UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

CERTIFICATION REPORT No. P141

Entrust/RA and Entrust/Authority

from Entrust/PKI 5.0

on Microsoft Windows NT Version 4.0 Service Pack 3

Issue 1.0

March 2000

UK IT Security Evaluation and Certification Scheme
Certification Body, PO Box 152
Cheltenham, Glos GL52 5UF
United Kingdom

ARRANGEMENT ON THE MUTUAL RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Arrangement of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.*

*Mutual recognition applies to EAL3 and to the augmented assurance components ACM_SCP.2 (problem tracking configuration management coverage), ADV_SPM.1 (informal TOE security policy model) and AVA_MSU.2 (misuse: validation of analysis) but not to ALC_FLR.2 (flaw reporting procedures) and AMA_CAT.1 (TOE component categorisation report).

CERTIFICATION STATEMENT

Entrust Technologies Limited's Entrust/RA is the administrative client of the Entrust Public Key Infrastructure. Entrust/Authority is the management server component of the Entrust Public Key Infrastructure and acts as the Certificate Authority within the Public Key Infrastructure, issuing and managing certificates and the revocation list, and controlling the policy of the Public Key Infrastructure.

Entrust/RA and Entrust/Authority from Entrust/PKI 5.0, running on Microsoft Windows NT Version 4.0 Service Pack 3, have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria Part 3 augmented requirements incorporating Evaluation Assurance Level EAL3 for the specified Common Criteria Part 2 conformant functionality in the specified environment.

Originator	**CESG** Certifier
Approval	**CESG** Technical Manager of the Certification Body
Authorisation	**CESG** Senior Executive UK IT Security Evaluation and Certification Scheme
Date authorised	6 March 2000

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

ADM	ADMinistration
API	Application Programming Interface
ARL	Authority Revocation List
AS	Administration Service
BIF	Bulk Input File
CA	Certificate Authority
CAST	Carlisle Adams Stafford Tavares
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CMP	Certificate Management Protocol
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DES	Data Encryption Standard
DIM	Dual In-line Memory Module
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptical Curve Digital Signature Algorithm
EDO	Extended Data Output
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	keyed-Hashing Message Authentication Code
IDEA	International Data Encryption Algorithm
ITSEC	Information Technology Security Evaluation Criteria
KMS	Key Management Server
MAC	Message Authentication Code
MB	MegaByte
MD 2,5	Message Digest 2,5
MHZ	MegaHertz
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
SEP	Secure Exchange Protocol
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SoF	Strength of Function
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
UKSP	United Kingdom Scheme Publication

(This page is intentionally left blank)

REFERENCES

a. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 3.0, 2 December 1996.

b. The Appointment of Commercial Evaluation Facilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Issue 3.0, 3 February 1997.

c. Security Target - Entrust/RA 5.0,
Entrust Technologies Limited,
Version 0.8, 26 November 1999.

d. Security Target - Entrust/Authority 5.0,
Entrust Technologies Limited,
Version 1.0, 16 February 2000.

e. FIPS 140-1 Entrust Cryptographic Kernel Version 5.0 Validation Report,
Domus Software IT Security Laboratory,
7 January 2000.

f. Letter to Entrust Technologies Limited,
Communications Security Establishment,
295-12 IID04/255-99, 26 November 1999.

g. Common Criteria Part 1,
Common Criteria Implementation Board,
CCIB-99-031, Version 2.1, August 1999.

h. Common Criteria Part 2,
Common Criteria Implementation Board,
CCIB-99-032, Version 2.1, August 1999.

i. Common Criteria Part 3,
Common Criteria Implementation Board,
CCIB-99-033, Version 2.1, August 1999.

j. Common Methodology for Information Technology Security Evaluation,
Part I: Introduction and General Model,
Common Evaluation Methodology Editorial Board,
Version 0.6, CEM-97/017, September 1997.

k. Common Methodology for Information Technology Security Evaluation,
Part II: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 0.6, CEM-99/008, January 1999.

l. Harmonised Information Technology Security Evaluation Criteria,
Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

m. Interim CC Evaluation Manual,
Common Evaluation Methodology UK Support Group,
UKSP05.CCINT, Version 2.0, 19 June 1998.

n. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.

o. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.

p. Manual of Computer Security Evaluation, Part III, Evaluation Tools and Techniques,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Version 2.0, 30 July 1997.

q. Manual of Computer Security Evaluation, Part V, Generic Potential Vulnerabilities,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Version 1.0, 30 July 1997.

r. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 1.0, CEM-99/045, August 1999.

s. Evaluation Technical Report,
Common Criteria EAL3 augmented Evaluation of Entrust/RA and Entrust/Authority v5.0,
Syntegra CLEF,
LFS/T304/ETR, Issue 1.0, 11 February 2000.

t. Administering Entrust/PKI 5.0 on Windows NT,
Entrust Technologies Limited,
1999.

u. Installing Entrust/PKI 5.0 on Windows NT,
Entrust Technologies Limited.

v. Informal Security Policy Model,
Entrust Technologies Limited,
Version 1.2, 30 November 1999.

w. Certification Report No. P122,
Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, March 1999.

(This page is intentionally left blank)

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the IT security evaluation of Entrust/RA and Entrust/Authority from Entrust/PKI 5.0 to the Sponsor, Entrust Technologies Limited, and is intended to assist potential consumers when judging the suitability of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Targets [Reference c, d], which specify the functional, environmental and assurance evaluation requirements.

Evaluated Products

3. The version of the products evaluated was:

Entrust/RA and Entrust/Authority from Entrust/PKI 5.0.

These products are also described in this report as the Target of Evaluation (TOE). The Developer was Entrust Technologies Limited. Details of the evaluated configuration, including the products' supporting guidance documentation, are given in Annex A.

4. Entrust/PKI 5.0 is a distributed cryptographic key and certificate delivery and management system which makes possible secure financial electronic transactions and exchanges of sensitive information.

5. The TOE interacts with end user client applications for key management operations, such as key initialisation or key recovery, using the PKIX Certificate Management Protocol (PKIX-CMP) or the Secure Exchange Protocol (SEP). With the exclusion of cryptographic functionality (which has already been subject to a separate assessment by the Canadian Communications Security Establishment (CSE) and by the US National Institute of Standards and Technology (NIST)), these key management transactions were within the scope of the evaluation of Entrust/Authority.

6. Entrust/RA is the administrative client of Entrust/PKI 5.0. Entrust/RA provides a Graphical User Interface (GUI) which is the interface to the Entrust/Authority functionality to enable TOE administrators to perform virtually all aspects of end user, operator, Certification Authority (CA) and directory management. With the exception of some minor certificate directory administration and search functions, which are provided by Entrust/RA, all of the administration services themselves are provided by Entrust/Authority. However, Entrust/RA does provide a secure communications channel to Entrust/Authority to ensure that all communications between the Entrust/RA and Entrust/Authority are secured for confidentiality and integrity.

7. Entrust/Authority is the management server component of Entrust/PKI 5.0 and acts as the CA within the Public Key Infrastructure (PKI), issuing and managing certificates and the revocation list and controlling the policy of the PKI. The functionality provided can be categorised as follows:

a. Entrust/Authority provides a CA key management service which is responsible for managing the CA signing key pair, master keys, and enforcing security policies.

b. Entrust/Authority provides end user and operator management services. The end user management service allows authorised administrators to create, initialise and delete users and to recover, revoke and update cryptographic keys. The operator management service provides the capability for authorised operators to manage the privileges and cryptographic keys of other operators.

c. Entrust/Authority provides a cross-certification management service which manages the generation and maintenance of cross-certificates.

d. Entrust/Authority provides a self management service to start, initialise and stop Entrust/Authority services and to validate passwords.

e. Entrust/Authority provides a database management service to maintain the database that stores the end users' key pairs, user information and system and security policy data.

f. Entrust/Authority provides an audit trail management service to maintain and analyse the audit record of security critical and non-critical events that have occurred within the TOE.

g. Entrust/Authority provides a directory management service to maintain the directory.

