[redacted]

Entrust Technologies

Security Target

Entrust/Authority 5.0

Authors: Marc Laroche, Darryl Stal
Date: February 16, 2000
Version: 1.0

Document version control log

Version	Date	Author(s)	Description
0.1	April 5, 1999	Marc Laroche, Darryl Stal	Initial draft of Entrust/Authority 5.0 Security Target.
0.2	May 28, 1999	Darryl Stal	Updated with additional information for Entrust/Authority 5.0. Added **FTA_SSL.3.b**.
0.3	July 6, 1999	Darryl Stal	Added justifications for mapping to Table 27. Refined **FIA_SOS.2** and **FMT_MTD.1**.
0.4	July 9, 1999	Darryl Stal	Refined **FCS_COP.1**, **FCS_CKM.1**, and **FMT_MTD.1** by removal of ECDSA as choice for CA signing algorithm.
re0.5	August 13, 1999	Darryl Stal	Updated with respect to Syntegra comments from RFC 1. Refined names of attributes and data for **FIA_ATD.1** and **FMT_MTD.1**, respectively. Added justification for augmented assurance components to Section 7.2.4.
0.6	September 14, 1999	Darryl Stal	Corrected grammatical error in Table 26. Updated reference to Version 2.1 of the Common Criteria ISO specification. Renamed “Entrust/PKI 5.0 Administation Guide” to “Administering Entrust/PKI 5.0”.
0.7	October 8, 1999	Darryl Stal	Updated with respect to Syntegra comments from EOR 4. Refined listed of audit events. Removed CAST5-80 as a SEP encryption algorithm, added LDAD v3 reference to LDAP v2, refined description of Entrust/Master Control to include the command line shell, refined list of audit events, and added the AutoRA Administrator role.
0.8	November 23, 1999	Darryl Stal	Updated with respect to Syntegra comments from RFC 7. Refined password rules.
0.9	November 26, 1999	Darryl Stal	Corrected typographical error in Table 26.
1.0	February 16, 2000	Darryl Stal	Corrected dependency in Table 28.

Table of contents

List of figures

List of tables

1 Introduction

1.1 ST Identification

Title: Security Target for Entrust/Authority 5.0 (component of Entrust/PKI 5.0)

Assurance level: EAL3-augmented (EAL3+)

Keywords: Commercial-off-the-shelf (COTS), certification 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

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.

Entrust/Authority is the core component of an Entrust public-key infrastructure. Acting as the Certification Authority (CA), Entrust/Authority issues X.509 public-key certificates and performs key and certificate management functions, including:

- Creating encryption key pairs for users
- Creating certificates for all public keys
- Managing a secure database of Entrust information
- Enforcing an organization's security policy

Entrust/Authority includes other capabilities to ensure the security of an organization, including:

- Ability to interoperate with other Entrust CAs or with other vendors' CA products.
- Ability to support and maintain a strict PKI hierarchy and peer-to-peer relationships with other CAs, and provide fine-grained control to limit relationships between CAs.
- Ability to specify and modify what administrators and users can do through the flexible configuration of roles, groups, user registration dialogs, and user settings.
- Use of flexible certificates (to include any extensions in the X.509v3 standard or any properly formatted proprietary extension).
- Ability to change the distribution of setup information to users and to specify the authorization code lifetime.
- Use of flexible password rules.
- Ability to specify either RSA 1024-bit, RSA 2048-bit, or DSA 1024-bit as the CA signing algorithm and CA signing key size.

- Ability to renew the CA signing key pair before it expires and to recover from possible CA key compromise.

Meeting the requirements established in this ST signifies that Entrust/Authority:

- Provides the functionality appropriate for controlling a community of benign (i.e., not intentionally hostile nor malicious) authorized users.
- Protects against technical attacks by individuals other than authorized users.
- Enforces an access control policy between active entities (subjects) and passive objects based on subject identity, authenticated role and allowed actions.
- Provides reliable and standardized cryptographic services, including key management.
- Provides mechanisms to detect corrupted data objects.
- Protects against re-use of deallocated data objects.
- Provides mechanisms for trusted recovery in the event of system failure or detection of insecurity.
- Supports these capabilities in distributed system environments.

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.
- 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.
- Physical security is provided as required.
- The abstract machine (i.e., hardware platform and operating system) operate in a correct and expected manner.
- Competent security administration is performed.

When used in conjunction with appropriate environmental constraints, the TOE is suitable for the generation and protection of public key certificates in real-world environments, both commercial and government.

1.3 CC Conformance Claim

This TOE is:

1) CC Version 2.1 Part 2-conformant.

2) CC Version 2.1 Part 3-conformant, 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

The TOE contains only one security function (i.e., Verification of Secrets) that is realized by a probabilistic or permutational mechanism. The minimum strength level claimed for this function is **SOF-Medium**. Thus, the global minimum strength level claimed for the TOE is also **SOF-Medium**.

2 TOE Description

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

The Entrust-based public key infrastructure (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 key pairs; and
- Publishes the public keys with the user's identification as certificates in open bulletin boards (e.g., X.500 directory services).

Entrust/Authority is the heart of Entrust-based Public Key Infrastructure. It is responsible for providing almost all of the functionality and security safeguards required in a PKI.

2.2 TOE Services

Entrust/Authority is responsible for creating and issuing end-entity public-key certificates, Certification Revocation Lists (CRLs), and Authorization Revocation Lists (ARLs) and publishing them in a X.500 public directory. In addition, Entrust/Authority provides the infrastructure support functions that are expected of a high-quality CA, such as maintaining end-entity encryption key-pair history and end-entity verification certificate history, providing automatic public key and certificate updates, auditing security-related events, and maintaining CA data confidentiality and integrity.

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

1) **Core Services:** The Core Services are the basis for all public key infrastructure management functionality.

2) **Support Services:** The Support Services comprise a set of services relating to management of Entrust/Authority-related components. These services include CA Self-Management, Entrust/Authority Database Management, Audit Trail Management, and Directory Management.

2.2.1 Core Services

Core Services are provided with each Entrust/Authority. They are required to provide encryption and authentication services to end-entities. They consist of:

1) **CA Key Management Service:** This service is, among other things, responsible for managing the CA signing key pair, master keys, enforcing infrastructure security policies, and specifying policy for subordinate CAs .

2) **End-entity Management Service:** Similar to Operator Management, the End-entity Management Service allows authorized operators to manage End users associated with a CA domain or group. This service allows, for example, for creating, initializing, and deleting users, recovering, revoking, and updating keys, and other functions.

3) **Operator Management Service:** This service is responsible for providing the capability to authorized operators to manage other operators. Passwords, keys, roles and privileges, and other operator attributes are managed through this service.

4) **Cross-Certificate Management Service:** This service manages the generation and maintenance of cross-certificates.

2.2.2 Support Services

Support Services are provided with each Entrust/Authority infrastructure. They provide support capabilities to the CA Core Services. The Support Services consist of:

1) **Self Management Service:** Service to initialize Entrust/Authority, start and stop Entrust services, and validate operator passwords.

2) **Database Management Service:** Service to operate and maintain the repository that stores security critical data Entrust/Authority needs for proper operation (e.g., security policy data, end user encryption key pairs).

3) **Audit Trail Management Service:** Service to maintain and analyze an audit record of critical and non-critical events that have occurred within the Entrust infrastructure.

4) **Directory Management Service:** Service to operate and maintain the Directory and Directory entries (e.g., search the directory, create new entries, modify attributes).

2.3 TOE High-Level Architecture

Entrust/Authority is comprised of several related and inter-dependent software and hardware modules that cooperate to provide all Entrust/Authority services, as can be seen in Figure 1.

2.3.1 Entrust operator roles

There are two human interfaces into Entrust/Authority: Entrust/Master Control (which is part of the Entrust/Authority TOE) and Entrust/RA.

Entrust/Master Control is used to manage Entrust/Authority itself. It is comprised of a GUI and a command line shell. The functions available through Entrust/Master Control include, but are not limited to: perform initial configuration of Entrust/Authority, enable/disable services, verification of the Entrust/Authority database, schedule database backups, and performing exceptional PKI-management events such as database re-encryption and Security Officer key recovery.

Entrust/RA is a remote administrative user interface for day-to-day management of Entrust end users and administrative users. Hence, management of Entrust/Authority and Entrust users is assigned to the defined Entrust roles listed below and presented in the following sections:

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

It should be noted that there is an additional role in Entrust, that of End User [1]. This type of user has no administrative access to Entrust/Authority via Entrust/RA or Entrust/Master Control.

2.3.1.1 Master User

Master Users, as the only Entrust operators who can access Entrust/Master Control, are responsible for the initial configuration of Entrust/Authority, for its ongoing maintenance and database integrity. Other functions include changing performing database backups and starting and stopping services as needed. The set of duties applicable only to Master Users is presented in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

2.3.1.2 Security Officer

The main role of the Security Officer is to set and administer the organization's security policy as it applies to all Entrust users in the organization. Security Officers may also add, delete, and configure other administrative users, including defining and configuring new roles. Although Security Officers use Entrust/RA to perform their duties, their privileges (permissions) are enforced by Entrust/Authority. Security Officers also have end-entity management privileges, and are Entrust end users (end-entities) themselves. The set of duties applicable to Security Officers is presented in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

2.3.1.3 Administrator

The main role of the Administrator is to add, enable, disable, change end user DNs, recover Entrust users, and to revoke certificates. Administrators may also set user certificate lifetimes and encryption and verification certificate policies. Although Administrators use Entrust/RA to perform their duties, their privileges (permissions) are enforced by Entrust/Authority. Administrators are also end-users. The set of duties applicable to Administrators is presented in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

[1] Also referred to as an Entrust user or end-entity.

2.3.1.4 Directory Administrator

Directory Administrators are responsible for maintaining the Directory used as a repository for certificates, CRLs and ARLs. As such, their main role is to add and delete Entrust users entries to and from the Directory, either in bulk or one at a time. Entrust/RA queries Entrust/Authority to determine the current user's directory administration privileges and enables or disables these services in its GUI as appropriate. Directory Administrators are also end users. The set of duties applicable to Administrators is presented in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of Administering Entrust/PKI 5.0 **[Reference 4]**.

2.3.1.5 Auditor

The main role of the Auditor is to review audit logs and create reports. Their privileges are enforced by Entrust/Authority. The set of duties applicable to Auditors is presented in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

2.3.1.6 AutoRA Administrator

The AutoRA Administrator role is intended to restrict the administrative functions that Entrust/AutoRA, an optional Entrust product, can perform. Entrust/AutoRA automates the process of adding users to Entrust/PKI. This role, which can only administer End-Users, has a similar, yet reduced set of permissions from that of the Administrator role. The set of duties applicable to the AutoRA Administrator is presented in the **Release Notes** to Entrust/PKI 5.0.

2.3.1.7 Custom-defined (flexible) roles

The configuration of roles provides the ability to grant or deny administrative access to various operations including: user administration operations (e.g., enable user, recover user, revoke certificate), types of certificates, security policy operations, audit log access, directory operations, and database operations. The creation of custom-defined roles is presented in the **Creating Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

2.3.1.8 End User

End Users are the ultimate recipients of Entrust/Authority services. An end user is a recipient of credentials, a creator of signed and/or encrypted information, or, in other terms, the ultimate consumer of the PKI services provided by Entrust/Authority. End users use an Entrust/Engine (e.g., as a subcomponent of Entrust/RA and Entrust/Entelligence) to perform their duties. Their privileges are enforced by Entrust/Authority, directly in the case of initialization and key recovery, and indirectly via certificates and revocation lists issued by Entrust/Authority. Cryptographic and PKI services are available to end users from any Entrust-Ready application via Entrust/Engine. The End User role is described in the **Entrust/PKI Roles** section of **Chapter 1 (About Entrust/PKI)** and in the **Overview of Roles** section of **Chapter 11 (Customizing Entrust/PKI)** of **Administering Entrust/PKI 5.0 [Reference 4]**.

2.3.2 Entrust/Authority components

The Entrust/Authority architecture is shown in Figure 1. As can be seen from this diagram, Entrust/Authority is comprised of several related and inter-dependent software and hardware modules that cooperate to provide all Entrust/Authority services. These services and the

components used to provide them are described below. Entrust/Authority is installed as a single package on a single node. All Entrust/Authority components execute only on that single node, including Entrust/Master Control.

2.3.2.1 Entrust/Authority Engine

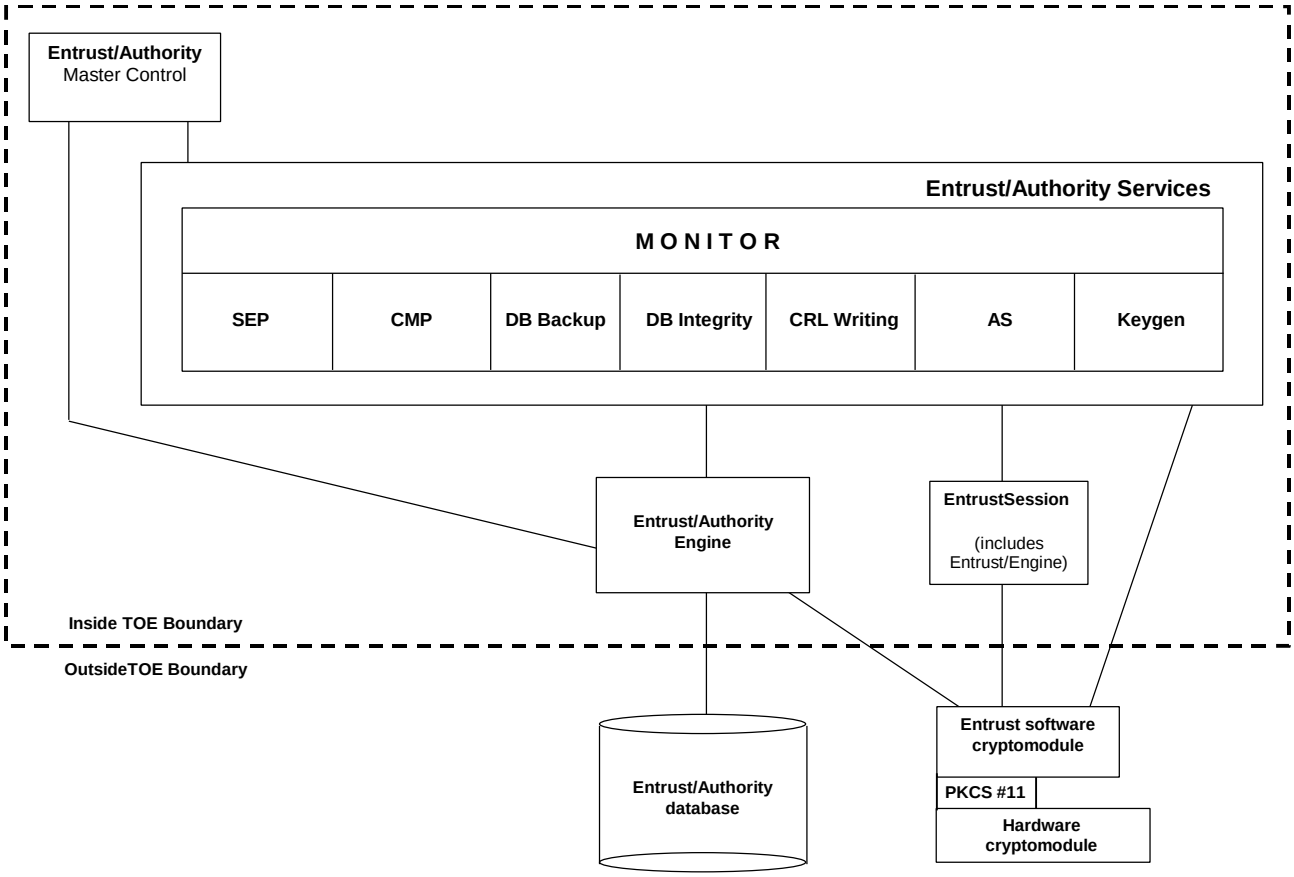
The Entrust/Authority Engine is the runtime library that implements and performs all Entrust/Authority functions. The executable components, described in Section 2.3.2.2 below, each access a subset of the Entrust/Authority Engine's capabilities. Entrust/Authority Engine is the component that implements database access, and that makes use of the Entrust cryptomodule to perform all cryptography-related Entrust/Authority functions, such as CA signing key pair generation, certificate signing, and end-entity encryption key pair generation.

2.3.2.2 Entrust/Authority executable components

2.3.2.2.1 Entrust/Master Control

Entrust/Master Control, comprised of a GUI and command line shell, is used to manage Entrust/Authority itself. That is, to perform initial configuration of Entrust/Authority based on data provided during software setup, to verify the integrity of the Entrust/Authority database, to schedule backups of the database, and to perform exceptional PKI-management events such as PKI operator recovery. In other words, Entrust/Master Control provides the interface into initialization and maintenance services, as well as certain support and operator management services.

Figure 1: Entrust/Authority architecture



2.3.2.2.2 Entrust/Authority Service (Monitor)

The Entrust/Authority Service (Monitor) executable will be used to launch and monitor the following subsystems:

- Secure Exchange Protocol (SEP)
- PKIX-CMP (Certificate Management Protocol)
- Administration Service (AS)
- Database Backup
- Database Integrity
- CRL/ARL Writing
- Key generation (Keygen)

All are built atop the core Entrust/Authority components, that is, atop the Entrust/Authority Engine, the Entrust cryptomodule, and the database. Each subsystem is actually an instantiation of the Entrust/Authority Service executable.

While the Entrust/Authority Service consists of several subsystems, each one is actually an instantiation of the same Entrust/Authority Service (Monitor) executable. There is always only a single instantiation of the Entrust/Authority Service. That is, there is only a single Entrust/Authority Service process. An argument to the function calling the process determines which subsystem is started.

The Entrust/Authority Service performs the following activities:

- acts as the initial startup process
- starts all the other processes (subsystems)
- monitors the progress of each of the other subsystems and detects the death of any of its subsystems
- signals a subsystem process to shutdown

2.3.2.2.3 AS subsystem

The Administration Service (AS) is a subsystem that listens for and processes requests from Entrust/RA. For each AS request that arrives, a new AS process is spawned. In addition to being built atop the core Entrust/Authority components, AS uses the EntrustSession toolkit to secure communications with Entrust/RA and to authenticate operator end-entities identities.

Therefore, AS makes use of the Entrust/Engine, the core PKI client module via EntrustSession, and makes use of Entrust cryptomodule via both Entrust/Authority Engine and Entrust/Engine (indirectly via EntrustSession). All use of the Entrust cryptomodule is transparent to AS, however.

