time of each sub-operation occurrence, identification of any errors occurred, and confirmation of a complete overwrite of the device.

When a verify operation is performed, the audit report displays the following information:

- License number, and expiration of license.
- For the target device, the name, size, vendor name, product number, revision number, serial number, disk type, number of blocks, and disk speed.
- Verification of the pattern performed within the last pass of the full overwrite operation, blocks used, time of the verification operation performed, number of blocks verified, verification of the device being overwritten, and verification of the verify operation being complete.

6.1.3 Identification Function

The identification function provides the capability for a user to authenticate to the TOE. The TOE then checks if the user is authenticated as UID 0 to determine if access to Los Altos Technologies UniShred Pro ® Version 3.3.1 is granted. The identification function is provided by the underlying operating system of Los Altos Technologies UniShred Pro ® Version 3.3.1.

6.1.4 Overwrite Function

The overwrite function provides the capability to securely overwrite all existing information residing on either a partition or entire disk, using industry known methods for remanence thru the use of a pre-defined set of patterns. A pre-defined pattern provides a variation of overwrite methods with a defined number of times the disk is overwritten in the pre-defined pattern. In addition, the overwrite operation also provides the capability of allowing a user to specify the range of blocks to be overwritten.

The overwrite operation is performed thru the execution of the command, “usp3”, from the command line interface.

6.1.5 Verification Function

The verification function provides the capability to ensure the successful completion of the overwrite function. The verification function also provides the pattern method performed within the last pass completed in the overwrite function.

Additionally, the verification function provides the capability to read a hard disk.

The verify operation is performed thru the execution of the command, “usp3 --verify”, from the command line interface.

6.2 Assurance Measures

The assurance requirements for this TOE are met by EAL1, which stresses assurance through Los Altos's actions that are within the bounds of current best-commercial practice. These assurance requirements provide, primarily via review of Los Altos-supplied evidence (i.e. assurance documents), independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

1. Verification of the unique TOE identifier (ACM)
2. Confirmation of system generation and installation procedures (ADO)
3. Verification that the system security state is not misrepresented (ADV, AGD)
4. Independent functional testing (ATE)

To define the assurance measures claimed to satisfy the security assurance requirements specified in Section 5.3, a mapping is provided between the Assurance Requirements and the Assurance Measures, which are intended to satisfy the Assurance Requirements. As shown in Table 12, the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

6.2.1 EAL Justification

Los Altos Technologies has chosen to pursue an EAL 1 assurance level of the UniShred Pro version 3.3.1 product because of government customer requirements that are mandated by NSTISSP 11 Policy Letter, which require a Common Criteria certification for a product to be sold to government agencies.

Additionally, an EAL 1 level of assurance was chosen for Los Altos Technologies UniShred Pro version 3.3.1 based on the consideration of the environment for the TOE to be a low risk.

7 Protection Profile Claims

There are no protection profile claims for this security target.

8 Rationale

This section demonstrates the completeness and consistency of this ST.

- *Traceability:* The security objectives for the IT and environment are explained in terms of OSPs, threats countered, and assumptions met. The SFRs are explained in terms of objectives met by the requirement. The traceability is illustrated through matrices that map the following:

  a) security objectives to OSPs and/or threats countered

  b) objectives to assumptions met

  c) SFRs to objectives met

- *Assurance Level:* A justification is provided for selecting an EAL1 level of assurance for this ST.

- *Dependencies:* A mapping is provided as evidence that all dependencies are met.

8.1 Security Objectives Rationale

This section provides evidence demonstrating coverage of the OSPs by the IT security objectives. The security objectives were derived exclusively from statements of OSPs, threats and assumptions. The following table and corresponding discussion provides evidence of coverage for each statement of organizational security policy.

8.1.1 Security Objectives Mapping

Table 3: Mapping of Security Environment to Security Objectives

TOE Security Environment	Objectives
Assumptions	
A.Admin_Credentials	OE.Admin_Trust
A.No_Evil_Admin	OE.Admin_Trust
A.Facility_Access	OE.TOE_Facilities
Threats	
T.Incomplete_Overwrite	O.Audit, O.Verify, O.Overwrite
T.Unauthorized_Access	OE.TOE_Facilities, O.Access, O.Authorization

Table 4: Reverse Mapping of Security Objectives to the Security Environment

Objectives	Policies / Threats / Assumptions
Security Objectives for the TOE	
O.Access	T.Unauthorized_Access
O.Audit	T.Incomplete_Overwrite
O.Authorization	T.Unauthorized_Access
O.Overwrite	T.Incomplete_Overwrite
O.Verify	T.Incomplete_Overwrite
Security Objectives for the Environment	
OE.Admin_Trust	A.Admin_Credentials, A.No_Evil_Admin, T.Unauthorized_Access
OE.TOE_Facilities	A.Facility_Access, T.Unauthorized_Access