8. All users of Entrust/RA and Entrust/Authority are administrators. There are no unprivileged users of the TOE. The administrator roles assigned by the TOE are as follows:

- Master User
- Security Officer
- Administrator
- Directory Administrator
- Auditor
- AutoRA Administrator
- Custom-defined Roles

9. Entrust/PKI 5.0 communicates with client applications for performing key management operations and enabling secure communications between end users through the generation and management of X.509 certificates. However, neither the client applications nor end user documentation were examined during this evaluation.

10. Details of the TOE's architecture can be found in Annex B to this report.

TOE Scope

11. The Entrust cryptomodule component of Entrust/RA and Entrust/Authority was outside the scope of the evaluation because it has been subject to a separate assessment. All of the algorithms used to implement cryptographic functions in the products' cryptomodules have been assessed successfully either by NIST under the US FIPS 140-1 to Security Level 3 for Electromagnetic Interference and Electromagnetic Compatibility, Security Level 2 for Roles and Services, Security Level 2 for Physical

Security, and Security Level 1 for Operating System Security for Microsoft Windows 95 and 98, Windows NT Versions 3.5 and 3.51 and Windows NT Version 4.0 with Service Packs 3, 4, 5 and 6 (single user mode, see the validation report [e]) or by CSE under their Cryptographic Endorsement Program (see the letter from CSE [f]). See Annex B to this report for more details.

12. The Entrust/Entelligence 5.0 client application does implement unassessed algorithms but the algorithms used by default for desk-top encryption and digital signature, CAST5 (128-bit) and RSA (1024-bit) using SHA-1, have been assessed by NIST or CSE. However, user client applications forming part of the PKI (so called Entrust-Ready applications) may implement cryptographic algorithms for desk-top encryption and digital signature which have not been assessed by any national authority, and may make use of them by default. See Annex B to this report for more details. The current list of unassessed algorithms available in Entelligence or Entrust-ready applications is as follows:

- CAST3 40 (desk-top encryption)
- CAST3 64 (desk-top encryption)
- RC2 (desk-top encryption)
- RC4 (desk-top encryption)
- HMAC-MD5 (digital signature hashing)
- HMAC-SHA-1 (digital signature hashing)
- HMAC-RMD160 (digital signature hashing)
- IDEA (desk-top encryption)
- MD2 (digital signature hashing)
- MD5 (digital signature hashing)

13. The Entrust/Authority database, a repository of system and user data, and the X.500 directory, a public directory of certificates and revocation information, were also outside the scope of the evaluation, although these components were used as a representative database and directory in the functional and penetration testing of the TOE.

14. The Entrust/Entelligence 5.0 client application was outside the scope of the evaluation, although it was used as a representative client in the Developer's functional testing of the TOE.

15. No security functionality was traced to the Entrust/Authority database, to the X.500 directory used, or to the Entrust/Entelligence 5.0 client application.

Protection Profile Conformance

16. The Security Targets [c, d] did not claim conformance to any protection profiles.

Assurance Level

17. The Security Targets [c, d] specify the assurance requirements for the resultant evaluation. The assurance incorporated predefined evaluation assurance level EAL3 augmented by ACM_SCP.2 (problem tracking configuration management coverage), ALC_FLR.2 (flaw reporting procedures), ADV_SPM.1 (informal TOE security policy model) and AVA_MSU.2 (misuse: validation of analysis) and AMA_CAT.1 (TOE component categorisation report). Common Criteria Part 3 [f] describes the scale of assurance given by predefined evaluation assurance levels EAL1 to EAL7. EAL0 represents no assurance.

Strength of Function

18. The TOE used the following probabilistic mechanisms to support its security functions:

- Key generation
- RSA key wrapping
- Encryption
- Digital signature
- Hashing
- Message Authentication Code (MAC)-ing
- Operator password
- Password generation
- Secrets' generation

19. The minimum Strength of Function (SoF) claim for the TOE was SoF-medium. The cryptographic functions in the TOE's cryptomodules were outside the scope of this evaluation because they were subject to a separate cryptographic evaluation, but a rating of SoF-medium was claimed for the operator password mechanism.

20. The minimum SoF for the search for vulnerabilities conducted by the Evaluators was SOF-medium to provide adequate protection against intruders with a moderate attack potential.

Security Claims

21. The Security Targets [c, d] fully specify the TOE's security objectives, threats and Organisational Security Policies which these objectives counter and meet, and functional requirements and security functions to elaborate the objectives. All of the functional requirements are taken from Common Criteria (CC) Part 2 [h]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [g].

Threats Countered

22. The threats that Entrust/RA counter are as follows:

a. An authorised user of the TOE may gain unauthorised 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.

b. An unauthorised individual (ie other than authenticated user) may gain unauthorised malicious access to TOE processing resources or security critical data, including cryptography-related assets, via technical attack.

23. The threats that Entrust/Authority counter are as follows:

a. An authorised user of the TOE may gain unauthorised 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.

b. An unauthorised individual (ie other than authenticated user) may gain unauthorised malicious access to TOE processing resources or security critical data, including cryptography-related assets, via technical attack.

c. Deliberate and accidental unauthorised modification or destruction of security events records by malicious individuals or because of equipment failure may not be noticeable.

d. 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.

e. The TOE may be subjected to an unsophisticated, denial-of-service attack, by a malicious unauthorised individual attempting to gain logical access to the TOE, potentially resulting in mid-term to long-term unavailability of TOE services.

Threats Countered by the TOE's Environment

24. The threats that are countered by the Entrust/RA's environment are as follows:

a. Those responsible for the TOE may install the TOE in a manner that undermines security, because of incompetence or negligence.

b. TOE Security policies may be circumvented because of improper operation of the TOE by an authorised user, resulting in unauthorised individuals gaining access to TOE data and resources.

c. The TOE and the abstract machine may be subject to physical attack by an unauthorised individual (ie other than authenticated user), resulting in unauthorised disclosure or unauthorised modification of TOE resources, which would compromise TOE security.

d. An unauthorised individual (ie other than authenticated user) may gain access to TOE processing resources or information, including cryptography-related assets, using non-technical means (eg social engineering).

25. The threats that are countered by the Entrust/Authority's environment are as follows:

a. Those responsible for the TOE may install the TOE in a manner that undermines security, because of incompetence or negligence.

b. TOE Security policies may be circumvented because of improper operation of the TOE by an authorised user, resulting in unauthorised individuals gaining access to TOE data and resources.

c. The TOE may be subject to physical attack by an unauthorised individual (ie other than authenticated user), resulting in unauthorised disclosure or unauthorised modification of TOE resources, which would compromise TOE security.

d. An unauthorised individual (ie other than an authenticated user) may gain unauthorised malicious access to TOE processing resources or security critical data, including cryptography-related assets, using sophisticated IT security defeating tools.

e. An unauthorised individual (ie other than authenticated user) may gain access to TOE processing resources or information, including cryptography-related assets, using non-technical means (eg social engineering).

f. TOE Security policies may be circumvented because of errors or omissions in the administration of the security features of the TOE, resulting in unauthorised individuals gaining access to TOE data and resources.

g. A deliberate or accidental threat occurrence corrupting the abstract machine of the TOE to enable future insecurities in the TOE may not be detected.

h. The TOE may be subjected to a sophisticated, denial-of-service attack, by a technically competent malicious unauthorised individual who would compromise availability of TOE services.

i. 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.

Threats and Attacks not Countered

26. The TOE does not provide complete countermeasures to any threats to or attacks on the TOE's environment or to those parts of Entrust/PKI that are outside the scope of the evaluation.