AS implements the server side analog to the ADM-API toolkit. That is, it responds to ADM-API requests. Since ADM-API is itself an application of EntrustSession, all connections between AS and ADM-API clients such as Entrust/RA are secured for confidentiality and

integrity using EntrustSession. Since the endpoints must mutually authenticate each other, an Entrust identity is required within AS.

2.3.2.2.4 SEP subsystem

SEP is a subsystem that listens for end-entity key management requests. That is, requests for client initialization, key update, or key recovery from Entrust/Engine or third-party SEP-aware client engines. For each SEP request that arrives, a new SEP process is spawned.

2.3.2.2.5 PKIX-CMP subsystem

CMP is a subsystem built from scratch to handle all PKIX-CMP requests. For each PKIX-CMP request that arrives, a new PKIX-CMP process is spawned. However, this addition to the architecture allows the older and new PKIX messages to co-exist and not break backwards compatibility and provide consistency for SEP and PKIX-CMP.

Depending on the clients that will need to access SEP or PKIX-CMP, both SEP and PKIX-CMP will be able to be stopped or started (turned on or off) as per the requirements. That is, SEP can be disabled if all clients are Entelligence 5.0 users or PKIX-CMP can be disabled if all clients are Entelligence 4.0 users or earlier.

2.3.2.2.6 Database Backup subsystem

The database backup subsystem is a process that performs all database backup activities. This subsystem runs transparently in the background and cannot be disabled from the Entrust/Master Control GUI. This subsystem will never have more than one process.

2.3.2.2.7 Database Integrity subsystem

The database integrity subsystem is a process that performs all database integrity validation activities. This subsystem runs transparently in the background and cannot be disabled from the Entrust/Master Control GUI. This subsystem will never have more than one process.

2.3.2.2.8 CRL/ARL Writing subsystem

The CRL writing backup subsystem is a process that performs all revocation list writing to the directory and CRL checking activities at Entrust/Authority. This subsystem runs transparently in the background and cannot be disabled from the Entrust/Master Control GUI. This subsystem will never have more than one process started.

2.3.2.2.9 Key generation subsystem

The key generation subsystem (Keygen) is a process that performs all pre-generation of public key pairs. This subsystem runs transparently in the background and cannot be disabled from the Entrust/Master Control GUI. This subsystem will never have more than one process started.

Keygen access the security kernel (SK) directly to generate keys. The AS, SEP, and CMP subsystems read keys directly from memory. They don't communicate directly with the Keygen process but use semaphores to co-ordinate Keygen, AS, SEP, and CMP using a producer-consumer queue/stack.

2.3.2.3 EntrustSession Toolkit

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

The TOE boundary is based on the support for the Entrust/Authority features and services by the Entrust/Authority 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/Authority TOE boundary is indicated in Figure 1.

The components that are included within the Entrust/Authority TOE boundary are:

- Entrust/Authority Service (Monitor)
- AS subsystem
- SEP subsystem
- PKIX-CMP subsystem
- Database backup subsystem
- Database integrity subsystem
- CRL/ARL writing subsystem
- Key generation subsystem
- Master Control
- EntrustSession Toolkit
- Entrust/Authority Engine

2.3.4 Exclusion from the TOE Boundary

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

- Entrust cryptographic module
- Entrust/Authority database
- Hardware and operating system platform (Abstract Machine) [2]

2.3.4.1 Entrust Cryptographic module

The justification for excluding the cryptomodule from the TOE boundary is that the Entrust 5.0 Security Kernel is validated to Level 2 under the FIPS 140-1 evaluation **[Reference 2]**.

[2] Not illustrated in Figure 1.

2.3.4.2 Entrust/Authority database

The justification for excluding the database from the Entrust/Authority TOE boundary is based on the following factors, described below:

1) **Database security provided by Entrust:** This Security Target makes no claims about inherent database security. All database security (i.e., confidentiality and integrity) is provided by Entrust, not the database. As such, all sensitive data items stored in the Entrust/Authority database are encrypted (using the Entrust Master and CA Master encryption keys) to support the TOE Access Control SFP, and provided with integrity protection (using the Entrust Master and CA Master integrity keys) to generate MACs for each data item.

2) **Database functionality not mapped to SFRs:** This Security Target makes no claims about database functionality (aside from the inherent, fundamental, and basic function of data storage). The Entrust/Authority database operates only as a data warehouse for user and system data. Database functionality is not mapped to any of the SFRs in this Security Target.

3) **Well-defined database interface:** The only interface to the database is through Entrust/Authority and the ODBC-API **[Reference 5]**. That is, database access is only available through a well-defined interface (ODBC-API). Any Entrust/Authority database data items are in plaintext only while within the Entrust/Authority TOE boundary. Any Entrust/Authority database data items transmitted across the TOE boundary are provided with confidentiality and integrity protection.

2.3.4.3 Hardware and operating system platform (Abstract Machine)

The TOE abstract machine consists of the ITSEC E3/F-C2 evaluated Windows NT 4.0 operating system with Service Pack 3 and any hardware for which the operating system and TOE configurations are valid. The justification for excluding the abstract machine from the Entrust/Authority 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 SP3 has been certified to the ITSEC E3/F-C2 level.

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 Server operating system (Intel-based U.S. version) with Service Pack 3 or 4.
   - 64 Mbytes of RAM
   - 128 Mbytes of swap space
   - Pentium 166 or better

- one 2X or faster CD-ROM drive
- TCP/IP stack installed
- 64 Mbytes of free disk space if using the ICL i500 Directory
- disk space requirements according to Installing Entrust/PKI 5.0 on Windows NT **[Reference 3]**

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 operating system, which is assumed to be trusted. The operating system, in turn, interacts with the hardware platform (e.g., via the computer's BIOS and/or various device drivers).

2.4 Cryptography-related IT Assets

The cryptographic aspect of the TOE requires that cryptography-related security critical items be protected. Entrust/Authority's functions and services ensure that the following security critical assets are protected against unauthorized disclosure and modification:

- Cryptographic variables (including private keys, public keys, public parameters, initialization vectors, etc.)
- Input and output data from the cryptographic function (e.g., plaintext input and ciphertext output)
- The implementation of the cryptographic services
- Other critical security parameters (e.g., authentication data)

3 TOE Security Environment

3.1 Introduction

This section identifies the following:

1) Significant assumptions about the TOE's operational environment (Section 3.2)

2) IT-related threats to the organization countered by TOE components (Section 3.3.1)

3) Threats requiring reliance on environmental controls to provide sufficient protection (Section 3.3.2)

4) Organizational security policies for which this TOE is appropriate (Section 3.4)

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

The specific conditions listed below 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.LOCATE	The TOE processing resources that depend on software as well as hardware features will be located within controlled access facilities that mitigate unauthorized physical access	The TOE cannot be expected to meet its security requirements unless physical security is provided.
	A.PROTECT	The TOE abstract machine is physically protected from unauthorized modification.	
Cryptographic Operations	A.CRYPTO	The cryptographic operations are performed on a FIPS 140-1 validated or equivalent cryptographic module.	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 after manual verification.	The TOE is independent of the hardware platform used, assuming the hardware platform meets the TOE system requirements and operates correctly. This assumption implies that the operating system has been manually verified as operating properly. The TOE is relying upon NT 4.0, which is trusted[3]. The TOE only interacts with the

[3] Microsoft Windows NT 4.0 with Service Pack 3 has been evaluated to the E3/F-C2 level under the UK ITSEC scheme.

Type	Assumption		Discussion
			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 [4] are competently installed and administered.	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.
Connectivity	A.CONNECT	All connections to peripheral devices reside within the controlled access facilities.	This ST addresses security concerns related to the manipulations of the TOE through its legitimate interface. Connections between the TOE and insecure networks are assumed to be protected against unauthorized remote access.

3.3 Threats to security

The TOE, in conjunction with its environment, counters the threats which may be broadly categorized as:

- Threats of malicious attacks from individuals other than authorized users
- Threats of authorized users attempting, non-maliciously, to gain unauthorized access or to perform an unauthorized operation. Such attempts may be performed to “get the job done”, out of curiosity, as a challenge, or as a result of an error.

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.

[4] 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.

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
3.	**T.AUDIT-CORRUPTED** Deliberate and accidental unauthorized modification or destruction of security events records by malicious individuals or because of equipment failure may not be noticeable.	O.DETECT O.MANAGE
4.	**T.DATA-CORRUPTED** A deliberate or accidental threat occurrence corrupting security critical data of the TOE, which could cause disruptions on the secure operations of the TOE, may not be detected.	O.DETECT
5.	**T.DENIAL** The TOE may be subjected to an unsophisticated, denial-of-service attack, by a malicious unauthorized individual attempting to gain logical access to the TOE, potentially resulting in mid-term to long-term unavailability of TOE services.	O.AVAILABLE

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 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

#	Threat Name and Description	Objectives (See Section 4)
4.	**T.ENTRY-SOPHISTICATED** An unauthorized individual (i.e., other than an authenticated user) may gain unauthorized malicious access to TOE processing resources or security critical data, including cryptography-related assets, using sophisticated IT security defeating tools.	O.ENTRY-SOPHISTICATED
5.	**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
6.	**T.ADMIN-ERROR** TOE Security policies may be circumvented because of errors or omissions in the administration of the security features of the TOE, resulting in unauthorized individuals gaining access to TOE data and resources.	O.MANAGE
7.	**T.SYSTEM-CORRUPTED** A deliberate or accidental threat occurrence corrupting the abstract machine of the TOE to enable future insecurities in the TOE may not be detected.	O.DETECT-ABSTRACT
8.	**T.DENIAL-SOPHISTICATED** The TOE may be subjected to a sophisticated, denial-of-service attack, by a technically competent malicious unauthorized individual who would compromise availability of TOE services.	O.DENIAL-SOPHISTICATED
9.	**T.CRASH** Human error or a failure of software, hardware, or power supplies may cause an abrupt interruption to the operation of the TOE, resulting in loss or corruption of security-critical data.	O.RECOVER

3.3.1 Threats addressed by TOE

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 high-grade sophisticated types of attacks, when such resistance is required, must be provided by the TOE operational environment.

3) **T.AUDIT-CORRUPTED:** Deliberate and accidental unauthorized modification or destruction of security events records by malicious individuals or because of equipment failure may not be noticeable.

   TOE security depends in part on the ability of the TOE to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized modification or destruction.

4) **T.DATA_CORRUPTED:** An accidental or deliberate unauthorized modification (i.e., other than those made by the TOE on behalf of an authenticated user or process) of security critical data objects which could affect the secure state of the TOE may not be detected.

   TOE security critical data objects are stored outside of the TOE boundary, where the TOE does not enforce its access control policy. The non-detection of such unauthorized modifications could compromise the security state of the TOE.

5) **T.DENIAL:** The TOE may be subjected to an unsophisticated, denial-of-service attack, by a malicious unauthorized individual attempting to gain logical access to the TOE, potentially resulting in mid-term to long-term unavailability of TOE services.

   This threat mainly includes attacks through the TOE logical interfaces.

3.3.2 Threats to be addressed by the operating environment

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

- not addressed by, or
- only partly addressed by the TOE

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 3]**.

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 correctly by system administrators and authorized users in accordance with security policy and guidance documentation.

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-SOPHISTICATED:** 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, using sophisticated IT security defeating tools.

   Such sophisticated security defeating tools include Trojan Horse, password capturing programs and others; attacks using these tools can be countered by TOE security functions in conjunction with physical security, firewalls, intrusion detection features, security training and awareness, and other protection mechanisms provided by the environment.

5) **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.

6) **T.ADMIN-ERROR:** TOE Security policies may be circumvented because of errors or omissions in the administration of the security features of the TOE, resulting in unauthorized individuals gaining access to TOE data and resources.

   Authorized users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain unauthorized access.

7) **T.SYSTEM-CORRUPTED:** A deliberate or accidental threat occurrence corrupting the abstract machine of the TOE to enable future insecurities in the TOE may not be detected.

   The TOE security depends to a large degree on the abstract machine. If this is intentionally corrupted, the TOE will be unable to maintain a secure state. The TOE can only partially protect against this threat.

8) **T.DENIAL-SOPHISTICATED:** The TOE may be subjected to a sophisticated, denial-of-service attack, by a technically competent malicious unauthorized individual who would compromise availability of TOE services.

   The TOE is not capable of resisting sophisticated denial of service attacks and must therefore, rely on protections provided by its environment to maintain availability in the face of such threats.

9) **T.CRASH:** Human error or a failure of software, hardware, or power supplies may cause an abrupt interruption to the operation of the TOE, resulting in loss or corruption of security-critical data.

   For the TOE to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service.

   System crash can occur with inadequate mechanisms for secure recovery. User data objects, TSF data objects, other security sensitive data and system or application software may be corrupted.

3.4 Organizational Security Policies

The TOE, in conjunction with 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.ACCESS** Users are granted access rights to services and specific data objects, including security sensitive cryptographic data objects such as private keys, as determined by object attributes assigned to objects, user identity and user attributes in accordance with an organizational security policy.	The TOE supports organizational policies which grant or deny access to objects using rules driven by attributes of the user, attributes of the object and type of access.	O.ACCESS O.AUTHORIZE

#	Policy Name and Description	Discussion	Objectives (See Section 4)
2.	**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
3.	**P.SURVIVE** The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	The TOE provides a measure of this resilience through functionality and assurances that resist, detect, and recover from insecurities. For sophisticated attacks, a large portion of this resilience is provided by the TOE environment.	O.RECOVER O.DETECT O.AVAILABLE O.RECORD O.DETECT-ABSTRACT O.DENIAL-SOPHISTICATED
4.	**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
5.	**P.ORIGIN** Public key certificates, Certificate Revocation Lists and Authority Revocation Lists must be electronically bound to their originating entity through digital signatures.	The TOE supports organizational policies requiring that public key certificates, CRLs and ARLs be digitally signed by the issuing entity.	O.ORIGIN
6.	**P.RECEIPT** Mechanisms must be provided to enforce the generation of evidence of receipt for distributed keys and certificates between trusted parties.	The TOE supports organizational policies requiring that evidence of receipt be generated for cryptographic keys and certificate it distributes.	O.RECEIPT
7.	**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 publishes public key certificates and lists of revoked certificates called Certificate Revocation Lists (CRLs). The TOE also uses protocols which provide for secure exchange of secret keys.	O.KEY-DISTRIBUTE

#	Policy Name and Description	Discussion	Objectives (See Section 4)
8.	**P.KEY-RECOVER** Mechanisms must be provided to allow for recovery of end-user encryption keys by authorized administrative users and automatic update of these keys as required.	The TOE maintains a backup of the user encryption keys it generates to allow for key recovery and also updates end users encryption keys automatically.	O.KEY-RECOVER
9.	**P.NETWORK** The organization's IT security policies (identified in 1 to 8 above) must be maintained when IT components need to interoperate via network connections.	The TOE maintains the enforcement of its security policies when interoperating with other IT components via network connections.	O.NETWORK

4 Security Objectives

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 IT Security Objectives

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.ACCESS** The TOE must provide access by authorized users to those objects and services for which they have been authorized.	P.ACCESS
2.	**O.KNOWN** The TOE must ensure that all users are identified and authenticated before being granted access to TOE mediated resources.	T.ENTRY
3.	**O.AUTHORIZE** The TOE must provide the ability to specify and manage user and system process access rights to individual objects and services.	P.ACCESS
4.	**O.ACCOUNT** The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	P.ACCOUNT
5.	**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
6.	**O.ENTRY** The TOE must prevent unauthorized logical entry to the TOE by technical methods used by persons without authority for such access.	T.ENTRY
7.	**O.DETECT** The TOE must enable the detection of corrupted security critical data, including audit trail, and the detection of replayed operations which could subsequently compromise the secure state of the TOE. The level of detection provided must correspond to the level of attack sophistication being protected against by the other security objectives.	P.SURVIVE T.AUDIT-CORRUPTED T.DATA-CORRUPTED
8.	**O.AVAILABLE** The TOE must protect itself from unsophisticated, denial-of-service attacks.	P.SURVIVE T.DENIAL

#	IT Security Objective	Addressed Threat or Policy
9.	**O.ORIGIN** The TOE must generate evidence of origin for transmitted public key certificates, CRLs and ARLs.	P.ORIGIN
10.	**O.RECEIPT** The TOE must successfully validate the evidence of receipt for received keys and certificates it distributes to trusted entities.	P.RECEIPT
11.	**O.KEY-DISTRIBUTE** The TOE must provide for authorized administrative users to distribute and revoke public key certificates, and be able to securely and transparently exchange secret keys as required.	P.KEY-DISTRIBUTE
12.	**O.KEY-RECOVER** The TOE must provide for authorized administrative users to recover end-user encryption keys, and automatically update these keys as required.	P.KEY-RECOVER
13.	**O.RECORD** The TOE must record security critical events to ensure that the information exists to support effective security management.	P.SURVIVE P.ACCOUNT
14.	**O.NETWORK** The TOE must continue to be able to meet its security objectives when networked with other IT resources. The TOE security policy must be maintained on exported data objects, including cryptographic keys.	P.NETWORK

4.2 Environmental Security Objectives

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 non-IT security objectives which are listed in Table 6.

Table 6: TOE environmental security objectives

#	TOE Environment Security Objectives	Addressed Threat or Policy

#	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.OPERATE** Those responsible for the TOE [5] must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	T.INSTALL T.OPERATE
3.	**O.MANAGE** Those responsible for the TOE must ensure that the TOE is managed and administered in a manner that maintains IT security.	T.ADMIN-ERROR T.AUDIT-CORRUPTED
4.	**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
5.	**O.ENTRY-SOPHISTICATED** The TOE environment must sufficiently counter the threat of an individual (other than an authorized user) gaining unauthorized access via sophisticated technical attack.	T.ENTRY-SOPHISTICATED
6.	**O.ENTRY-NON-TECHNICAL** The TOE environment must provide sufficient protection against non-technical attacks by other than authorized users.	T.ENTRY-NON-TECHNICAL
7.	**O.DETECT-ABSTRACT** The TOE environment must provide the ability to detect unauthorized modification and corruption of the TOE abstract machine.	P.SURVIVE T.SYSTEM-CORRUPTED
8.	**O.DENIAL-SOPHISTICATED** The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.	P.SURVIVE T.DENIAL-SOPHISTICATED
9.	**O.RECOVER** The TOE, in conjunction with its environment, must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity.	P.SURVIVE T.CRASH

[5] "Those responsible for the TOE" are those that are have been designated in their organization to ensure that the TOE is installed and operated correctly, in accordance with the organizational security policy. They may, but not necessarily, consist of TOE authorized users (e.g., Master User or Security Officer).

5 IT Security Requirements

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

This section identifies and specifies the SFR components that the Entrust/Authority 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).

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/Authority, and assist in making the demonstration of traceability easier.

