[redacted]

Entrust Technologies

Security Target

Entrust/RA 5.1

Authors: Darryl Stal
Date: November 14, 2000
Version: 1.2

© Entrust Technologies Limited, 2000.

Entrust is a registered trademark of Entrust Technologies Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Technologies Limited. All other Entrust Technologies product names and service names are trademarks of Entrust Technologies. All other company and product names are trademarks or registered trademarks of their respective owners.

Document version control log

Version	Date	Author	Description
1.0	August 1, 2000	Darryl Stal	Initial draft of Entrust/RA 5.1 Security Target. Grouped SFRs in Section 5 by Functional Class.
1.1	November 13, 2000	Darryl Stal	Corrected reference in Footnote 4. Corrected typographical errors in Table 24 and Section 7.2.4.
1.2	November 14, 2000	Darryl Stal	Updated Windows NT service pack to SP6a.

-PROPRIETARY-

Table of contents

1 Introduction 1

1.1 ST Identification 1
1.2 ST Overview 1
1.3 CC Conformance Claim 2
1.4 Strength of Function Claim 2

2 TOE Description 3

2.1 Background 3
2.2 TOE Services 3
2.3 TOE High-Level Architecture 4
2.3.1 Entrust operator roles 4
2.3.2 Entrust/RA components 4
2.3.2.1 Entrust/RA GUI 4
2.3.2.2 ADM-API 5
2.3.2.3 EntrustSession Toolkit 5
2.3.3 TOE boundary 6
2.3.4 Exclusion from the TOE boundary 6
2.3.4.1 Entrust cryptographic module 6
2.3.4.2 Hardware and operating platform (abstract machine) 6

3 TOE Security Environment 9

3.1 Introduction 9
3.2 Secure Usage Assumptions 9
3.3 Threats to security 11
3.3.1 Threats addressed by TOE 12
3.3.2 Threats to be addressed by the operating environment 13
3.4 Organizational Security Policies 14

4 Security Objectives 15

4.1 TOE Security Objectives 15
4.2 Environmental Security Objectives 16

5 IT Security Requirements 17

5.1 TOE Security Functional Requirements 17
5.1.1 Security Audit (FAU) 17
5.1.1.1 FAU_SAR.1 Audit review 18
5.1.1.2 FAU_SAR.3 Selectable audit review 18
5.1.2 Cryptographic Support (FCS) 18
5.1.2.1 FCS_CKM.2 Cryptographic key distribution 18
5.1.2.2 FCS_CKM.3 Cryptographic key access 19
5.1.3 User data protection (FDP) 19
5.1.3.1 FDP_RIP.1 Subset residual information protection 19
5.1.3.2 FDP_UIT.1 Data exchange integrity 19
5.1.4 Identification & authentication (FIA) 19
5.1.4.1 FIA_AFL.1 Authentication failure handling 20
5.1.4.2 FIA_SOS.1 Verification of secrets 20
5.1.4.3 FIA_UAU.2 User authentication before any action 20
5.1.4.4 FIA_UAU.6 Re-authenticating 20
5.1.4.5 FIA_UAU.7 Protected authentication feedback 21
5.1.4.6 FIA_UID.2 User identification before any action 21

5.1.5 Protection of the TSF (FPT) 21
5.1.5.1 FPT_ITI.1 Inter-TSF detection of modification 21
5.1.5.2 FPT_RVM.1 Non-bypassability of the TSP 21
5.1.5.3 FPT_TDC.1 Inter-TSF basic TSF data consistency 22
5.1.6 TOE Access (FTA) 22
5.1.6.1 FTA_SSL.1 TSF-initiated session locking 22
5.1.6.2 FTA_SSL.2 User-initiated locking 22
5.1.7 Trusted Path/Trusted Channels (FTP) 23
5.1.7.1 FTP_ITC.1a Inter-TSF trusted channel 23
5.1.7.2 FTP_ITC.1b Inter-TSF trusted channel 23
5.2 TOE Environment Security Functional Requirements 23
5.2.1 Entrust/Authority 24
5.2.2 Key management 24
5.2.2.1 FCS_CKM.1 Cryptographic key generation 25
5.2.2.2 FCS_CKM.4 Cryptographic key destruction 26
5.2.2.3 FCS_COP.1 Cryptographic operation 26
5.2.3 Abstract machine services 27
5.2.3.1 FPT_SEP.1 TSF domain separation 27
5.3 TOE Security Assurance Requirements 28

6 TOE Summary Specification 31

6.1 IT Security Functions 31
6.1.1 Security Audit (FAU) 31
6.1.1.1 Audit review 31
6.1.1.2 Selectable audit review 31
6.1.2 Cryptographic Support (FCS) 31
6.1.2.1 Key distribution 31
6.1.2.2 Key access 31
6.1.3 User data protection (FDP) 32
6.1.3.1 Residual information protection 32
6.1.3.2 Data exchange integrity 32
6.1.4 Identification and authentication (FIA) 32
6.1.4.1 Authentication failure 32
6.1.4.2 User and operator password criteria 32
6.1.4.3 Authentication of users 32
6.1.4.4 Re-authentication of operators 32
6.1.4.5 Non-echoing of passwords 32
6.1.4.6 Identification of users 32
6.1.5 Protection of the TSF (FPT) 33
6.1.5.1 Data exchange integrity 33
6.1.5.2 Non-bypassability of security functions 33
6.1.5.3 Data consistency 33
6.1.6 TOE Access (FTA) 33
6.1.6.1 Entrust/RA-initiated session locking 33
6.1.6.2 Operator-initiated session locking 33
6.1.7 Trusted path/channels (FTP) 33
6.1.7.1 Trusted channel 33
6.2 Assurance Measures 33

7 Rationale 35

7.1 Security Objectives Rationale 35
7.2 Security Requirements Rationale 39
7.2.1 Suitability of security functional requirements 39
7.2.2 Dependency analysis 43

7.2.3 Demonstration of mutual support between security requirements..... 44
7.2.4 Appropriateness of assurance requirements 45
7.3 TOE Summary Specification Rationale..... 46
7.3.1 IT security functions rationale..... 46
7.3.2 Minimum Strength of Function Level rationale..... 47
7.4 Assurance measures rationale 47

8 Glossary..... 50

9 References..... 52

List of figures

Figure 1: Entrust/RA architecture 5

List of tables

Table 1: Security assumptions 9
Table 2: Security threats addressed by the TOE 11
Table 3: Security threats addressed by the TOE's environment 11
Table 4: Security policies 14
Table 5: Security objectives for the TOE 15
Table 6: TOE environment security objectives 16
Table 7: Security Audit security requirements 17
Table 8: Cryptographic Support security requirements 18
Table 9: User data protection security requirements 19
Table 10: Identification & authentication security requirements 19
Table 11: Protection of the TSF security requirements 21
Table 12: TOE Access security requirements 22
Table 13: Trusted path/trusted channels security requirements 23
Table 14: Required functional components provided by Entrust/Authority 24
Table 15: Required functional components provided by the FIPS 140-1 validated cryptographic module 24
Table 16: Required functional component provided by the abstract machine 24
Table 17: Key management (environmental) security requirements 25
Table 18: Abstract machine security requirements 27
Table 19: TOE assurance components 28
Table 20: Augmentation to EAL3 28
Table 21: Correct objectives - mapping security objective to rationale 35
Table 22: Complete functionality - mapping security objective to functionality 39
Table 23: Correct functionality – dependency mapping 43
Table 24: Security functions mapping 46
Table 25: Assurance measures 48

1 Introduction

1.1 ST Identification

Title: Security Target for Entrust/RA (component of Entrust/PKI 5.1)

Assurance level: EAL3-augmented (EAL3+)

Keywords: Commercial-off-the-shelf (COTS), registration authority, key management, cryptographic services, digital certificate management, public-key infrastructure, digital signature, encryption, confidentiality, integrity, networked information systems, baseline information protection.

1.2 ST Overview

1. This Security Target (ST) couples public key management functionality with assurances selected to provide a maximum amount of confidence consistent with existing best practices for COTS development.

2. Entrust/RA is an administrative interface to an Entrust public-key infrastructure. It is used by Security Officers, Administrators, Directory Administrators, Auditors, and custom-defined roles (with a customizable set of permissions) either remotely across a network or on the workstation that hosts Entrust/Authority. Primary uses for Entrust/RA include:

    - Adding and deleting users
    - Revoking certificates
    - Initiating key recovery operations

3. Security Officers, Administrators, and other Entrust/RA roles connecting to Entrust/Authority authenticate themselves using digital signatures. Once complete, all messages between Entrust/RA and Entrust/Authority are then secured for confidentiality, integrity, and authentication.

4. Cryptographic operations for Entrust/RA and Entrust/Authority are performed on the FIPS 140-1 (Level 2)-validated Entrust Security Kernel 5.1 cryptographic module or optional hardware cryptographic module.

5. Meeting the requirements established in this ST signifies that Entrust/RA:

    - Provides the functionality appropriate for controlling a community of benign (i.e., not intentionally hostile nor malicious) authorized users
    - Protects against unauthorized access by individuals other than authorized users
    - Provides reliable and standardized cryptographic services and supports standardized key management
    - Provides mechanisms for establishment of trusted data communication channels
    - Provides mechanisms to detect corrupted data objects

- Supports these capabilities in distributed system environments

6. Key environmental constraints that apply to the use of this product are:

    - Cryptographic operations, including key generation and key destruction, are performed on a FIPS 140-1 validated or equivalent cryptographic module.
    - Connections with an operational Entrust/Authority Certification Authority (CA) can be established and maintained
    - Authorized users recognize the need for a secure IT environment
    - Authorized users can be reasonably trusted to correctly apply the organization's security policies in their discretionary actions
    - The abstract machine is protected against unauthorized modification
    - Competent security administration is performed

7. When used in conjunction with appropriate environmental constraints, this TOE is suitable for both commercial and government real-world environments.

1.3 CC Conformance Claim

1. This TOE is:

    1) CC Version 2.1 Part 2-conformant

    2) CC Version 2.1 Part 3-augmented with:

    - ACM_SCP.2 (Problem Tracking Configuration Management Coverage);
    - ADV_SPM.1 (Informal TOE Security Policy Model);
    - ALC_FLR.2 (Flaw Reporting Procedures);
    - AMA_CAT.1 (TOE Component Categorization Report); and
    - AVA_MSU.2 (Validation of Analysis).

1.4 Strength of Function Claim

1. The overall Strength of Function (SoF) claim for Entrust/RA is **SoF - Medium**.

2 TOE Description

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

2.1 Background

1. The Entrust-based PKI is a cryptographic key and certificate delivery and management system which makes possible secure financial electronic transactions and exchanges of sensitive information between relative strangers. An Entrust-based PKI provides privacy, access control, integrity, authentication, and support for the non-repudiation process to support information technology applications and electronic commerce transactions. An Entrust-based PKI :

    - Manages the generation and distribution of public/private key pairs; and
    - Publishes the public keys with the user's identification as certificates in open bulletin boards (i.e., X.500 directory services).