Environmental Assumptions and Dependencies

27. Entrust/RA's environment must also satisfy the following assumptions:

a. The TOE abstract machine is physically protected from unauthorised modification.

b. The cryptographic operations are performed on a FIPS 140-1 validated or equivalent cryptographic module.

c. The abstract machine of the TOE operates in a correct and expected manner.

d. Authorised users recognize the need for a secure IT environment.

e. Authorised users are trusted to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine.

f. The TOE and the TOE environment are competently installed and administered to allow for correct operation of the TOE**.**

g. Entrust/Authority, as part of the TOE environment and using identification and information provided by the TOE, records necessary security critical events to ensure that the information exists to support effective security management.

h. Entrust/Authority, as part of Entrust/RA's environment, must provide for authorised administrative users to distribute and revoke public key certificates.

i. Entrust/Authority, as part of Entrust/RA's environment, must provide for authorised administrative users to recover end-user encryption keys and support for automatic update of end-entity signing and encryption key pairs as required.

28. Entrust/Authority's environment must also satisfy the following assumptions:

a. The TOE processing resources that depend on software as well as hardware features will be located within controlled access facilities that mitigate unauthorised physical access.

b. The TOE abstract machine is physically protected from unauthorised modification.

c. The cryptographic operations are performed on a FIPS 140-1 validated or equivalent cryptographic module.

d. The abstract machine of the TOE operates in a correct and expected manner after manual verification.

e. Authorised users recognize the need for a secure IT environment.

f. Authorised users are trusted to perform discretionary actions in accordance with security policies and not to interfere with the abstract machine.

g. The TOE and the TOE environment are competently installed and administered**.**

h. All connections to peripheral devices reside within the controlled access facilities.

29. Entrust/RA relied on the Entrust/RA cryptomodule to provide generation of cryptographic keys (FCS_CKM.1), destruction of cryptographic keys (FCS_CKM.4) and operation of the cryptographic functions (FCS_COP.1).

30. Entrust/RA relied on the underlying operating system to run a suite of automatically initiated tests that demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TOE Security Functions (TSF) - see Security Functional Requirement (SFR) FPT_AMT.1 in the Security Target [c]. This instance of FPT_AMT.1 relates only to the self-testing of the cryptographic module in the TOE environment. The cryptomodule itself was outside the scope of this evaluation because it was subject to a separate evaluation by CSE and NIST.

31. Entrust/RA relied on the underlying operating system to enforce TSF domain separation, ie ensuring that each trusted process runs in its own security domain which is free from interference or tampering by untrusted users - see SFR FPT_SEP.1 in the Security Target [c].

32. Entrust/RA relied on Entrust/Authority to provide audit data generation (FAU_GEN.1) and subset access control (FDP_ACC.1).

33. Entrust/Authority relied on the underlying operating system to enforce TSF domain separation (FPT_SEP.1), to provide a reliable time stamp (FPT_STM.1), to protect audit records from unauthorised deletion (FAU_STG.2.1).

34. Entrust/Authority relied on the TOE environment to run a suite of manually initiated tests that demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF (FPT_AMT.1). This instance of FPT_AMT.1 was included for completeness as a dependency of automated recovery (FPT_RCV.2) and maps to the Entrust/Authority method of use assumption that the abstract machine will function correctly.

35. Entrust/Authority relied on the underlying hardware platform to provide a reliable time stamp (FPT_STM.1).

36. Entrust/Authority relied on the Entrust/Authority cryptomodule to provide generation of cryptographic keys (FCS_CKM.1), destruction of cryptographic keys (FCS_CKM.4), operation of the cryptographic functions (FCS_COP.1) and generation of secrets (FCS_SOS.2.1).

37. To demonstrate the required assurance, the TOE was evaluated on the Microsoft Windows NT Version 4.0 Service Pack 3 operating system platform. The platform was relied on to provide supporting security functionality correctly and was not subject to evaluation except in the context of the vulnerability analysis and functional and penetration testing of the TOE. The limited dependencies of the TOE on the underlying operating system indicate that the security of the TOE is likely to be maintained on any operating system which satisfies the environmental SFRs detailed above. However, the Evaluators did not assess the TOE running on any operating system other than Microsoft Windows NT Version 4.0 Service Pack 3. Accordingly, the certification is restricted to that platform and to underlying hardware that can produce a reliable time stamp. The full platform configuration used to support the evaluation is given in Annex A.

IT Security Objectives

38. The IT security objectives in the Entrust/RA Security Target [c] are as follows:

a. The TOE must ensure that, except for users accessing the help menu, all users are identified and authenticated before being granted access to TOE resources.

b. The TOE must prevent errant or non-malicious, authorised software or users from bypassing or circumventing TOE security policy enforcement.

c. The TOE must prevent logical entry to the TOE using technical methods, by persons without authority for such access.

d. The TOE must be able to securely and transparently exchange secret keys as required.

e. The TOE must provide the functionality necessary to support automatic key update of the TOE user encryption and signing key pairs, as required.

f. The TOE must validate the origin and integrity of the exchange data it receives from trusted remote IT products, and must provide the same validation capability to the trusted IT products receiving data from the TOE.

g. The TOE must protect exchanged data with trusted remote IT products against unauthorised disclosure while the data is in transit.

h. The TOE must provide authorised users with the capability to review audit records.

39. The IT security objectives in the Entrust/Authority Security Target [d] are as follows:

a. The TOE must provide access by authorised users to those objects and services for which they have been authorised.

b. The TOE must ensure that all users are identified and authenticated before being granted access to TOE mediated resources.

c. The TOE must provide the ability to specify and manage user and system process access rights to individual objects and services.

d. The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.

e. The TOE must prevent errant or non-malicious, authorised software or users from bypassing or circumventing TOE security policy enforcement.

f. The TOE must prevent unauthorised logical entry to the TOE by technical methods used by persons without authority for such access.

g. 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.

h. The TOE must protect itself from unsophisticated, denial-of-service attacks.

i. The TOE must generate evidence of origin for transmitted public key certificates, Certificate Revocation Lists (CRLs) and Authority Revocations Lists (ARLs).

j. The TOE must successfully validate the evidence of receipt for received keys and certificates it distributes to trusted entities.

k. The TOE must provide for authorised administrative users to distribute and revoke public key certificates, and be able to securely and transparently exchange secret keys as required.

l. The TOE must provide for authorised administrative users to recover end-user encryption keys, and automatically update these keys as required.

m. The TOE must record security critical events to ensure that the information exists to support effective security management.

n. 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.

Environmental Security Objectives

40. The environmental security objectives in the Entrust/RA Security Target [c] are as follows:

a. 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.

b. The TOE environment must provide for authorised administrative users to distribute and revoke public key certificates.

c. The TOE environment must provide for authorised administrative users to recover the TOE user encryption key pair.

d. The TOE environment must ensure that all TOE users can subsequently be held accountable for their security relevant actions.

e. Those responsible for the TOE must ensure that the TOE and its underlying abstract machine are installed and operated in a manner which maintains IT security.

f. Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorised physical modification and from technical attacks at the hardware and operating system level.

g. The TOE environment must provide sufficient protection against non-technical attacks by other than authorised users.

h. The TOE environment, using identification and authentication information provided by the TOE, must record necessary security critical events to ensure that the information exists to support effective security management.

41. The environmental security objectives in the Entrust/Authority Security Target [d] are as follows:

a. 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.

b. Those responsible for the TOE must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.

c. Those responsible for the TOE must ensure that the TOE is managed and administered in a manner that maintains IT security.

d. Those responsible for the TOE must ensure that the TOE and its underlying hardware and software are physically protected from unauthorised physical modification and from technical attacks at the hardware and operating system level.

e. The TOE environment must sufficiently counter the threat of an individual (other than an authorised user) gaining unauthorised access via sophisticated technical attack.

f. The TOE environment must provide sufficient protection against non-technical attacks by other than authorised users.

g. The TOE environment must provide the ability to detect unauthorised modification and corruption of the TOE abstract machine.

h. The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.

i. 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.