The headings used to group the Entrust/Authority SFRs are listed below:

1) Access Control

2) Separation of Duties

3) Identification & Authentication

4) Key Management

5) Audit

6) Trusted Path and Data Protection

7) Non-bypassability and Recovery

5.1.1 Access control

This section specifies the Access Control security requirements for Entrust/Authority. The Access controls security requirements are summarized in Table 7.

Table 7: Access control security requirements

#	Security Requirement		Component
1.	Access control	Scope of policy (subjects, objects, and operations)	FDP_ACC.2
		Access rules	FDP_ACF.1
2.	Access control attributes	Management of security attributes	FMT_MSA.1
		Enforcement of secure security attribute values	FMT_MSA.2
		Initialization of security attributes	FMT_MSA.3
		Definition of user security attributes	FIA_ATD.1

#	Security Requirement		Component
3.	Access control data management	Management of system data	FMT_MTD.1
		Secure system data values	FMT_MTD.3
4.	Residual information protection	Subset residual information protection	FDP_RIP.1

5.1.1.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the ***Access Control SFP*** on ***all Entrust/Authority objects associated with operations performed by Master Users, Security Officers, Administrators, Directory Administrators, Auditors, AutoRA Administrators, and any custom-defined roles*** and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Note: The Access Control SFP refers to the access control security policy enforced by a security function.

5.1.1.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***Access Control SFP*** to objects based on ***security attributes (i.e., user identity and role permissions).***

FDP_ACF.1.2 The TSF shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: ***Entrust/Authority shall control access to objects by all users through the permissions associated with the identity and role of the user.***

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rule: ***all users shall have access to the objects associated with the permissions of the user's role's permissions.***

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the ***role permissions and identity of the user. All users shall be denied access to the objects not associated with the user's role's permissions.***

5.1.1.3 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***Access Control SFP*** to restrict the ability to ***change defaults, query, modify, delete, or read*** the security attributes ***shown in Table 8*** to ***the roles indicated in Table 8***.

5.1.1.4 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.1.5 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the ***Access Control SFP*** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***authorized identified roles, with the privileges to do so, as indicated in Table 8*** to specify alternative initial values to override the default values when an object or information is created.

5.1.1.6 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users ***as shown in Table 8***.

Table 8: Management of user security attributes

#	Security attribute	Role	Access
1.	***RoleId*** Indicator of the role of the user. Adding users sets the attribute to the Role ID of the associated role.	Security Officer	From Entrust/RA: Query, read, modify, and delete.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: Query, read, modify, and delete.
2.	***State*** Indicates user state. The user's state can change based on operation performed on him/her by a Security Officer, Administrator, or custom-defined role with appropriate privileges (e.g., Enabling the user, Disabling the user, Setting the user for key recovery, etc.).	Security Officer	From Entrust/RA: Query, read, modify, and delete.
		Administrator	From Entrust/RA: Query, read, modify, and delete.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: Query, read, modify, and delete.
3.	***RolloverAllowed*** Indicates whether the user is set for automatic key update when the default settings are not used. Modified when setting the security policy, associating a user with a different role, or changing the role's definition.	Security Officer	From Entrust/RA: Change default, query, read, modify, and delete.
		Administrator	From Entrust/RA: Change default, query, read, modify, and delete.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: Change default, query, read, modify, and delete.
4.	***UserPermissions*** Vector corresponding to a user's role's permissions. Modified when setting the security policy, associating a user with a different role, or changing the role's permissions.	Security Officer	From Entrust/RA: Change default, query, read, modify, and delete.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: Change default, query, read, modify, and delete.
5.	***Tok*** Master User password token. Created at installation and modified when changing a Master User password.	Master User	From Entrust/Master Control GUI: Read and Modify.

5.1.1.7 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to ***modify, delete, or clear*** the ***TSF data indicated in Table 9*** to ***the authorized identified roles indicated in Table 9***.

Table 9: Management of Entrust system data

#	Data Description	Role	Access
1.	***SEP subsystem disabled*** Indicates whether SEP starts with Entrust/Authority service.	Master User	From Entrust/Master Control: may modify between TRUE or FALSE (default).
2.	***PKIX subsystem disabled*** Indicates whether PKIX starts with Entrust/Authority service.	Master User	From Entrust/Master Control: may modify between TRUE or FALSE (default).
3.	***AS subsystem disabled*** Indicates whether AS starts with Entrust/Authority service.	Master User	From Entrust/Master Control: may modify between TRUE or FALSE (default).
4.	***Integrity check rate*** Indicates the rate for automatic integrity checks.	Master User	From Entrust/Master Control: may change default from once per day (Modify).
5.	***Database backup rate*** Indicates the rate for scheduled database backups.	Master User	From Entrust/Master Control: may change default from 1 day (Modify). No default.
6.	***Limit on Entrust users*** Specifies the maximum allowed limit of Entrust users.	Security Officer	From Entrust/RA: may be specified (Modify). No default.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be specified (Modify). No default.
7.	***Authorizes user limit*** Specifies the license string to increase the allowed limit of Entrust users.	Security Officer	From Entrust/RA: may be specified (Modify). No default.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be specified (Modify). No default.
8.	***CA Master secret*** Entrust/Authority key variable used in encrypting the database.	Master User	From Entrust/Master Control: may be updated by re-encrypting database (modify).
9.	***Entrust Master secret*** Entrust/Authority key variable used in encrypting the database.	Master User	From Entrust/Master Control: may be updated by re-encrypting database (modify).
10.	***Master User secret*** Entrust/Authority key variable used in encrypting the database.	Master User	From Entrust/Master Control: may be updated by changing Master User password (modify).
11.	***CA signing algorithm*** The CA signing key algorithm.	Security Officer	From Entrust/RA. Choice of RSA 1024, RSA 2048, or DSA 1024 (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA. Choice of RSA 1024, RSA 2048, or DSA 1024 (modify).
12.	***CRL lifetime*** The lifetime of the certificate revocation list.	Security Officer	From Entrust/RA: may be modified within allowed limits: 4 hours to 48 hours (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be modified within allowed limits: 4 hours to 48 hours (modify).

#	Data Description	Role	Access
13.	***Cross-certificate lifetime*** The lifetime of the cross-certificate.	Security Officer	From Entrust/RA: may be set within allowed limits: 2 months to 60 months (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be set within allowed limits: 2 months to 60 months (modify).
14.	***Certificate and revocation list hashing algorithm*** The hashing algorithm used to for certificates and revocation lists.	Master User	Selection made at installation and may be modified from Entrust/Master Control: choice of SHA-1 or MD5 (modify)
15.	***Automatically push CRLs to the directory*** A boolean indicator whether CRLs should be published after each certificate revocation.	Security Officer	From Entrust/RA: may be changed to either ON or OFF (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be changed to either ON or OFF (modify).
16.	***Number of Master User authorizations required for sensitive operations***	Master User	From Entrust/Master Control GUI: may be modified within allowed limits: 1 or 2 (modify).
17.	***Administration Service password*** Password used automatically by the AS.	Master User	From Entrust/Master Control GUI: may be modified by recovering the AS (modify).
18.	***Database encryption algorithm*** The algorithm used to encrypt sensitive data in the database.	Master User	Selection made at installation only: choice of CAST5-128 or Triple-DES (modify).
19.	***SEP encryption algorithm*** The algorithm used to for the session key in SEP transactions.	Master User	Selection made at installation and may be modified from Entrust/Master Control GUI: choice of CAST5-128 or Triple-DES (modify).
20.	***Forward cross-certificate expire date*** The expiry date of the forward cross-certificate.	Security Officer	From Entrust/RA: may be modified from default (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be modified from default (modify).
21.	***Cross-certification authorization code*** The authorization code for the cross-certification.	Security Officer	From Entrust/RA: may be modified and deleted by canceling cross-certification (clear, delete).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be modified and deleted by canceling cross-certification (clear, delete).
22.	***Reverse certificate expire date*** The expiry date of the reverse cross-certificate.	Security Officer	From Entrust/RA: may be modified from default (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be modified from default (modify).

#	Data Description	Role	Access
23.	***Next available certificate serial number***	Master User	From Entrust/Master Control: May be automatically modified during database incremental restore operation (modify).
24.	***Role permissions*** The permissions defined for each defined role.	Security Officer	From Entrust/RA: Modify, clear, and delete.
		Custom-defined role (with appropriate privilege)	From Entrust/RA: Modify, clear, and delete.
25.	***Number of authorizations required for sensitive operations***	Security Officer	From Entrust/RA: may be modified within allowed limits: 0 to 10 or number of Officers – whichever is lower (modify).
		Master User	From Entrust/Master Control (for Officers only): may be reset to 1 (modify).
		Custom-defined role (with appropriate privilege)	From Entrust/RA: may be modified within allowed limits: 0 to 10 or number of Officers – whichever is lower (modify).

5.1.1.8 FMT_MTD.3 Secure TSF data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

5.1.1.9 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:

- ***Master User passwords***

5.1.2 Separation of duties

This section specifies the Separation of Duties security requirements for Entrust/Authority. The Separation of Duties security requirements are summarized in Table 10.

Table 10: Separation of duties security requirements

#	Security Requirement		Component
1.	Roles and privileges	Entrust roles	FMT_SMR.2
		Management of security functions behavior	FMT_MOF.1
		Management of end user password lifetime	FMT_SAE.1a FMT_SAE.1b

5.1.2.1 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: ***Master User, Security Officer, Administrator, Auditor, Directory Administrator, AutoRA Administrator, End User, and custom-defined (flexible) roles.***

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the following conditions are satisfied:

- ***A user may be associated or disassociated with the Security Officer, Administrator, Auditor, Directory Administrator, AutoRA Administrator, or custom-defined roles only as explicitly assigned by a Security Officer or a custom-defined role with sufficient privileges.***

- ***A user may be associated or disassociated with the End User role by a Security Officer, Administrator, AutoRA Administrator, or a custom-defined role with sufficient privileges.***

- ***No one other than the existing Master Users may be associated with the Master User role.***

- ***No existing Master Users may be disassociated with the Master User role (i.e., and associated with a different role).***

5.1.2.2 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***disable, enable, and modify the behaviour of*** the functions to the roles ***indicated in Table 11***.

Table 11: Management of Entrust security functions

#	Function	Role	Action
1.	Master User multiple authorizations	Master User	Master User may enable/disable the function and modify the number of Master User authorizations required.
2.	Automatic integrity verification	Master User	Master User may modify the timing of the automatic integrity verification function.
3.	Automatic database backup	Master User	Master User may modify the timing of the automatic database backup function.
4.	Security Officer multiple authorizations	Master User	Master User may modify (reset) the number to one.
		Security Officer	Security Officer may modify the number within allowed limits.
5.	Administrator multiple authorizations	Security Officer	Security Officer may modify the number within allowed limits.
		Custom-defined role	With sufficient privileges, may modify the number within allowed limits.
6.	Password rules	Security Officer	Security Officer may enable/disable criteria or modify criteria within allowed limits.
		Custom-defined role	With sufficient privileges, may enable/disable criteria or modify criteria within allowed limits.
7.	Grant/deny administrative access	Security Officer	Security Officer may create/configure roles and privileges.
		Custom-defined role	With sufficient privileges, may create/configure roles and privileges.

5.1.2.3 FMT_SAE.1a Time-limited authorization

FMT_SAE.1.1a The TSF shall restrict the capability to specify an expiration time ***for any administrative user and End user passwords*** to ***Security Officers or custom-defined roles with sufficient privileges.***

FMT_SAE.1.2a For each of these security attributes, the TSF shall be able to ***force a password change*** after the expiration time for the indicated security attribute (user password) has passed.

5.1.2.4 FMT_SAE.1b Time-limited authorization

FMT_SAE.1.1b The TSF shall restrict the capability to specify an expiration time for ***authorization codes and reference numbers*** to ***Security Officers or custom-defined roles with sufficient privileges.***

FMT_SAE.1.2b For each of these security attributes, the TSF shall be able to ***invalidate activation codes (authorization code and reference number)*** after the expiration time for the indicated security attribute has passed.

5.1.3 Identification & authentication

This section specifies the Identification & Authentication security requirements for Entrust/Authority. The Identification & Authentication security requirements are summarized in Table 12.

Table 12: Identification & authentication security requirements

#	Security Requirement		Component
1.	Logon controls	User authentication before any action	FIA_UAU.2
		User identification before any action	FIA_UID.2
2.	Password selection	User and operator password criteria	FIA_SOS.1
3.	Authentication controls	Protection against reuse	FIA_UAU.4
		Re-authentication of users and operators	FIA_UAU.6
		Non-echoing of passwords	FIA_UAU.7
4.	Session termination	Session termination following inactivity	FTA_SSL.3a FTA_SSL.3b
5.	Authentication failure	Authentication failure handling	FIA_AFL.1

5.1.3.1 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.

5.1.3.2 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.

5.1.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following criteria:

1) ***Specified Master User password rules applicable to:***

   - ***minimum number of upper case letters (default: 1)***

- ***minimum number of digits (default: 1)***
- ***minimum number of lower case letters (default: 1)***
- ***minimum number of characters (default: 10)***
- ***character restriction (default: must not be part of home directory path)***
- ***valid characters (default: 0-9, a-z, A-Z, ~!@#$%^&*_+-=\|:;<>?,./)***
- ***word restriction (default: must not include the words "Entrust" or "Entrust Technologies")***
- ***character restriction (default: must not be a keyboard sequence)***
- ***word restriction (default: must not contain names, words or combination of words specified in dictionary files)***

2) ***Specified Security Officer, Administrator, Auditor, Directory Administrator, AutoRA Administrator, End User, and custom-defined roles 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)***

5.1.3.4 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to:

- ***user initialization***
- ***user key recovery***

- ***enabling CA cross-certification***

5.1.3.5 FIA_UAU.6 Re-authenticating

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

- ***to complete sensitive operations in Entrust/Master Control when the required number of Master User authorizations is set to one***
- ***to complete a Master User password change in Entrust/Master Control***
- ***after the hard-coded Entrust/Master Control timeout period (5 minutes) has lapsed***

5.1.3.6 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.

5.1.3.7 FTA_SSL.3a TSF-initiated termination

FTA_SSL.3.1a The TSF shall terminate an interactive session ***with Entrust/Master Control after the hard-coded Entrust/Master Control timeout period (5 minutes) has lapsed.***

5.1.3.8 FTA_SSL.3b TSF-initiated termination

FTA_SSL.3.1b The TSF shall terminate an interactive session ***with Entrust/RA after the Administration Service subsystem session timeout period (default: 2 minutes) has lapsed.***

5.1.3.9 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when ***three*** unsuccessful authentication attempts occur related to ***initial and subsequent authentication via Entrust/Master Control.***

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 Key management

This section specifies the Key Management security requirements for Entrust/Authority. The Key Management security requirements are summarized in Table 13.

Table 13: Key management security requirements

#	Security Requirement		Component
1.	Cryptographic key operations	Key distribution (initialization, update, revocation)	FCS_CKM.2
		Key access (update, recovery, backup)	FCS_CKM.3
2.	Generation of secrets	Machine-generated password	FIA_SOS.2.1
3.	Proof of receipt	Enforced proof of receipt	FCO_NRR.2
4.	Replay detection	Replay detection	FPT_RPL.1

5.1.4.1 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 key agreement)***
- ***RFC 1777 (Lightweight Directory Access Protocol v2) and RFC 2251 (Lightweight Directory Access Protocol v3)***
- ***Secure Exchange Protocol (SEP)***
- ***RFC 2510 (PKIX-CMP)***

5.1.4.2 FCS_CKM.3 Cryptographic key access

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

- ***Secure Exchange Protocol (SEP)***
- ***RFC 2510 (PKIX-CMP)***
- ***FIPS PUB 140-1***

5.1.4.3 FIA_SOS.2 TSF Generation of secrets

FIA_SOS.2.1 is satisfied by the TOE environment (i.e., FIPS 140-1 validated cryptographic module). Refer to Section 5.2.1.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for:

- ***Derivation of the Entrust Master encryption key and Entrust Master integrity key***
- ***Derivation of CA Master encryption key and CA Master integrity key***
- ***Derivation of MAC keys used for integrity and authentication in SEP and PKIX-CMP***

5.1.4.4 FCO_NRR.2 Enforced proof of receipt

FCO_NRR.2.1 The TSF shall enforce the generation of evidence of receipt for received ***public key certificates.***

FCO_NRR.2.2 The TSF shall be able to relate the ***identity*** of the recipient of the information, and the ***authorization code (used for generating MACs) or digital signature*** of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to ***the originator (Entrust/Authority) and recipient (Entrust/RA operators and End Users)*** given ***that public key certificates are transferred via SEP or PKIX-CMP and the evidence is automatically generated via an acknowledgement message and audited during the session.***

5.1.4.5 FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: ***issuance of certificates to existing Entrust Users.***

FPT_RPL.1.2 The TSF shall ***prevent creation of a directory entry, prevent issuance of certificates, and display an error message indicating that a user with that same name already exists*** when replay is detected.

5.1.5 Audit

This section specifies the Audit security requirements for Entrust/Authority. The Audit security requirements are summarized in Table 14.

Table 14: Audit security requirements

#	Security Requirement		Component
1.	Audit events	Specification of auditable events and recorded information	FAU_GEN.1
		Accountability of users	FAU_GEN.2
2.	Audit trail protection	Audit data integrity and availability	FAU_STG.2.2 FAU_STG.2.3

5.1.5.1 FAU_GEN.1 Audit data generation

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

1) Start-up and shutdown of the audit functions ***(not applicable)***;

2) All auditable events for the ***(not specified)*** level of audit; and

3) ***The events listed in Table 15.***

Table 15: Entrust audit events

Audit	Severity	Audit record message and information
7669	Event	An administrator requested that all changed CRLs be issued to the Directory. An administrator has issued all changed CRLs from Entrust/RA. The number of CRLs issued is included with the audit. For each CRL issued, audit 7943 will precede this audit.