2. Entrust/RA provides a trusted interface to Entrust/Authority functionality for Security Officers, Administrators, Directory Administrators, Auditors, and custom-defined roles. Entrust/RA uses EntrustSession to establish a confidential and mutually authenticated session with Entrust/Authority.

3. As the primary administrative interface into an Entrust-based PKI, Entrust/RA is used to perform all aspects of end-entity management, most aspects of operator management (some exceptional events are performed by Entrust/Master Control, a component of Entrust/Authority), and CA management, including cross-certification and registration of subordinate CAs, and may be used to perform many aspects of directory management as well. Entrust/RA provides other facilities, such as, troubleshooting PKI problems, viewing PKI configuration, and determining PKI status.

4. The two interfaces to Entrust/RA are its GUI and its bulk processing capabilities. All Entrust/RA capabilities are available from the GUI. Bulk processing supports most aspects of end-entity management as a subset of Entrust/RA's complete directory management capabilities.

2.2 TOE Services

1. Entrust/RA is a GUI which is the operator interface to Entrust/Authority functionality. Using Entrust/RA, operators perform various administrative tasks in the system. Security Officers set high-level electronic policies and perform infrequent tasks (e.g., cross-certification with other CA domains). Administrators perform the day-to-day duties involved in administering electronic identities for users. Directory administrators perform similar tasks as they apply to the Directory. Auditors review the audit files. The roles, including custom-defined (flexible) roles, are functionally divided, however, so that organizations can partition tasks among individuals according to their security policies.

2. The functionality provided by the Entrust/RA can be categorized into the following set of services:

    1) Trusted Interface to Entrust/Authority functionality: Entrust/RA's primary function is to provide a trusted interface for the aforementioned operators to

access Entrust/Authority services and their data objects. Together with Entrust/Authority, Entrust/RA creates and maintains a secure communications channel with Entrust/Authority to ensure that all communications traffic between the two products maintain data integrity and confidentiality.

2) **Directory Management:** Entrust/RA can access the directory to perform some directory management and search functions. Entrust/RA may locate entries for purposes of Entrust administration and may manage directory entries for purposes of directory and Entrust administration (e.g., to add or delete user and CA entries).

2.3 TOE High-Level Architecture

2.3.1 Entrust operator roles

1. Entrust/RA is the primary operator interface for day-to-day management of Entrust users and other Entrust operators. Hence, management of the Entrust configuration and Entrust users via Entrust/RA is assigned to the defined Entrust roles listed below and described in Section 2.3.1 (Entrust operator roles) of the **Security Target - Entrust/Authority [Reference 3]**.

    - Security Officer
    - Administrator
    - Directory Administrator
    - Auditor
    - AutoRA Administrator
    - Custom-defined (flexible) roles

2. It should be noted that there are two additional roles in Entrust, that of Master User and End User. These users types have no administrative access to Entrust/RA.

2.3.2 Entrust/RA components

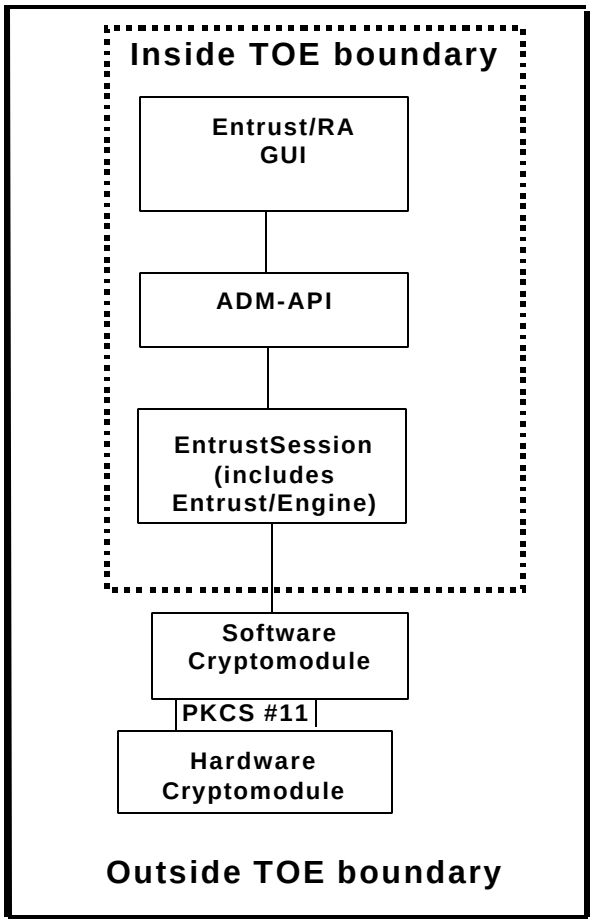
1. The Entrust/RA architecture is shown in Figure 1. As shown in this diagram, Entrust/RA uses ADM-API to invoke services offered by Entrust/Authority. Since ADM-API is itself an EntrustSession application, the session between Entrust/RA and Entrust/Authority is secured for confidentiality and integrity. Furthermore, session establishment serves to mutually authenticate the operator with Entrust/Authority . Based on this authentication, Entrust/Authority will either terminate the session (i.e., if the Entrust/RA user is not an end-entity or is an end-entity but is not an operator) or accept the session and return to Entrust/RA the operator's privilege vector.

2.3.2.1 Entrust/RA GUI

1. The GUI is the primary interface to Entrust/RA services. For every service offered by Entrust/RA, there is at least one corresponding GUI element that enables operators to invoke that service.

2. The other interface to Entrust/RA services are the bulk input files. These files are used for batch processing of Entrust/RA services; they are used to perform either directory management services, such as adding new user entries, or end-entity or operator management services, such as enabling end-entities. Bulk-input file (BIF) processing is initiated via the GUI.

Figure 1: Entrust/RA architecture



2.3.2.2 ADM-API

1. The Administration Application Programming Interface (ADM-API) is effectively a remote interface to Entrust/Authority services. One of the more important features of the ADM-API is that it is responsible for mutually authenticating the Entrust/RA operator and the AS sub-component of the Entrust/Authority. After the mutual authentication is complete, the ADM-API establishes a session that is secure for confidentiality and integrity between Entrust/RA and the AS subsystem of Entrust/Authority. This is done via EntrustSession, as ADM-API is itself an application of the EntrustSession toolkit.

2.3.2.3 EntrustSession Toolkit

1. The EntrustSession Toolkit provides the portable Application Programming Interface (API) to the security services available from Entrust. EntrustSession Toolkit was specifically designed to address secure real-time communication between two points. EntrustSession

Toolkit does not provide communications services: those are provided by the applications using EntrustSession. Rather, the EntrustSession API provides a means for applications to supplement their existing communications software with security services. EntrustSession includes the Entrust/Engine which encapsulates the common security services required by all the Entrust/Toolkits and Entrust applications. In the case of Entrust/RA the toolkit used is the EntrustSession Toolkit.

2.3.3 TOE boundary

1. The TOE boundary for the Entrust/RA product is based on the support for the Entrust/RA features and services by the Entrust/RA components. The set of software of the TOE that must be relied upon for the correct enforcement of the TSP is included in the TOE boundary. The Entrust/RA TOE boundary is indicated in Figure 1.

2. The components that are included in the Entrust/RA INFOSEC boundary are:

    - GUI
    - ADM-API
    - EntrustSession

2.3.4 Exclusion from the TOE boundary

1. The components excluded from the Entrust/RA boundary are given below. The justification for excluding these components is provided in the sections to follow.

    - Entrust cryptographic module
    - Hardware and operating system platform (Abstract Machine)[1]

2.3.4.1 Entrust cryptographic module

1. The justification for excluding the cryptomodule from the TOE boundary is that the Entrust cryptomodule is already validated to Level 2 under the FIPS 140-1 evaluation **[Reference 2]**.

2.3.4.2 Hardware and operating platform (abstract machine)

1. The TOE abstract machine consists of the TCSEC C2-evaluated Windows NT 4.0 operating system with Service Pack 6a and any hardware for which the operating system and TOE configurations are valid.

2. The justification for excluding the abstract machine from the Entrust/RA TOE boundary is based on the following factors, described below:

    1) Operating system: The TSP is enforced by the TOE, and the SFRs are completely satisfied by TOE functions (aside from those with environmental dependencies). The operating system with which the TOE interfaces is assumed to be trusted, meaning that it can be relied upon to correctly execute the TOE functions. As well, Windows NT 4.0 with SP6a has been certified to the TCSEC C2 level.

[1] Not illustrated in Figure 1.

2) **Hardware independence:** The Entrust software is optimized to execute any x86 (i.e., Intel or equivalent processor)-based machines, regardless of the hardware vendor. That is, any hardware platform that meets the following minimum Entrust system requirements:

   - Windows NT 4.0
   - Pentium 133 or better
   - 32 Mbytes of RAM
   - 5 Mbytes of free disk space
   - one 2X or faster CD-ROM drive
   - TCP/IP stack installed

3) **No interaction with hardware platform:** The Entrust software does not interact with the hardware platform directly. That is, the Entrust software interacts with the Windows NT 4.0 operating system (e.g., via Windows function calls), which is assumed to be trusted. The operating system, in turn, interacts with the hardware platform (e.g., via the computer's BIOS and various device drivers).

3 TOE Security Environment

3.1 Introduction

1. This section identifies the following:

    - Significant assumptions about the TOE's operational environment (Section 3.2)
    - IT-related threats to the organization countered by TOE components (Section 3.3.1)
    - Threats requiring reliance on environmental controls to provide sufficient protection (Section 3.3.2)
    - Organizational security policies for which this TOE is appropriate (Section 3.4)

2. By providing the information described above, this section gives the basis for the security objectives described in Section 4 and, subsequently, the specific security requirements listed in Section 5.

3.2 Secure Usage Assumptions

1. The specific conditions listed below in Table 1 are assumed to exist in the TOE environment. These assumptions include essential environmental constraints on the use of the TOE.

Table 1: Security assumptions

Type	Assumption		Discussion
Physical	A.PROTECT	The TOE abstract machine is physically protected from unauthorized modification.	The system integrity of the TOE can only be ensured when the system integrity of the abstract machine is preserved.