Security Functional Requirements

42. Entrust/RA provided security functions to satisfy the following SFRs:

- C User identification before any action (FIA_UID.2)
- C User authentication before any action (FIA_UAU.2)
- C Verification of secrets (FIA_SOS.1)
- C Re-authenticating (FIA_UAU.6)
- C Protected authentication feedback (FIA_UAU.7)
- C Authentication failure handling (FIA_AFL.1)
- C TSF-initiated session locking (FTA_SSL.1)
- C User-initiated session locking (FTA_SSL.2)
- C Cryptographic key distribution (FCS_CKM.2)
- C Cryptographic key access (FCS_CKM.3)
- C Security audit review (FAU_SAR.1)
- C Selectable audit review (FAU_SAR.3)
- C Inter-TSF trusted channel (FTP_ITC.1a)
- C Inter-TSF trusted channel (FTP_ITC.1b)
- C Data Exchange Integrity (FDP_UIT.1)
- C Inter-TSF detection of modification (FPT_ITI.1)

- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- Subset residual information protection (FDP_RIP.1)
- Non-bypassability of the TOE Security Policy (TSP) (FPT_RVM.1)

43. Entrust/Authority provided security functions to satisfy the following SFRs:

- Complete access control (FDP_ACC.2)
- Security attribute based access control (FDP_ACF.1)
- Management of security attributes (FMT_MSA.1)
- Secure security attributes (FMT_MSA.2)
- Static attribute initialisation (FMT_MSA.3)
- User attribute definition (FIA_ATD.1)
- Management of TSF data (FMT_MTD.1)
- Secure TSF data (FMT_MTD.3)
- Subset residual information protection (FDP_RIP.1)
- Restrictions on security roles (FMT_SMR.2)
- Management of security functions behaviour (FMT_MOF.1)
- Time-limited authorisation (FMT_SAE.1a)
- Time-limited authorisation (FMT_SAE.1b)
- User identification before any action (FIA_UID.2)
- User authentication before any action (FIA_UAU.2)
- Verification of secrets (FIA_SOS.1)
- Single-use authentication mechanisms (FIA_UAU.4)
- Re-authenticating (FIA_UAU.6)
- Protected authentication feedback (FIA_UAU.7)
- TSF-initiated termination (FTA_SSL.3a)
- TSF-initiated termination (FTA_SSL.3b)
- Authentication failure handling (FIA_AFL.1)
- Cryptographic key distribution (FCS_CKM.2)
- Cryptographic key access (FCS_CKM.3)
- Generation of secrets (FIA_SOS.2.2)
- Enforced proof of receipt (FCO_NRR.2)
- Replay detection (FPT_RPL.1)
- Audit data generation (FAU_GEN.1)
- User identity association (FAU_GEN.2)
- Guarantees of audit data availability (FAU_STG.2)
- Trusted path (FTP_TRP.1)
- Inter-TSF trusted channel (FTP_ITC.1)
- Data Exchange Integrity (FDP_UIT.1)
- Inter-TSF detection of modification (FPT_ITI.1)
- Inter-TSF basic TSF data consistency (FPT_TDC.1)
- Enforced proof of origin (FCO_NRO.2)
- Basic data authentication (FDP_DAU.1)
- Stored data integrity monitoring (FDP_SDI.1)
- Non-bypassability of the TSP (FPT_RVM.1)
- Automated recovery (FPT_RCV.2)
- TSF testing (FPT_TST.1)

Security Function Policy

44. Entrust/RA does not have any explicit security function policies in the Entrust/RA Security Target [c]. Details of the implicit security policies modelled can be found in the "Security Policy Model" section.

45. Entrust/Authority has an explicit security function policy defined in the complete access control SFR (FDP_ACC.2), the security attribute based access SFR (FDP_ACF.1), the management of security attributes (FMT_MSA.1) and static attribute initialisation (FMT_MSA.3). This policy is to control access to all Entrust/Authority objects administered through any default or custom-defined administration role by user identity and role. The access control applies to the ability of a user or role to read, delete, modify, query or change defaults on an object based on a set of restrictive default values.

Evaluation Conduct

46. The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UKSP 01 and UKSP 02 [a, b]. The Scheme has established a Certification Body which is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry on behalf of Her Majesty's Government.

47. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Targets [c, d]. To ensure that the Security Targets gave an appropriate baseline for a Common Criteria evaluation, they were first themselves evaluated, as outlined by CC Part 3 [i].

48. Whilst the TOE was evaluated against criteria taken from those agreed internationally in CC Part 3 [i], the evaluation was started prior to the finalisation of the Common Evaluation Methodology (CEM) and used the same methodology as the Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a evaluation (see Certification Report No. P122 [w]) where the same assurance classes were evaluated. As previously, to ensure an appropriate application of the criteria, available drafts of CEM [j, k] were consulted and current UK CC interpretations were checked. In addition, as the CC are broadly equivalent to the Information Technology Security Evaluation Criteria (ITSEC) [l] in many respects, the UK's Interim CC Evaluation Manual [m] was used, which is based on the IT Security Evaluation Manual [n] and elaborated in the UK ITSEC Manual of Computer Security Evaluation UKSP 05 [o, p]. Otherwise the criteria were applied in a manner consistent with both this basis and the overall objectives of EAL3 augmented by ACM_SCP.2, ALC_FLR.2 and AMA_CAT.1 in CC Part 3 [i].

49. The evaluation of the augmentations ADV_SPM.1 and AVA_MSU.2 was performed against CEM Version 1.0 [r].

50. The Evaluators did not use any tools during the evaluation.

51. The Certification Body monitored the evaluation which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed in February 2000 when the

CLEF submitted the final Evaluation Technical Report (ETR) [s] to the Certification Body which, in turn, produced this Certification Report.

Certification Result

52. For the certification result see the "Evaluation Outcome" section.

General Points

53. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the products and whether such patches have been evaluated and certified. Consumers are reminded of the security dangers inherent in downloading 'hot-fixes' where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner. More up to date information on known security vulnerabilities within individual certified products and systems can be found on the IT Security Evaluation and Certification Scheme web site www.itsec.gov.uk.

54. The evaluation addressed the security functionality claimed in the Security Targets [c, d], with reference to the assumed environment specified in the Security Targets. The configuration evaluated was that specified in Annex A. Prospective consumers of the TOE are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

55. The issue of a Certification Report is not an endorsement of a product.

II. EVALUATION FINDINGS

56. The Evaluators examined the following assurance classes and components taken from CC Part 3 [i]. Components marked with an asterisk,"*", are not EAL3 assurance components, but with the exception of ALC_FLR.2 are hierarchical to EAL3 components.

Assurance class	Assurance components
Configuration management	Authorisation Controls (ACM_CAP.3)
	Problem Tracking Configuration Management coverage (ACM_SCP.2)*
Delivery and operation	Delivery procedures (ADO_DEL.1)
	Installation, generation and startup procedures (ADO_IGS.1)
Development	Informal functional specification (ADV_FSP.1)
	Security enforcing high-level design (ADV_HLD.2)
	Informal correspondence demonstration (ADV_RCR.1)
	Informal TOE Security Policy (ADV_SPM.1)
Guidance documents	Administrator guidance (AGD_ADM.1)
	User guidance (AGD_USR.1)
Life cycle support	Identification of security measures (ALC_DVS.1)
	Flaw reporting procedures (ALC_FLR.2)*
Security Target	TOE description (ASE_DES)
	Security Environment (ASE_ENV)
	Security Target introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	Protection Profile claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)
Tests	Analysis of coverage (ATE_COV.2)
	Testing: high-level design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability Assessment	Misuse: examination of guidance (AVA_MSU.2)*
	Strength of TOE security function evaluation (AVA_SOF.1)
	Independent vulnerability analysis (AVA_VLA.1)
Maintenance of Assurance	TOE component categorisation report (AMA_CAT.1)

57. All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

58. There are a number of aspects of the evaluation that are relevant to consumers. These are summarised in the sections that follow.