Audit	Severity	Audit record message and information
7670	Event	Automatic login has been disabled. A master user has disabled automatic services login. Services will require a master user to be present and enter their password for the services to start.
7671	Event	Automatic login has been enabled. A master user has enabled automatic services login to allow the services to be started unattended as part of system startup.
7672	Alarm	Authentication in Entrust/RA failed three successive times. The Password entry for an administrator has failed three times in succession. This could indicate somebody attempting to guess the password of an Entrust profile.
7673	Event	Directory operation - successfully renamed Directory entry. An administrator successfully renamed a Directory entry.
7674	ALARM	Directory operation - rename Directory entry failed. An attempt to rename a Directory entry by an administrator failed.
7675	Event	Directory operation - Directory administrator password changed in the Directory. An administrator successfully changed their password.
7678	ALARM	Administrator trying to access ASH does not have a local verification certificate. The administrator attempting access does not have the correct credentials and is not recognized by this CA. The DN of the administrator is included with the audit. Contact the administrator with the DN in the audit if they have not been trying to log in this may indicate a break in attempt.
7688	Event	Directory Browser - successfully added a directory entry. A new directory entry has been added using the Directory Browser tool.
7689	ALARM	Directory Browser - delete directory attribute value failed. An attempt to delete a directory attribute value from an existing directory attribute has failed.
7690	Event	Directory Browser - successfully deleted a directory attribute value. A directory attribute value has been deleted from an existing directory attribute.
7691	ALARM	Directory Browser - delete directory attribute failed. An attempt to delete a directory attribute from an existing directory entry has failed.
7692	Event	Directory Browser - successfully deleted a directory attribute. A directory attribute has been deleted from an existing directory entry.
7693	ALARM	Directory Browser - replace directory attribute failed. An attempt to replace an existing directory attribute value has failed.
7694	Event	Directory Browser - successfully replaced a directory attribute. A directory attribute value has been replaced with a new value.
7695	ALARM	Directory Browser - add directory attribute failed. An attempt to add an attribute to an existing directory entry has failed.
7696	Event	Directory Browser - successfully added a directory attribute. A Directory attribute has been added to an existing Directory entry.
7705	Log	A new Certification Authority (CA) key pair has been generated.

Audit	Severity	Audit record message and information
		The CA has generated a new key pair for its own use. This keypair is used for signing and verifying certificates and CRLs. This is done during the installation of a new CA or when a CA performs a CA key rollover.
7708	ALARM	Combined certificate revocation list (CRL) size larger than specified threshold. The CombinedCRL has stopped being published to the Directory since it is larger than the specified threshold in entmgr.ini. The threshold purpose is to protect directories against large entries. If your Directory can handle the size of the CombinedCRL you can re-enable publishing to the Directory by increasing the size of the threshold or removing the threshold entry from entmgr.ini. The CombinedCRL is always maintained in the database regardless of its size and of the threshold value.
7710	Log	User import from another Certification Authority (CA) has completed. A user who has has been imported from another CA has logged in and completed the process. The user's current DN and the user's DN at the other CA are included in the audit. An administrator at the user's other CA can now complete the export operation and archive the user if they want.
7711	Alarm	Audit trial integrity check has failed. The audit trial integrity is checked each time an integrity check is done. Such checks are done periodically or can be done manually.
7712	Log	Audit trial integrity check has passed. The audit trial integrity is checked each time an integrity check is done. Such checks are done periodically or can be done manually.
7713	Log	The Certification Authority (CA) key is nearing its expiry. The signing key of your subordinate CA is nearing expiry. This audit is generated if the age of the signing key exceeds 70% of its lifetime. You should install a newer version of Entrust/Authority and roll over the keys of your subordinate CA.
7715	Log	Key update requested by client. A key update request has been received by a client using the PKIX-CMP protocol. If the client is an Entrust client, the reason for the key update is included with the audit.
7716	ALARM	Restore First Officer Failed Unable to restore the First Officer entry and certificate to the Directory after a Restore To Directory operation. Restoring the First Officer may fail for the following reasons: • The First Officer DN entry is missing from the policy section in the entmgr.ini file. • The DN listed for the First Officer in the entmgr.ini file is not a valid DN or does not correspond to any user in the Entrust/Authority database • The First Officer entry is not present in the Directory and creation of the entry failed. This may occur if the parent of the First Officer entry does not exist or some other Directory problem has occurred. • The First Officer certificate could not be recovered. The preceding log entries in the manager.log should clarify the cause of the failure.
7717	Event	First Officer Restored The First Officer entry and certificate have been restored to the Directory after a Restore To Directory operation.
7718	Log	Certification Authority (CA) certificate written to the Directory. The CA certificate has been written to the Directory. This occurs when the CA certificate has been successfully written to the Directory during a Restore to Directory operation.
7719	Event	Authority advanced setting changed.

Audit	Severity	Audit record message and information
		An advanced setting has been changed by a master user using the entsh application. The audit includes the name, description and the old and new value for the setting.
7725	Event	A CA key has been revoked. This audit is generated when a CA key is revoked. CA key revocation is triggered from Entrust/RA. The key identifier (in hexadecimal form) is logged with this audit.
7727	Event	The CA signing key has been updated. A new CA signing key pair was created. This audit is generated when the CA keys roll over. This can be triggered by one of three ways: manually from Entrust/RA; automatically if the private CA signing key nears its expiry; or automatically if the current CA signing key is revoked
7731	Event	Policy Certificate written to directory. A policy certificate was written to the directory. The audit information will include the DN, identifier, name and FCS type of the certificate.
7732	Event	Policy Certificate updated. A policy certificate was updated because it was about to expire, the certificates were restored to directory or the CA key was rolled over. The audit information includes the DN, identifier, name and FCS certificate type.
7733	Event	Policy Certificate changed. A policy certificate was changed by an administrator. The audit information will include the DN, identifier, name and FCS type of the certificate. The attributes and values are included with the audit.
7734	Event	Policy Certificate created. A policy certificate was created. The audit information will include the DN, identifier, name and FCS type of the certificate. The attributes and values are included with the audit.
7735	Event	Default policy certificates created. The default policy certificates have been created during first-time initialization
7740	Event	External CA user public key deleted. An administrator has deleted a CA user public key that was previously imported. The DN of the CA's keys that were deleted is included with the audit.
7741	Event	External CA user public key imported. An administrator has imported the CA user public key from another CA. The audit includes the DN of the other CA.
7742	Event	CA user public key exported. The CA user public key has been exported to a file by an administrator. This file is transferred to another CA to allow users to be moved between the CAs. This is only necessary if the CAs do not have a trust link through either cross-certification or strict-hierarchy. The hash of the CA user public key file, the serial number of the CA user certificate and the expiration date of the CA user public encryption key is included with the audit.
7743	Event	User slavaged from permanent storage. An administrator has salvaged a user from permanent storage. The user is now an Entrust user in the disabled state. The DN is included with the audit.
7744	Event	User archived to permanent storage. An administrator has archived a user to permanent storage. The user will no longer

Audit	Severity	Audit record message and information
		appear as an Entrust user. The DN is included with the audit.
7745	Event	User imported and set for key recovery. A user has been imported by an administrator and set to the key recover state. The DN of the user, the user's old DN, and old CA DN are included with the audit.
7746	Event	User imported and set active A user has been imported by an administrator and set to the active state. The DN of the user, the user's old DN, and old CA DN are included with the audit.
7747	Event	User export canceled. An administrator has canceled the export of a user either in the export or export hold state. The DN of the user is included with the audit.
7748	Event	User exported to another Certification Authority (CA). The export of a user from one CA to another has been completed by an administrator. The user is no longer supported at this CA and is now in the export state. The DN of the user is included with the audit.
7749	Event	User put in export hold state. The first stage of exporting a user to another CA has been done by an administrator. The export hold state means the user can still operator at the current CA until the new CA imports the user. The DN of the user is included with the audit.
7750	Event	Search base changed. A searchbase has been changed. The audit information will include the name, DN and identifier of the searchbase and will also indicate if the searchbase is an end-user or administrator searchbase.
7751	Event	Searchbase created. A searchbase has been created. The audit information will include the name, DN and identifier of the new searchbase. The audit information will also indicate if the searchbase is an end-user searchbase or administrator searchbase.
7752	Event	Searchbase deleted. A searchbase has been deleted. The audit information will include the name and identifier of the deleted searchbase.
7753	Event	User templates modified. The user templates information has been modified.
7754	Event	User templates initialized. The user templates information has been initialized from the templates.ini file during first-time initialization.
7756	Event	A user's authorization code has been refreshed by an administrator. The DN of the user is included with the audit. Only the authorization code is changed; the reference number is not changed. All members of a group have been removed from the group. The audit information will include the name and group identifier of the group. In addition, the number of users successfully deleted and the number of users that could not be deleted from the group will be displayed.
7757	Event	Delete all group members. All members of a group have been removed from the group. The audit information will include the name and group identifier of the group. In addition, the number of users successfully deleted and the number of users that could not be deleted from the group will

Audit	Severity	Audit record message and information
		be displayed.
7758	Event	Copy all group members. The members of a group have been copied to another group. The audit information will include the names of the source and target groups. As well, a count of the number of users successfully copied and the number of users that could not be copied will be displayed.
7759	Event	Group(s) of user has changed. The groups to which a user belongs has changed. The audit information will include the DN of the user as well as a list of groups to which the user has been added and a list of groups from which the user has been deleted.
7760	Event	Role of user has changed. The role of a user has been changed. The audit information will include the DN of the user being changed as well as the name and role identifier of the new role.
7761	Event	Administrator does not have access to perform operation. The audit information will include information describing the current administrator, what operation was being performed and why the administrator did not have access to perform the operation.
7762	Event	Gro7up deleted. A group has been deleted. The name and group identifier of the deleted group will be shown in the audit information.
7763	Event	Role deleted. A role has been deleted. The name and role identifier of the deleted role is shown in the audit information.
7764	Event	Group changed. The name of a group has been changed. The old and new names of the group as well as the group identifier display in the audit information.
7765	Event	Role changed. A role has been changed. Multiple audit records are written and display the various changes to role attributes. Each audit message will contain the name and role identifier of the role being changed.
7766	Event	Group created. A group has been created. The audit information will contain the name and group identifier of the new group.
7767	Event	Role created. A role has been created. Multiple audit records are written displaying the various attributes of the new role. Each audit message will contain the name and role identifier of the new role
7768	Event	Initial roles created. The default roles are created during first-time initialization. The name and role identifiers of the default roles are provided in the audit information.
7769	Event	Initial group created. The initial group is created during first-time initialization. The name and group identifier of the group are given in the audit information.
7770	Alarm	Free disk space is critically low. Entrust will not start if disk space falls below the level set on the entmgrMinFree

Audit	Severity	Audit record message and information
		parameter in the entmgr.ini file. If a value for entmgrMinFee has not been specified, the default is 5 MB.
7775	Event	Offline cross-certificate requested. A Security Officer has created a PKCS #10 offline cross-certificate request. The Security Officer name and main CA DN are included with the audit.
7776	Event	User State History database table trimmed. The user state history table has been automatically trimmed. This table is used for creating reports of user state changes. Trimming this table ensures that it does not take up too much space. This is done periodically by the Key Management Service. Trimming does not result in lost information. All events are recorded in the audit trails, which should be archived. Trimming is controlled by the entUserStateHistTrim parameters in the entmgr.ini file.
7777	Event	CA key transferred from software to hardware. A CA signature key that was created by software and stored encrypted in the database has been transferred from software to hardware. This can be done after upgrading from Entrust 3.0c to Entrust 4.0, or if the hardware is obtained after installing Release 4.0. The key transfer is done by a Master User using Entrust/Master Control. All systems have a main CA signing key. This key is always moved. If a system also has a SET CA message signing key, and any number of additional CA signing keys, these keys are moved as well. There is one audit for each key moved. The names of the CA and the Master User are included in the audit. All subsequent additional CAs created are created in hardware. These keys cannot be moved from hardware back to software.
7784	Event	Password for Setup Information Distribution changed. The password used to protect the files written for authorization code distribution has been changed. A Master User performs this activity using Entrust/Master Control. The name of the Master User is included with the audit.
7785	Event	State of setup information distribution changed. The setup information (reference number and authorization code) distribution state has been changed by a Master User using Entrust/Master Control. The audit log contains the old state and the new state. There are four possible states: distribution is off/security is off (no encryption for files on disk), distribution is on/security is off (no encryption), distribution is on/security is on, distribution is off/security is on (no files are written to disk, but when the distribution feature is turned on the files are encrypted when they are written to disk on the Entrust/Authority machine).
7788	Event	Enterprise security policy changed. A Security Officer has changed the enterprise-specific security policy. A description of the change and the Security Officer's name are included in the audit.
7790	Event	User's flexible certificate type changed. A Security Officer or Administrator has changed the user category of an end user. The user's name and administrator's name is included in the audit.
7791	Event	User category changed. A Security Officer or Administrator has changed the user category of an end user. A user's category can only be changed if they are enabled and they have not yet completed initialization. Administrators and Security Officers are always in the enterprise category. Their user category cannot be changed. The administrator's name and the user name is

Audit	Severity	Audit record message and information
		included in the audit.
7803	Alarm	Free disk space is getting low (time to clean up?). In the entmgr.ini file, the parameter entmgrWarnFree determines when Entrust prints a warning about disk space being low. If no one has provided an entmgrWarnFree parameter in the .ini file, the default is to issue a warning when 20 MB of space is free. Note that Entrust will not start if disk space is below the amount specified in the entmgrMinFree parameter in the entmgr.ini file. See alarm 7770.
7813	Alarm	CMS request adjusted. Entrust/Authority adjusted a setting in an Entrust/CMS request. The request is still processed. If a single request has more than one adjustment, there is an audit for each one. Each audit includes a description of the change. A list of changes is also returned to the originator of the Entrust/CMS request.
7815	Event	Directory restore canceled. Restoration of Entrust data to the Directory has been canceled with no harm done.
7817	Log	Cross-certificate pairs written to Directory. Either a cross-certificate operation was performed or Directory data was recovered by a Master User or Security Officer.
7818	Event	Secure Exchange Protocol (SEP) encryption algorithm changed. The SEP algorithm has been changed by a Master User in Entrust/Master Control. The change description is included in the audit.
7819	ALARM	Certificate signature hash changed. The certificate hasher for the system has been changed by a Master User in Entrust/Master Control. The change description is included in the audit.
7820	Event	Expired revoked certificate re-added to revocation list. Removal of expired certificates from CRLs or ARLs is an option that can be set by Security Officers. If the removal setting is changed from Yes to No, expired certificates that have been removed previously are re-added—not immediately when the setting is changed, but the next time the CRL or ARL is updated.
7821	Event	Entrust full data backup canceled. The full data backup has been canceled with no harm done. The incomplete backup data should be discarded.
7822	Log	Master user logged off. A Master User has logged off from Entrust/Master Control.
7824	Event	License information changed. A Security Officer has changed the license information for the Entrust installation.
7826	Event	Database re-encryption completed successfully. This audit will appear with audits 7853 (Administration service password change), 7955 (Entrust master key), and 7956 (CA master key).
7828	Event	Database integrity check canceled. A database integrity check was canceled with no harm done. Any errors found before cancellation will be audited.
7830	Log	Infrastructure data files backup completed successfully. The infrastructure data files have been backed up successfully either manually by a

Audit	Severity	Audit record message and information
		Master User in Entrust/Master Control, or automatically by Key Management Service.
7832	Log	Database backup completed successfully. Backup of the Entrust/Authority database was completed successfully either manually by a Master User in Entrust/Master Control, or automatically by Key Management Service.
7834	Log	Directory database backup completed successfully. The Directory has been successfully backed up either manually by a Master User in Entrust/Master Control, or automatically by Key Management Service.
7835	ALARM	Integrity failure. An integrity failure has been detected in the Entrust/Authority database . The table and row that have failed integrity are included in the audit.
7840	Event	User alternate name changed. An end-user's alternate name (usually an e-mail address) for insertion in certificates has been changed by an Administrator or Security Officer. The end-user's DN, old e-mail address, and new e-mail address are included in the audit.
7841	Event	User verification certificate policy changed. The end-user's verification certificate policy list has been changed by an Administrator or Security Officer. The end-user's DN is included with the audit, plus the changes to the list.
7842	Event	User encryption certificate policy changed. The end-user's encryption certificate policy list has been changed by an Administrator or Security Officer. The end-user's DN is included with the audit, plus the changes to the list.
7843	Event	User private signature key lifetime changed. The lifetime of an end-user's signing private key (set as a percentage of the verification public key certificate lifetime) has been changed by an Administrator or Security Officer.
7848	Event	Administration Service profile recovered. The Administration Service profile has been recovered automatically by Entrust/Master Control when it starts and discovers that the verification public key certificate in the Administration Service profile has expired. The profile can also be recovered manually by a Master User in Entrust/Master Control.
7849	Event	Directory Administrator password changed. The Directory Administrator's password has been changed by an Administrator or Security Officer.
7851	Event	The Administration Service profile password has been changed. The password to unlock the profile used by the Administration Service has been changed. This only occurs during a Re-encrypt Database operation done by a Master User in Entrust/Master Control. Will appear with audits 7955, 7956, and 7828.
7854	Log	Database integrity check was successful. The integrity check performed by a Master User was successful.
7855	ALARM	Database integrity check failed. An integrity check of the Entrust/Authority database has failed. Other audits indicating what failed is listed before this audit. Also check manager.log. Contact Entrust Support; recovery from the last backup may be necessary.
7858	Event	Automatic key update has been enabled for the end-user. An Administrator or Security Officer has enabled automatic key update for an end-user.