Type	Assumption		Discussion
Cryptographic Operations	A.CRYPTO	The cryptographic operations are performed on a FIPS 140-1 validated or equivalent cryptographic module, which is assumed to provide an acceptable level of assurance.	The TOE can only meet its security requirements if the cryptographic operations it relies upon are performed by a trusted cryptographic module. FIPS 140-1 provides the minimum assurance level that the cryptographic module must achieve.
Abstract Machine	A.ABSTRACT	The abstract machine of the TOE operates in a correct and expected manner.	The TOE is independent of the hardware platform used, assuming the hardware platform meets the TOE system requirements and operates correctly. The TOE is relying upon NT 4.0, which is trusted[2]. The TOE only interacts with the hardware platform though the NT operating system, and thus will work correctly on any hardware platform which meets the TOE minimum system requirements the operating system executes on.
Personnel	A.USER-NEED	Authorized users recognize the need for a secure IT environment.	It is essential that the authorized users appreciate the need for security. Otherwise they are sure to try and circumvent it.
	A.USER-TRUST	Authorized users are trusted to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine.	Authorized users will have some discretion with the TOE. It is important that they be adequately trained and motivated to make wise choices in these actions. These users are assumed to be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions.
	A. ADMIN	The TOE and the TOE environment [3] are competently installed and administered to allow for correct operation of the TOE.	It is essential that security administration be both competent and on-going, and means are taken to support the detection of a corrupt abstract machine. This is required to support correct operation of the TOE.
Entrust/Authority	A.RECORD	Entrust/Authority, as part of the TOE environment and using I&A information provided by the TOE, records necessary security critical events to ensure that the information exists to support effective security management.	It is assumed that Entrust/Authority is trusted to record necessary security critical events to ensure that the information exists to support effective security management of the TOE.

[2] Microsoft Windows NT 4.0 with Service Pack 6a has been evaluated to the C2 level under the US TCSEC scheme.
[3] Competent administration of the TOE Environment includes proper configuration and operation of the abstract machine (e.g., operating system security features and system clock), and enforcement of appropriate operational procedures, including physical access control as appropriate.

Type	Assumption		Discussion
	A.DISTRIBUTE	Entrust/Authority, as part of the TOE environment, must provide for authorized administrative users to distribute and revoke public key certificates.	It is assumed that Entrust/Authority is trusted to distribute and revoke public key certificates as per requested by administrative users through the TOE.
	A.REVOKE	Entrust/Authority, as part of the TOE environment, must provide for authorized administrative users to recover end-user encryption keys and support for automatic update of end-entity signing and encryption key pairs as required.	It is assumed that Entrust/Authority is trusted to recover end user encryption keys as per requested by administrative users through the TOE, and support automatic update of TOE encryption and signing keys.

3.3 Threats to security

1. The threats facing the TOE and its environment are listed in Table 2 and Table 3 and discussed further in Section 3.3.1 and Section 3.3.2 below.

Table 2: Security threats addressed by the TOE

#	Threat Name and Description	Objectives (See Section 4)
1.	**T.UNAUTH-ACCESS** An authorized user of the TOE may gain unauthorized access to a resource or information, including cryptography-related assets, or perform operations for which no access rights have been granted, via user error, system error, or non-malicious actions.	O.BYPASS
2.	**T.ENTRY** An unauthorized individual (i.e. other than authenticated user) may gain unauthorized malicious access to TOE processing resources or security critical data, including cryptography-related assets, via technical attack.	O.ENTRY O.KNOWN

Table 3: Security threats addressed by the TOE's environment

#	Threat Name and Description	Objectives (See Section 4)

1.	**T.INSTALL** Those responsible for the TOE may install the TOE in a manner that undermines security, because of incompetence or negligence.	O.OPERATE
2.	**T.OPERATE** TOE Security policies may be circumvented because of improper operation of the TOE by an authorized user, resulting in unauthorized individuals gaining access to TOE data and resources.	O.OPERATE
3.	**T.PHYSICAL** The TOE and the abstract machine may be subject to physical attack by an unauthorized individual (i.e. other than authenticated user), resulting in unauthorized disclosure or unauthorized modification of TOE resources, which would compromise TOE security.	O.PHYSICAL
4.	**T.ENTRY-NON-TECHNICAL** An unauthorized individual (i.e. other than authenticated user) may gain access to TOE processing resources or information, including cryptography-related assets, using non-technical means (e.g. social engineering).	O.ENTRY-NON-TECHNICAL

3.3.1 Threats addressed by TOE

1. The TOE address the threats discussed below.

1) T.UNAUTH-ACCESS: An authorized user of the TOE may gain unauthorized access to a resource or information, including cryptography-related assets, or perform operations for which no access rights have been granted, via user error, system error, or non-malicious actions.

An authorized user is someone who:

- is uniquely identifiable by the system,
- has legitimate access, and
- is authenticated prior to being granted such access.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, and, because they have some rights of access, are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.
- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. The TOE will be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

2) **T.ENTRY:** An unauthorized individual (i.e. other than authenticated user) may gain unauthorized malicious access to TOE processing resources or security critical data, including cryptography-related assets, via technical attack.

The mechanisms and assurances of the TOE will resist technical attacks. However, resistance to higher-grade sophisticated types of attacks, when such resistance is required, must be provided by the TOE operational environment.

3.3.2 Threats to be addressed by the operating environment

1. The threats discussed below must be countered in order to support the TOE security capabilities but are either:

    1) not addressed by the TOE, or

    2) only partly addressed by the TOE.

2. Such threats must therefore, be addressed in conjunction with the operating environment.

    1) **T.INSTALL:** Those responsible for the TOE may install the TOE in a manner that undermines security, because of incompetence or negligence.

    The security offered is predicated upon the TOE being installed properly, as described in the TOE Installation Guide documentation **[Reference 4]**.

    2) **T.OPERATE:** TOE Security policies may be circumvented because of improper operation of the TOE by an authorized user, resulting in unauthorized individuals gaining access to TOE data and resources.

    The security offered can be assured only to the extent that the TOE is operated by authorized users in accordance with security policy.

    3) **T.PHYSICAL:** The TOE may be subject to physical attack by an unauthorized individual (i.e. other than authenticated user), resulting in unauthorized disclosure or unauthorized modification of TOE resources, which would compromise TOE security.

    The security offered by the TOE can be assured only to the extent that the underlying hardware and software is physically protected from unauthorized physical modification and from technical attacks at the hardware and operating system level.

    4) **T.ENTRY-NON-TECHNICAL:** An unauthorized individual (i.e. other than authenticated user) may gain access to TOE processing resources or information, including cryptography-related assets, using non-technical means (e.g. social engineering).

    The use of non-technical attack means; for example, social engineering is beyond the scope of TOE protections and must be addressed by the environment, mainly through training and awareness and good security practices.

3.4 Organizational Security Policies

1. The TOE and its environment addresses the following organizational security policies as shown in Table 4:

Table 4: Security policies

#	Policy Name and Description	Discussion	Objectives (See Section 4)
1.	**P.ACCOUNT** Security relevant actions must be recorded and traceable to the user or system process associated with the event, so that users can be held accountable for security relevant actions.	The TOE supports organizational policies requiring that users be held accountable for their actions, through authentication and auditing functions, facilitating after-the-fact investigations and providing some deterrence to improper actions.	O.ACCOUNT O.RECORD O.AUDIT-REVIEW
2.	**P.CRYPTO** The cryptographic operations required for encryption, digital signature, and key management services, must be performed using a FIPS 140-1 validated cryptographic module.	The TOE uses a FIPS 140-1 validated cryptographic module to deliver its cryptographic services.	O.CRYPTO
3.	**P.KEY-DISTRIBUTE** Mechanisms must be provided to allow for distribution and revocation of public key certificates by authorized administrative users and for secure transparent exchange of secret keys as required.	The TOE environment (Entrust/Authority) creates and publishes public key certificates and lists of revoked certificates called Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs). The TOE uses protocols which provide for secure exchange of secret keys.	O.CERT-DISTRIBUTE O.KEY-EXCHANGE
4.	**P.KEY-RECOVER** Mechanisms must be provided to allow for recovery of end-user encryption keys by authorized administrative users and automatic update of the end-user encryption and signing keys as required.	The TOE environment (Entrust/Authority) maintains a backup of the user encryption keys it generates to allow for key recovery. The TOE initiates and provides the mechanisms required to automatically update user encryption and signing key pairs.	O.KEY-RECOVER O.KEY-UPDATE
5.	**P.DATA-EXCHANGE** Mechanisms must be provided to allow for the origin and integrity of exchanged data to be validated on receipt, and to allow for the protection of such data against unauthorized disclosure while it is in transit between trusted remote IT components.	The TOE provides a trusted channel function with data integrity, data confidentiality and non-repudiation capabilities.	O.SIGNED-DATA O.DATA-CONF

4 Security Objectives

1. This section defines the security objectives for the TOE and its environment. The security objectives address all of the security environment aspects identified and are suitable to counter all the previously identified threats.

4.1 TOE Security Objectives

1. Table 5 lists the security objectives that the TOE meets.

Table 5: Security objectives for the TOE

#	IT Security Objective	Addressed Threat or Policy
1.	**O.KNOWN** The TOE must ensure that, except for users accessing the help menu, all users are identified and authenticated before being granted access to TOE resources.	T.ENTRY
2.	**O.BYPASS** The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement.	T.UNAUTH-ACCESS
3.	**O.ENTRY** The TOE must prevent logical entry to the TOE using technical methods, by persons without authority for such access.	T.ENTRY
4.	**O.KEY-EXCHANGE** The TOE must be able to securely and transparently exchange secret keys as required.	P.KEY-DISTRIBUTE
5.	**O.KEY-UPDATE** The TOE must provide the functionality necessary to support automatic key update of the TOE user encryption and signing key pairs, as required.	P.KEY-RECOVER
6.	**O.SIGNED-DATA** The TOE must validate the origin and integrity of the exchange data it receives from trusted remote IT products, and must provide the same validation capability to the trusted IT products receiving data from the TOE.	P. DATA-EXCHANGE
7.	**O.DATA-CONF** The TOE must protect exchanged data with trusted remote IT products against unauthorized disclosure while the data is in transit.	P. DATA-EXCHANGE
8.	**O.AUDIT-REVIEW** The TOE must provide authorized users with the capability to review audit records.	P.ACCOUNT

4.2 Environmental Security Objectives

1. Some policies and threats are beyond the capability of the TOE to adequately mitigate without support from the TOE operational environment. These policies and threats derive security objectives for the TOE environment which are listed in Table 6.

