# Certification Report

# EAL 1 Evaluation of Entrust TrueDelete

**Version 4.0 (Build 4.0.5.403)**

Issued by:

**Communications Security Establishment**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**



**Evaluation number**: 1999-CGI-02
**Version**: 1.00
**Date**: 13 May, 1999
**Pagination**: i to iii, 1 to 9

# DISCLAIMER

The IT product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 0.6, for conformance to the Common Criteria for IT Security Evaluation, Version 2.0. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, is either expressed or implied.

# FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS for short) provides a third-party evaluation service for determining the trustworthiness of IT security products. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the CCS CB is accreditation to the requirements of the ISO Guide 25, General requirements for the accreditation of calibration and testing laboratories. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN) administered by the Standards Council of Canada.

By awarding a certificate a certifying body asserts, to some degree of confidence, that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification like document that also defines and scopes the evaluation activities. A consumer of certified IT products should review the ST, in addition to the certification report, to gain an understanding of any assumptions made during evaluation, the IT product's intended environment, its security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. The ST associated with this CR is identified by the following nomenclature:

Security Target for Entrust/TrueDelete (EAL 1)
CGI File number: CGI-ITSETF-99-01-ST-04
Issue number: 1.3
Dated: March 31, 1999

# TABLE OF CONTENTS

**Disclaimer** ..... **i**

**Foreword** ..... **ii**

**Table of contents** ..... **iii**

**Executive summary** ..... **1**

**1 Identification of Target of Evaluation** ..... **2**

**2 Security target** ..... **2**

**3 Security policy** ..... **2**

**4 Assumptions and clarification of scope** ..... **3**

4.1 USAGE ASSUMPTIONS ..... 3
4.2 ENVIRONMENTAL ASSUMPTIONS ..... 3
4.3 CLARIFICATION OF SCOPE ..... 3

**5 Architectural information** ..... **4**

5.1 OVERVIEW ..... 4
5.2 SYSTEM REQUIREMENTS ..... 4

**6 Documentation** ..... **4**

**7 ITS product testing** ..... **5**

**8 Evaluated configuration** ..... **5**

**9 Results of the evaluation** ..... **6**

**10 Comments, observations and recommendations** ..... **6**

**11 Glossary** ..... **8**

11.1 ABBREVIATIONS AND ACRONYMS ..... 8
11.2 VOCABULARY ..... 8

**12 References and bibliography** ..... **9**

# EXECUTIVE SUMMARY

Entrust TrueDelete version 4.0 (Build 4.0.5.403) for Windows 95 and Windows NT from Entrust Technologies Inc. is the Target of Evaluation (TOE) for this EAL 1 evaluation. Entrust/TrueDelete is a software program that is included with Entrust/ICE and with Entrust Enterprise Desktop. Entrust/TrueDelete makes deleted information unrecoverable in accordance with U.S. Department of Defense specifications [5] for file clearing (secure overwriting of file contents prior to file deletion). Entrust/TrueDelete accomplishes this via a single write over the complete contents of a deleted file and the Windows 95 swap. The threat is that an unauthorized user may access information on a hard disk believed deleted by the owner of that information.

The Common Criteria Evaluation Facility (CCEF) that conducted the evaluation of Entrust/TrueDelete is the CGI Information Technology Security Evaluation and Test Facility, a facility within CGI Information Systems and Management Consultants Inc. regional office in Ottawa, Ontario. The evaluation commenced on February 1st, 1999 and was completed on March 31st, 1999.

The evaluation of Entrust/TrueDelete has determined that the TOE can be trusted, to a level of assurance of **EAL 1**, to conform to the requirements of the Security Target (ST) [6]. The TOE is CC Part 2 conformant (functional requirements from CC Part 2 only) and CC Part 3 conformant (assurance requirements from CC Part 3 only).

The evaluated configuration is the default configuration installed in accordance with the supplied guidance.

The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (the Canadian CCS). The Canadian CCS has established a Certification Body that is managed by the Communications Security Establishment (CSE). The evaluation was performed using the Common Criteria (CC) [1], applied using the Common Methodology for Information Technology Security Evaluation (CEM) [3][4].