Audit	Severity	Audit record message and information
		The end-user's DN is included with the audit.
7859	Event	Automatic key update has been disabled for the end-user. An Administrator or Security Officer has disabled automatic key update for an end-user. The end-user's DN is included with the audit.
7860	Event	End-user signing key lifetime property changed. An Administrator or Security Officer has changed the signing private key lifetime for an end-user. The end-user's DN is included with the audit.
7861	Event	End-user encryption key lifetime property changed. An Administrator or Security Officer has changed the encryption public key certificate lifetime for an end-user. The end-user's DN is included with the audit.
7862	Event	The end-user verification expire date has been changed. An Administrator or Security Officer has changed the expiry date of an end-user's verification public key certificate. The end-user's DN is included with the audit.
7863	Event	The end-user signing/encryption expire date has been changed. An Administrator or Security Officer has changed the expiry date of an end-user's signing or encryption key. The end-user's DN is included with the audit.
7864	ALARM	Failed to receive signing key update acknowlegement from Entrust/Entelligence. The new end-user signing certificate has been revoked. Key Management Service revoked the end-user's verification public key certificate because Entrust/Entelligence did not acknowledge receiving it. The user's DN, the certificate's serial number, and the certificate's validity period are included in this audit. If Entrust/Entelligence picked up the the new verification public key certificate, the user will have to be set up for key recovery. The manger.log file give the reason for the failure.
7865	ALARM	Failed to receive encryption key update acknowlegement from Entrust/Entelligence. An Entrust/Entelligence encryption key pair update failed after cryptographic information was sent to Entrust/Entelligence. The newly created encryption public key cerificate and decryption private key are archived by Key Management Service. If the key update failed at Entrust/Entelligence, and Entrust/Entelligence tries the encryption key pair update again, it will receive the encryption key pair that was just archived by Key Management Service. The manger.log file give the reason for the failure.
7866	ALARM	Failed to receive key recover acknowlegement from Entrust/Entelligence. The new user certificate has been revoked. A Recover operation failed after cryptographic information was sent to Entrust/Entelligence. Key Management Service revoked the newly created end-user verification public key certificate and encryption public key certificate (if one was created). The user's DN, the certificate's serial number, and the certificate's validity period are included in this audit. If the user received no errors during the Entrust/Entelligence Recover User operation, set the user up for key recovery. Ask the user to delete their existing profile (.epf file) and to repeat the Recover User operation. If this audit recurs, the manager.log file will give the reason for the failure.
7867	ALARM	Failed to receive user initialization acknowlegement from Entrust/Entelligence. The new user verification certificate will be revoked. A new user initialization operation failed after cryptographic information was sent to Entrust/Entelligence. Key Management Service revoked the newly created user verification public key certificate and encryption public key certificate. The user's DN, the certificate's serial number, and the certificate's validity period are included in this audit. If the user received no errors during the Entrust/Entelligence Create New User operation, set the user up for key recovery. Ask the user to delete their existing profile (.epf file) and to

Audit	Severity	Audit record message and information
		perform the Recover User operation. If this audit recurs, the manager.log file will give the reason for the failure.
7881	Event	Distinguished name change for end-user completed by the Entrust/Entelligence. Entrust/Entelligence has completed the DN change operation. The end-user's DN is included in the audit.
7882	Event	Distinguished name change for an end-user approved. A Security Officer or Administrator has approved an end-user DN change. The Security Officer's or Administrator's name and the end-user's DN are included in the audit.
7883	Event	Distinguished name change for an end-user canceled. An end-user had been set up for a DN change but this was canceled by a Security Officer or an Administrator before the Entrust/Entelligence completed the DN change. The Security Officer's or Administrator's name and the end-user's DN are included in the audit.
7889	Event	New certificate revocation list created. The current ARL space is reserved for future certificate revocations and a new ARL is created. The name of the entry where the CRL is stored (distribution point) is included with the audit.
7895	Event	Certification Authority (CA) policy certificate updated. The certificate has been updated wither due to a user search base change done by a Security Officer, or because it is about to expire and has been update by Key Management Service. This audit always appears with audit 7899.
7897	Event	Certification Authority (CA) policy certificate written to the Directory. This audit occurs with audits 7900 and 7897 when a user search base is modified. It appears by itself when the Directory data is recovered back to the Directory. It appears with audit 7987 when the CA attribute certificate is updated by Key Management Services because it is close to expiring.
7898	Event	Entrust search base information updated. Searchbase information is updated. There are two searchbase lists: one for end-users (the user searchbase list) which is placed in the CA attribute certificate, and one for Security Officers and Administrators when using Entrust/RA (the admin searchbase list). Security Officers can modify both lists; Administrators can modify only the admin searchbase list. The type of list modified is included in the audit. If the user searchbase list is modified, this audit will appear with audits 7899 and 7897.
7899	Event	CA policy certificate created. The first certificate has been created. The CA policy certificate is stored in the CA Directory entry and contains Directory searchbase information for Entrust/Entelligence. This audit occurs only during the first-time start-up of Entrust/Master Control.
7900	Log	Authority revocation list written to the Directory. The DN of the issuer (which is always the CA) is included in the audit.
7915	Log	Entrust full data backup completed successfully. The Entrust/Authority database, data files, and (optionally) the Directory data has been backed up successfully. Backups are run automatically by Key Management Service or manually by a Master User in Entrust/Master Control.
7916	Event	CA Directory password changed. The CA Directory password stored in the Directory has been changed by a Master User in Entrust/Master Control. The name of the Master User and the CAs DN are included in the

Audit	Severity	Audit record message and information
		audit.
7919	Event	Entrust subsystem stopped. Windows NT only. A Key Management Assistant process has stopped. A process identifier is included with the audit, along with optional text indicating if the process stopped because of an error.
7920	Event	Entrust subsystem started. Windows NT only. A Key Management Assistant process has started. A process identifier is included with the audit.
7921	Event	Master Control stopped. The Entrust/Master Control application has stopped. If the process was terminated by the application because of an error, the error text will be included in the audit.
7922	Event	Master Control started. The Entrust./Master Control application has started. The process ID is included in the audit.
7930	Event	Security policy has been modified. One or more Security Officers have modified a security policy item. The old value, new value and user name of the Security Officer(s) who performed the modification are included in the audit. If more than one item is modified at a time, there will be one audit per item.
7931	Log	Expired certificate removed from revocation list. An Entrust/Entelligence user encryption public key certificate or verification public key certificate that was on the CRL, or a cross-certificate on the ARL, has been removed because the certificate has reached the end of its validity period. The serial number of the certificate is included in the audit.
7939	Event	User encryption certificate revoked. A user's latest encryption certificate has been revoked by a Security Officer or an Administrator using Entrust/RA. The certificate revoked was the last encryption public key certificate that the Entrust/Entelligence has retrieved. If a Security Officer or an Administrator has updated an end-user's encryption key pair and the Entrust/Entelligence has not yet retrieved it, the certificate in the Directory is not revoked but the previous certificate (which the Entrust/Entelligence has retrieved) is revoked. The certificate serial number and end-user DN are included in the audit.
7941	Event	User verification certificate revoked. A user's latest verification public key certificate has been revoked by a Security Officer or an Administrator using Entrust/RA. The certificate's serial number and end-user's DN are included in the audit.
7943	Log	Certificate revocation list written to the Directory. The CRL has been written to the Directory. The DN of the issuer (which is always that of the CA) is included in the audit.
7948	Event	Entrust first-time initialization complete. The first-time initialization of the Entrust/Master Control application completed successfully.
7950	Log	Certificate recovered back to Directory. When a Master User does a Recover Directory operation, this audit appears for each certificate that is written back to the Directory. The certificate owner's DN is included in the

Audit	Severity	Audit record message and information
		audit.
7951	Event	Protocol verification certificate created. The protocol verification certificate has been created. This audit occurs during the initial start of the Entrust/Master Control application and when Key Management Service automatically updates the protocol signing key pair.
7952	Event	CA certificate created. The CA certificate has been created. This audit occurs only during the initial start of Entrust/Master Control.
7953	Event	Entrust master key created. This audit occurs only during the initial start of Entrust/Master Control.
7954	Event	Certification Authority (CA) master key created. This audit occurs only during the initial start of Entrust/Master Control.
7955	Event	Entrust master key updated. The Entrust master key was updated by a Master User in Entrust/Master Control, who re-encrypted the database. The name of the Master User who performed the operation is included in the audit. Will appear with audits 7956, 7853, and 7828.
7956	Event	Certification Authority (CA) master key updated. The CA master key has been updated by a Master User in Entrust/Master Control, who re-encrypted the database. The name of the Master User who performed the operation is included in the audit. Will appear with audits 7955, 7853, and 7828.
7957	Event	Protocol signing key pair updated. The protocol signing key pair has been updated automatically by Key Management Service.
7958	Event	Protocol signing key pair created. The protocol signing key has been created. This audit only occurs during the initial start of Entrust/Master Control.
7960	Event	CA signing key pair created. The CA signing key pair has been created. This audit only occurs at the initial start of Entrust/Master Control.
7963	Event	Master User password reset. A Master User's password has been reset. This Master User's name and that of the Master User who performed the operation are included in the audit.
7964	Event	Master User password change. A Master User has changed their own password. The name of the Master User is included in the audit.
7965	Log	Successful Administrator login. An Administrator or Security Officer using Entrust/RA has connected to Entrust/Authority. The IP address of the machine on which the administrator is running Entrust/RA is included in the audit.
7966	Event	Successful Master User login. A Master User has successfully started Entrust/Master Control, Administration Service, or Key Management Service. The name of the Master User is included in the audit.
7968	Event	Invalid Master User login attempt.

Audit	Severity	Audit record message and information
		A non-existent Master User name and/or invalid password was entered when running the Entrust/Master Control. The audits should be monitored for excessive events of this type as this may indicate that an unauthorized person is trying to use Entrust. The name that was entered is included with the audit.
7972	Event	Master User created. A Master User has been created by Entrust/Master Control during first-time installation of the infrastructure. The name of the Master User is included in the audit.
7977	Log	User verification certificate created. A verification public key certificate has been created for an Entrust/Entelligence user. This occurs when: an Entrust/Entelligence user is initialized; an Entrust/Entelligence user performs a Recover User operation; or an Entrust/Entelligence does a signing key pair update. The end-user's DN is included with the audit.
7978	Log	User encryption certificate created. A encryption public key certificate has been created for an Entrust/Entelligence user. This occurs when: an Entrust/Entelligence user is initialized; an Entrust/Entelligence does an encryption key pair update; or an Administrator manually updates an Entrust/Entelligence user's encryption key pair. The end-user's DN is included with the audit.
7979	Event	End-user key recovery canceled. The key recovery that has been set up for a user was canceled by an Administrator.
7981	Event	End-user key recovery completed. An Entrust/Entelligence user has successfully recovered the encryption key pair history. The end-user DN is included with the audit.
7982	Event	End-user key recovery initialized. An Entrust/Entelligence username in the active state has been set up for key recovery by an Administrator. The end-user's DN is included with the audit.
7985	Event	End-user signing key pair updated. Entrust/Entelligence has done a successful signing key pair update. This transaction is transparent to the Entrust/Entelligence user. The end-user's DN and the reason for the update are included with the audit. The various reasons are described here: • Close to expiration. Entrust/Entelligence has done a signing key pair update because the current key pair is nearing its expiry date. • Pending DN change. Entrust/Entelligence has done a signing key pair update because the user's DN has changed.
7987	Event	User encryption key pair update done when previous key pair had expired. Entrust/Entelligence has successfully updated its encryption key pair after the previous encryption key pair expired. The end-user's DN is included with the audit.
7988	Event	User encryption key pair updated. Entrust/Entelligence has done a successful encryption key pair update. This transaction is transparent to the Entrust/Entelligence user. The end-user's DN and reason for update are included with the audit. The various reasons are described here: • Close to expiration or revoked—Entrust/Entelligence has done a encryption key pair update because the current key pair it has is revoked or nearing expiration.

Audit	Severity	Audit record message and information
		• Pending DN change—Entrust/Entelligence has done an encryption key pair update because the end-user's DN has changed. • Retrieval of previous key pair—Entrust/Entelligence has done an encryption key pair update but Key Management Service found that the client possessed the second last encryption key pair. In this case, Key Management Service does not update the pair but sends the latest encryption key pair to the Client. This occurs if Entrust/Entelligence has done an encryption key pair update and the user is not using their latest profile. • Initiated by Administrator—A Security Officer or an Administrator has forced the update of a user's encryption key pair. • Update pending—Entrust/Entelligence is doing an encryption key pair update when the key has already been updated by a Security Officer or an Administrator. • Automatic update changes—A Security Officer or an Administrator has enabled or disabled automatic key update or changed the signing private key/encryption public key expiry date or the verification public key expiry date.
7989	Event	User disabled. An Entrust/Entelligence user has been disabled by a Security Officer or an Administrator. This means that the latest encryption public key certificate for that user is removed from the Directory and the Entrust user license count is decreased by one. The end-user's DN and the reason for disabling the user are included with the audit. An end-user can be disabled by a Security Officer or an Administrator or may be disabled because of three consecutive failures during key update operations. The various reasons are described here: • Disabled by Administrator. • Disabled because of errors during user initialization. • Disabled because of errors during key recovery. • Disabled because of errors during encryption key update. • Disabled because of errors during signing key update.
7990	Event	User enabled. An Entrust/Entelligence user which was previously disabled has been enabled. This means that the latest encryption public key certificate for the user has been replaced in the Directory and the Entrust user license count is increased by one. The end-user's DN is included with the audit.
7992	Event	User initialized. An Entrust/Entelligence user has been successfully created a profile. The end-user's DN is included with the audit.
7993	Log	User removed. An Entrust/Entelligence user which has been enabled is then disabled by a Security Officer or an Administrator. The user's data files are removed from the Entrust/Authority database. This is of no consequence because the encryption key pair has not yet been retrieved by the Entrust/Entelligence for use. The end-user's DN is included with the audit.
7994	Log	User added. An Entrust/Entelligence user has been added and enabled. The Entrust administrator can enable the end-user at the same time as creating the end-user or at a later time.

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

1) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

2) For each audit event type, based on the auditable event definitions of the functional components included in the ST:

- ***log number***
- ***description of event***
- ***severity level***
- ***user type***
- ***state***

5.1.5.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.5.3 FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 is satisfied by the TOE environment (i.e., the abstract machine hosting the TOE). Refer to Section 5.2.2.

FAU_STG.2.2 The TSF shall be able to ***detect*** modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that ***101 Kb (as the first 101Kb of)*** audit records will be maintained when the following conditions occur: ***audit storage exhaustion after the first 101Kb***.

5.1.6 Trusted path and data protection

This section specifies the Trusted Path security requirements for Entrust/Authority. The Trusted Path security requirements are summarized in Table 16.

Table 16: Trusted path security requirements

#	Security Requirement		Component
1.	Trusted path and channel	Distinct secure communications path	FTP_TRP.1
		Trusted channel	FTP_ITC.1
2.	Data exchange integrity	User data integrity	FDP_UIT.1
		System data integrity	FPT_ITI.1
3.	Data consistency and availability	Data consistency	FPT_TDC.1
4.	Non-repudiation	Proof of origin of certificates, CRLs and ARLs	FCO_NRO.2
5.	Data integrity	Generation and authentication data	FDP_DAU.1
		Monitoring of stored data integrity	FDP_SDI.1

5.1.6.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***the following remote users*** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

- ***Administrative users (operators) interfacing with Entrust/Authority remotely from Entrust/RA via EntrustSession.***
- ***Administrative users (operators) interfacing with Entrust/Authority remotely from Entrust/RA via PKIX-CMP (excluding automatic key management functions)***
- ***External CAs interfacing with Entrust/Authority remotely via SEP or PKIX-CMP***
- ***End Users interfacing with Entrust/Authority remotely via SEP or PKIX-CMP.***

FTP_TRP.1.2 The TSF shall permit ***the remote users identified in FTP_TRP.1.1*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***initial operator authentication and access to any TOE services authorized for the authenticated operator.***

5.1.6.2 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 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.1.2 The TSF shall permit for ***automatic key management functions (encryption key pair update, signature key pair update), the remote trusted product*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***no operations.***

5.1.6.3 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, and 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.

5.1.6.4 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 EntrustSession, SEP, and PKIX-CMP messages is always integrity-protected using digital signatures or MACs.***

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 and audit a failure*** if modifications are detected.

5.1.6.5 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:

- ***SEP protocol data***
- ***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, PKIX-CMP, and SEP.***

5.1.6.6 FCO_NRO.2 Enforced proof of origin

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for the following transmitted information types at all times:

- ***CA certificate, all user certificates, CRLs, and ARLs posted to the directory and downloaded to users via LDAP.***

FCO_NRO.2.2 The TSF shall be able to relate the ***identity*** of the originator of the information, ***and entire certificates, CRLs, and ARLs*** of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to: ***any user for certificates, CRLs, and ARLs*** given ***that the evidence may be guaranteed only during the lifetime of the verification public key.***

5.1.6.7 FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of ***CA certificate, all user certificates, CRLs, and ARLs***.

FDP_DAU.1.2 The TSF shall provide ***anyone with access to Directory*** with the ability to verify evidence of the validity of the indicated information. ***Certificates, CRLs, and ARLs are received by and verified by users. The ability to verify evidence of the validity of the digitally signed information is available to any entity in possession of the digitally signed information and access to the signer's verification public key.***

5.1.6.8 FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for ***integrity errors*** on all objects, based on the following attributes: ***all MACed data stored by Entrust/Authority in the Entrust/Authority database.***

5.1.7 Non-bypassability and recovery

This section specifies the non-bypassability and automated recovery security requirements for Entrust/Authority. These requirements are summarized in Table 17.

Table 17: Non-bypassability security requirements

#	Security Requirement		Component
1.	Non-bypassability	Non-bypassability of security functions	FPT_RVM.1
2.	Trusted recovery	Automated recovery	FPT_RCV.2
3.	Testing	TSF testing	FPT_TST.1

5.1.7.1 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.

5.1.7.2 FPT_RCV.2 Automated recovery

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 ***For failures/service discontinuities of the AS, SEP, PKIX-CMP, DB Backup, DB Integrity, CRL Writing, and Keygen subsystems***, the TSF shall ensure the return of the TOE to a secure state using automated procedures.

5.1.7.3 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests ***during initial start-up, periodically during normal operation, and at the request of the authorized user, at the conditions (no conditions)*** to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

5.2 TOE Environment Security Functional Requirements

The environment is required to satisfy the secure usage assumptions in Section 3.2 and to meet all of the environmental security objectives outlined in Section 4.2. This section identifies and specifies the environmental SFR components that the environment of the TOE 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 environmental security objectives for the TOE.

Table 18 lists the functional requirements delivered by the FIPS 140-1 (Level 2)-validated Entrust Security Kernel 5.0 (software cryptomodule) upon which the TOE depends **[Reference 2**.

Table 18: 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.	FIA_SOS.2.1	Generation of secrets	O.CRYPTO

Table 19 lists the functional requirements delivered by the abstract machine hosting the TOE.

Table 19: Required functional component provided by the abstract machine

#	CC Component	Name	Dependency for the TOE to meet
1.	FPT_STM.1	Reliable time stamp	FAU_GEN.1
2.	FAU_STG.2.1	Guarantees of audit data availability	O.ACCOUNT O.BYPASS O.DETECT O.RECORD
3.	FPT_SEP.1	TSF domain separation	O.PHYSICAL
4.	FPT_AMT.1	Abstract machine testing	FPT_TST.1 O.OPERATE

5.2.1 Cryptographic services

This section specifies the cryptographic services (environmental security requirements) for Entrust/Authority. The cryptographic services (environmental security requirements) are summarized in Table 20.

Table 20: Cryptographic services security requirements

#	Security Requirement		Component
1.	Cryptographic key operations	Key generation	FCS_CKM.1
		Key destruction	FCS_CKM.4
		Cryptographic operations	FCS_COP.1
2.	Generation of secrets	Generation of secrets	FIA_SOS.2.1

5.2.1.1 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***

- ***CAST5***
- ***DES***
- ***Triple-DES***

and specified cryptographic key sizes:

- ***RSA: 2048-bit, 1024-bit***
- ***DSA: 1024-bit***
- ***CAST5: 128-bit, 80-bit***
- ***DES: 56-bit***
- ***Triple-DES: 168-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***
- ***CAST5: ANSI X9.17, RFC 2144***
- ***DES: ANSI X9.17, ANSIX3.92, and FIPS PUB 46-2***
- ***Triple-DES: ANSI X9.17 and X9.52***

5.2.1.2 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***.

