Certification Report

EAL 4+ Evaluation of Entrust Inc.

Entrust Authority Security Manager 7.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-11
Version:	1.0
Date:	15 November 2004
Pagination:	*i* to *iv*, *1* to *15*

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. This certification report and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

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

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, 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.

The CCEF that carried out this evaluation is DOMUS IT Security Laboratory, located in Ottawa, Ontario, Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 15 November 2004, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Windows 2000 which is a registered trademark of Microsoft Corporation; Intel and Pentium which are registered trademarks of Intel Corporation; Entrust Entelligence which is a registered trademark of Entrust Inc.; and Informix which is a registered trademark of IBM Corporation.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The Entrust Authority Security Manager 7.0, from Entrust Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Entrust Authority Security Manager 7.0, hereafter referred to as **Entrust Authority**, is designed to manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization. As the organization's Certification Authority (CA) system, Entrust Authority Security Manager software enables the use of digital signature, digital receipt, encryption and permissions management services across a wide variety of applications and solutions.

Entrust Authority Security Manager represents the centerpiece of the Entrust Authority products portfolio, built specifically to:

- securely store the certification authority (CA) private key
- issue certificates for users and devices
- publish user and application certificate revocation lists (CRLs) to allow verifiable communications
- maintain an auditable database of users' private key histories for recovery purposes in the event that users lose access to their keys
- Publishes the public keys with the user’s identification as certificates in open bulletin boards (e.g., X.500 directory services).

DOMUS IT Security Laboratory is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 27 October 2004, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Entrust Authority, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of Entrust Authority are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The following augmentation is claimed:

- ALC_FLR.2 – Flaw Reporting Procedures.

Entrust Authority conforms to the *Certificate Issuing and Management Components Family of Protection Profiles, Security Level 3, Version 1.0, 31 October 2001 (CIMCPP-SL3).*

The Communications Security Establishment, as the CCS Certification Body, declares that the Entrust Authority Security Manager 7.0 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the Entrust Authority Security Manager 7.0, from Entrust Inc.

2 TOE Description

Entrust Authority Security Manager 7.0, hereafter referred to as **Entrust Authority**, is a Certificate Issuing and Management Component (CIMC) system. A CIMC is a cryptographic key and certificate delivery and management system that makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. Entrust Authority enables the use of digital signature, digital receipt, encryption, and permissions management services across a wide variety of applications by providing:

- Security audit that includes a chronological logging of events to act as a deterrent against security violations;
- Protection of a user's private and public keys, and CIMC secret keys against unauthorized modification and disclosure;
- Key management and operational use of cryptographic keys;
- Protection of user data including certificate issuance, revocation, backup and recovery, and profile management of certificates and Certificate Revocation List (CRL);
- Identification and Authentication that supports the administration and enforcement of access control policies to unambiguously identify the person and/or entity performing functions on the CIMC;
- Management of security functions including distinct roles to maintain the security of the CIMC;
- Functions that manage and protect the integrity of confidential data from disclosure and modification through the use of encryption, reliable time stamps, backup and recovery procedures, self-tests and audit logs; and
- Protection from modification and disclosure of transmitted data by means of a secure communications path between the CIMC and local and remote users.

This enables organizations to establish and maintain enhanced secure networking environments for internal and external relationships.

A high-level view of Entrust Authority is presented in Figure 1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Entrust Authority is identified in Section 5.2 of the ST.

The cryptographic module, Entrust Security Kernel Version 7.0, is used by Entrust Authority; and has been validated to FIPS 140-1 Security Level 2 (FIPS 140-1 Certificate #308) under the Cryptographic Module Validation Program (CMVP). This included validating the following Government of Canada approved algorithms for correct implementation:

- Data Encryption Standard (DES), FIPS 46-3 Certificate #56;
- Triple-DES, FIPS 46-3 Certificate #6;
- Advanced Encryption Standard (AES), FIPS 197 Certificate #10;
- HMAC-SHA-1, FIPS 186-2 Certificate #10;
- DSA/SHA-1, FIPS 186-2 Certificate #10; and
- DES-MAC[2].

The following approved Government of Canada algorithms were explicitly tested as part of this evaluation, with assistance provided by CSE, as they were outside of the scope of the CMVP:

- CAST5;
- Diffie-Hellman;
- Elliptic Curve Digital Signature Algorithm (ECDSA); and
- RSA.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

[2] Confirmation that DES-MAC is correctly implemented is done through a code review, and does not result in a validation certificate issued by the CMVP.