8.1.2 Security Objectives Justification

Table 5: Security Objectives Justification

Security Environment	Security Objectives
Assumptions	
A.Admin_Credentials: Disclosure of Administrative Credentials Administrators (UID 0) of the TOE are assumed not to disclose their authentication credentials to any individual that is not authorized for access to the TOE.	**OE.Admin_Trust** supports this assumption by requiring that any administrator of the TOE is trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
A.No_Evil_Admin: Trustworthy Administrator The Administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation.	**OE.Admin_Trust** supports this assumption by requiring that any administrator of the TOE is trusted for access to the TOE.
A.Facility_Access: Controlled Access to TOE Facility The processing platform in which the TOE resides on is assumed to be located within a facility that provides controlled access, so that unauthorized access to the disk media is prevented.	**OE.TOE_Facilities** supports this assumption by requiring that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.
Threats	
T.Incomplete_Overwrite: Incomplete Overwrite Operation 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.	**O.Audit** supports this threat by requiring the TOE to provide the ability to generate, display, store, and print all outcomes of the overwrite and verify operations in the form of an audit report. **O.Overwrite** supports this threat by providing the capability to overwrite all information within a disk or partition rendering the information unrecoverable by any disk recovery program. **O.Verify** supports this threat by requiring the TOE to provide the capability to verify that a disk or partition is successfully overwritten, as well as, specify the overwrite pattern used within the last pass performed.

Security Environment	Security Objectives
T.Unauthorized_Access: Unauthorized Access to the TOE An unauthorized individual gains access to the TOE and its resources resulting in the disclosure of the information within the disk media.	**O.Access** supports this threat by requiring the TOE to provide restricted access to the TOE configuration file, and audit reports generated by the TOE. **O.Authorization** supports this threat by requiring the TOE to authorize users attempting to access the TOE, and ensure that only users authorized as UID0 are provided access to the TOE. **OE.TOE_Facilities** supports this threat by requiring that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility.

8.2 Security Requirements Rationale

This section provides evidence demonstrating that the security objectives for the TOE and the TOE IT Environment is satisfied by the security requirements.

These mappings demonstrate that all TOE security requirements can be traced back to one or more TOE security objective(s), and all TOE security objectives are supported by at least one security requirement.

8.2.1 Security Functional Requirements Mapping

This section provides evidence demonstrating that the security objectives of the TOE are satisfied by the security requirements. The following tables and corresponding discussions provide the security requirement to security objective mappings and rationale to justify the mapping.

Table 6: Mapping of Security Objectives to Security Requirements

Objectives	Security Requirements
TOE Security Objectives	
O.Access	FDP_ACC.1, FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3
O.Audit	FAU_ARM.1
O.Authorization	FIA_UID.1-NIAP-0405, FMT_SMR.1
O.Overwrite	FDP_OOP.1
O.Verify	FDP_VOP.1

8.2.2 Security Functional Requirements Suitable to Meet Objectives

Table 7: Reverse Mapping of Security Requirements to Security Objectives

Security Requirements	Objectives
TOE Security Functional Requirements	
FDP_ACC.1	O.Access
FDP_ACF.1	O.Access
FDP_UID.1	O.Authorization
FMT_MOF.1	O.Access
FMT_MSA.1	O.Access
FMT_MSA.3	O.Access
FMT_SMR.1	O.Authorization
Explicitly Stated TOE Security Functional Requirements	
FAU_ARM.1	O.Audit
FDP_OOP.1	O.Overwrite
FDP_VOP.1	O.Verify

8.2.3 Security Functional Requirements Justification

Table 8: Security Functional Requirements Justification

Security Objectives for the TOE	TOE Security Functional Requirements
O.Access: Access Control The TOE must provide restricted access to the TOE configuration file, and the audit reports generated by the TOE.	**FDP_ACC.1** satisfies this security objective by enforcing an access control policy for access to the TOE configuration file and audit reports. **FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416** satisfies this security objective by enforcing the access control policy on all users of the TOE. **FMT_MOF.1** satisfies this security objective by requiring authentication of UID 0 or a member of the administrator's group to enable the overwrite and verify functions. **FMT_MSA.1** satisfies this security objective by enforcing the access control policy to restrict the ability to modify configuration file and audit reports to UID 0 or a member of the administrator's group. **FMT_MSA.3** satisfies this security objective by enforcing the access control policy to provide restrictive default values for security attributes.
O.Audit: Audit Report Management The TOE must provide the ability to generate, display, store, and print all outcomes of the overwrite and verify operations in the form of an audit report.	**FAU_ARM.1** satisfies this security objective by providing an audit report upon the completion of an overwrite or verify function being performed.
O.Authorization: Authorization of a User The TOE must authorize users attempting to access the TOE, and ensure that only users authorized as UID 0 are provided access to the TOE.	**FIA_UID.1-NIAP-0405** satisfies this security objective by restricting the actions a user may perform before they are identified. **FMT_SMR.1** satisfies this security objective by associating users with roles.
O.Overwrite: Overwrite Operation The TOE must overwrite all information within a disk or partition rendering the information unrecoverable by any disk recovery program.	**FDP_OOP.1** satisfies this security objective by providing the capability to overwrite a partition or hard disk.