Security Policy Model

59. The Security Policy Model [v] identifies 6 security policies for Entrust/RA, which completely define the conditions under which a user and administrator can interact with the TOE. These policies are as follows:

- Identification and authentication security policy
- Key management security policy
- Audit security policy
- Self-test security policy
- Trusted path security policy
- Domain integrity security policy

60. The identification and authentication security policy requires that Entrust/RA provides an identification and authentication function to verify the unique identity of operators attempting to access TOE services, that Entrust/RA ensures that operators' requests are initiated only once identification and authentication has been successfully performed, and that Entrust/RA ensures that identification and authentication data is protected from unauthorised access, modification or destruction. The operator password mechanism was within the scope of this evaluation.

61. The key management security policy requires that Entrust/RA enforces a split-knowledge mechanism on sensitive key management operations, that Entrust/RA ensures that cryptographic keys and certificates are distributed to end users, operators and external CAs and their authenticity, confidentiality and integrity is protected, and that Entrust/RA ensures that all cryptographic operations are performed in a FIPS 140-1 validated cryptomodule.

62. The audit security policy requires that Entrust/RA provides an audit viewer mechanism for viewing and analysing recorded security relevant events.

63. The self-test security policy requires that Entrust/RA enforces a self-test mechanism on start up of Entrust/RA, and upon failure of the self-test enters an error state which requires manual intervention before normal operation can be resumed.

64. The trusted path security policy requires that Entrust/RA provides a communications path between itself and operators, end users and external CAs that is logically distinct from other communications paths, that Entrust/RA provides assured identification and authentication and protection against modification or disclosure, and ensures that the trusted path is initiated by the appropriate operator, end user or external CA.

65. The domain integrity security policy requires that Entrust/RA ensures that TOE services are only available through specified TOE interfaces and that TOE functions are invoked and succeed before any security related operation is allowed to proceed.

66. All security policies are modelled in the Security Policy Model [v] by properties of the implementation of Entrust/RA described in the administration guidance [t, u].

67. The Security Policy Model [v] identifies 9 security policies for Entrust/Authority, which completely define the conditions under which a user and administrator can interact with the TOE. These policies are as follows:

- Access control security policy
- Separation of duties security policy
- Identification and authentication security policy
- Key management security policy
- Audit security policy
- Self-test security policy
- Trusted path security policy
- Recovery security policy
- Domain integrity security policy

68. The access control security policy requires that Entrust/Authority enforces access controls on all TOE data objects and services, restricting access to authorised operators, end users and external CAs. Access is based on the identity, state and role of the operators, end users and external CAs. Access control must be supported by the identification and authentication and separation of duties security policies.

69. The separation of duties security policy requires that Entrust/Authority enforces the services available to the Master User, Security Officer, Administrator, Directory Administrator, Auditor, AutoRA Administrator and Custom-defined operator roles, and enforces the permissions assigned to operators, end users and external CAs.

70. The identification and authentication security policy requires that Entrust/Authority provides an identification and authentication function to verify the unique identities of all operators, end users and external CAs attempting access to the TOE services, that Entrust/Authority ensures that operators' requests are initiated only once identification and authentication has been successfully performed, that Entrust/Authority ensures that identification and authentication data is protected from unauthorised access, modification or destruction, and that Entrust/Authority ensures that successful identification and authentication results are recorded in the Entrust/Authority audit log. Entrust/Authority is also required to provide to each operator, end user and external CA a set of security attributes to enforce the identification and authentication security policy.

71. The key management security policy requires that Entrust/Authority enforces a split-knowledge mechanism on sensitive key management operations, that Entrust/Authority ensures that cryptographic keys are distributed to end users, operators and external CAs and their authenticity, confidentiality and integrity is maintained, and that Entrust/Authority ensures that all cryptographic functions are performed in a FIPS 140-1 validated module. Entrust/Authority is also required to ensure that end user private signing keys are never backed up by the TOE.

72. The audit security policy requires that Entrust/Authority provides an audit mechanism for monitoring and recording of a predefined set of security relevant events, that Entrust/Authority

ensures that the audit trail is protected from unauthorised access, modification or destruction, that the date, time, location, type and success or failure of each audited event is recorded, and that Entrust/Authority provides sufficient information to identify users, processes and objects involved in each security relevant event.

73. The self-test security policy requires that Entrust/Authority enforces a self-test mechanism on start up of Entrust/Authority, and upon failure of the self-test enters an error state which requires manual intervention before normal operation can be resumed. Entrust/Authority is also required to ensure that the self-test can be performed periodically to validate the correct operation of Entrust/Authority's security critical functions and on demand by authorised operators to validate the correct operation of Entrust/Authority, and to ensure that failure of a self-test is itself an audited security relevant event.

74. The trusted path security policy requires that Entrust/Authority provides a communications path between itself and operators, end users and external CAs that is logically distinct from other communications paths, that Entrust/Authority provides assured identification and authentication and protection against modification or disclosure, and ensures that the trusted path is initiated by the appropriate operator, end user or external CA.

75. The recovery security policy requires that Entrust/Authority ensures that the TOE is in a known trusted state after failure or a service discontinuity which can only be returned to a normal state by the manual intervention of authorised operators.

76. The domain integrity security policy requires that Entrust/RA ensures that TOE services are only available through specified TOE interfaces and that TOE functions are invoked and succeed before any security related operation is allowed to proceed.

77. All security policies are modelled in the Security Policy Model [v] by properties of the implementation of Entrust/Authority described in the administration guidance [t, u].

Delivery and Installation

78. The consumer receives the TOE as a shrink-wrapped package. It is sent by a courier to the consumer sealed in a package with tamper-evident seals. This will ensure that interference with the TOE will be detectable.

79. The TOE has a number of configuration options which the consumer must perform in order to use the TOE. These options are described in the Installation Guide [u] and summarised in Annex A to this report. The Evaluators were satisfied that all configuration options lead to a secure installation of the TOE.

User Guidance

80. As the only operators of the TOE were TOE administrators, user guidance documentation was not required and user guidance (AGD_USR.1) was therefore not applicable.

81. The Installation Guide [u] provides guidance and warnings on the allocation of administration roles and privileges. The Administration Guide [t] documented the administration of each relevant security function and provided adequate warnings where necessary. The administrator should follow the guidance in the administration guidance documentation in order to ensure that the TOE operates in a secure manner.

Misuse

82. The Evaluators found that the TOE did not have any insecure states and that the administration guidance [t, u] provides the consumer with sufficient information to administer and use the security functions of the TOE effectively.

Developer's Tests

83. The TOE was installed and tested on the hardware platforms as specified in Annex A.

84. The Developer's testing was designed to test the security functions that are provided by or which relate to the behaviour of all of the TOE's security functions at all the internal and external interfaces of the TOE. There were 5 test suites:

- Master Control GUI
- Entrust/RA user interface
- the TOE security functions
- other interfaces including the Master Control Shell interface
- flexible rules functionality

85. The Evaluators examined all of the test scripts and confirmed that the actual test results were consistent with the expected test results. The expected results were also consistent with the actual results of the Evaluators' repeated sample of the Developer's tests.

Evaluators' Tests

86. The Evaluators sampled 43% of the Developer's tests. All Developer tests relevant to the security functionality of the TOE were repeated.

87. Each area of TOE functionality and each external and internal interface of the TOE was tested by at least one additional test devised by the Evaluators. The Evaluators constructed 14 additional tests to provide coverage of the 12 functional areas.

88. The configuration of the Evaluators' test environment is described in Annex A.

(This page is intentionally left blank)

III. EVALUATION OUTCOME

Certification Result

89. After due consideration of the ETR [s], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Entrust/RA and Entrust/Authority from Entrust/PKI 5.0 meet the specified CC Part 3 [i] augmented requirements incorporating Evaluation Assurance Level EAL3 for the specified CC Part 2 [h] conformant functionality in the specified environment.

90. The minimum SoF of the operator password verification mechanism was SoF-medium as claimed.

Recommendations

91. Prospective consumers of the products should understand the specific scope of the certification by reading this report in conjunction with the Security Targets [c, d].