Title: Security Target for Entrust Authority Security Manager 7.0
Version: 1.7
Date: August 6, 2004

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*, incorporating all final Common Criteria interpretations issued prior to Nov 20, 2003. Entrust Authority is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;
b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c) Common Criteria EAL 4 augmented, with all the security assurance requirements in the EAL 4, as well as the following:
    - ALC_FLR.2, Flaw Reporting Procedures

Entrust Authority conforms with *Certificate Issuing and Management Components Family of Protection Profiles Security Level 3, Version 1.0, 31 October 2001 (CIMCPP-SL3).*

6 Security Policy

The security policy for Entrust Authority includes the following components: Access Control; Separation of Duties; Identification and Authentication (I&A); Key Management; Audit; Self-Test; Trusted Path; Recovery; and Domain Integrity.

6.1 Access Control security policy

The Access Control security policy requires that Entrust Authority security functions shall:

- Control the access of data objects to authorized operators, end users, and external Certificate Authorities (CAs);
- Ensure that access controls apply to all services and the data objects associated with those services;
- Ensure that access controls are based on the identity, state, and role of operators, end users, and external CAs; and
- Ensure that access rights to services by operators, end users, and external CAs are supported by the I&A and Separation of Duties services.

6.2 Separation of Duties security policy

The Separation of Duties security policy requires that Entrust Authority security functions shall:

- Ensure that services are available to the following defined roles: Master User, Security Officer, Auditor, Administrator, Directory Administrator, and custom-defined roles; and
- Enforce the permissions assigned to operators, end users and external CAs.

6.3 Identification & Authentication security policy

The I&A security policy requires that Entrust Authority security functions shall:

- Provide an I&A mechanism to uniquely verify the identity of operators, end users, and external CAs attempting to access services;
- Ensure that requests from operators are only initiated once I&A has been successfully performed;
- Provide for each operator, end user, and external CA, a set of security attributes necessary to enforce the I&A security policy;
- Ensure that the I&A data is protected from unauthorized access, modification, and/or destruction; and
- Ensure that successful I&A results are recorded in the audit log.

6.4 Key Management security policy

The Key Management security policy requires that the Entrust Authority security functions shall:

- Ensure that cryptographic keys and certificates stored in the database or distributed to users, operators, and external CAs, are protected for authenticity, confidentiality, and integrity;
- Ensure that end user private signing keys are never retained; and
- Ensure that all cryptographic operations such as key generation, key destruction, encryption/decryption, signature generation and verification, hashing, and random number generation are performed in a FIPS 140-1 validated cryptomodule.

6.5 Audit security policy

The Audit security policy requires that the Entrust Authority security functions shall:

- Provide an Audit mechanism that allows for the monitoring and recording of a pre-defined set of security-relevant events and cannot be turned off;
- Ensure that unauthorized modification of the audit trail is detected;
- Record within the audit trail information pertaining to the date, time, location, type, and success or failure of each audited event; and provide sufficient information to discern the identity of the users, processes and/or objects involved in each security relevant event; and
- Provide an Audit viewer mechanism to allow viewing and analysis of recorded security-relevant events.

6.6 Self-Test security policy

The Self-Test security policy requires that the Entrust Authority security functions shall:

- Ensure that the self-test mechanism is run upon start-up;
- Ensure that the self-test mechanism is run periodically in order to validate the correct operation of critical functions, and on demand by authorized operators to validate correct operation;
- Ensure that if a self-test fails, an error state is entered requiring manual intervention before normal operations can be resumed; and
- Ensure that failure of a self-test is considered a security relevant event and is recorded within the audit log.

6.7 Trusted Path security policy

The Trusted Path security policy requires that the Entrust Authority security functions shall:

- Provide a communications path for operators, end users and external CAs that is logically distinct from other communication paths;
- Ensure that the communications path provides assured I&A;
- Ensure that the communications path provides protection against modification or disclosure; and
- Ensure that the applicable operator, end user, or external CA will initiate communications in the appropriate path.

6.8 Recovery security policy

The Recovery security policy requires that the Entrust Authority security functions shall:

- Ensure that a known trusted state can be returned to after a failure or service discontinuity; and
- Ensure that Entrust Authority enters a state where only authorized operators can return it to normal operation using a manual procedure.

6.9 Domain Integrity security policy

The Domain Integrity security policy requires that the Entrust Authority security functions shall:

- Ensure that Entrust Authority services are only accessible through specified interfaces; and
- Ensure that the security policy enforcement functions are invoked and succeed before any security related operation is allowed to proceed.