Security Objectives for the TOE	TOE Security Functional Requirements
O.Verify: Verify Operation The TOE must provide the capability to verify that a disk or partition was successfully overwritten.	**FDP_VOP.1** satisfies this security objective by verifying that a partition or hard disk was successfully overwritten.

8.2.4 Explicitly Stated Security Functional Requirements Justification

This section identifies the appropriateness for the three explicitly stated requirements of the TOE, and the explicitly stated requirement for the environment of the TOE.

Table 9: Explicitly Stated Requirements for the TOE

FAU_ARM.1: Audit Report Management *The TSF shall generate audit reports upon completion of an overwrite or verification operation that has been performed.* *The TSF shall provide capabilities to display and store the audit reports that are generated.*	*FAU_ARM.1 was explicitly stated because the functionality alone is not intended to meet FAU_GEN, in that it does not provide time stamping or record the start-up and shutdown of the audit function. In addition, it does not record user ID since there is only one user defined to access the TOE which is UID 0. Therefore, an explicit requirement was stated to provide definition to the intended functionality of the Audit Report Management function.*
FDP_OOP.1: Overwrite Operation *The TSF shall overwrite disks and partitions.*	*FDP_OOP.1 was explicitly stated 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 since the functionality provided by the overwrite operation is intended for protecting data thru securely overwriting the data making it unrecoverable. This type of data protection is useful for systems containing classified or secret information that is not to be disclosed, but destroyed.*
FDP_VOP.1: Verify Operation *The TSF shall verify the successful overwrite of a disk or partition.*	*FDP_VOP.1 was explicitly stated 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 could be possible that the overwrite operation did not perform completely. Therefore, leaving user data recoverable by an attacker.*

8.2.5 Requirements are Justified

The following table provides a cross reference for each security functional requirement within this ST and their dependencies, showing overall that all requirements are satisfied.

Table 10: Security Functional Requirements Dependencies Mapping

Security Functional Requirements	Dependencies
FDP_ACC.1	FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416
FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416	FDP_ACC.1, FMT_MSA.3
FIA_UID.1-NIAP-0405	*No Dependencies*
FMT_MOF.1	FMT_SMR.1
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1
FMT_SMR.1	FIA_UID.1-NIAP-0405
FAU_ARM.1	FDP_OOP.1, FDP_VOP.1
FDP_OOP.1	*No Dependencies*
FDP_VOP.1	FDP_OOP.1

8.3 TOE Summary Specification Rationale

8.3.1 Security Functions Satisfy Functional Requirements

The following table represents a mapping between the security functions identified in Section 6.1 to their related security functional requirements identified in section 5.1.

Table 11: Mapping of Security Functions to Security Functional Requirements

Security Functions (6.1)	Security Functional Requirements (5.1)
Access Control Function	FDP_ACC.1, FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMR.1
Audit Report Management Function	FAU_ARM.1
Identification Function	FIA_UID.1-NIAP-0405
Overwrite Function	FDP_OOP.1
Verification function	FDP_VOP.1

The access control function is suitable to meet FDP_ACC.1, FDP_ACF.1-NIAP-0405-NIAP-0407-NIAP-0416, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, and FMT_SMR.1 by controlling access to executing Los Altos Technologies UniShred Pro ® Version 3.3.1 and modifying or deleting the Los Altos Technologies UniShred Pro ® Version 3.3.1 configuration file and generated audit reports. The TOE restricts access to perform these functions to UID 0 or a user with the administrator's role.

The audit report management function is suitable to meet FAU_ARM.1 by providing the capability to generate, store, and display audit reports.

The identification function is suitable to meet FIA_UID.1-NIAP-0405 by providing the capability for a user to identify themselves.

The overwrite function is suitable to meet FDP_OOP.1 by providing the capability to overwrite a hard disk.

The verification function is suitable to meet FDP_VOP.1 by providing the capability to verify that a hard disk has been overwritten.