Table 6: TOE environment security objectives

#	TOE Environment Security Objectives	Addressed Threat or Policy
1.	**O.CRYPTO** The cryptographic operations required by the TOE, including key generation, key destruction, encryption, decryption, signature generation and verification, checksum generation and verification, and hashing must be done on a FIPS 140-1 validated cryptographic module.	P.CRYPTO
2.	**O.CERT-DISTRIBUTE** The TOE environment must provide for authorized administrative users to distribute and revoke public key certificates.	P.KEY-DISTRIBUTE
3.	**O.KEY-RECOVER** The TOE environment must provide for authorized administrative users to recover the TOE user encryption key pair.	P.KEY-RECOVER
4.	**O.ACCOUNT** The TOE environment must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	P.ACCOUNT
5.	**O.OPERATE** Those responsible for the TOE must ensure that the TOE and its underlying abstract machine are installed and operated in a manner which maintains IT security.	T.INSTALL T.OPERATE
6.	**O.PHYSICAL** Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical modification and from technical attacks at the hardware and operating system level.	T.PHYSICAL
7.	**O.ENTRY-NON-TECHNICAL** The TOE environment must provide sufficient protection against non-technical attacks by other than authorized users.	T.ENTRY-NON-TECHNICAL
8.	**O.RECORD** The TOE environment, using I&A information provided by the TOE, must record necessary security critical events to ensure that the information exists to support effective security management.	P.ACCOUNT

5 IT Security Requirements

1. This section contains the security functional requirements and security assurance requirements that are satisfied by the TOE. These requirements consist of functional components from the CC Version 2.1 Part 2 and assurance components from Part 3 **[Reference 1]**, respectively.

5.1 TOE Security Functional Requirements

1. This section identifies and specifies the SFR components that the Entrust/RA product is intended to meet for the purposes of this CC evaluation. All of these SFR components are chosen to directly or indirectly (i.e., via a functional component dependency) satisfy the security objectives for the TOE (as specified in Section 4).

2. Operations that are completed on the SFR components are indicated throughout this section through the use of ***Bold Italic text***. The SFRs specified in this section have been organized according to logical groupings according to various aspects of security. These groupings should simplify the specification of functionality, provide a consistent approach to the security functionality in Entrust/RA, and assist in making the demonstration of traceability easier.

3. The Entrust/RA SFRs are grouped according to the functional classes listed below:

    1) Security Audit (FAU)

    2) Cryptographic Support (FCS)

    3) User data protection (FDP)

    4) Identification & Authentication (FIA)

    5) Protection of the TSF (FPT)

    6) TOE Access (FTA)

    7) Trusted Path/Trusted Channels (FTP)

5.1.1 Security Audit (FAU)

1. This section specifies the Security Audit security requirements for Entrust/RA. The Security Audit security requirements are summarized in Table 7.

Table 7: Security Audit security requirements

#	Security Requirement	Component
1.	Audit review	FAU_SAR.1
2.	Selectable audit review	FAU_SAR.3

5.1.1.1 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ***Master Users, Security Officers, Administrators, Auditors, and custom-defined roles with the appropriate privilege*** with the capability to read ***all audit information*** [4] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.1.2 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform ***searches and sorting*** of audit data based ***on a time range, character string, audit event number, or severity for searching and any of the following for sorting (ascending or descending): Number, Time, Event text, Severity, Administrator Name, Target Name, Extra, and Audit State.***

5.1.2 Cryptographic Support (FCS)

1. This section specifies the Cryptographic Support security requirements for Entrust/RA. The Cryptographic Support security requirements are summarized in Table 8.

Table 8: Cryptographic Support security requirements

#	Security Requirement	Component
1.	Cryptographic key distribution	FCS_CKM.2
2.	Cryptographic key access	FCS_CKM.3

5.1.2.1 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***(certificate-based key management)*** that meets the following standards:

- ***X.509v3 (Section 11: Management of Keys and Certificates and Section 12: Certificate and CRL Extensions)***
- ***PKCS #1 (RSA Cryptography Standard)***
- ***FIPS PUB 186-1 (Digital Signature Algorithm)***
- ***PKCS #3 (Diffie-Hellman (DH) key agreement)***
- ***RFC 1777 and RFC 2251 (Lightweight Directory Access Protocol v2 and v3)***
- ***RFC 2510 (PKIX-CMP)***

[4] As described in Section 5.1.1.1 (FAU_GEN.1 Audit data generation) of the **Security Target - Entrust/Authority [Reference 3]**.

5.1.2.2 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform ***operator initialization, operator key update, and operator key recovery*** in accordance with a specified cryptographic key access method ***(in accordance with Access Control SFP)*** that meets the following standards:

- ***PKIX-CMP (RFC 2510)***
- ***FIPS PUB 140-1***

5.1.3 User data protection (FDP)

1. This section specifies the User data protection security requirements for Entrust/RA. The User data protection security requirements are summarized in Table 9.

Table 9: User data protection security requirements

#	Security Requirement		Component
1.	Residual information protection	Subset residual information protection	FDP_RIP.1
2.	Data exchange integrity	Data exchange integrity	FDP_UIT.1

5.1.3.1 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the ***deallocation of the resource from*** the following objects:

- ***Entrust/RA operator passwords***

5.1.3.2 FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1 The TSF shall enforce the ***Access Control SFP*** to be able to ***transmit and receive*** user data in a manner protected from ***modification, deletion, insertion, replay*** errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether ***modification, deletion, insertion, or replay*** has occurred.

5.1.4 Identification & authentication (FIA)

1. This section specifies the Identification & Authentication security requirements for Entrust/RA. The Identification & Authentication security requirements are summarized in Table 10.

Table 10: Identification & authentication security requirements

#	Security Requirement	Component
1.	Authentication failure handling	FIA_AFL.1
2.	Verification of secrets	FIA_SOS.1
3.	User authentication before any action	FIA_UAU.2
4.	Re-authentication	FIA_UAU.6
5.	Protected authentication feedback	FIA_UAU.7

#	Security Requirement	Component
6.	User identification before any action	FIA_UID.2

5.1.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***three*** unsuccessful authentication attempts occur related to ***initial authentication at Entrust/RA.***

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall ***terminate the process in question.***

5.1.4.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets ***(passwords for Security Officer, Administrator, Auditors, Directory Administrators, End users, and custom-defined roles)*** meet the following criteria:

1) ***Specified Security Officer, Administrator, Auditor, Directory Administrator, End User, or custom-defined role password rules applicable to:***

   - ***time to password expiry (default: 0)***
   - ***password history (default: 8)***
   - ***password length (default: 8)***
   - ***at least one non-alphanumeric character (default: OFF)***
   - ***at least one upper case letter (default: ON)***
   - ***at least one lower case letter (default: ON)***
   - ***at least one digit (default: OFF)***
   - ***must not contain many occurrences of the same character (i.e., the most occurrences of the same character allowed in the password is half the length of the password) (always ON)***
   - ***must not be the same as the Entrust profile username (always ON)***
   - ***must not contain a long substring of the Entrust profile name (i.e., the longest allowable profile (.epf) username substring is equal to half the length of the password) (always ON)***

5.1.4.3 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.4.4 FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions:

1) ***For all operators, to complete "sensitive operations" when the number of required authorizations is set to one;***

2) ***For all operators, to complete their password change.***

3) ***To unlock Entrust/RA after a 10 minute (default) operator inactivity time-out;***

4) ***To unlock an operator-initiated lock of Entrust/RA;***

5.1.4.5 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide ***only asterisks (*) on the display screen to the user*** while the authentication is in progress.

5.1.4.6 FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Protection of the TSF (FPT)

1. This section specifies the Protection of the TSF security requirements for Entrust/RA. The Protection of the TSF security requirements are summarized in Table 11.

Table 11: Protection of the TSF security requirements

#	Security Requirement		Component
1.	Data exchange integrity	Inter-TSF detection of modification	FPT_ITI.1
2.	Non-bypassability	Non-bypassability of the TSP	FPT_RVM.1
3.	Data consistency	Inter-TSF basic TSF data consistency	FPT_TDC.1

5.1.5.1 FPT_ITI.1 Inter-TSF detection of modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: ***all data in all EntrustSession messages and PKIX-CMP key update messages is always integrity-protected using digital signatures.***

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and ***terminate the session*** if modifications are detected.

5.1.5.2 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.5.3 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret the ***following TSF data types*** when shared between the TSF and another trusted IT product:

- ***PKIX-CMP protocol data***
- ***EntrustSession protocol data***

FPT_TDC.1.2 The TSF shall use ***the following interpretation rules to be applied by the TSF*** when interpreting the TSF data from another trusted IT product: ***the use of common protocol implementations and the standards upon which they are based: EntrustSession and PKIX-CMP.***

5.1.6 TOE Access (FTA)

1. This section specifies the TOE Access security requirements for Entrust/RA. The TOE Access security requirements are summarized in Table 11.

Table 12: TOE Access security requirements

#	Security Requirement	Component
1.	TSF-initiated session locking	FTA_SSL.1
2.	User-initiated locking	FTA_SSL.2

5.1.6.1 FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after ***10 minutes (default)*** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session:

- ***the operator currently logged into Entrust/RA must be successfully re-authenticated.***

5.1.6.2 FTA_SSL.2 User-initiated locking

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session:

- ***the operator currently logged into Entrust/RA must be successfully re-authenticated.***

5.1.7 Trusted Path/Trusted Channels (FTP)

1. This section specifies the User data protection security requirements for Entrust/RA. The Trusted path/trusted channels security requirements are summarized in Table 9.

Table 13: Trusted path/trusted channels security requirements

#	Security Requirement		Component
1.	Trusted channel	Inter-TSF trusted channel	FTP_ITC.1a
			FTP_ITC.1b

5.1.7.1 FTP_ITC.1a Inter-TSF trusted channel

FTP_ITC.1a.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1a.2 The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1a.3 The TSF shall initiate communication via the trusted channel for:

- ***all Entrust/RA operator-initiated functions that require interactions with Entrust/Authority via EntrustSession.***
- ***Entrust/RA operator initialization and operator key recovery functions via PKIX-CMP.***

5.1.7.2 FTP_ITC.1b Inter-TSF trusted channel

FTP_ITC.1b.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1b.2 The TSF shall permit ***the TSF*** to initiate communication via the trusted channel.

FTP_ITC.1b.3 The TSF shall initiate communication via the trusted channel for:

- ***automatic Entrust/RA operator encryption key update and signature key update via PKIX-CMP.***

5.2 TOE Environment Security Functional Requirements

1. The environment is required to satisfy the secure usage assumptions in Section 3.1 and to meet all of the environmental security objectives outlined in Section 4.2.

2. Table 14 lists the functional requirements delivered by Entrust/Authority upon which the TOE depends. The security functions associated with these requirements are described in **Security Target - Entrust/Authority [Reference 3]**.

Table 14: Required functional components provided by Entrust/Authority

#	CC Component	Name	Dependency for the TOE to meet
1.	FAU_GEN.1	Audit data generation	FAU_SAR.1
2.	FDP_ACC.1	Subset access control	FDP_UIT.1

3. Table 15 lists the functional requirements delivered by the FIPS 140-1 (Level 2) validated Entrust Security Kernel 5.1 (software cryptomodule) upon which the TOE depends **[Reference 2]**.