92. Only the evaluated product configuration, specified in Annex A, should be installed. The products should be used in accordance with the guidance documentation [t, u].

93. The products should only be used in accordance with the environmental considerations outlined in the Security Targets [c, d].

94. The following cryptographic algorithms were not assessed by NIST under FIPS 140-1 or by CSE, and should not be used in any user client applications without checking that they are correctly implemented and that they are suitable to meet the potential consumer's requirements:

- CAST3 40 (desk-top encryption)
- CAST3 64 (desk-top encryption)
- RC2 (desk-top encryption)
- RC4 (desk-top encryption)
- HMAC-MD5 (digital signature hashing)
- HMAC-SHA-1 (digital signature hashing)
- HMAC-RMD160 (digital signature hashing)
- IDEA (desk-top encryption)
- MD2 (digital signature hashing)
- MD5 (digital signature hashing)

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

   Entrust/RA and Entrust/Authority from Entrust/PKI 5.0.

2. The supporting guidance documents evaluated were:

   - Administrator's Guide [t]
   - Installation Guide [u]

TOE Configuration

3. The TOE had the following configuration options:

   a. use of the ICL PeerLogic i500 directory or another X.500 directory;

   b. installation of the X.500 directory on the same server as Entrust/Authority or on a different server; and

   c. installation of Entrust/RA on the same server as Entrust/Authority or on a different platform.

4. The configurable items of the TOE were:

   - Entrust/Authority licence information
   - Entrust/Authority data file location (default: C:\entmgrdata)
   - Entrust/Authority backup file location (default: C:\entbackup)
   - Directory node name
   - Directory listen port (default: 389)
   - Directory attributes (default: LDAPv3)
   - CA distinguished name
   - CA Directory Access password
   - Director Administrator distinguished name
   - Directory Access password
   - First Officer distinguished name
   - Custom attributes (default: mail)
   - Initial search base (default: CA DN)
   - Client version supported (default: only v5 clients)
   - Entrust/Authority node name
   - Entrust/Authority listen port (default: 709)
   - Administration Service listen port (default: 710)
   - PKIX-CMP server port (default: 829)
   - CA Key Generation (default: use software)
   - CA Key Pair algorithm (default: RSA-1024)

- Database encryption algorithm (default CAST-128)
- Entrust user signature algorithm (default: RSA-1024)
- Entrust user encryption algorithm (default: RSA-2048)
- Signing certificate hashing algorithm (default: SHA-1)
- Policy certificate lifetime (default: 30 days)
- CA type (default: Root CA)
- Informix password

5. There were no configuration options for the underlying operating system, Microsoft Windows NT Version 4.0 Service Pack 3, relevant to the TOE. The operating system requirements for installation of the TOE are documented in the Installation Guide [u].

6. There were no configuration options for the X.500 directory or the Entrust/Authority database relevant to the TOE, ie the TOE cannot be configured insecurely if the guidance documents are followed.

7. The Evaluators determined that no TOE configuration options affected the security of the TOE.

Environmental Configuration

8. The specific configurations of the machines used during the Developer's and Evaluators' tests for Entrust/Authority were:

- Microsoft Windows NT Server Version 4.0 Service Pack 3 operating system
- Hewlett Packard NetServer LH Pro with dual 200 MHZ Pentium processors
- 2 x 64 EDO DIMM RAM
- Entrust/Authority database (Informix Online Workgroup Server Version 7.23.TC14X running on Entrust/Authority server)

9. The specific configurations of the machines used during the Evaluators' tests for Entrust/RA were:

- Microsoft Windows NT Workstation Version 4.0 Service Pack 3 operating system
- Hewlett Packard Vectra VA with 200 MHZ MMX Pentium processor
- 64 MB RAM

10. The specific configurations of the machines used during the Evaluators' tests for the X.500 directory were:

- ICL PeerLogic i500 Version 8.0a General Release 2 running on
- Microsoft Windows NT Server Version 4.0 Service Pack 3 operating system
- Hewlett Packard NetServer LH Pro SMP with dual 200 MHZ Pentium processors
- 2 x 64 EDO DIMM RAM

11. Entrust/RA, Entrust/Authority and the X.500 directory components were connected by a common 3Com Ethernet Office Hub (10 Base-T Hub8/TPO).

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. Entrust/PKI uses a distributed architecture to deliver PKI services. Entrust/Authority, Entrust/Engine (Base) and Entrust/RA are 3 major components of the Entrust system architecture. Entrust/Engine (Base) is encapsulated in EntrustSession which is part of both the Entrust/Authority and Entrust/RA.

2. Entrust/Authority is the PKI management server component. It acts as the CA within the PKI, issuing and managing end-entity certificates and the revocation lists and controlling PKI policy.

3. Entrust/Engine (Base) is a PKI client component, integrated into applications that require PKI services. It provides for user initialisation, automatic key management, signature verification and certificate validation, as well as having integrated encryption and encryption key management capabilities. Entrust/Engine (Base) is encapsulated within EntrustSession.

4. The third major component of the architecture is the administrative client, Entrust/RA. Entrust/RA can be used from virtually any network node, as all interactions between it and Entrust/Authority are protected using the service of the PKI itself.

5. Whilst not a member of the Entrust family of products, the directory plays a vital role in the PKI services: Entrust/Authority publishes certificates, revocation lists, and other PKI control information to the directory, from which it will be accessed by clients. In other words, the directory acts as a repository for current PKI data and distributes that data throughout the network in order to make it available to all clients.

6. The Entrust family of products also includes several components designed to add value to the base PKI by increasing the security of user private information, by supporting particular types of application requirements, especially in the area of data formatting or encryption key protection mechanisms and by extending the capabilities of the PKI to include time stamping and notarisation services.

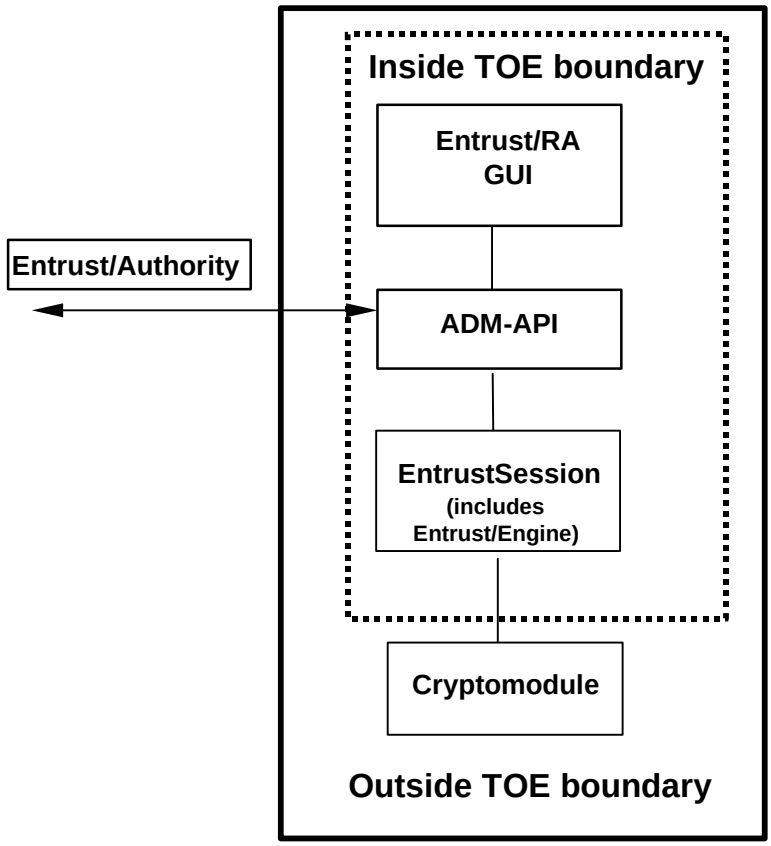
7. Entrust/RA, Entrust/Engine (Base) and Entrust/Authority are discussed in the following sections in terms of their high level design components and interfaces.