The scope of the evaluation is defined by the ST [6], which identifies assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers of Entrust/TrueDelete are advised to verify that their own environment is consistent with the ST [6], and to give due consideration to the comments, observations and recommendations stated in this report.

# 1 Identification of Target of Evaluation

The Target of Evaluation (TOE), the subject of this certification report, is the Entrust Technologies "Entrust/TrueDelete version 4.0" program (Build 4.0.5.403), a component of Entrust/ICE version 4.0 and Entrust/Enterprise version 4.0 Desktop Client[1]. This product is intended for use on a PC (desktop, laptop, or notebook) running either Windows 95 (version 4.00.950a or higher) or Windows NT 4.0 (or higher).

# 2 Security target

The ST associated with this CR is identified by the following nomenclature:

Security Target for Entrust/TrueDelete (EAL 1)
CGI File number: CGI-ITSETF-99-01-ST-04
Issue number: 1.3
Dated: March 31, 1999

# 3 Security policy

Some users may not realize that performing a typical delete function on a file in Microsoft Windows 95 and Microsoft Windows NT does not necessarily delete the information contained in that file. The delete function simply removes the directory pointers to that information, leaving the information accessible on the computer (using disk-editing tools) until new information is saved overtop of the original disk space. The threat is that an unauthorized user may access information on a hard disk believed deleted by the person who owns, or is responsible for, that information.

Entrust/TrueDelete was created to counter that threat. Entrust/TrueDelete makes deleted files unrecoverable by meeting U.S. Department of Defense specifications [5] for file clearing (secure overwriting of file contents prior to file deletion).

Entrust/TrueDelete performs a single write over the file contents of deleted files. Files may be deleted explicitly by users using any of the available methods provided by Windows for this function, such as the delete key, or may be deleted unbeknownst to the user by applications that use temporary files during the course of their normal operations.

[1] TrueDelete is not available to consumers as a separate product, but as a component of Entrust/ICE and Entrust Enterprise.

Entrust/TrueDelete overwrites the Windows 95 swap file upon system shutdown so that information stored in virtual memory also cannot be retrieved. In the case of Entrust/TrueDelete for Windows NT, the operating system overwrites hard disk storage allocated for virtual memory paging files upon re-allocation of that storage. Hence the need for similar functionality in Entrust/TrueDelete for Windows NT is eliminated. Note, however, there may be a period of time before virtual memory storage is overwritten presenting an opportunity to retrieve information that has been swapped to disk. This period of time varies and depends upon system resources and usage.

# 4 Assumptions and clarification of scope

The security aspects of the environment/configuration in which the IT product is expected to be used is included in this section.

## 4.1 Usage assumptions

It is assumed that Entrust/TrueDelete will be installed and configured using the supplied guidance documentation and that the minimum hardware requirements will be satisfied.

## 4.2 Environmental assumptions

It is assumed that Entrust/TrueDelete will be used only to make files unrecoverable under a PC's normal operating conditions, or using disk editors, but not to declassify floppy or hard disks. Organizational security procedures must be in effect that prevent the loss of the floppy or physical disk media, which would enable the conduct of laboratory attacks on disk media that exploit magnetic remanence. Retaining the disk media under positive inventory control and storage until ready for disposal, and the destruction of the media at that time, are recommended. Disks that have at any time been used for the storage of sensitive information must never be released into an uncontrolled environment (i.e., sold or given, while in a usable state, to unauthorized persons/organizations for their intended re-use or disposal).

## 4.3 Clarification of scope

Deleting a file in many operating systems does not result in the deletion of the stored information but rather results in the deletion of file directory pointers to that information. The information is still accessible using disk editing tools until new information is written overtop of the file's original storage location. The threat is that an unauthorized user may access information or resources without having permission from the person who owns, or is responsible for, the information. Entrust/TrueDelete was created to counter that threat.

Entrust/TrueDelete overwrites files when deleted so that they cannot be read using disk editors. Entrust/TrueDelete does not provide access control to files or otherwise ensure their availability, integrity or confidentiality beyond that provided by the overwriting of deleted files.

Entrust/TrueDelete may not be sufficient to protect against laboratory attacks on disk media that exploit magnetic remanence.