Table 15: Required functional components provided by the FIPS 140-1 validated cryptographic module

#	CC Component	Name	Dependency for the TOE to meet
1.	FCS_CKM.1	Cryptographic key generation	FCS_CKM.2
			FCS_CKM.3
			O.CRYPTO
2.	FCS_CKM.4	Cryptographic key destruction	FCS_CKM.2
			FCS_CKM.3
			O.CRYPTO
3.	FCS_COP.1	Cryptographic operation	O.CRYPTO

4. Table 16 lists the functional requirement delivered by the abstract machine hosting the TOE.

Table 16: Required functional component provided by the abstract machine

#	CC Component	Name	Dependency for the TOE to meet
1.	FPT_SEP.1	TSF domain separation	O.PHYSICAL

5.2.1 Entrust/Authority

1. The security functions associated with the requirements met by Entrust/Authority are defined in **Security Target - Entrust/Authority [Reference 3]**.

5.2.2 Key management

1. This section specifies the Key Management (environmental) security requirements for Entrust/RA. The Key Management (environmental) security requirements are summarized in Table 17.

Table 17: Key management (environmental) security requirements

#	Security Requirement	Component
1.	Cryptographic key generation	FCS_CKM.1
2.	Cryptographic key destruction	FCS_CKM.4
3.	Cryptographic operation	FCS_COP.1

5.2.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- ***RSA***
- ***DSA***
- ***ECDSA***
- ***CAST5***
- ***DES***
- ***Triple-DES***
- ***IDEA***

and specified cryptographic key sizes:

- ***RSA: 2048-bit, 1024-bit***
- ***DSA: 1024-bit***
- ***ECDSA: 192-bit***
- ***CAST5: 128-bit, 80-bit***
- ***DES: 56-bit***
- ***Triple-DES: 168-bit***
- ***IDEA: 128-bit***

that meet the following:

- ***RSA: PKCS #1, FIPS PUB 186-1, and ANSI X9.31***
- ***DSA: FIPS PUB 186-1 and ANSI X9.30***
- ***ECDSA: ANSI X9.62***
- ***CAST5: ANSI X9.17 and RFC 2144***
- ***DES: ANSI X9.17, ANSIX3.92, and FIPS PUB 46-2***
- ***Triple-DES: ANSI X9.17 and X9.52***

5.2.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method ***(zeroization)*** that meets the following:

- ***FIPS PUB 140-1***

5.2.2.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform:

- ***Pseudo-random number generation***
- ***encryption and decryption***
- ***digital signature generation and verification***
- ***key management***
- ***hashing***
- ***Message Authentication Code (MAC) generation and verification***

in accordance with a specified cryptographic algorithm:

- ***Random number generation: ANSI X9.17***
- ***Encryption and Decryption: CAST5 encryption, DES encryption, Triple-DES encryption, IDEA encryption***
- ***Digital Signature/Verification: RSA digital signature, DSA digital signature, ECDSA digital signature***
- ***Key Management: X.509 v3, RSA, EntrustSession Toolkit Diffie-Hellman (DH) key agreement, LDAP, PKIX-CMP***
- ***Hashing: SHA-1, MD5***
- ***MACing: FIPS PUB 113, ANSI X9.9, X9.19***

and cryptographic key sizes:

- ***RSA: 2048-bit, 1024-bit***
- ***DSA: 1024-bit***
- ***ECDSA: 192-bit***
- ***CAST5: 128-bit, 80-bit***
- ***DES: 56-bit***
- ***Triple-DES: 168-bit***
- ***IDEA: 128-bit***

that meet the following standards:

- ***Pseudo-random number generation: ANSI X9.17 Appendix C***

- ***CAST5 encryption: RFC 2144***
- ***DES encryption: FIPS PUB 46-2 and ANSI X3.92***
- ***Triple-DES encryption: ANSI X9.52***
- ***DES, CAST5, triple-DES encryption in CBC mode: FIPS PUB 81, ANSI X3.106, and ISO/IEC 10116***
- ***IDEA encryption: ISO/IEC 9979-2***
- ***RSA digital signature: PKCS #1, FIPS PUB 186-1, and ANSI X9.31***
- ***DSA digital signature: FIPS PUB 186-1 and ANSI X9.30***
- ***ECDSA digital signature: ANSI X9.62***
- ***RSA: PKCS #1***
- ***EntrustSession Toolkit authentication: ISO/IEC 9798-3 and FIPS PUB 196***
- ***EntrustSession Toolkit Diffie-Hellman key agreement: PKCS #3***
- ***Lightweight Directory Access Protocol v2 and v3: RFC 1777 and RFC 2251***
- ***PKIX-CMP: RFC 2510***
- ***SHA-1 hash: FIPS PUB 180-1 and ANSI X9.30 Part 2***
- ***MD5 hash: RFC 1321***
- ***MAC: FIPS PUB 113, ANSI X9.9, and ANSI X9.19***

5.2.3 Abstract machine services

1. This section specifies the abstract machine provided services (environmental security requirements) for Entrust/RA. These services (environmental security requirements) are summarized in Table 18.

Table 18: Abstract machine security requirements

#	Security Requirement	Component
1.	TSF domain separation	FPT_SEP.1

5.2.3.1 FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 TOE Security Assurance Requirements

1. The assurance components for the Entrust/RA Security Target are summarized in Table 19.

Table 19: TOE assurance components

Component	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization Controls
	ACM_SCP.2	Problem Tracking CM Requirements
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security Enforcing High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE Security Policy Model
Guidance Documents	AGD_ADM.1	Administrator Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw Remediation Requirements
Tests	ATE_COV.2	Analysis of Coverage
	ATE_DPT.1	Testing - High-Level Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer Vulnerability Analysis
	AMA_CAT.1	Categorization Report

2. Table 20 lists those components that augment EAL3 from CC Version 2.1 Part 3 **[Reference 1]** for this ST.

Table 20: Augmentation to EAL3

EAL3	EAL3-augmented	Nature of Augmentation	
ACM_SCP.1	ACM_SCP.2	Upgraded	Requires that security flaws be included in the Configuration Management documentation to show how they are tracked.
n/a	ADV_SPM.1	Added	Provides a TSP model which describes the rules and characteristics of all policies of the TSP that can be modeled and includes a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled. Demonstrates correspondence between the functional specification and the TSP model which shows that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.
n/a	ALC_FLR.2	Added	Establishes a procedure for accepting and acting

EAL3	EAL3-augmented	Nature of Augmentation	
			upon user reports of security flaws and requests for corrections to those flaws. The procedures for processing reported security flaws ensure that any reported flaws are corrected and the correction issued to TOE users. The procedures for processing reported security flaws provide safeguards that any corrections to these security flaws do not introduce any new flaws.
n/a	AMA_CAT.1	Added	Provides a TOE component categorization report for the TOE which categorizes each component of the TOE according to its relevance to security The TOE component categorization report describes the categorization scheme used, so that it can be determined how to categorize new components introduced into the TOE, and also when to re-categorize existing TOE components following changes to the TOE or its security target. The TOE component categorization identifies any tools used in the development environment that, if modified, will have an impact on the assurance that the TOE satisfies its security target.
AVA_MSU.1	AVA_MSU.2	Upgraded	Documents an analysis of the guidance documentation which demonstrates that the guidance documentation is complete.

6 TOE Summary Specification

6.1 IT Security Functions

1. This section describes the IT security functions provided by the TOE to meet the security functional requirements specified for Entrust/RA in Section 5.1. For each IT security function listed in this section, each section title also references the associated SFRs. A complete mapping of security functions and SFRs is provided in Table 24.

6.1.1 Security Audit (FAU)

6.1.1.1 Audit review

1. Entrust/RA provides an audit viewer to allow authorized operators to view audit data, presented in a human-friendly manner, from the audit trail.

6.1.1.2 Selectable audit review

1. The Entrust audit viewer allows authorized operators to search through the audit trail based on a supplied time range, character string, audit event number, or severity, as well to sort the retrieved audit data based on a number of audit data fields (e.g., event type, severity, etc.).

6.1.2 Cryptographic Support (FCS)

6.1.2.1 Key distribution

1. Entrust/RA generates and exchanges secret keys with Entrust/Authority in a secure way, meaning that such secret keys are always protected against unauthorized disclosure and modification using the following methods and standards: X.509 v3 (Section 11 and Section 12); RSA key transfer (PKCS #1); DSA key transfer (FIPS PUB 186-1); Diffie-Hellman key agreement (PKCS #3); LDAP v2 (RFC 1777) and LDAP v3 (RFC 2251); and PKIX-CMP (RFC 2510).

6.1.2.2 Key access

1. Entrust/RA accesses cryptographic keys to perform client-end operations for supporting operator initialization, operator encryption and signing key pair update, and operator key recovery in accordance with the relevant standards: PKIX-CMP (RFC 2510) and FIPS PUB 140-1.

2. For initialization, Entrust/RA supplies to Entrust/Authority operator verification keys and protocol encryption keys. Entrust/RA receives from Entrust/Authority operator decryption private keys in encrypted form and session keys in encrypted form.

3. For key update, Entrust/RA supplies to Entrust/Authority newly generated operator decryption private keys in encrypted form, and protocol encryption keys. Entrust/RA receives from Entrust/Authority the session key in encrypted form.

4. For key recovery, Entrust/RA supplies to Entrust/Authority newly generated operator verification keys as well as protocol encryption keys.

6.1.3 User data protection (FDP)

6.1.3.1 Residual information protection

1. After login to Entrust/RA, the operator's password is cleared from memory when no longer in use, preventing memory scanners from retrieving this data.

6.1.3.2 Data exchange integrity

1. Entrust/RA provides the capability to transmit and receive data in a manner protected from modification, deletion, insertion, and replay errors for all data in EntrustSession or PKIX-CMP messages as all data is always integrity-protected using digital signatures or MACs. EntrustSession and PKIX-CMP use random numbers and time stamps to reduce the likelihood of replay or insertion attacks. Entrust/RA terminates any communication sessions via EntrustSession or PKIX-CMP upon detection of data modification, deletion, insertion, or replay.

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication failure

1. Entrust/RA detects initial authentication failures via the Entrust/RA login GUI. After three unsuccessful login attempts, the authentication process must be restarted by first restarting the Entrust/RA application.

6.1.4.2 User and operator password criteria

1. Entrust/RA enforces that operator-generated secrets (passwords for Security Officer, Administrator, Directory Administrator, Auditor, and custom-defined roles) meet the password criteria specified in Section 5.1.4.2. **(SoF - Medium)**.

6.1.4.3 Authentication of users

1. Entrust/RA allows the initiation only of the help, find profile, create profile, and recover profile operations on behalf of Entrust operators before the operator is successfully authenticated. All other functions require the operator to be authenticated before allowing any Entrust-mediated action.

6.1.4.4 Re-authentication of operators

1. Entrust/RA forces the re-authentication of operators to complete sensitive operations (if the number of authorizations is set to one), after a 10 minute (default) operator inactivity timeout at Entrust/RA, after operator-initiated locking of Entrust/RA, and to complete an Entrust/RA operator password change.