Entrust/RA

8. Entrust/RA is the primary operator interface for day-to-day management of Entrust users and other Entrust operators. Management of the Entrust PKI policies, operators and end users via Entrust/RA is assigned to the following Entrust roles listed below:

- Security Officer
- Administrator
- Directory Administrator
- Auditor
- AutoRA Administrator
- Custom-defined roles

9. The Entrust/RA architecture is shown below.



10. As illustrated, Entrust/RA uses the ADMinistration Application Programming Interface (ADM-API) subsystem to invoke services offered by Entrust/Authority. As ADM-API is itself an EntrustSession application, the session between Entrust/RA and Entrust/Authority is secured for confidentiality and integrity. Furthermore, session establishment serves to mutually authenticate the operator with Entrust/Authority. Based on this authentication, Entrust/Authority will either terminate the session or accept the session and return to Entrust/RA the user's privilege vector.

11. The GUI is the primary interface to Entrust/RA services. For every service offered by Entrust/RA, there is at least one corresponding GUI element that enables operators to invoke that service. From the Entrust/RA GUI it is possible to access the bulk input files interface and the Directory interface.

12. The bulk interface allows for batch processing of Entrust/RA services through the use of files. The activities that can be performed through the bulk interface include directory management services, such as adding new user entries, or end-entity and operator management services, such as enabling end-entities. The bulk input file, or BIF, processing is initiated via the GUI.

13. The Directory interface allows authorised users of Entrust/RA to access the Directory service directly. The activities that can be performed through the Directory interface are those that are available through any Directory Management interface. Access to this interface is only available through Entrust/RA.

14. The ADM-API is a remote interface to Entrust/Authority. One of the more important features of the interface is that it is responsible for mutually authenticating the Entrust/RA operator and the

Administration Service sub-system of the Entrust/Authority. After mutual authentication is complete, a session is established that is secured for confidentiality and integrity between Entrust/RA and Entrust/Authority. This is done via EntrustSession, as ADM-API is an administrative interface that makes use of the security services provided by the EntrustSession toolkit.

Entrust/Engine (Base)

15. The EntrustSession Toolkit was specifically designed to address secure real-time communications between 2 points. The EntrustSession Toolkit does not provide communications services: those are provided by the application using EntrustSession. Rather, the EntrustSession API provides a means for the application to supplement its existing communications interface with security services. EntrustSession includes the Entrust/Engine (Base) component that encapsulates the common security services required by all of the Entrust/Toolkits and Entrust applications.

Entrust/Authority

16. Entrust/Authority is the core component of an Entrust PKI. Acting as the CA, Entrust/Authority issues X.509 public-key certificates and performs key and certificate management functions. There are 2 human interfaces into Entrust/Authority: Entrust/RA and Entrust/Master Control (GUI and Command Shell) which are part of the TOE.

17. Entrust/Master Control is the part of Entrust/Authority which is used to manage Entrust/Authority itself. The functions available through Entrust/Master Control include:

a. performing initial configuration of Entrust/Authority;

b. verifying the Entrust/Authority database;

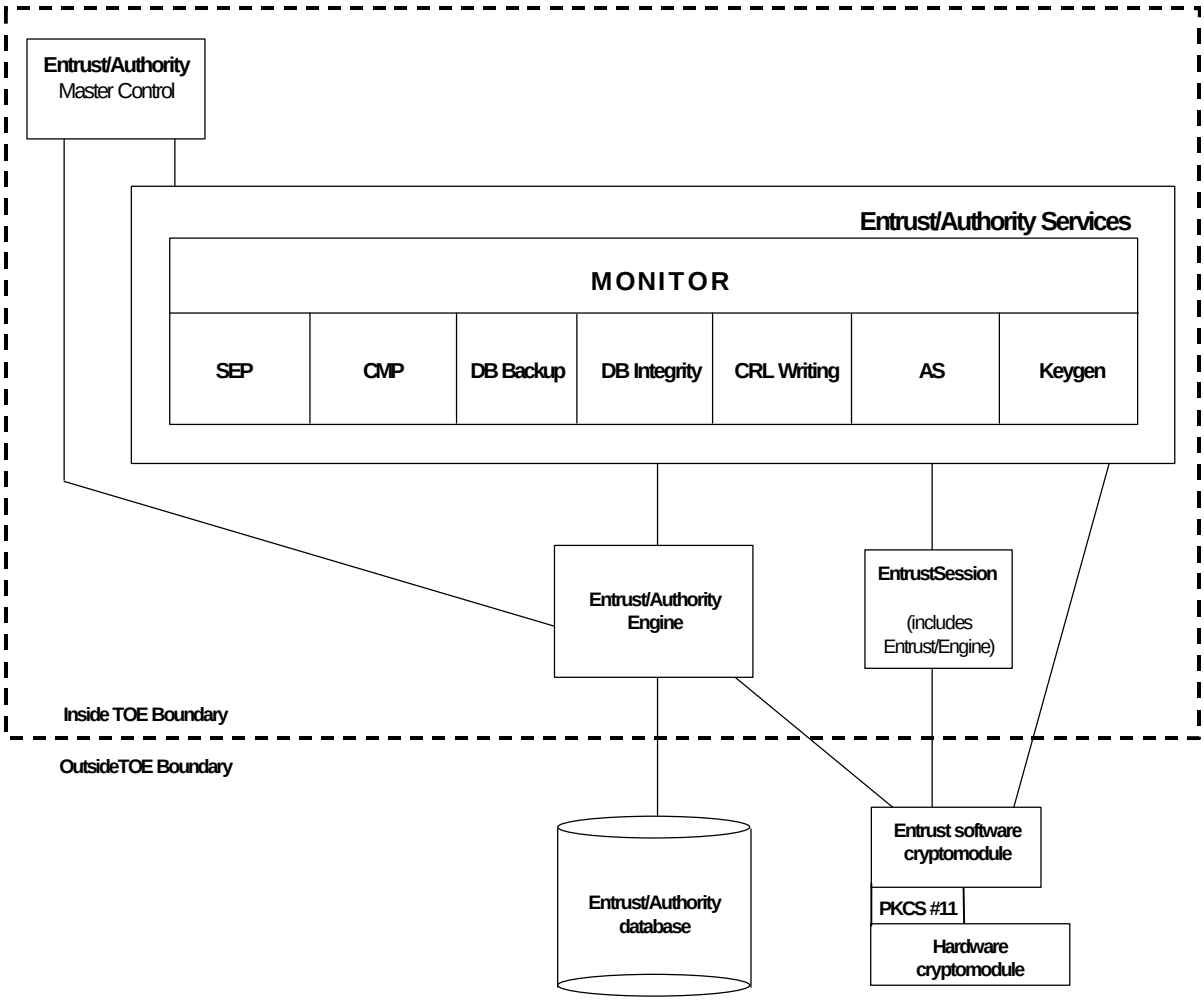
c. scheduling database backups; and

d. performing exceptional PKI-management events such as Security Officer recovery.

18. 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:

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

19. The Entrust/Authority architecture is shown below.



20. Individual components of Entrust/Authority architecture are identified as follows.

- Entrust/Authority Service (Monitor)
- Entrust/Master Control
- Secure Exchange Protocol (SEP) subsystem
- PKIX-CMP subsystem
- Administration Service (AS) subsystem
- Database backup subsystem
- Database Integrity subsystem
- CRL writing subsystem
- Keygen (key generation) system
- Entrust/Authority Engine
- EntrustSession

21. The Entrust/Authority Service (Monitor) is responsible for monitoring the state of the following subsystems:

- SEP subsystem
- PKIX-CMP subsystem

- C AS subsystem
- C Database backup subsystem
- C Database Integrity subsystem
- C CRL writing subsystem
- C Keygen (key generation) subsystem

22. Should one of these subsystems stop functioning, the Entrust/Authority Service (Monitor) will re-start them (assuming they have been enabled).