5.2.1.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform:

- ***Pseudo-random number generation***
- ***key storage***
- ***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***

- ***Private key storage: PKCS #5 and PKCS #8***
- ***Encryption and Decryption: CAST5 encryption, DES encryption, Triple-DES encryption***
- ***Digital Signature/Verification: RSA digital signature, DSA digital signature, ECDSA verification only***
- ***Key Management: RSA, Diffie-Hellman key agreement, LDAP, SEP, 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***

that meet the following standards:

- ***Pseudo-random number generation: ANSI X9.17 Appendix C***
- ***Private key storage: PKCS #5, PKCS #8***
- ***Certificates and CRLs: X.509 v3***
- ***CAST5 encryption: RFC 2144***
- ***DES encryption: FIPS PUB 46-2, ANSI X3.92***
- ***Triple-DES encryption: ANSI X9.52***
- ***DES, CAST5, triple-DES encryption in CBC mode: FIPS PUB 81, ANSI X3.106, ISO/IEC 10116***
- ***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: ANSI X9.62***
- ***EntrustSession Diffie-Hellman key agreement: PKCS #3***
- ***Lightweight Directory Access Protocol v2 and v3: RFC 1777 and RFC 2251***

- ***SEP protocol built using Generic Upper Layers Security (GULS) standards: ITU-T Recommendations X.830, X.832, and ISO/IEC 11586-1, 11586-2, 11586-3***
- ***PKIX-CMP: RFC 2510***
- ***SHA-1 hash: FIPS PUB 180-1, ANSI X9.30 Part 2***
- ***MD5 hash: RFC 1321***
- ***MAC: FIPS PUB 113, ANSI X9.9, X9.19***

5.2.1.4 FIA_SOS.2.1 Generation of secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet the following criteria: ***The TOE shall generate secrets using a FIPS 140-1 (or equivalent) validated cryptographic module*.**

5.2.2 Abstract machine services

This section specifies the abstract machine services (environmental security requirements) for Entrust/Authority. These services (environmental security requirements) are summarized in Table 20.

Table 21: Abstract machine security requirements

#	Security Requirement		Component
1.	Time stamp	Reliable time stamp for audited events	FPT_STM.1
2.	Audit availability	Guarantees of audit data availability	FAU_STG.2.1
3.	Domain separation	TSF domain separation	FPT_SEP.1
4.	OS Testing	Abstract machine testing	FPT_AMT.1

5.2.2.1 FPT_STM.1 Reliable time stamps

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

5.2.2.2 FAU_STG.2.1 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorized deletion.

5.2.2.3 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.

5.2.2.4 FPT_AMT.1 Abstract machine testing

FPT_AMT.1.1 The TSF shall run a suite of tests ***manually initiated*** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.3 TOE Security Assurance Requirements

The assurance components for the Entrust/Authority Security Target are summarized in Table 22.

Table 22: 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

Table 23 lists those components that augment EAL3 from CC Version 2.1 Part 3 **[Reference 1]** for this ST.

Table 23: Augmentation to EAL3

EAL3 Assurance Component		Augmentation to EAL3 for this ST
ACM_SCP.1	TOE CM Coverage	upgrade: ACM_SCP.2 Problem Tracking CM Requirements
AVA_MSU.1	Examination of Guidance	upgrade: AVA_MSU.2 Validation of Analysis
n/a		add: ADV_SPM.1 Informal TOE Security Policy Model
n/a		add: ALC_FLR.2 Flaw Remediation requirements
n/a		add: AMA_CAT.1 Categorization Report

6 TOE Summary Specification

6.1 IT Security Functions

This section describes the IT security functions provided by the TOE to meet the security functional requirements specified for Entrust/Authority in Section 5.1.

6.1.1 Access control

6.1.1.1 Scope of policy

The TOE controls access to all Entrust system data associated with operations initiated by any Entrust operator: Master User, Security Officer, Administrator, Auditor, AutoRA Administrator, Directory Administrator, or any custom-defined role.

6.1.1.2 Access rules

The TOE controls access to all Entrust system data on the basis of the following security attributes: Identity; Role; Privileges (i.e., permissions); and State (Entrust state: e.g., enabled, disabled, set for key recovery, etc.).

6.1.1.3 Management of security attributes

User security attributes may only be initialized, accessed, or modified by certain operators for certain operations, as specified in Table 8.

6.1.1.4 Secure security attribute values

Secure (acceptable) values for security attributes are hard-coded in Entrust/Authority. Attribute values outside the acceptable range are rejected. Table 24 illustrates the specific values which are considered secure for the security attributes.

Table 24: Justification of secure attribute values

#	Security attribute	Secure Values	Comment
1.	***RoleId***	Any existing role ID.	Values for roles can only be assigned from existing role IDs. Therefore, any value for an existing role ID is acceptable.
2.	***State***	1 to 11.	Values for state can only be 1 to 11 (reflecting the number of user states) based on the operation performed on the user.
3.	***RolloverAllowed***	True or False	This database object is defined as a boolean. Therefore, only True or False is accepted. TRUE implies the user will automatically proceed with key updates.
4.	***UserPermissions***	Vector containing binary indicators of specific permissions.	This database object is defined as a vector of binary data. Any setting in the permission vector is secure for that role.
5.	***Tok***	Machine generated based on entered Master User password.	Generated to conform to criteria for generation of secrets. All generated values are secure.

6.1.1.5 Initialization of security attributes

Entrust/Authority provides restrictive default values for security attributes. However, Entrust/Authority allows authorized Entrust operators to specify alternative initial values for user security attributes, as shown in Table 8.

6.1.1.6 Definition of user security attributes

Entrust/Authority maintains in its database a set of security attributes for each user. These security attributes are listed in Table 8.

6.1.1.7 Management of system data

Entrust/Authority restricts the ability of operators to access (e.g., modify, delete, clear) system data based on the operator's Entrust role (e.g., Master User, Security Officer), as specified in Table 9.

6.1.1.8 Secure system data values

Secure (acceptable) values for system data are hard-coded in Entrust/Authority. System data values outside the acceptable range are rejected. Table 25 illustrates the specific values which are considered secure for the system data.

Table 25: Justification of secure data values

#	System Data	Secure Values	Comment
1.	***SEPDisabled***	TRUE or FALSE.	This object is a BOOLEAN. Hence, only True or False is acceptable.
2.	***CMPDIsabled***	TRUE or FALSE.	This object is a BOOLEAN. Hence, only True or False is acceptable.
3.	***ASHDisabled***	TRUE or FALSE.	This object is a BOOLEAN. Hence, only True or False is acceptable.
4.	***EntIntegrityPeriod***	1 hour to 840 hours.	As part of a comprehensive security policy, Entrust integrity checks are enforced to at least once every 840 hours (35 days).
5.	***EntbackupFrequency***	1 hour to 840 hours.	As part of a comprehensive security policy, Entrust backups are enforced to at least once every 840 hours (35 days).
6.	***UserLimit***	Based on license string from Entrust.	Value associated with license string is secure. Only one value is derived from the license string.
7.	***Key***	Based on license string from Entrust.	Value associated with license string is secure. Only one value is derived from the license string.
8.	***CASecret***	Machine generated under criteria for generation of secrets.	Generated to conform to criteria for generation of secrets (CA Master secret). All generated values are secure.
9.	***EntSecret***	Machine generated under criteria for generation of secrets.	Generated to conform to criteria for generation of secrets (Entrust Master secret). All generated values are secure.
10.	***PassSecret***	Machine generated under criteria for generation of secrets.	Generated to conform to criteria for generation of secrets (Master User secret). All generated values are secure.

#	System Data	Secure Values	Comment
11.	***CAKeyPairType***	RSA 1024, RSA 2048, or DSA 1024.	Algorithms are hard-coded.
12.	***CRLLifetime***	4 hours to 48 hours.	Only a value in the given range is accepted. Values outside this range are considered impractical or unreasonable.
13.	***CrossCertLt***	3 days to 60 months.	Only a value in the given range is accepted. Values outside this range are considered impractical or unreasonable.
14.	***HasherType***	SHA-1 or MD5.	Algorithms are hard-coded.
15.	***AutoPushCRL***	TRUE or FALSE.	This database object is defined as a BOOLEAN. Hence, only True or False is acceptable.
16.	***NumMasterUsers***	1 or 2.	Any value in the given range is considered secure. This establishes the number of Master Users required for sensitive operations.
17.	***ASHEpfPw***	Machine generated under criteria for generation of secrets.	Generated to conform to criteria for generation of secrets (Administrator password). All generated values are secure.
18.	***EncAlg***	CAST5-128 or Triple-DES.	Algorithms are hard-coded.
19.	***SepEncAlg***	CAST5-128 or Triple-DES.	Algorithms are hard-coded.
20.	***ForCertExpireDate***	3 months to 60 months.	Only a value in the given range is accepted. Values outside this range are considered impractical or unreasonable.
21.	***MgXcPassword***	Machine generated under criteria for generation of secrets.	Generated to conform to criteria for generation of secrets (authorization code). All generated values are secure.
22.	***RevCertExpireDate***	3 months to 60 months.	Only a value in the given range is accepted. Values outside this range are considered impractical or unreasonable.
23.	***NextSerNum***	Machine selected.	Counter is reset to next available certificate serial number. Only this value is considered secure.
24.	***UserPermissions***	Any combination of permissions.	A user's role's permission vector may contain any combination of permissions. Any selection is considered secure.
25.	***NumForSensitive***	0 to 10 (or number of users in that administrative role – whichever is lower).	The maximum limit is 10. Operational limit is the number of administrative users in that role.

6.1.1.9 Residual information protection

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

6.1.2 Separation of duties

6.1.2.1 Entrust roles

Entrust/Authority maintains the roles Master User, Security Officer, Administrator, Directory Administrator, Auditor, AutoRA Administrator, and End User. Entrust/Authority allows for authorized operators to define new roles. These roles are described in Section 2.3.1.

When a new user is created (with the exception of Master Users), an operator with sufficient privileges has the option of associating the new user with the roles of Security Officer, Administrator, Directory Administrator, Auditor, AutoRA Administrator, End User, or any custom roles that may exist. The End User role actually has no privileges to access Entrust/Authority via Entrust/RA or Entrust/Master Control (i.e., an End User cannot log in to Entrust/RA or Entrust/Authority except for key management operations which are transparent to the End User).

Some conditions must hold in order for the role to be assigned to the user. A user can be associated with the Security Officer, Administrator, Directory Administrator, Auditor, AutoRA Administrator, or other custom-defined role only as explicitly assigned by a Security Officer or operator with sufficient privileges. The Security Officer and End User roles are assigned a fixed set of privileges which can be assigned or revoked. Master User can never be deleted. No Master Users past the original three may be added. A user cannot be disassociated from the Master User role.

6.1.2.2 Management of security functions behavior

Each Entrust role provides access to a specific set of operations, including the ability to modify the behavior of the Entrust system. Certain operations are available to certain operators, as listed in Table 11.

6.1.2.3 Management of end user password and authorization code lifetime

Entrust/Authority restricts the capability to specify an expiration time for the one-time authorization code and password security attributes. Only Security Officers and custom-defined roles can have this capability.

After the authorization code lifetime is reached without being used, the authorization code and corresponding reference number are deleted and cannot be used. After the password expiration is reached, Entrust/Authority can force a user password change upon the user's next login.

6.1.3 Identification and authentication

6.1.3.1 Authentication of users

Entrust/Authority does not allow the selection of any Entrust/Authority-mediated function from Entrust/Master Control before the operator is successfully authenticated. All functions require the operator to be authenticated before allowing any Entrust/Authority-mediated action.

6.1.3.2 Identification of users

Entrust/Authority does not allow selection of any Entrust/Authority-mediated function from Entrust/Master Control before the operator is successfully identified. All functions require the operator to be identified before allowing any Entrust/Authority-mediated action.

6.1.3.3 User password criteria (Verification of secrets)

Entrust/Authority enforces that user-generated secrets (passwords for Master User, Security Officer, Administrator, Auditor, Directory Administrator, End Users, and any custom-defined roles) meet the password criteria specified for the role, as described in Section 5.1.3.3. **(SoF - Medium)**

6.1.3.4 Protection against reuse

Entrust/Authority prevents the reuse of authentication data related to user key management and CA cross-certification using a one-time authorization code and reference number in the SEP and PKIX-CMP protocol for Entrust/Authority key management operations.

6.1.3.5 Re-authentication of operators

Entrust/Authority forces the re-authentication of Master Users to complete sensitive operations in Entrust/Master Control, for a Master User password change, and for Master Users after the hard-coded Entrust/Master Control timeout period (5 minutes) has lapsed.

6.1.3.6 Non-echoing of passwords

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

6.1.3.7 Session termination following inactivity

Entrust/Authority terminates its session with Entrust/Master Control after the hard-coded Entrust/Master Control timeout period (5 minutes) has lapsed.

The Administration Service subsystem at Entrust/Authority terminates its session with Entrust/RA after the Administration Service session timeout period (default: 2 minutes) has lapsed.

6.1.3.8 Authentication failure

Entrust/Authority detects three consecutive authentication failures via the Entrust/Master Control GUI interface for initial or subsequent authentication, then terminates the process and generates the appropriate audit event.

6.1.4 Key management

6.1.4.1 Key distribution

Entrust/Authority distributes cryptographic keys as follow:

- End entity public encryption and public verification keys wrapped in X.509 v3 certificates. Entrust/Authority distributes these certificates to the Directory, to end users, and the database.

- End entity private encryption keys are distributed to end entities via a trusted channel at user initialization or via a trusted channel for automatic key update. These keys are always distributed via trusted path or channel, ensuring protection of the keys against unauthorized disclosure and modification.

- Key agreement with remote entities is always performed in a secure manner.

Entrust/Authority distributes cryptographic keys in accordance with the relevant standards: X.509v3 (Section 11 and Section 12); RSA (PKCS #1 and FIPS PUB 186-1); DSA (FIPS PUB 186-1); Diffie-Hellman key agreement (PKCS #3); LDAP (RFC 1777 and RFC 2251); SEP and PKIX-CMP (RFC 2510).

6.1.4.2 Key access

Entrust/Authority accesses cryptographic keys to perform initialization, key update, key recovery, and key backup in accordance with the relevant standards: SEP, PKIX-CMP, and FIPS PUB 140-1.

For initialization, Entrust/Authority receives from Entrust/RA operators or end users newly generated user verification keys and protocol encryption keys. Entrust/Authority supplies to Entrust/RA operators or end users newly generated decryption private keys in encrypted form and session keys in encrypted form.

For key update, Entrust/Authority receives from Entrust/RA operators or end users protocol encryption keys or verification public keys. Entrust/Authority supplies Entrust/RA operators or end users newly generated decryption private keys in encrypted form and session keys in encrypted form.

For key recovery, Entrust/Authority receives from Entrust/RA operators or end users newly generated verification public keys and protocol encryption keys. Entrust/Authority supplies Entrust/RA operators or end users the session key in encrypted form.

For key backup, Entrust/Authority needs to access private and public keys which are stored in the Entrust/Authority database. Entrust/Authority never sees these keys in plain text as they are stored in encrypted form.

6.1.4.3 Machine-generated secrets

Entrust/Authority-generated secrets (Entrust Master secret, CA Master secret, authorization code) meet the criteria as specified in Section 5.1.4.2 and are used only for the specified purposes.

Entrust Master secret is used to derive the Entrust Master encryption key and Entrust Master integrity key. These keys are used to protect most fields in the Entrust/Authority database by encryption and application of MACs.

CA Master secret is used to protect only the CA signing key pair in the Entrust/Authority database by encryption and application of MACs.

Authorization code is used to derive a MAC key (for integrity and authentication) for communications between users and Entrust/Authority and between Entrust/Authority and another Entrust/Authority using the SEP or PKIX-CMP protocol for user initialization, key update, key recovery, and cross-certification.

6.1.4.4 Enforced proof of receipt for distributed key and certificates

Proof of receipt for distributed keys, contained within public key certificates, and distributed via the SEP or PKIX-CMP protocols is based upon automated acknowledgement messages generated by the end user upon receiving the certificates. This acknowledgement is received and processed by Entrust/Authority and an audit event is generated indicating a successful key management operation (e.g., initialization, key update).

6.1.4.5 Detection of duplicate certificate issuance

Entrust/Authority checks the distinguished name (DN) of new users before entries are created for them in the Entrust/Authority database and the Directory. Entries with duplicate names are not allowed, and, therefore, cannot be created if an entry already exists with the same DN. Hence, duplicate certificates cannot be generated because replay has been detected.

6.1.5 Audit

6.1.5.1 Specification of auditable events and recorded information

Entrust/Authority audits all of the events specified in Table 15 including the following information: data and time of event, type of event, subject identity, outcome, log number, event description, severity level, user type, state, extra text, and MAC.

6.1.5.2 Accountability of users

Each audit event is uniquely associated with the identity of the user who caused the event, as appropriate.

6.1.5.3 Audit data integrity and availability

Entrust/Authority protects the stored audit records from unauthorized deletion by not providing administrative users with direct access to the audit files. Only a copy of the audit records may be viewed by Security Officers, Administrators, and Auditors via Entrust/RA workstations without the option to delete records. The audit files are only stored on Entrust/Authority.

Entrust/Authority detects unauthorized modification to the audit data based on the application of MACs. It also ensures that a minimum of 101 kb of audit data is always maintained.

6.1.6 Trusted path and data protection

6.1.6.1 Distinct secure communications path

Entrust/Authority provides a trusted path for remote operators accessing Entrust/Authority from Entrust/RA via EntrustSession, SEP, or PKIX-CMP. A trusted path exists for remote external CAs and remote end users accessing Entrust/Authority via SEP. Another trusted path exists for end users accessing Entrust/Authority via PKIX-CMP. Any data, including TSF and user data, transmitted through this trusted path is always protected against unauthorized disclosure and modification. Any services available to remote operators including administrative services, user initialization and key recovery services, and cross-certification establishment services require use of a trusted path.

6.1.6.2 Trusted channel

Entrust/Authority provides a trusted channel between itself and remote Entrust entities (i.e., Entrust/RA and Entrust/Entelligence) via SEP or PKIX-CMP. A trusted channel is required for automatic key update of end user encryption key and signing key pairs. The key update operations are initiated by the remote Entrust entities. Any sensitive data transmitted through this trusted channel is always protected against unauthorized disclosure and modification.

6.1.6.3 Data exchange integrity

Entrust/Authority provides the capability to transmit and receive data in a manner protected from modification, deletion, insertion, and replay errors for all data in EntrustSession, SEP, or PKIX-CMP messages as all data is always integrity-protected using digital signatures or MACs. Entrust/Authority terminates communication sessions via EntrustSession, SEP, or PKIX-CMP upon detection of data modification, deletion, insertion, or replay, and audits the failure. Entrust/Authority disables an end user when three transactions with that user are terminated due to detection of modified data.