# 5 Architectural information

## 5.1 Overview

Entrust/TrueDelete is a software program that is included with Entrust/ICE and with Entrust Enterprise Desktop for Microsoft Windows 95 and Microsoft Windows NT environments. Entrust/TrueDelete performs a single write over file contents upon file deletion. This includes overwriting temporary files deleted by applications and the Microsoft Windows 95 swap file upon system shutdown.

## 5.2 System requirements

The following are the minimum system requirements needed to support the operation of Entrust/TrueDelete:

- 486 processor (Pentium-class recommended);
- 1 MB disk space;
- 16 MB RAM;
- Microsoft Windows 95, version 4.00.950a or higher or Microsoft Windows NT 4.0 or higher; and

Entrust/TrueDelete does not require an Entrust profile.

# 6 Documentation

The installation, administration and user guidance for TrueDelete 4.0 comprises guidance documentation and "readme" files that accompanies Entrust/ICE version 4.0 and Entrust/Enterprise version 4.0 Desktop Client. This is because TrueDelete is not available to consumers as a separate product, but as a component of Entrust/ICE and Entrust Enterprise.

# 7 ITS product testing

All testing in support of the evaluation was performed by the CCEF.

Testing involved creating and deleting test files containing unique (for each test) key words with Entrust/TrueDelete on and off and in each circumstance analyzing the storage media with a disk editor to determine whether the test data was actually overwritten or not. Overwriting of deleted persistent files, temporary files and, in the case of Windows 95, the swap file was verified by testing. Detailed practical test procedures are described in the Test Plan attached to the Evaluation Technical Report and provided to the CCS Certification Body.

Two PCs were used for the purpose of performing evaluation tests. The first PC, an IBM 390 Series Pentium 233 MHz notebook computer with 64 MB RAM and a 3.02GB hard disk was used as the Test PC. The hard disk was configured as a dual-boot/dual-partition environment with each operating system configured to run independently from its own partition. This computer was used to perform the TrueDelete operations in the Windows 95 and Windows NT environments. The second PC, an IBM iSeries Pentium 266 MHz notebook computer with 64 MB RAM and a 3.02GB hard disk was used to run a disk editing utility. This utility was used to view the contents of floppy disks after each file deletion test was performed (this utility was also loadable by bootable diskette and used view the hard disk contents of the first PC). Both computers were equipped with identical 3.5 inch 1.44 megabyte floppy disk drives.

Entrust/ICE version 4.0, including Entrust/TrueDelete, was installed in both the Windows 95 partition and the Windows NT partition using the default settings. Microsoft Office 97 was also installed in both partitions to provide an application for the creation and modification of data files for the tests.

The testing results were favorable. Observations that may be useful to the consumer of this product noted during testing are described in section 10, Comments, observations and recommendations.

# 8 Evaluated configuration

The evaluated ITS product is the Entrust Technologies “Entrust/TrueDelete version 4.0” program (Build 4.0.5.403), a component of Entrust/ICE version 4.0 and Entrust/Enterprise version 4.0 Desktop Client. This product is intended for use on a PC (desktop, laptop, or notebook) running either Windows 95 or Windows NT 4.0.

The evaluated configuration is the default configuration installed in accordance with the supplied guidance.

# 9 Results of the evaluation

The evaluation of Entrust/TrueDelete has determined that the TOE can be trusted, to an **EAL 1** level of assurance, to conform to the requirements of its ST. The TOE is CC Part 2 conformant (functional requirements from CC Part 2 only) and CC Part 3 conformant (assurance requirements from CC Part 3 only).

EAL 1 provides a basic level of assurance by an analysis of the security functions described in a functional specification [11] and guidance documentation to understand the security behavior. Independent testing of the TOE security functions supports the analysis.

# 10 Comments, observations and recommendations

This section is used to impart additional information of possible interest to the consumer learned by the evaluator during the course of the evaluation.

1. It is recommended that organizations establish their own security policy to specify the maximum sensitivity level of information for which it is appropriate to clear using Entrust/TrueDelete.