6.1.4.5 Non-echoing of passwords

1. Only special characters are presented during authentication to hide the entered password. The entered password appears as asterisks (*) on the screen in Entrust/RA.

6.1.4.6 Identification of users

1. Entrust/RA allows the initiation only of the help, find profile, create profile, and recover profile operations on behalf of Entrust operators before the operator is successfully

identified. All other functions require the operator to be identified before allowing any Entrust-mediated action.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Data exchange integrity

1. Entrust/RA provides the capability to transmit and receive data in a manner protected from modification, deletion, insertion, and replay errors for all data in EntrustSession or PKIX-CMP messages as all data is always integrity-protected using digital signatures or MACs. EntrustSession and PKIX-CMP use random numbers and time stamps to reduce the likelihood of replay or insertion attacks. Entrust/RA terminates any communication sessions via EntrustSession or PKIX-CMP upon detection of data modification, deletion, insertion, or replay.

6.1.5.2 Non-bypassability of security functions

1. To maintain the security domain for Entrust/RA, all security-policy enforcing functions are invoked and succeed before each function is allowed to proceed.

6.1.5.3 Data consistency

1. The data in the EntrustSession and PKIX-CMP protocols are consistently interpreted by Entrust/RA based on common implementations of the protocols.

6.1.6 TOE Access (FTA)

6.1.6.1 Entrust/RA-initiated session locking

1. Entrust/RA locks an interactive session with an operator after 10 minutes (default) of operator inactivity. The operator must successfully re-authenticate themselves to Entrust/RA to unlock the session.

6.1.6.2 Operator-initiated session locking

1. An operator may initiate a lock of an interactive session with Entrust/RA. The operator must successfully re-authenticate themselves to Entrust/RA to unlock the session.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Trusted channel

1. Entrust/RA provides a trusted channel between itself and Entrust/Authority via EntrustSession for all operator-initiated Entrust/RA services that require interactions with Entrust/Authority and PKIX-CMP for automatic key update and operator initialization and recovery. All data transmitted via EntrustSession and PKIX-CMP is protected for confidentiality and integrity.

6.2 Assurance Measures

1. The assurance requirements for this TOE are met by the EAL3-augmented assurance components, which stresses assurance through Entrust actions that are within the bounds of current best-commercial-practice. These assurance requirements provide, primarily via

review of Entrust-supplied evidence, independent confirmation that these actions have been competently performed. They also include the following independent, third-party analysis:

1) Confirmation of system generation and installation procedures

2) Verification that the system security state is not misrepresented

3) Verification of a sample of the vendor functional testing

4) Searching for obvious vulnerabilities

5) Independent functional testing

2. 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 25, the Assurance Measures are provided in the form of references to the relevant and appropriate document associated with each requirement.

7 Rationale

7.1 Security Objectives Rationale

1. The security objectives described in Section 4address all of the security environment aspects identified and are suitable to counter all of the previously identified threats.

2. Table 2, Table 3, and Table 4 show that all threats and policies are covered by security objectives. Table 5 shows the mapping of security objectives to threats and policies. This table indicates that each objective contributes to countering a threat or satisfying a policy. Thus there are no unnecessary objectives.

3. Table 21 provides a rationale for the correctness of each security objectives. Where there is a one-to-one match between a policy or threat, that policy or threat is the rationale. For the environment objectives, an explanation is provided for not including the objective in the list of TOE security objectives.

Table 21: Correct objectives - mapping security objective to rationale

#	Security Objective	Rationale	Environmental Assumptions
1.	**O.KNOWN** The TOE must ensure that, except for users accessing the help menu, all users are identified and authenticated before being granted access to TOE resources.	T.ENTRY	
2.	**O.BYPASS** The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement..	T.UNAUTH-ACCESS	
3.	**O.ENTRY** The TOE must prevent logical entry to the TOE using technical methods, by persons without authority for such access.	T.ENTRY	
4.	**O.KEY-EXCHANGE** The TOE must be able to securely and transparently exchange secret keys as required.	“secure transparent exchange of secret keys” (P.KEY-DISTRIBUTE)	
5.	**O.KEY-UPDATE** The TOE must provide the functionality necessary to initiate and support automatic key update of the TOE user encryption and signing key pairs, as required.	“automatic update of the end-user encryption and signing keys” (P.KEY-RECOVER)	

#	Security Objective	Rationale	Environmental Assumptions
6.	**O.SIGNED-DATA** The TOE must validate the origin and integrity of the exchange data it receives from trusted remote IT products, and must provide the same validation capability to the trusted IT products receiving data from the TOE.	P. DATA-EXCHANGE	
7.	**O.DATA-CONF** The TOE must protect exchanged data with trusted remote IT products against unauthorized disclosure while the data is in transit.	P. DATA-EXCHANGE	
8.	**O.AUDIT-REVIEW** The TOE must provide authorized users with the capability to review audit records.	P.ACCOUNT	
9.	**Environment - O.CRYPTO** The cryptographic operations required by the TOE, including key generation, key destruction, encryption, decryption, signature generation and verification, checksum generation and verification, and hashing must be done on a FIPS 140-1 validated cryptographic module.	P.CRYPTO The cryptographic module used by the TOE has been successfully validated against FIPS 140-1, thus it is not required to be included in the TOE.	A.CRYPTO
10.	**Environment - O.CERT-DISTRIBUTE** The TOE environment must provide for authorized administrative users to distribute and revoke public key certificates.	"authorized administrative users to distribute and revoke public key certificates" (P.KEY-DISTRIBUTE) The TOE provides the administrative user interface required for operating and managing certificate distribution and revocation. However, the actual certificate distribution and revocation being in fact implemented in Entrust/Authority (TOE Environment), this objective requires the TOE environment to be fully satisfied.	A.DISTRIBUTE

#	Security Objective	Rationale	Environmental Assumptions
11.	**Environment - O.KEY-RECOVER** The TOE environment must provide for authorized administrative users to recover TOE user encryption keys.	"recovery of end-user encryption keys by authorized administrative users" (P.KEY-RECOVER) The TOE provides the administrative user interface required for backing-up and recovering end user encryption keys. However, the actual key back-up and recovery functions are performed by Entrust/Authority (TOE environment). Consequently, this objective requires services provided by the TOE environment to be fully satisfied.	A.REVOKE
12.	**Environment - O.ACCOUNT** The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	P.ACCOUNT Security relevant actions, from an organization view point, have to do with the services provided by Entrust/Authority. Consequently, all auditable events involve interactions with Entrust/Authority, and are recorded by Entrust/Authority which is included in the TOE environment. Each audited event is associated with a user ID which is provided by the TOE. Thus, this objective ensures that users can subsequently be held accountable for their security relevant actions.	A.RECORD

#	Security Objective	Rationale	Environmental Assumptions
13.	**Environment - O.OPERATE** Those responsible for the TOE must ensure that the TOE and its underlying abstract machine are installed and operated in a manner which maintains IT security.	T.INSTALL T.OPERATE This is an environmental objective because the actions required include, to a large degree, non-technical countermeasures, including means taken to: 1) make users to recognize the need for security; 2) establish trust in users; and 3) properly install and administer the TOE and its abstract machine. The TOE is expected to support, however, by providing mechanisms and interfaces that ease the burden of ensuring correct operation.	A.USER-NEED A.USER-TRUST A.ABSTRACT A.ADMIN
14.	**Environment - O.PHYSICAL** Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical modification and from technical attacks at the hardware and operating system level.	T.PHYSICAL The TOE does not provide physical security, thus physical security is an environmental objective.	A.PROTECT
15.	**Environment - O.ENTRY-NON-TECHNICAL** The TOE environment must provide sufficient protection against non-technical attacks by other than authorized users.	T.ENTRY-NON-TECHNICAL Effectively dealing with non-technical types of attacks requires countermeasures provided by the TOE environment.	A.USER-NEED A.USER-TRUST A.ADMIN
16.	**Environment - O.RECORD** The TOE environment, using I&A information provided by the TOE, must record necessary security critical events to ensure that the information exists to support effective security management.	P.ACCOUNT TOE auditable events are recorded by Entrust/Authority. Each audited TOE event is associated with a user ID which is provided by the TOE; this ensures that information exists to support effective security management. Thus, this objective requires services provided by the TOE environment (Entrust/Authority) to be fully satisfied.	A.RECORD

7.2 Security Requirements Rationale

7.2.1 Suitability of security functional requirements

1. Table 22 shows the mapping of security objectives to security functional requirements. This table demonstrates that each functional security requirement addresses at least one IT security objective or is necessary to meet a required dependency for another functional security requirement that directly addresses security objectives.

2. This table also demonstrates completeness of the functional set with respect to covering each security objective by at least one security functional requirement.

3. This table also provides a justification as to why the security functional requirements (mapped to the security objectives) are sufficient to meet their associated security objective(s).

Table 22: Complete functionality - mapping security objective to functionality

#	Security Objective	TOE Functionality	Justification
1.	**O.KNOWN** The TOE must ensure that, except for users accessing the help menu, all users are identified and authenticated before being granted access to TOE resources.	FIA_UAU.2 FIA_UID.2	These requirements ensure that users are successfully identified and authenticated before any TSF-mediated actions for that user: **FIA_UAU.2** ensures that each user is successfully authenticated before allowing any TSF-mediated actions for that user. **FIA_UID.2** ensures that each user is successfully identified before allowing any TSF-mediated actions for that user.
2.	**O.BYPASS** The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement.	FDP_RIP.1 FIA_AFL.1 FIA_SOS.1 FIA_UAU.6 FIA_UAU.7 FPT_RVM.1 FTA_SSL.1 FTA_SSL.2	These requirements ensure that users are prevented from bypassing or circumventing TOE security policies: **FDP_RIP.1** ensures that any previous information content of Entrust/RA passwords is made unavailable after its deallocation. **FIA_AFL.1** ensures that authentication failures are handled appropriately, preventing malicious use of the software. **FIA_SOS.1** ensures that password rules are enforced against all operators and end users, preventing the bypassing or circumvention of password policies. **FIA_UAU.6** ensures that operators must be re-authenticated under specific conditions, preventing the bypassing or circumvention of access control security policy. **FIA_UAU.7** ensures that authentication data feedback is protected, preventing the bypassing