6.1.6.4 Data consistency

The data in the EntrustSession, SEP, and PKIX-CMP protocols are consistently interpreted by Entrust/Authority based on common implementations of the protocols. The various information types used in these protocols are as follow:

1) The data types associated with the SEP protocol are:

- Entrust version information for backwards compatibility
- reference number, authorization code, and random numbers for authentication
- cryptographic data (public and private keys, session keys, and encryption and verification certificates) for key management
- system time for time limitation to prevent replay
- message contents (data to transmit securely)

2) The data types associated with the PKIX-CMP protocol are:

- reference number, authorization code, and random numbers for authentication
- cryptographic data (public and private keys, session keys, and encryption and verification certificates) for key management
- cryptographic algorithm identification, source and destination names for authentication
- system time for time limitation to prevent replay
- message contents (data to transmit securely)

3) The data types associated with EntrustSession are:

- context identification, source and destination names, and random numbers for authentication
- timestamp for time limitation to prevent replay
- cryptographic data (Diffie-Hellman exponential), algorithm, and session establishment data for proper configuration of session
- cryptographic data (verification certificate) for data integrity
- message contents (data to transmit securely)

6.1.6.5 Proof of origin

Entrust/Authority provides a capability to generate evidence that can be used as a guarantee of the proof of origin of CA certificates, user certificates, CRLs, and ARLs.

6.1.6.6 Validity of certificates, CRLs and ARLs

Entrust/Authority provides a capability to generate evidence that can be used as a guarantee of the validity of CA certificates, user certificates, CRLs, and ARLs.

6.1.6.7 Detection of errors in stored data

Entrust/Authority monitors for integrity errors all data it stores in the Entrust/Authority database. The data objects are checked for integrity when accessed. The database can be continuously validated for integrity and on-demand by Master Users.

6.1.7 Non-bypassability and Recovery

6.1.7.1 Non-bypassability of security functions

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

6.1.7.2 Automated re-start of services

The Monitor service (Entrust/Authority Service) can be enabled to automatically re-start after a system failure or service discontinuity. The SEP, PKIX-CMP, AS, DB Backup, DB Integrity, CRL Writing, and Keygen subsystems can then themselves be restarted automatically by the Monitor service.

6.1.7.3 Testing

On start-up, Entrust/Authority verifies the integrity of the CA signing key pair, the most sensitive piece of data in Entrust/Authority. If verification fails, Entrust/Authority will not start. The integrity of all stored Entrust/Authority data is verified in the Entrust/Authority database, performed by the Entrust/Authority DB Integrity subsystem. Moreover, whenever Entrust/Authority initializes or makes function calls to its cryptomodule, the cryptomodule functions are verified for proper operation.

Entrust/Authority, through the Entrust/Master Control interface, provides the capability to Master Users to verify the integrity of all stored TSF data in the Entrust/Authority database.

Entrust/Authority also provides the capability for the Entrust cryptomodule to verify the integrity of the executable or dynamic link library which has made a function call to the cryptomodule.

6.2 Assurance Measures

The assurance requirements for this TOE are met by EAL3-augmented, 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

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 30, 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

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

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.

Table 26 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. A mapping between the environmental assumptions showed in Table 1 and the environment objectives is included and an explanation is provided for not including the objective in the list of TOE security objectives.

Table 26: Correct objectives - mapping security objective to rationale

#	Security Objective	Rationale	Environmental Assumptions
1.	**O.ACCESS** The TOE must provide access by authorized users to those objects and services for which they have been authorized.	P.ACCESS	
2.	**O.KNOWN** The TOE must ensure that all users are identified and authenticated before being granted access to TOE mediated resources.	T.ENTRY	
3.	**O.AUTHORIZE** The TOE must provide the ability to specify and manage user and system process access rights to individual objects and services.	P.ACCESS This objective is also implied by O.ACCESS. In order to provide access to “authorized” users, there must be a means of authorizing.	
4.	**O.ACCOUNT** The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	P.ACCOUNT	
5.	**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	

#	Security Objective	Rationale	Environmental Assumptions
6.	**O.ENTRY** The TOE must prevent unauthorized logical entry to the TOE by technical methods used by persons without authority for such access.	T.ENTRY O.ENTRY-SOPHISTICATED is the companion environmental objective.	
7.	**O.DETECT** The TOE must enable the detection of corrupted security critical data, including audit trail, and the detection of replayed operations which could subsequently compromise the secure state of the TOE. The level of detection provided must correspond to the level of attack sophistication being protected against by the other security objectives.	T.DATA-CORRUPTED T.AUDIT-CORRUPTED P.SURVIVE O.DETECT-ABSTRACT is the companion environmental objective.	
8.	**O.AVAILABLE** The TOE must protect itself from unsophisticated, denial-of-service attacks.	T.DENIAL P.SURVIVE O.DENIAL-SOPHISTICATED is the companion environmental objective.	
9.	**O.ORIGIN** The TOE must generate evidence of origin for transmitted public key certificates, CRLs and ARLs.	P.ORIGIN Best security practices stipulates that public key certificates, CRLs and ARLs be digitally signed by their originated CA.	
10.	**O.RECEIPT** The TOE must successfully validate the evidence of receipt for received keys and certificates it distributes to end users.	P.RECEIPT	
11.	**O.KEY-DISTRIBUTE** The TOE must provide for authorized administrative users to distribute and revoke public key certificates, and be able to securely and transparently exchange secret keys as required.	P.KEY-DISTRIBUTE	
12.	**O.KEY-RECOVER** The TOE must provide for authorized administrative users to recover end-user encryption keys, and automatically update these keys as required.	P.KEY-RECOVER	
13.	**O.RECORD** The TOE must record security critical events to ensure that the information exists to support effective security management.	P.ACCOUNT P.SURVIVE	

#	Security Objective	Rationale	Environmental Assumptions
14.	**O.NETWORK** The TOE must continue to be able to meet its security objectives when networked with other IT resources. The TOE security policy must be maintained on exported data objects, including cryptographic keys.	P.NETWORK During day-to-day operations, connections will be established between the TOE and other Entrust/Authority and Entrust/RA entities.	
15.	**Environment - O.CRYPTO** The cryptographic operations, 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, on behalf of the TOE.	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
16.	**Environment - O.OPERATE** Those responsible for the TOE must ensure that the TOE is delivered, 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. The TOE is expected to support, however, by providing mechanisms and interfaces that ease the burden of ensuring correct delivery, installation, and operation.	A.USER-NEED A.USER-TRUST A.ABSTRACT A.ADMIN
17.	**Environment - O.MANAGE** Those responsible for the TOE must ensure that the TOE is managed and administered in a manner that maintains IT security.	T.ADMIN-ERROR T.AUDIT-CORRUPTED See rationale for O.OPERATE.	A.ADMIN
18.	**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 Physical security is not provided by the TOE, thus it is an environmental objective.	A.LOCATE A.PROTECT
19.	**Environment - O.ENTRY-SOPHISTICATED** The TOE environment must sufficiently counter the threat of an individual (other than an authorized user) gaining unauthorized access via sophisticated technical attack.	T.ENTRY-SOPHISTICATED The TOE provides mechanisms that seek to deal with this threat. However, effectively dealing with real-world threat-agents requires the addition of countermeasures provided by the TOE environment.	A.LOCATE A.PROTECT A.CONNECT

#	Security Objective	Rationale	Environmental Assumptions
20.	**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 The TOE provides mechanisms that seek to deal with this threat. However, effectively dealing with real-world threat-agents requires the addition of countermeasures provided by the TOE environment.	A.USER-NEED A.ADMIN
21.	**Environment - O.DETECT-ABSTRACT** The TOE environment must provide the ability to detect unauthorized modification and corruption of the TOE abstract machine.	T.SYSTEM-CORRUPTED P.SURVIVE	A.ADMIN
22.	**Environment – O.DENIAL-SOPHISTICATED** The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.	T.DENIAL-SOPHISTICATED P.SURVIVE The TOE provides mechanisms that seek to deal with this threat. However, effectively dealing with real-world threat-agents requires the addition of countermeasures provided by the TOE environment.	A.LOCATE A.PROTECT A.CONNECT
23.	**Environment - O.RECOVER** The TOE, in conjunction with its environment, must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity.	T.CRASH P.SURVIVE	A.ADMIN

7.2 Security Requirements Rationale

7.2.1 Suitability of security functional requirements

Table 27 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.

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

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 27: Complete functionality - mapping security objective to functionality

#	Security Objective	TOE Functionality	Justification
1.	**O.ACCESS** The TOE must provide access by authorized users to those objects and services for which they have been authorized.	FCS_CKM.3 FDP_ACC.2 FDP_ACF.1 FMT_MTD.1 FMT_SAE.1a FMT_SAE.1b	These requirements ensure that access controls are provided allow and/or prevent access to TSF objects and services: **FCS_CKM.3** ensures that cryptographic keys are accessed by the TSF for specific operations in accordance with specific standards. **FDP_ACC.2** ensures that complete access control is enforced on all operations between any subject and any object. **FDP_ACF.1** ensures that an access control security policy is enforced on all subjects based on user security attributes. **FMT_MTD.1** ensures that access to TSF data is restricted to specific roles for specific purposes. **FMT_SAE.1a** and **FMT_SAE.1b** ensure that the capability to access the password and activation code lifetimes is restricted to specific roles.
2.	**O.KNOWN** The TOE must ensure that all users are identified and authenticated before being granted access to TOE mediated resources.	FIA_UAU.2 FIA_UAU.4 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_UAU.4** ensures that reuse of authentication data is prevented, so that each user must be 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.
3.	**O.AUTHORIZE** The TOE must provide the ability to specify and manage user and system process access rights to individual objects and services.	FIA_ATD.1 FMT_MOF.1 FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SAE.1a FMT_SAE.1b FMT_SMR.2	These requirements ensure that the TSF can specify and manage user and system data and system functions and provide controls to access them: **FIA_ATD.1** ensures that a set of user security attributes is maintained and managed by the TOE. **FMT_MOF.1** ensures that the ability to modify TSF behavior is restricted to specific roles. **FMT_MSA.1** ensures that an access control security policy is enforced to restrict the ability to modify security attributes to specific roles for specific purposes. **FMT_MSA.2** ensures that only secure values are

#	Security Objective	TOE Functionality	Justification
			accepted for security attributes as managed by the TOE. **FMT_MSA.3** ensures that a TOE access control security policy is enforced to restrict the ability to provide default security attribute values to specific roles. **FMT_SAE.1a** and **FMT_SAE.1b** ensure the TOE capability to access the password and activation code lifetimes is restricted to specific roles. **FMT_SMR.2** ensures that roles are maintained by the TOE and can be associated with users under specific conditions.
4.	**O.ACCOUNT** The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	FAU_GEN.1 FAU_GEN.2 FAU_STG.2	These requirements ensure that users can be held accountable for their actions: **FAU_GEN.1** ensures that audit data is generated for user-initiated operations. **FAU_GEN.2** ensures that each audit event can be associated with the identity of the user that caused the event so the user can be held accountable for their actions. **FAU_STG.2** ensures that audit data is available under specific conditions and that modifications to audit data are detected so the integrity of the audit data is maintained.
5.	**O.BYPASS** The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement.	FAU_GEN.1 FAU_GEN.2 FAU_STG.2 FDP_ACC.2 FDP_DAU.1 FDP_RIP.1 FIA_AFL.1 FIA_SOS.1 FIA_SOS.2.2 FIA_UAU.4 FIA_UAU.6 FIA_UAU.7 FMT_MTD.3 FPT_RVM.1 FTA_SSL.3a FTA_SSL.3b	These requirements ensure that users are prevented from bypassing or circumventing TOE security policies: **FAU_GEN.1** ensures that audit data is generated for user-initiated operations so that attempts to bypass or circumvent security policy is captured in the audit log. **FAU_GEN.2** ensures that each audit event can be associated with the identity of the user that caused the event so that attempts to bypass or circumvent security policy is captured in the audit log. **FAU_STG.2** ensures that audit data is available under specific conditions and that modifications to audit data are detected so the integrity of the audit data is maintained as well as the security policy. **FDP_ACC.2** ensures that complete access control is enforced on all operations between any subject and any object., preventing the bypassing or circumvention of access control security policy. **FIA_UAU.4** ensures that reuse of authentication

#	Security Objective	TOE Functionality	Justification
			data is prevented, so that each user must be successfully authenticated before allowing any TSF-mediated actions for that user, preventing the bypassing or circumvention of access control security policy. **FDP_DAU.1** ensures that there is a capability to generate evidence to be used as a guarantee of the validity of specific data. **FDP_RIP.1** ensures that any previous information content of the Master User password 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_SOS.2.2** ensures that machine generated secrets are used only for their intended purposes, preventing their misuse. **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 or circumvention of access control security policy. **FMT_MTD.3** ensures that only secure values are accepted for TSF data as managed by the TOE. **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.3a** and **FTA_SSL.3b** ensure that an interactive session with Entrust/Master Control and Entrust/RA, respectively, is terminated after a period of time.
6.	**O.ENTRY** The TOE must prevent unauthorized logical entry to the TOE by technical methods used by persons without authority for such access.	FDP_ACC.2 FDP_ACF.1 FDP_DAU.1 FDP_RIP.1 FIA_AFL.1 FMT_SAE.1a FMT_SAE.1b	These requirements ensure that the TOE prevents logical access to the TOE by unauthorized users: **FDP_ACC.2** ensures that complete access control is enforced on all operations between any subject and any object. **FDP_ACF.1** ensures that an access control security policy is enforced on all subjects based on user

#	Security Objective	TOE Functionality	Justification
			security attributes. **FDP_DAU.1** ensures that there is a capability to generate evidence to be used as a guarantee of the validity of specific data. **FDP_RIP.1** ensures that any previous information content of the Master User password is made unavailable after its deallocation. **FIA_AFL.1** ensures that authentication failures are handled appropriately, preventing malicious use of the software. **FMT_SAE.1a** and **FMT_SAE.1b** ensure the TOE capability to access the password and activation code lifetimes is restricted to specific roles.
7.	**O.DETECT** The TOE must enable the detection of corrupted security critical data, including audit trail, and the detection of replayed operations which could subsequently compromise the secure state of the TOE. The level of detection provided must correspond to the level of attack sophistication being protected against by the other security objectives.	FAU_STG.2 FDP_UIT.1 FDP_SDI.1 FIA_SOS.2.2 FPT_ITI.1 FPT_RPL.1	These requirements ensure that the TOE detects corrupted stored TSF data: **FAU_STG.2** ensures that audit data is available under specific conditions and that modifications to audit data are detected. **FIA_SOS.2.2** ensures that machine generated secrets are used only for their intended purposes, preventing their misuse. **FDP_UIT.1** ensures that user data is transmitted and received protected from modification, deletion, insertion, and replay. **FDP_SDI.1** ensures that all MACed data stored in the database is monitored for integrity errors. **FPT_ITI.1** ensures that modified data in EntrustSession, SEP, and PKIX-CMP is detected based on digital signatures and/or MACs. **FPT_RPL.1** ensures that certificates are not issued to users based on replayed operations (e.g., initialization using replayed activation codes).
8.	**O.AVAILABLE** The TOE must protect itself from unsophisticated, denial-of-service attacks.	FDP_ACC.2 FDP_ACF.1 FPT_RCV.2 FPT_TST.1	These requirements ensure that the TOE protects itself from unsophisticated, denial-of-service attacks: **FDP_ACC.2** ensures that complete access control is enforced on all operations between any subject and any object. **FDP_ACF.1** ensures that an access control security policy is enforced on all subjects based on user security attributes. **FPT_RCV.2** ensures that recovery from service discontinuities is automated and the system can

#	Security Objective	TOE Functionality	Justification
			return to a secure state. **FPT_TST.1** ensures that the TSF is tested at various times to demonstrate its correct operation.
9.	**O.ORIGIN** The TOE must generate evidence of origin for transmitted public key certificates.	FCO_NRO.2	This requirement ensures that the TOE generates evidence of origin for transmitted public key certificates: **FCO_NRO.2** ensures that evidence of origin is generated for certificates, CRLs, and ARLs so the identity of the originator can be related to the information.
10.	**O.RECEIPT** The TOE must generate evidence of receipt for transmitted public key certificates.	FCO_NRR.2	This requirement ensures that the TOE generates evidence of receipt for transmitted public key certificates: **FCO_NRR.2** ensures that evidence of receipt is generated automatically for public key certificates received via SEP or PKIX-CMP.
11.	**O.KEY-DISTRIBUTE** The TOE must provide for authorized administrative users to distribute and revoke public key certificates, and be able to securely and transparently exchange secret keys as required.	FCS_CKM.2 FIA_SOS.2.2	These requirements ensure that the TOE allows authorized operators to distribute and revoke public key certificates and to securely exchange secret keys in support for certificate distribution: **FCS_CKM.2** ensures that cryptographic keys are securely distributed in accordance with specific methods and standards. **FIA_SOS.2.2** ensures that machine generated secrets are used only for their intended purposes.
12.	**O.KEY-RECOVER** The TOE must provide for authorized administrative users to recover end-user encryption key pairs, and automatically update these keys as required.	FCS_CKM.3	This requirement ensures that the TOE allows authorized operators to update and recover end-user encryption key pairs: **FCS_CKM.3** ensures that cryptographic keys are accessed by the TSF for specific operations (e.g., key recovery, key update) in accordance with specific standards.
13.	**O.RECORD** The TOE must record security critical events to ensure that the information exists to support effective security management	FAU_GEN.1 FAU_GEN.2 FAU_STG.2	These requirements ensure that the TOE records and maintains security critical events in the audit log. **FAU_GEN.1** ensures that audit data is generated for user-initiated operations. **FAU_GEN.2** ensures that each audit event can be associated with the identity of the user that caused the event so the user can be held accountable for their actions. **FAU_STG.2** ensures that audit data is available under specific conditions and that modifications to audit data are detected so the integrity of the audit data is maintained.
14.	**O.NETWORK**	FDP_UIT.1 FPT_ITI.1	These requirements ensure that the TOE can meet its security objectives when networked with

#	Security Objective	TOE Functionality	Justification
	The TOE must continue to be able to meet its security objectives when networked with other IT resources. The TOE security policy must be maintained on exported data objects, including cryptographic keys.	FPT_TDC.1 FTP_ITC.1 FTP_TRP.1	other IT products, based on confidentiality, integrity, authentication, and consistent data interpretation: **FDP_UIT.1** ensures that user data is transmitted and received in a manner protected from modification, deletion, insertion, and replay. **FPT_ITI.1** ensures that modified data in EntrustSession, SEP, and PKIX-CMP is detected based on digital signatures and/or MACs. **FPT_TDC.1** ensures that TSF data is consistently interpreted via EntrustSession, SEP, and PKIX-CMP when shared between the TSF and another trusted IT product. **FTP_ITC.1** ensures that a trusted channel is provided for automatic key management operations for operators and end users that is logically distinct from other channels and provides assured identification of its end points and protection of transmitted data from modification or disclosure. **FTP_TRP.1** ensures that a trusted path is provided for EntrustSession, SEP, and PKIX-CMP under specific conditions that is logically distinct from other channels and provides assured identification of its end points and protection of transmitted data from modification or disclosure.
15.	**O.OPERATE** Those responsible for the TOE must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	Addressed by the TOE environment.	
16.	**O.MANAGE** Those responsible for the TOE must ensure that it is managed and administered in a manner that maintains IT security.	Addressed by the TOE environment.	
17.	**O.CRYPTO** The cryptographic operations, including key generation, key destruction, encryption, decryption, signature generation and verification, checksum generation and verification and hashing must be performed on a FIPS 140-1 validated cryptographic module, on behalf of the TOE.	Addressed by the TOE environment (FIPS 140-1 validated cryptomodule) FCS_CKM.1 FCS_CKM.4 FCS_COP.1 FIA_SOS.2.1	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.