8.3.2 Assurance Measures Meet Assurance requirements

The following table represents the assurance requirements for an assurance level of EAL 1, along with a mapping of the assurance measures (UniShred Pro ® documentation) that are required to demonstrate the product's conformance to an EAL 1 assurance level.

Table 12: Assurance Measures that Fulfill Assurance Requirements (EAL1)

Assurance Requirements:	Assurance Requirement Description:	Assurance Measures: (UniShred Pro ® Documentation)
ACM_CAP.1.1D	The developer shall provide a reference for the TOE.	Los Altos Technologies UniShred Pro Version 3.3.1 HP HP/UX 9 HP HP/UX 10 HP HP/UX 11 IBM AIX 4 GNU Linux /w kernel 2.x SGI IRIX 6.5 SUN Solaris 2 SUN Solaris 7 SUN Solaris 8 SUN Solaris 9
ADO_IGS.1.1D	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.	UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1 Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For AIX Operating Systems Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For HP/UX Release 9 Operating System Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For HP/UX Release 10 and 11 Operating Systems Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For Linux Operating Systems Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For IRIX Version 6.5 Operating System Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For Solaris Operating Systems
ADV_FSP.1.1D	The developer shall provide a functional specification.	Informal Functional Specification and Correspondence Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.1 USP Program Design
ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.	Informal Functional Specification and Correspondence Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.1

Assurance Requirements:	Assurance Requirement Description:	Assurance Measures: (UniShred Pro ® Documentation)
AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.	Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1 UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual
AGD_USR.1.1D	The developer shall provide user guidance.	Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1 UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual
ATE_IND.1.1D	The developer shall provide the TOE for testing.	Los Altos Technologies UniShred Pro ® Version 3.3.1 products

Los Altos Technologies UniShred Pro Version 3.3.1, HP HP/UX 9, HP HP/UX 10, HP HP/UX 11, IBM AIX 4, GNU Linux /w kernel 2.x, SGI IRIX 6.5, SUN Solaris 2, SUN Solaris 7, SUN Solaris 8, and SUN Solaris 9 meet ACM_CAP.1.1D by providing a unique identification of all TOE components.

The UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual, Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1, Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For AIX Operating Systems, Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For HP/UX Release 9 Operating System, Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For HP/UX Release 10 and 11 Operating Systems, Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For Linux Operating Systems, Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For IRIX Version 6.5 Operating System, and Los Altos Technologies UniShred Pro ® Version 3.3.1 Installation Guide For Solaris Operating Systems meet ADO_IGS.1.1D by providing procedures necessary for the secure installation, generation, and start-up of the TOE.

The Informal Functional Specification and Correspondence Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.1, and USP Program Design meet ADV_FSP.1.1D by providing a high-level description of the user-visible interface and behavior of the TOE security functions.

The Informal Functional Specification and Correspondence Analysis for Los Altos Technologies UniShred Pro ® Version 3.3.1 meet ADV_RCR.1.1D by providing a correspondence between the various TOE security functions representations (i.e. TOE summary specification, functional specification) to address the correct and complete instantiation of the requirements to the least abstract TOE security functions representation.

Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1, and UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual meets AGD_ADM.1.1D by providing written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the TOE in a correct manner for maximum security.

Secure Installation, Generation, and Start-up Procedures for Los Altos Technologies UniShred Pro ® Version 3.3.1, and UniShred Pro ® Version 3.3 Disk Overwriting Software User's Manual meets AGD_USR.1.1D by providing material that is intended to be used by non-administrative human users of the TOE, and by others (e.g. programmers) using the TOE's external interfaces.

The Los Altos Technologies UniShred Pro ® Version 3.3.1 products meet ATE_IND.1.1D by devising and conducting tests with the objective of confirming that the TOE security functional requirements are met.

8.3.3 Validation of Strength-of-Function

No strength of function is specified for this security target

8.4 PP Claims Rationale

There are no protection profile claims for this security target.

9 References

9.1 Acronyms

This section provides a list of acronyms used within the ST

CC:	Common Criteria version 2.1 (IS 15408)
EAL:	Evaluation Assurance Level
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 ®

9.2 Interpretations

The following table identifies the national and international interpretations applied when constructing this ST. In addition, it identifies which requirements were affected by which interpretations.

Table 13: Interpretations

Interpretation:	Interpretation Description:	Requirements Affected by Interpretation:
National Interpretations		
NIAP-0405	American English Is An Acceptable Refinement	FDP_ACF.1 FIA_UID.1
NIAP-0407	Empty Selections Or Assignments	FDP_ACF.1
NIAP-0416	Association Of Access Control Attributes With Subjects And Objects	FDP_ACF.1