7 Assumptions and Clarification of Scope

Consumers of Entrust Authority should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of Entrust Authority.

7.1 Secure Usage Assumptions

The following are assumptions about the secure usage of Entrust Authority:

- Security-relevant events are audited and the resulting audit logs are reviewed by the Auditors;
- An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.);
- Competent Administrators, Officers and Auditors are assigned to manage Entrust Authority and the security of the information it contains;
- All Administrators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which Entrust Authority is operated;
- Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility);
- Malicious code destined for Entrust Authority is not signed by a trusted entity;
- Administrators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data;
- Users, Administrators, Officers and Auditors are trained in techniques to thwart social engineering attacks; and
- Users act in a cooperative manner.

7.2 Environmental Assumptions

The following are assumptions about the environment Entrust Authority is to be used in:

- The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the *CIMCPP-SL3* protection profile;

- Entrust Authority is physically protected; and
- The hardware, software, and firmware critical to security policy enforcement are protected from unauthorized physical modification.

For more information about the Entrust Authority security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

Entrust Authority does provide comprehensive countermeasures to ensure that unauthorized users cannot compromise the cryptographic key and certificate delivery and management system. However, it should operate in a physically secure environment where access is permitted only to authorized individuals. It does not counter threats related to deliberate, compromising actions performed by an authorized administrative user, such as installation of a Trojan Horse on the host(s) running Entrust Authority to capture Master User passwords.

8 Architectural Information

Entrust Authority is composed of the following interdependent software components: *Security Manager, Security Manager Control, Security Manager Service (Monitor), Security Manager Core,* and *Security Manager Administration (SMA)*. *Security Manager Control* and *SMA* provide human interfaces to *Security Manager*.

Security Manager is the Certification Authority (CA) and core component of the Entrust Authority system. It is responsible for creating encryption key pairs for users, creating certificates for all public keys, enforcing the organization's security policy and various other capabilities that enhance the security of an organization.

Security Manager Control is used to manage *Security Manager* itself, that is, to perform the initial configuration of *Security Manager* based on data provided during software setup, to verify the integrity of the database, to schedule backups of the database, and to perform exceptional Public Key Infrastructure (PKI) management events such as PKI operator recovery. In other words, *Security Manager Control* provides the interface into initialization and maintenance services, as well as certain support and operator management services.

The *Security Manager Service (Monitor)* executable is used to launch and monitor the following modules: Secure Exchange Protocol (SEP), Certificate Management Protocol (PKIX-CMP), Administration Service (AS), Database Backup, Database Integrity, CRL Writing, and Keygen (key generation). These modules make use of the functionality provided by *Security Manager Core*.

The *Security Manager Core* implements and performs all PKI core functions. It implements database access and makes use of the Entrust Security Kernel Version 7.0 cryptographic module to perform all cryptography-related *Security Manager* functions, such as CA signing key pair generation, certificate signing, and end-entity encryption key pair generation. It is also responsible for all key generation (including pre-generation of public key pairs on behalf of Keygen), use, protection, and destruction.

SMA manages PKI identities and their key material by providing an interface into end-entity management, operator management, policy management services, and certain support services. *SMA* uses EntrustSession to establish a confidential and mutually authenticated session with *Security Manager,* so *SMA* can be installed and executed on any computer server or workstation, including the *Security Manager* host. Typically though, *Security Manager* will be installed in a physically secure restricted-access area, while *SMA* will be installed on a workstation located with convenient operator access in mind, such as on an operator's desktop machine.

All these components work together to manage end-entity public-key certificates, including creating and issuing certificates, Certification Revocation Lists (CRLs), and Authorization Revocation Lists (ARLs) and publishing them in a X.500 public directory. In addition, these components provide the infrastructure functions that are necessary for maintaining end-entity encryption key-pair history and end-entity verification certificate history, providing automatic public key and certificate updates, auditing security-related events, and maintaining CA data confidentiality and integrity.

9 Evaluated Configuration

The evaluated configuration for Entrust Authority is comprised of:

1. *Security Manager* running on a Windows® 2000 Server operating system with Service Pack 3, NTFS file system, Informix® Dynamic Server 2000, and Critical Path 4.0 LDAP directory; and

2. *SMA* running on a Windows® 2000 Professional, Windows® 2000 Server, or Windows® 2000 Advanced Server with Entrust Entelligence™ 6.0.