#	Security Objective	TOE Functionality	Justification
			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. **FIA_SOS.2.1** ensures that secrets are generated using a FIPS 140-1 (or equivalent) validated cryptographic module.
18.	**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.
19.	**O.ENTRY-SOPHISTICATED** The TOE environment must sufficiently counter the threat of an individual (other than an authorized user) gaining unauthorized access via sophisticated technical attack.	Addressed by the TOE environment.	
20.	**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.	
21.	**O.DETECT-ABSTRACT** The TOE environment must provide the ability to detect unauthorized modification and corruption of the TOE abstract machine.	Addressed by the TOE environment.	
22.	**O.DENIAL-SOPHISTICATED** The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.	Addressed by the TOE environment.	
23.	**O.RECOVER** The TOE, in conjunction with its environment, must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity.	Addressed by the TOE environment.	

7.2.2 Dependency analysis

Table 28 demonstrates that the functional set of security requirements meets all functional dependencies. The italic text used in Table 28 represents those functional components that are met by the FIPS 140-1 validated Entrust cryptomodule or abstract machine as listed in Table 18 and Table 19, respectively.

Table 28: Correct functionality – dependency mapping

#	Component	Name	Hierarchical To	Dependencies
1.	FAU_GEN.1	Audit data generation	—	*FPT_STM.1*
2.	FAU_GEN.2	User identity generation	—	FAU_GEN.1 FIA_UID.1
3.	FAU_STG.2.2 FAU_STG.2.3	Guarantees of audit data availability	FAU_STG.1	FAU_GEN.1
4.	FCO_NRO.2	Enforced proof of origin	FCO_NRO.1	FIA_UID.1
5.	FCO_NRR.2	Enforced proof of receipt	FCO_NRR.1	FIA_UID.1
6.	FCS_CKM.2	Cryptographic key distribution	—	*FCS_CKM.1* *FCS_CKM.4* FMT_MSA.2
7.	FCS_CKM.3	Cryptographic key access	—	*FCS_CKM.1* *FCS_CKM.4* FMT_MSA.2
8.	FDP_ACC.2	Complete access control	FDP_ACF.1	FDP_ACF.1
9.	FDP_ACF.1	Security attribute based access control	—	FDP_ACC.1 FMT_MSA.3
10.	FDP_DAU.1	Basic data authentication	—	—
11.	FDP_RIP.1	Subset residual information protection	—	—
12.	FDP_SDI.1	Stored data integrity monitoring	—	—
13.	FDP_UIT.1	Data exchange integrity	—	FTP_ITC.1 FTP_TRP.1 FDP_ACC.1
14.	FIA_AFL.1	Basic authentication failure handling	—	FIA_UAU.1
15.	FIA_ATD.1	User attribute definition	—	—
16.	FIA_SOS.1	Selection of secrets	—	—
17.	FIA_SOS.2.2	TSF generation of secrets	—	—
18.	FIA_UAU.2	User authentication before any action	FIA_UAU.1	FIA_UID.1
19.	FIA_UAU.4	Single-use authentication mechanisms	—	—
20.	FIA_UAU.6	Re-authenticating	—	—
21.	FIA_UAU.7	Protected authentication feedback	—	FIA_UAU.1
22.	FIA_UID.2	User identification before any action	FIA_UID.1	—
23.	FMT_MOF.1	Management of security functions behavior	—	FMT_SMR.1
24.	FMT_MSA.1	Management of security attributes	—	FDP_ACC.1 FMT_SMR.1
25.	FMT_MSA.2	Secure security attributes	—	ADV_SPM.1 FMT_MSA.1 FDP_ACC.1 FMT_SMR.1
26.	FMT_MSA.3	Static attribute initialization	—	FMT_MSA.1 FMT_SMR.1
27.	FMT_MTD.1	Management of TSF data	—	FMT_SMR.1
28.	FMT_MTD.3	Secure TSF data	—	ADV_SPM.1 FMT_MTD.1
29.	FMT_SAE.1a FMT_SAE.1b	Time-Limited authorization	—	FMT_SMR.1 FPT_STM.1
30.	FMT_SMR.2	Restrictions on security roles	FMT_SMR.1	FIA_UID.1
31.	FPT_ITI.1	Inter-TSF detection of modification	—	—
32.	FPT_RCV.2	Automated recovery	FPT_RCV.1	FPT_TST.1 AGD_ADM.1 ADV_SPM.1
33.	FPT_RPL.1	Replay detection	—	—

#	Component	Name	Hierarchical To	Dependencies
34.	FPT_RVM.1	Non-bypassability of the TSP	—	—
35.	FPT_TST.1	TSF testing	—	*FPT_AMT.1*
36.	FPT_TDC.1	Inter-TSF basic TSF data consistency	—	—
37.	FTA_SSL.3a FTA_SSL.3b	TSF-initiated termination	—	—
38.	FTP_ITC.1	Inter-TSF trusted channel	—	—
39.	FTP_TRP.1	Trusted path	—	—

7.2.3 Demonstration of mutual support between security requirements

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.

FPT_RVM.1 ensures that SFRs cannot be bypassed.

FIA_UAU.2, FIA_UAU.4, FIA_UAU.6, and FIA_UAU.7 provide additional 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 on behalf of a user until the user is uniquely identified to the TOE. FIA_UAU.2 supports FIA_AFL.1 and FIA_UAU.7. FIA_AFL.1 provides that unsuccessful authentication attempts are detected and takes action upon a certain threshold.

FMT_SMR.2 enforces which roles operators may take in the TOE and the conditions associated with assuming the role and supports FMT_MOF.1. FMT_MOF.1 restricts the ability of operators under different roles to modify the behavior of functions that control security attributes or configuration data. FMT_MSA.1 restricts the ability to modify security attributes or configuration data, protecting against tampering attacks through unauthorized modification of data. FMT_MSA.2 and FMT_MSA.3 restrict the accepted values for security attributes or configuration data controlled under FMT_MOF.1 and FMT_MSA.1.

Based on FMT_SMR, FMT_MOF, and FMT_MSA, FMT_SAE.1a and FMT_SAE.1b restrict the capability to specify an expiration time for security attributes to certain roles and then take action after the expiration time has been reached.

FMT_MTD.1 restricts the ability to modify any other security relevant data, protecting against tampering attacks through unauthorized modification of data. FMT_MTD.3 restricts the accepted values for TSF data controlled under FMT_MTD.1.

FDP_ACF.1 controls rules governing user access to objects based on security attribute values and supports FDP_ACC.2. FDP_ACC.2 provides complete access control and enforces access controls on subjects and objects and all operations among the subjects and objects.

FTP_TRP.1and FTP_ITC.1 protect privacy of exchanged security critical data, including security attributes, protecting against tampering attacks based on spoofing.

FCO_NRO.2 ensures that the TSF will generate evidence to prove the origin of transmitted data, without fear of the origin be spoofed. Conversely, FCO_NRR.2 ensures that the TSF will generate evidence to prove the receipt of transmitted data.

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.

FIA_SOS.1, FIA_SOS.2.2, 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.4, FIA_UAU.6 and FIA_UAU.7.

FPT_STM.1 support time entries in audit records for FAU_GEN.1, as provided by the TOE abstract machine.

FAU_STG.2.2 and FAU_STG.2.3 provide for storage of audit data, and therefore supports FAU_GEN.1. FAU_STG.2.1 ensures that audit data is not deleted in an unauthorized manner, which is provided by the abstract machine.

FAU_GEN.1 provides the ability to detect possible attacks aimed at defeating particular SFRs, or potential mis-configuration which could leave the TOE prone to attacks, and thus support the SFRs. FAU_GEN.2 ensures that the individual responsible for generating an audit event is uniquely and unambiguously identified along with the audit data.

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.

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.

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.

FDP_DAU.1 provides the ability to verify the validity and integrity of user certificates, CRLs and ARLs after these have been exported from the TOE.

FDP_SDI.1 ensures that unauthorized modification or corruption of stored data is detected before it can be used by the TOE.

FCS_CKM.2 provides for the ability to distribute (including revoke) cryptographic keys to operators, users, or processes. FCS_CKM.3 provides for the ability to access keys as necessary in the course of key management operations (e.g., key update, key rollover, key backup), respectively. FPT_RPL.1 ensures that initialization of users and creation and distribution of duplicate certificates to users already holding certificates cannot occur due to replay detection.

FTA_SSL.3a and FTA_SSL..3b, respectively, provide that the TSF terminates an interactive session to Entrust/Master Control and Entrust/RA after a period of time to free-up TOE resources and reduce the likelihood of tempering attacks on non-active connections.

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.

FPT_RCV.2 supports the automated recovery of Entrust/Authority services after a system failure or service discontinuity, which is provided by the TOE by FPT_TST.1, which is itself supported by testing of the abstract machine FPT_AMT.1.

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

7.2.4 Appropriateness of assurance requirements

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 a trusted third-party Certification Authority (CA) responsible for authenticating and certifying users. As such, the TOE establishes trust in the binding between a user's public key and other information in a certificate by digitally signing the certificate information using its own private signing key. This trust is based on three general 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 private signing 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 private signing key, the CA cannot deny having signed the certificate.

The EAL3-augmented assurance requirements listed in Table 22, 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 a trusted third-party CA..

The augmentation to EAL3 addresses the area of problem tracking (ACM_SCP.2) and flaw remediation (ALC_FLR.1), providing assurance that any problems or flaws that may appear would be effectively remedied. The augmentation also adds the TOE component categorization report (AVA_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 6]**.

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

7.3 TOE Summary Specification Rationale

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.

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:

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

- That the started assurance measures are compliant with the assurance requirements.

7.3.1 IT Security Functions rationale

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 29, will show that:

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

- Each IT security function is mapped onto at least one SFR.

As can been seen from Table 29, 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 29: Security functions mapping

Security Function	CC Component	
Access Control		
Section 6.1.1.1 Scope of policy	FDP_ACC.2	Complete access control
Section 6.1.1.2 Access rules	FDP_ACF.1	Security attribute based access control
Section 6.1.1.3 Management of security attributes	FMT_MSA.1	Management of security attribute
Section 6.1.1.4 Secure security attribute	FMT_MSA.2	Secure security attributes
Section 6.1.1.5 Initialization of security attributes	FMT_MSA.3	Static attribute initialization
Section 6.1.1.6 Definition of user security attributes	FIA_ATD.1	User attribute definition
Section 6.1.1.7 Management of system data	FMT_MTD.1	Management of TSF data
Section 6.1.1.8 Secure system data values	FMT_MTD.3	Secure TSF data
Section 6.1.1.9 Residual information protection	FDP_RIP.1	Subset residual information protection
Separation of Duties		
Section 6.1.2.1 Entrust roles	FMT_SMR.2	Restrictions on security roles
Section 6.1.2.2 Management of security functions behavior	FMT_MOF.1	Management of security functions behavior
Section 6.1.2.3 Management of end user password and authorization code lifetime	FMT_SAE.1a FMT_SAE.1b	Time-limited authorization
Identification and Authentication		
Section 6.1.3.1 Authentication of users	FIA_UAU.2	User authentication before any action
Section 6.1.3.2 Identification of users	FIA_UID.2	User identification before any action
Section 6.1.3.3 User password criteria	FIA_SOS.1	Verification of secrets
Section 6.1.3.4 Protection against reuse	FIA_UAU.4	Single-use authentication mechanisms
Section 6.1.3.5 Re-authentication of operators	FIA_UAU.6	Re-authenticating
Section 6.1.3.6 Non-echoing of passwords	FIA_UAU.7	Protected authentication feedback
Section 6.1.3.7 Session termination following inactivity	FTA_SSL.3a FTA_SSL.3b	TSF-initiated termination
Section 6.1.3.8 Authentication failure	FIA_AFL.1	Basic authentication failure handling

Security Function	CC Component	
Key Management		
Section 6.1.4.1 Key distribution	FCS_CKM.2	Cryptographic key distribution
Section 6.1.4.2 Key access	FCS_CKM.3	Cryptographic key access
Section 6.1.4.3 Machine-generated secrets	FIA_SOS.2.2	TSF generation of secrets
Section 6.1.4.4 Enforced proof of receipt for distributed key and certificates	FCO_NRR.2	Enforced proof of origin
Section 6.1.4.5 Detection of duplicate certificate issuance	FPT_RPL.1	Replay detection
Audit		
Section 6.1.5.1 Specification of auditable events and recorded information	FAU_GEN.1	Audit data generation
Section 6.1.5.2 Accountability of users	FAU_GEN.2	User identity generation
Section 6.1.5.3 Audit data integrity and availability	FAU_STG.2.2 FAU_STG.2.3	Guarantees of audit data availability
Trusted Path and Data Protection		
Section 6.1.6.1 Distinct secure communications path	FTP_TRP.1	Trusted path
Section 6.1.6.2 Trusted channel	FTP_ITC.1	Trusted channel
Section 6.1.6.3 Data exchange integrity	FDP_UIT.1 FPT_ITI.1	Basic data exchange integrity Inter-TSF detection of modification
Section 6.1.6.4 Data consistency	FPT_TDC.1	Inter-TSF basic TSF data consistency
Section 6.1.6.5 Proof of origin	FCO_NRO.2	Enforced proof of origin
Section 6.1.6.6 Validity of certificates, CRLs and ARLs	FDP_DAU.1	Basic data authentication
Section 6.1.6.7 Detection of errors in stored data	FDP_SDI.1	Stored data integrity monitoring
Non-bypassability		
Section 6.1.7.1 Non-bypassability of security functions	FPT_RVM.1	Non-bypassability of the TSP
Section 6.1.7.2 Automated re-start of services	FPT_RCV.2	Automated recovery
Section 6.1.7.3 Testing	FPT_TST.1	Testing

7.3.2 Minimum Strength of Function Level rationale

The TOE mechanisms will resist 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, is 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.

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

This part of the ST rationale is to show that the identified assurance measures are appropriate to meet the assurance requirements of Section 6.2. This is best demonstrated in the form of a table, mapping the identified assurance measures onto the assurance requirements, as shown in Table 22.

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 30: Assurance measures

CC Assurance Component		Assurance Measure (Entrust document)
ACM_CAP.3	Configuration Management Plan	Configuration Management Plan v1.6
ACM_SCP.2	Problem Tracking CM Coverage	Configuration Management Plan v1.6
ADO_DEL.1	Delivery Procedures	Delivery Procedures v1.3
ADO_IGS.1	Installation, Generation, and start-up	Installing Entrust/PKI 5.0 on Windows NT
ADV_FSP.1	Informal Functional Specification	Administering Entrust/PKI 5.0 Addendum to Administering Entrust/PKI 5.0 v1.2
ADV_HLD.2	High Level Design	Entrust System Architecture (High-Level Design) v1.9
ADV_RCR.1	Informal Correspondence Demonstration	Informal Correspondence Demonstration v2.2
ADV_SPM.1	Informal Security Policy Model	Informal Security Policy Model v1.1
AGD_ADM.1	Administrator Guidance	Administering Entrust/PKI 5.0 on Windows NT
ALC_DVS.1	Identification of Security Measures	Development Security: Security Measures v1.2
ALC_FLR.2	Flaw Reporting Procedure	Problem Reporting System (PRS) v1.4
AMA_CAT.1	TOE Component categorization Report	Categorization Report v1.4
ATE_COV.2	Analysis of Coverage	Analysis of Coverage v1.6
ATE_DPT.1	Testing - High Level Design	Analysis of Depth of Testing v1.5
ATE_FUN.1	Functional Testing	Entrust/PKI 5.0 Security Function Tests v1.3 Entrust/PKI 5.0 Functionality and Interface Test Case Suite v1.2 Entrust/PKI 5.0 Administrative Restrictions Test Case Suite v0.3 Entrust/Master Control 5.0 Full Test Case Suite v1.1 Entrust/RA 5.0 Full Test Case Suite v1.1
ATE_IND.2	Independent Testing	Independent Testing Resources v1.4
AVA_MSU.2	Validation of Analysis	Validation of Analysis v1.0
AVA_SOF.1	Strength of TSF Evaluation	Strength of Function Analysis v1.5
AVA_VLA.1	Developer vulnerability analysis	Vulnerability Analysis v1.2

8 Glossary

ADM-API	Administration API
API	Application Programming Interface
ARL	Authority Revocation List
AS	Administration Service
CA	Certification Authority
CAST	Carlisle Adams, Stafford Tavares [Entrust symmetric key algorithm]
CC	Common Criteria
CDA	Certificate Distribution Agent
CMS	Certificate Management System
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 Digital Signature Algorithm
EOR	Evaluation Observation Report
FIPS PUB	Federal Information Processing Standard Publication
GUI	Graphical User Interface
GULS	Generic Upper Layers Security
I&A	Identification and Authentication
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
MAC	Message Authentication Code
MD 5	Message Digest 5
NIST	National Institute of Standards and Technology
ODBC	Open Database Connectivity
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request For Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman [public key algorithm]
SBU	Sensitive But Unclassified
SET	Secure Electronic Transaction
SEP	Secure Exchange Protocol
SF	Security Function
SFP	Security Function Policy

SFR	Security Functional Requirement
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 Functions
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 5.0. 1999.

[Reference 3] Installing Entrust/PKI 5.0 on Windows NT. Entrust Technologies Ltd. 1999.

[Reference 4] Administering Entrust/PKI 5.0 on Windows NT. Entrust Technologies Ltd. 1999.

[Reference 5] ODBC 2.5 (Informix-CLI) Programmer's Reference. Informix Corporation. October 1997.

[Reference 6] CS2 Protection Profile Guidance for Near-Term COTS. Gary Stoneburner NIST. Version 0.5. March 25, 1999.