23. The AS is a server that listens for and processes requests from Entrust/RA through EntrustSession.

24. The Keygen subsystem is a process that performs all pre-generation of public key pairs. It runs transparently in the background and cannot be disabled from the Entrust/Master Control GUI (but can be disabled from the Command Shell). This subsystem never has more than one process. Keygen accesses the security kernel to generate keys.

25. The Entrust/Authority Engine is the runtime library that implements and performs all Entrust/Authority functions. The executable components each access a subset of the Entrust/Authority Engine's capabilities. Entrust/Authority Engine is the component that implements database access, and makes use of the Entrust cryptomodule.

26. Entrust/Master Control comprises a GUI and command shell interfaces that are used to initialise and manage Entrust/Authority. Entrust/Master Control can only be run directly on the machine running Entrust/Authority. The role of Entrust/Master Control is to provide Entrust/Authority initialisation and maintenance services, and certain other services. It is the first Entrust/Authority executable activated after installation of the Entrust/Authority software, and it performs all of the bootstrapping necessary to configure Entrust/Authority based on supplied set-up information.

27. SEP is a subsystem that listens for end-entity key management requests that are using the SEP protocol. These include client initialisation, key update and key recovery from Entrust/Engine (Base) or a third party. This functionality used to reside in the Key Management Service in the Release 4.0, and is provided for backwards compatibility with earlier versions of the product.

28. CMP is a subsystem that handles all PKIX-CMP requests. For each PKIX-CMP request that arrives, a new PKIX-CMP process is spawned. This subsystem is provided to handle client initialisation, key update and key recovery from Entrust/PKI Release 5.0 products.

29. The database backup subsystem is a process that performs all the database backup activities. It runs transparently in the background, and cannot be disabled from the Entrust/Master Control GUI (but can be disabled from the Command Shell). This subsystem never has more than one process.

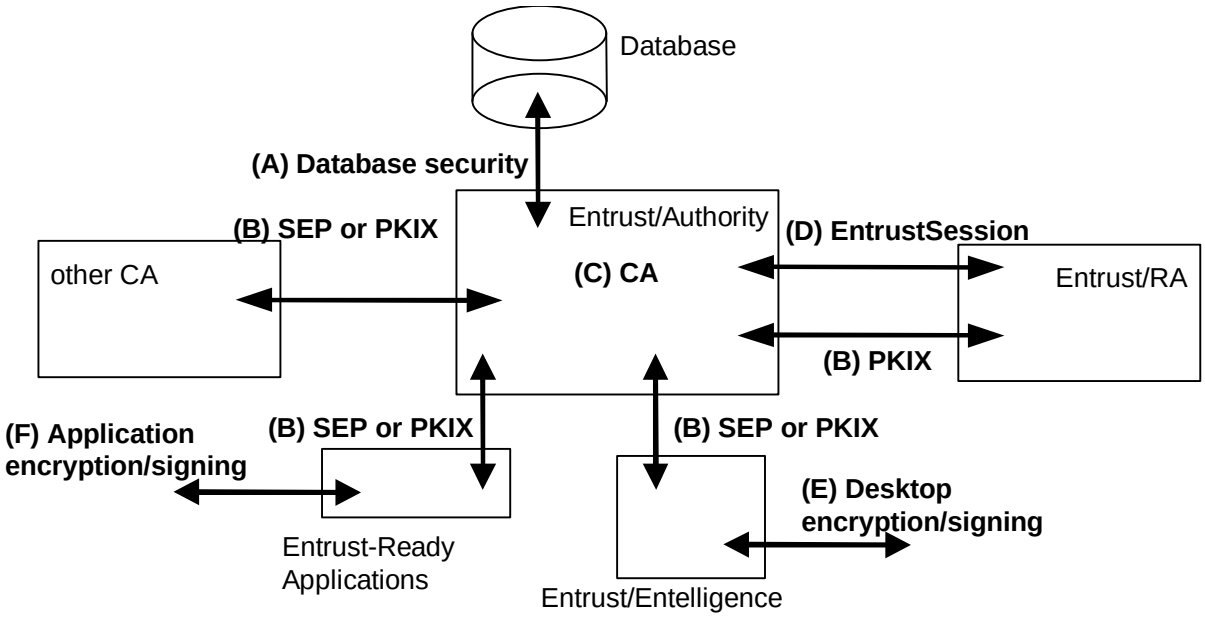
30. The database integrity subsystem is a process that performs all the database integrity validation activities. It runs transparently in the background, and cannot be disabled from the Entrust/Master Control GUI (but can be disabled from the Command Shell). This subsystem never has more than one process.

31. The CRL writing subsystem is a process that performs all CRL writing and checking activities for Entrust/Authority. It runs transparently in the background, and cannot be disabled from the

Entrust/Master Control GUI (but can be disabled from the Command Shell). This subsystem never has more than one process.

Cryptographic Algorithms and Interfaces

32. The diagram illustrates the various interfaces where different algorithms are used within and by the Entrust/Authority TOE. These interfaces are labelled A, B, C, and D and are included in the tables below.



33. The table below identifies the cryptographic algorithms used by Entrust/Authority for each interface.

Interface	Cryptographic Algorithms
(A) Database security	CAST5 80, CAST5 128, SHA-1, Triple DES
(B) SEP or PKIX	CAST5 80, CAST5 128, DSA 1024, ECDSA 192, RSA 512 (PKIX), RSA 1024, RSA 2048, SHA-1, Triple DES
(C) CA	CAST5 80, CAST5 128, DES 56, DSA 1024, RSA 1024, RSA 2048, Triple DES
(D) EntrustSession	CAST5 128, Diffie-Hellman (RSA 1024), SHA-1

34. The approval status of the implementation of the cryptographic algorithms of Entrust/Authority is as follows:

Algorithm Name	Approving Authority
CAST5 80, 128	CSE [f]
Diffie-Hellman	CSE [f]
DSA	NIST (FIPS 140-1) [e]
DES	NIST (FIPS 140-1) [e]
SHA-1	NIST (FIPS 140-1) [e]
Triple DES	CSE, NIST (FIPS 140-1) [f, e]
RSA	CSE, NIST (FIPS 140-1) [f, e]
ECDSA	CSE, NIST (FIPS 140-1) [f, e]

35. The table below identifies the cryptographic algorithms used by Entrust/RA.

Interface	Cryptographic Algorithms
(B) PKIX	CAST5 80, CAST5 128, DSA 1024, RSA 1024, RSA 2048, Triple DES
(D) EntrustSession	CAST5 128, DSA 1024, ECDSA 192, RSA 512 (PKIX), RSA 1024, RSA 2048

36. The approval status of the implementation of the cryptographic algorithms of Entrust/Authority is as follows:

Algorithm Name	Approving Authority
CAST5 80, 128	CSE [f]
DSA	NIST (FIPS 140-1) [e]
Triple DES	CSE, NIST (FIPS 140-1) [f, e]
RSA	CSE, NIST (FIPS 140-1) [f, e]
ECDSA	CSE, NIST (FIPS 140-1) [f, e]

37. The table below identifies the cryptographic algorithms used by Entrust/Entelligence or Entrust-Ready applications. These client applications were not within the scope of the evaluation.

Interface	Cryptographic Algorithms
(E) Desktop Encryption/Signing	CAST3 64, CAST5 80, CAST5 128, DSA 1024, DES, ECDSA 192, IDEA, MD5, RC2 40, RC2 128, RSA 1024, RSA 2048, SHA-1, Triple DES

Interface	Cryptographic Algorithms
(F) Entrust-Ready Application Encryption/Signing	CAST3 40, CAST3 64, CAST5 80, CAST5 128, DES, DSA 1024, ECDSA 192, HMAC-MD5, HMAC-RMD160, HMAC-SHA-1, IDEA, MD2, MD5, RC2 40, RC2 128, RC4, RSA 1024, RSA 2048, SHA-1, Triple DES