10 Documentation

The documentation for Entrust Authority consists of:

- Entrust Authority Security Manager Administration 7.0 Installation Guide;
- Entrust Authority Security Manager Administration 7.0 User Guide;
- Entrust Authority Security Manager 7.0 Installation Guide for Windows; and
- Entrust Authority Security Manager 7.0 Operations Guide for Windows.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Entrust Authority, including the following areas:

Configuration management: An analysis of the Entrust Authority development environment and associated documentation was performed. The evaluators found that Entrust Authority configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Entrust Authority during distribution to the consumer. In addition, the documentation described the various procedures and technical measures used to detect modifications or discrepancies to Entrust Authority. The evaluators determined that the delivery documentation described the various mechanisms and procedures used to detect masquerading. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Entrust Authority functional specification, high-level design, low-level design and a subset of the implementation representation; they determined that the documents were internally consistent and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Entrust Authority user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Entrust Authority design and implementation. The evaluators also assessed the flaw remediation procedures, which provide for the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to users. In addition, the evaluators assessed the developer's life-cycle definition, including tools and techniques employed in the development and maintenance of Entrust Authority.

Vulnerability assessment: The evaluator analyzed the administrator guidance to ensure the absence of ambiguities that could result in inadvertent misuse of Entrust Authority. In addition, the strength of function claim was validated through independent evaluator analysis. Finally, the evaluator also validated the developer’s vulnerability analysis, performed an independent vulnerability analysis, and developed penetration tests that focused on potential vulnerabilities in Entrust Authority.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL4 consists of the following activities: assessing developer tests; designing independent functional tests and penetration tests based on knowledge obtained from guidance documentation, design documentation, and the developer’s test documentation; performing independent functional tests; sampling the developer’s tests; and performing independent penetration tests.

12.1 Assessing Developer Tests

The developer provided test documentation, which consisted of a test suite, and test coverage and depth analyses. The evaluator verified that the developer’s functional test documentation was sufficient to demonstrate that security functions perform as specified, and that the security functionality has been systematically tested against the functional specification and high-level design.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a large sample of the developer's test cases, and creating test cases that augmented the developer tests.

The tests focused on the following areas, based upon the security functional requirements in the ST and the security functions defined in the functional specification:

- Security audit;
- Role definition and management of security functions behaviour;
- Backup and recovery;
- Access control;
- Identification and authentication;
- Remote data entry and export;

- Certificate management; and
- Key management.

12.3 Independent Penetration Testing

During this evaluation, the evaluator developed independent penetration tests based on the Entrust Authority vulnerability analysis and strength of function analysis, as well as the functional specification, high-level design, low-level design, implementation representation, guidance documentation, and installation guidance.

The penetration tests focused on:

- Port scanning;
- Traffic interception, alteration, and replay;
- Direct access to database;
- Memory scan;
- System time change; and
- Audit change.

12.4 Conduct of Testing

Entrust Authority was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Testing facility at DOMUS IT Security Laboratory located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the Evaluation Technical Report (ETR)[3].

12.5 Testing Results

The evaluator's independent functional and penetration tests yielded the expected results, giving assurance that Entrust Authority behaves as specified in its ST and functional

[3] The Evaluation Technical Report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

specification. The independent functional testing resulted in a **PASS** verdict, as the evaluators were able to confirm that all security functionality was present and performed properly. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 4+** level of assurance, including the augmentation identified in Section 5 of this report. The overall verdict for the evaluation is a **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The infrastructure is critical to the security of the whole Entrust Authority Security Manager 7.0 system. It is strongly advised to ensure that the servers hosting the Entrust Authority infrastructure are physically and network-secure by installing *Security Manager* on a server separate from the machine that will host the third-party, Lightweight Directory Access Protocol (LDAP)-compliant Directory (although it is possible to install all components on the same server). Moreover, it is strongly recommended to install *SMA* on a machine separate from the server hosting the Entrust Authority infrastructure. It is also well advised to follow tips in the installation manual to secure the server and to apply a tamper-evident label to the server hosting the Entrust Authority infrastructure.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CA	Certification Authority
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CIMC	Certificate and Issuing Management Component
CR	Certification Report
CRL	Certificate Revocation List
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report

FIPS	Federal Information Processing Standard
I&A	Identification & Authentication
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
PKI	Public Key Infrastructure
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

16 References

This section lists all documentation used as source material for this report:

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Entrust Authority Security Manager 7.0 Security Target, Version 1.7, 6 August 2004.

e) Entrust Authority Security Manager 7.0 Evaluation Technical Report (ETR), Version 0.8, 27 August 2004.

f) Addendum to Evaluation Technical Report, Version 0.2, 27 October 2004.