2. Entrust/TrueDelete version 4.0 is designed and advertised as meeting the US Department of Defense requirements for clearing secondary storage media by the overwriting procedure defined in NCSC-TG-025 [5]. The vendor only claims that the TOE meets the NCSC-TG-025 file clearing requirement (single overwrite) and not the file purging (multiple overwrite) requirement. There remains some concern that the claim of NCSC-TG-025 compliance for file clearing could easily be misinterpreted by users as meeting the more stringent purging requirement. Entrust/TrueDelete is intended for use only to make files unrecoverable under a PC's normal operating conditions, not to declassify floppy or hard disks. Retaining the disk media under positive inventory control and storage until ready for disposal, and the destruction of the media at that time, are recommended.

3. While testing Entrust/TrueDelete in the presence of an active undelete program, the evaluator observed that when a file was created and subsequently deleted, data from the file was still recoverable. Testing with both TrueDelete and an undelete program active verified that deleted information is recoverable from numerous hard disk locations. Further testing indicated that the undelete program prevents a "true delete" of the file by making one or more copies of the file. Although the original file is overwritten properly by TrueDelete, the copies made by the undelete program are not. While this is a logical outcome of having an undelete program active while TrueDelete is active, it may not be immediately apparent to some users.

4. Entrust/TrueDelete does not overwrite file names. As a result, it is possible that sensitive information may reside on the hard disk after deletion with Entrust/TrueDelete active if the file name comprises sensitive information. This may occur, for example, if a user accepts a file name that is based on the files contents suggested by an application when first saving a new file. An example of an application that provides such a feature is MSWord 97.

# 11 Glossary

This section expands upon abbreviations and acronyms, and defines vocabulary used in a special way to help increase the readability of this report.

## 11.1 Abbreviations and acronyms

| | |
|---|---|
| CB | Certification Body |
| CC | Common Criteria for Information Technology Security Evaluation |
| CCEF | Common Criteria Evaluation Facility |
| CCS | Common Criteria Evaluation and Certification Scheme |
| CEM | Common Methodology for Information Technology Security Evaluation |
| CR | Certification Report |
| CSE | Communications Security Establishment |
| EAL | Evaluation Assurance Level |
| IT | Information Technology |
| PALCAN | Program for the Accreditation of Laboratories Canada |
| ST | Security Target |
| TOE | Target of Evaluation |

## 11.2 Vocabulary

*Paging*: A virtual memory technique employing predefined sized blocks of memory, or pages. Windows NT uses such virtual memory technique.

*Swap file*: A file located on a hard disk used in a virtual memory scheme. Windows 95 employs a swap file in its virtual memory scheme.

*Target of evaluation*: The product, products or product subset that is the focus of evaluation activities defined by the assurance requirements.

*Temporary files*: short-lived files created by some applications to provide features such as "undo" while a user creates and modifies a document. Temporary files are generally deleted by the application that created them when a user has closed the related data file.

*Virtual memory*: A method to effectively increase the size of main memory beyond the physical size by augmenting with storage on a hard disk.

# 12 References and bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

1. Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998;
2. CCS#4, Technical oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), version 0.82 - Draft;
3. Common Methodology for Information Technology Security Evaluation, CEM-97/017, Part 1: Introduction and general model, Version 0.6, 11 January 1997;
4. Common Methodology for Information Technology Security Evaluation, CEM-99/008, Part 2: Evaluation methodology, Version 0.6, January 1999;
5. A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025, Library No. 5-236,082, Version-2;
6. Security Target for Entrust/TrueDelete (EAL 1), CGI-ITSETF-99-01-ST-04, issue number 1.3, March 31, 1999;
7. Evaluation Technical Report, CGI-ITSETF-99-01-ETR-02, March 31, 1999;
8. Evaluation Test Plan For Entrust/TrueDelete™ (EAL 1), CGI-ITSETF-99-01-ETP-01, 29 March 1999;
9. Preliminary Certification Report for Entrust/TrueDelete (EAL 1), CGI-ITSETF-99-01-PCR-02, 31 March 1999.
10. CGI ITSETF - Trial Evaluation Lab Log, Entrust/TrueDelete (EAL 1), 31 March 1999;
11. Entrust/TrueDelete version 4.0 Functional Specification;