#	Security Objective	TOE Functionality	Justification
			or circumvention of access control security policy. **FPT_RVM.1** ensures that security policy enforcement functions are invoked and succeed before each function is allowed to proceed so access control security policy is always enforced. **FTA_SSL.1** ensures that the TSF locks an interactive session after a defined period of time, making the display contents unreadable and disabling the user interface, and requiring the operator to re-authenticate themselves to unlock the session. **FTA_SSL.2** ensures that a user may initiate locking of an interactive session at any time, making the display contents unreadable and disabling the user interface, and requiring the operator to re-authenticate themselves to unlock the session.
3.	**O.ENTRY** The TOE must prevent unauthorized logical entry to the TOE by technical methods used by persons without authority for such access.	FDP_RIP.1 FIA_AFL.1 FIA_SOS.1 FIA_UAU.2 FIA_UAU.7 FIA_UID.2 FTA_SSL.1 FTA_SSL.2	These requirements ensure that the TOE prevents logical access to the TOE by unauthorized users: **FDP_RIP.1** ensures that any previous information content of Entrust/RA operator passwords is made unavailable after its deallocation. **FIA_AFL.1** ensures that authentication failures are handled appropriately, preventing malicious use of the software. **FIA_SOS.1** ensures that password rules are enforced against all operators and end users, preventing the bypassing or circumvention of password policies. **FIA_UAU.2** ensures that each user is successfully authenticated before allowing any TSF-mediated actions for that user. **FIA_UAU.7** ensures that authentication data feedback is protected, preventing the bypassing or circumvention of access control security policy. **FIA_UID.2** ensures that each user is successfully identified before allowing any TSF-mediated actions for that user. **FTA_SSL.1** ensures that the TSF locks an interactive session after a defined period of time, making the display contents unreadable and disabling the user interface, and requiring the operator to re-authenticate themselves to unlock

#	Security Objective	TOE Functionality	Justification
			the session. **FTA_SSL.2** ensures that a user may initiate locking of an interactive session at any time, making the display contents unreadable and disabling the user interface, and requiring the operator to re-authenticate themselves to unlock the session.
4.	**O.KEY-EXCHANGE** The TOE must be able to securely and transparently exchange secret keys as required.	FCS_CKM.2	This requirement ensures that the TOE is able to secure exchange secret keys in support of key management operations: **FCS_CKM.2** ensures that cryptographic keys are securely distributed (exchanged) in accordance with specific methods and standards.
5.	**O.KEY-UPDATE** The TOE must provide the functionality necessary to initiate and support automatic key update of TOE user encryption and signing key pairs, as required.	FCS_CKM.3	This requirement ensures that the TOE provides manual and automatic key update of end user key pairs: **FCS_CKM.3** ensures that cryptographic keys are accessed by the TSF for specific operations, including key update, in accordance with specific standards.
6.	**O.SIGNED-DATA** The TOE must validate the origin and integrity of the exchange data it receives from trusted remote IT products, and must provide the same validation capability to the trusted IT products receiving data from the TOE.	FDP_UIT.1 FPT_ITI.1 FPT_TDC.1 FTP_ITC.1a FTP_ITC.1b	These requirements ensure that the TOE validates the origin and integrity of exchanged data it receives: **FDP_UIT.1** ensures that user data is transmitted and received protected from modification, deletion, insertion, and replay. **FPT_ITI.1** ensures that modified data in EntrustSession and PKIX-CMP is detected based on digital signatures and/or MACs. **FPT_TDC.1** ensures that TSF data is consistently interpreted via EntrustSession and PKIX-CMP when shared between the TSF and another trusted IT product. **FTP_ITC.1a** and **FTP_ITC.1b** ensure that a trusted channel is provided for operator-initiated functions and key management operations for operators that is logically distinct from other channels and provides assured identification of its end points and protection of transmitted data from modification or disclosure.
7.	**O.DATA-CONF** The TOE must protect exchanged data with trusted remote IT products against unauthorized disclosure while the data is in transit.	FTP_ITC.1a FTP_ITC.1b	This requirement ensures that the TOE protects exchanged data against unauthorized disclosure: **FTP_ITC.1a** and **FTP_ITC.1b** ensure that a trusted channel is provided for operator-initiated functions and key management operations for operators that is logically distinct from other

#	Security Objective	TOE Functionality	Justification
			channels and provides assured identification of its end points and protection of transmitted data from modification or disclosure.
8.	**O.AUDIT-REVIEW** The TOE must provide authorized users with the capability to review audit records.	FAU_SAR.1 FAU_SAR.3	These requirements ensure that the TOE provides authorized users with the capability to review audit records: **FAU_SAR.1** ensures that operators have the capability to read (access) audit information. **FAU_SAR.3** ensures that the TSF provides the ability to perform searches and sorting of audit data.
9.	**O.ACCOUNT** The TOE environment must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	Addressed by the TOE and TOE environment (Entrust/Authority).	
10.	**O.CRYPTO** The cryptographic operations required by the TOE, including key generation, key destruction, encryption, decryption, signature generation and verification, checksum generation and verification, and hashing must be done on a FIPS 140-1 validated cryptographic module.	Addressed by the TOE environment (FIPS 140-1 validated cryptographic module) FCS_CKM.1 FCS_CKM.4 FCS_COP.1	These requirements ensure that the TOE cryptographic operations are performed on a FIPS 140-1 (or equivalent) validated cryptomodule: **FCS_CKM.1** ensures that cryptographic keys are generated by the cryptomodule in accordance with a specified algorithm and key size, compliant with cryptographic standards. **FCS_CKM.4** ensures that cryptographic keys are destroyed by the cryptomodule in accordance with a specified cryptographic key destruction method, compliant with FIPS 140-1. **FCS_COP.1** ensures that all cryptographic operations are performed by the cryptomodule, in accordance with specified cryptographic algorithms and cryptographic key sizes, compliant with cryptographic standards.
11.	**O.CERT-DISTRIBUTE** The TOE environment must provide for authorized administrative users to distribute and revoke public key certificates.	Addressed by the TOE environment.	
12.	**O.KEY-RECOVER** The TOE environment must provide for authorized administrative users to recover the TOE user encryption key pair as required.	Addressed by the TOE environment.	
13.	**O.RECORD** The TOE environment, using I&A	Addressed by the TOE environment	

#	Security Objective	TOE Functionality	Justification
	information provided by the TOE, must record security critical events to ensure that the information exists to support effective security management.		
14.	**O.PHYSICAL** Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorized physical modification and from technical attacks at the hardware and operating system level.	Addressed by the TOE environment (including FPT_SEP.1)	This requirement ensures that the TOE and its underlying hardware and software are physically protected from unauthorized physical modification and technical attacks: **FPT_SEP.1** ensures that a security domain is maintained for the execution of the TSF, protecting it from interference and tampering by untrusted subjects.
15.	**O.OPERATE** Those responsible for the TOE must ensure that the TOE and its underlying abstract machine are installed and operated in a manner which maintains IT security.	Addressed by the TOE environment	
16.	**O.ENTRY-NON-TECHNICAL** The TOE environment must provide sufficient protection against non-technical attacks by other than authorized users.	Addressed by the TOE environment	

7.2.2 Dependency analysis

1. Table 23 demonstrates that the functional set of security requirements meets all functional dependencies. The *italic text* used in Table 23 represents those functional components that are met by either Entrust/Authority, the FIPS 140-1 validated Entrust cryptomodule, or the abstract machine. These functional components are listed in Table 14, Table 15, and Table 16, respectively.

Table 23: Correct functionality – dependency mapping

#	Component	Name	Hierarchical To	Dependencies
1.	FAU_SAR.1	Audit review	—	*FAU_GEN.1*
2.	FAU_SAR.3	Selectable audit review	—	FAU_SAR.1
3.	FCS_CKM.2	Cryptographic key distribution	—	*FCS_CKM.1* *FCS_CKM.4* *FMT_MSA.2*
4.	FCS_CKM.3	Cryptographic key access	—	*FCS_CKM.1* *FCS_CKM.4* *FMT_MSA.2*
5.	FDP_RIP.1	Subset residual information protection	—	—
6.	FDP_UIT.1	Data exchange integrity	—	*FDP_ACC.1* FTP_ITC.1

#	Component	Name	Hierarchical To	Dependencies
7.	FIA_AFL.1	Basic authentication failure handling	—	FIA_UAU.1
8.	FIA_SOS.1	Verification of secrets	—	—
9.	FIA_UAU.2	User authentication before any action	FIA_UAU.1	FIA_UID.1
10.	FIA_UAU.6	Re-authenticating	—	—
11.	FIA_UAU.7	Protected authentication feedback	—	FIA_UAU.1
12.	FIA_UID.2	User identification before any action	FIA_UID.1	—
13.	FPT_ITI.1	Inter-TSF detection of modification	—	—
14.	FPT_RVM.1	Non-bypassability of the TSP	—	—
15.	FPT_TDC.1	Inter-TSF basic TSF data consistency	—	—
16.	FTA_SSL.1	TSF-initiated session locking	—	FIA_UAU.1
17.	FTA_SSL.2	User-initiated locking	—	FIA_UAU.1
18.	FTP_ITC.1a FTP_ITC.1b	Inter-TSF trusted channel	—	—

7.2.3 Demonstration of mutual support between security requirements

1. The dependency analysis provided in Section 7.2.2 shows how supportive dependencies between SFRs, as identified in **[Reference 1]**, are satisfied. This section shows that the SFRs are mutually supportive by highlighting and discussing the additional supportive dependencies which ensures that the SFRs cannot be bypassed, tampered with, or circumvented.

2. FIA_UAU.2, FIA_UAU.6, and FIA_UAU.7 provide protection as it ensures that SFRs cannot be bypassed by impersonation of a different user. FIA_UID.2 ensures that no Entrust/Authority-mediated functions can be initiated until the user is uniquely identified to the TOE.

3. FAU_GEN.1 ensures that relevant events with specific data are captured in the audit log, as provided by Entrust/Authority. FAU_SAR.1 and FAU_SAR.3 ensure that authorized users have the capability to review data from the audit records with the ability to perform a search on audit data.

4. FPT_SEP.1 prevents tampering attacks against SFRs from external domains by preventing external interference by untrusted subjects, as supported by the abstract machine.

5. FTP_ITC.1a and FTP_ITC.1b protect privacy and integrity of exchanged data and prevent tampering attacks based on spoofing.

6. FDP_RIP.1 ensures that data is overwritten before it is made available to other subjects, preventing errant or non-malicious authorized software or users from bypassing or circumventing TOE security policy enforcement.

7. FIA_SOS.1 and FIA_AFL.1 reduce the likelihood of successful direct attack aimed at the identification and authentication functions, and thus support FIA_UAU.2, FIA_UAU.6, and FIA_UAU.7.

8. FDP_ACC.1 enforces access controls on all users, data objects, and operations on those objects, in support of exchanged data integrity, as provided by Entrust/Authority.

9. FDP_UIT.1 provides the ability to detect modification of exchanged security critical data, including security attributes, protecting against tampering attacks through unauthorized modification of data.

10. FPT_ITI.1 provides the ability to detect modification of inter-TSF security critical data, including security attributes, during transmission, protecting against tampering attacks through unauthorized modification of data.

11. FPT_TDC.1 provides the ability to detect of inconsistent inter-TSF security critical data, including security attributes, during transmission, protecting against tampering attacks through corruption of data.

12. FMT_MSA.2 ensures that only secure values are accepted for security attributes in support of key distribution and key access, as provided by Entrust/Authority.

13. FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 support key generation, key destruction, and cryptographic operations, respectively, as provided by the FIPS 140-1 validated Entrust software cryptomodule.

14. FCS_CKM.2 provides for the ability to securely exchange cryptographic keys with Entrust/Authority. FCS_CKM.3 provides for the ability to access keys as necessary in the course of key update and key recovery operations.

15. FTA_SSL.1 and FTA_SSL.2 provide that the TSF or operator locks an interactive session after a hard-coded period of time or manually, respectively, to free-up TOE resources and reduce the likelihood of tempering attacks on non-active connections.

7.2.4 Appropriateness of assurance requirements

1. This part of the ST rationale is to show that the identified assurance measures in Section 6.2 are appropriate for the TOE. The TOE is used as an interface to Entrust/Authority, a third-party trusted Certification Authority (CA) product responsible for certifying and authenticating users. As such, the TOE helps in establishing trust in the binding between a user's public key and other information in a certificate by digitally signing the certificate information using its signing private key. This trust is based on three basic principles:

    1) A valid digital signature on a certificate is a guarantee of the certificate's integrity;

    2) Since the CA is the only entity with access to its signing private key, anyone verifying the CA's signature on the certificate is guaranteed that only that CA could have created the signature; and

    3) Since only the CA has access to its signing private key, the CA cannot deny signing the certificate.

2. The EAL3-augmented assurance requirements listed in Table 19 and the TOE environment described in Section 5.2, together bring enough assurance elements for the TOE, operating within its environment as described in this document and under the assumptions made in Section 3.2, to be operated as an interface to a trusted third-party CA.

3. The augmentation to EAL3 addresses the area of problem tracking (ACM_SCP.2) and flaw remediation (ALC_FLR.2), providing assurance that any problems or flaws that may appear would be effectively remedied. The augmentation also adds the TOE component categorization report (AMA_CAT.1) which is required for maintaining the assurance rating of

the TOE, an Informal Security Policy Model (ADV_SPM.1) which is required as a dependency from several SFRs, and Validation of Analysis (AVA_MSU.2). Each of these augmented assurance components are included in this ST for informal compliance (i.e., without a formal compliance claim) with the NIST CS2 Protection Profile **[Reference 5]**.

4. In summary, the EAL3-augmented assurance level is technically feasible, achievable, and appropriate to satisfy the needs for trusted third-party CAs.

7.3 TOE Summary Specification Rationale

1. The TOE summary specification rationale is intended to show that the TOE security functions and assurance measures are suitable to meet the TOE security (functional and assurance) requirements.

2. To show that the selection of TOE security functions and assurance measures are suitable to meet TOE security requirements (functional and assurance), it is important to demonstrate the following:

   1) The specified TOE IT security functions work together so as to satisfy the TOE security functional requirements.

   2) The strength of TOE function claims are valid, or that assertions that such claims are unnecessary are valid.

   3) That the started assurance measures are compliant with the assurance requirements.

7.3.1 IT security functions rationale

1. This section of the ST rationale is intended to provide a demonstration that the specified IT security functions satisfy all SFRs included in the ST. This is best accomplished by mapping the IT security functions onto the SFRs by means of a table. This mapping, as shown in Table 24, will show that:

   1) Each SFR is mapped onto at least one IT security function, and

   2) Each IT security function is mapped onto at least one SFR

2. As can been seen from Table 24, each IT security function is mapped onto at least one SFR. As well, each SFR is mapped onto at least one IT security function. Thus, looking at the coverage of the IT security functions, it may be said that the specified TOE IT security functions work together so as to satisfy the TOE security functional requirements.

Table 24: Security functions mapping

IT Security Functions	CC Component	
Security Audit (FAU)		
Section 6.1.1.1 Audit review	FAU_SAR.1	Audit review
Section 6.1.1.2 Selectable audit review	FAU_SAR.3	Selectable audit review

IT Security Functions	CC Component	
Cryptographic Support (FCS)		
Section 6.1.2.1 Key distribution	FCS_CKM.2	Cryptographic key distribution
Section 6.1.2.2 Key access	FCS_CKM.3	Cryptographic key access
User Data Protection (FDP)		
Section 6.1.3.1 Residual information protection	FDP_RIP.1	Subset residual information protection
Section 6.1.3.2 Data exchange integrity	FDP_UIT.1	Data exchange integrity
Identification and Authentication (FIA)		
Section 6.1.4.1 Authentication failure	FIA_AFL.1	Basic authentication failure handling
Section 6.1.4.2 User and operator password criteria	FIA_SOS.1	Selection of secrets
Section 6.1.4.3 Authentication of users	FIA_UAU.2	User authentication before any action
Section 6.1.4.4 Re-authentication of operators	FIA_UAU.6	Re-authenticating
Section 6.1.4.5 Non-echoing of passwords	FIA_UAU.7	Protected authentication feedback
Section 6.1.4.6 Identification of users	FIA_UID.2	User identification before any action
Protection of the TSF (FPT)		
Section 6.1.5.1 Data exchange integrity	FPT_ITI.1	Non-Bypassability of the TSP
Section 6.1.5.2 Non-bypassability of security functions	FPT_RVM.1	Inter-TSF detection of modification
Section 6.1.5.3 Data consistency	FPT_TDC.1	Inter-TSF basic TSF data consistency
TOE Access (FTA)		
Section 6.1.6.1 Entrust/RA-initiated session locking	FTA_SSL.1	TSF-initiated session locking
Section 6.1.6.2 Operator-initiated session locking	FTA_SSL.2	User-initiated locking
Trusted Path/Trusted Channels (FTP)		
Section 6.1.7.1 Trusted channel	FTP_ITC.1a	Trusted channel
	FTP_ITC.1b	

7.3.2 Minimum Strength of Function Level rationale

1. The TOE mechanisms will resist medium-grade technical attacks by unauthorized users. The TOE mechanisms will also resist user errors, system errors, or non-malicious actions by authorized users. Resistance to high-grade sophisticated types of attacks, when such resistance is required, must be provided by the TOE operational environment. The environment also assumes that those individuals who have authorized physical access to the TOE are trusted to not behave maliciously.

2. Consequently, a level of strength of function medium (**SoF-Medium**) which indicates that a function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential is consistent with the security objectives of the TOE.

7.4 Assurance measures rationale

1. This part of the ST rationale is to show that the identified assurance measures in Section 6.2 are appropriate to meet the assurance requirements. This is best demonstrated in the form of a table, mapping the identified assurance measures onto the assurance requirements, as shown in Table 25.

2. In this case, the specification of assurance measures is done by reference to the appropriate document (e.g., Configuration Management Plan, System Architecture, User Guide, etc.). Obviously, analysis of the relevant documentation is required to show that the

referenced document (assurance measure) meets the requirements of the associated assurance requirement.

Table 25: Assurance measures

CC Assurance Component		Assurance Measure (Entrust document)
ACM_CAP.3	Configuration Management Plan	Configuration Management Plan v1.7
ACM_SCP.2	Problem Tracking CM Coverage	Configuration Management Plan v1.7
ADO_DEL.1	Delivery Procedures	Delivery Procedures v1.3
ADO_IGS.1	7Installation, Generation, and start-up	Installing Entrust/PKI 5.1 on Windows NT
ADV_FSP.1	Informal Functional Specification	Administering Entrust/PKI 5.0 on Windows NT Entrust/PKI 5.1 Supplement for Windows NT Addendum to Administering Entrust/PKI 5.0 v1.3
ADV_HLD.2	High Level Design	Entrust System Architecture (High-Level Design) v2.0
ADV_RCR.1	Informal Correspondence Demonstration	Informal Correspondence Demonstration v2.3
ADV_SPM.1	Informal Security Policy Model	Informal Security Policy Model v1.3
AGD_ADM.1	Administrator Guidance	Administering Entrust/PKI 5.0 on Windows NT Entrust/PKI 5.1 Supplement for Windows NT
ALC_DVS.1	Identification of Security Measures	Development Security: Security Measures v1.3
ALC_FLR.2	Flaw Reporting Procedure	Problem Reporting System (PRS) v1.4
AMA_CAT.1	TOE Component categorization Report	Categorization Report v1.5
ATE_COV.2	Analysis of Coverage	Analysis of Coverage v1.7
ATE_DPT.1	Testing - High Level Design	Analysis of Depth of Testing v1.6
ATE_FUN.1	Functional Testing	Entrust/PKI 5.1 Regression Testing Plan v0.2 Entrust/PKI 5.1 Security Function Tests v1.4 Entrust/PKI 5.1 Functionality and Interface Test Case Suite v1.3 Entrust/PKI 5.1 Administrative Restrictions Test Case Suite v0.4 Entrust/Master Control 5.1 Full Test Case Suite v1.1 Entrust/RA 5.1 Full Test Case Suite v1.2
ATE_IND.2	Independent Testing	Independent Testing Resources v1.5
AVA_MSU.2	Validation of Analysis	Validation of Analysis v1.1
AVA_SOF.1	Strength of TSF Evaluation	Strength of Function Analysis v1.6
AVA_VLA.1	Developer vulnerability analysis	Vulnerability Analysis v1.4

-PROPRIETARY-

-PROPRIETARY-

8 Glossary

ADM-API	Administration API
ANSI	American National Standards Institute
API	Application Programming Interface
ARL	Authority Revocation List
AS	Administration Service
BIF	Bulk Input File
CA	Certification Authority
CAST	Carlisle Adams, Stafford Tavares [Entrust symmetric key algorithm]
CC	Common Criteria
CMP	Certificate Management Protocols
COTS	Commercial Off The Shelf
CRL	Certificate Revocation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DN	Distinguished Name
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve DSA
FIPS PUB	Federal Information Processing Standard Publication
GUI	Graphical User Interface
GULS	Generic Upper Layers Security
I&A	Identification and Authentication
ID	Identity
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission
IP	Internet Protocol

IT	Information Technology
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MAC	Message Authentication Code
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX-CMP	Public Key Infrastructure (X.509) – Certificate Management Protocols
PP	Protection Profile
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman [public key algorithm]
SF	Security Function
SFP	Security Function Policy
SHA-1	Secure Hash Algorithm 1
SoF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

9 References

[Reference 1] Common Criteria for Information Security Evaluation. Version 2.1. CCIMB-99-031. August 1999.

[Reference 2] FIPS 140-1 Validation Report: Entrust Cryptographic Kernel Version 5.1. 2000. (not yet released).

[Reference 3] Security Target - Entrust/Authority 5.1. D. Stal. Entrust Technologies Ltd. Version 1.2. November 14, 2000.

[Reference 4] Installing Entrust/PKI 5.1 on Windows NT. Entrust Technologies Ltd. 2000.

[Reference 5] CSPP - Guidance for COTS Security Protection Profiles. Gary Stoneburner. NIST. Version 1.0. December 1999.