

UK ITSEC SCHEME CERTIFICATION REPORT No. P122

Entrust/Admin and Entrust/Authority

from Entrust/PKI 4.0a

on Microsoft Windows NT Version 4.0 Service Pack 3

Issue 1.0

March 1999

© Crown Copyright 1999

Reproduction is authorised provided the report
is copied in its entirety

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 Agreement 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 component ACM_SCP.2 (problem tracking configuration management coverage) but not to ALC_FLR.2 (flaw reporting procedures) and AMA_CAT.1 (TOE component categorisation report).

Trademarks:

Entrust is a registered trademark of Entrust Technologies Limited.

All Entrust product names are trademarks of Entrust Technologies Limited.

All other company and product names are trademarks or registered trademarks of their respective owners.

CERTIFICATION STATEMENT

Entrust Technologies Limited's Entrust/Admin 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.

As detailed in this report, Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a running on Microsoft Windows NT Version 4.0 Service Pack 3 have been evaluated under the terms of the UK ITSEC 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	Dr. A W Powell Certifier
Approval	Dr. R Pizer Head of the Certification Body
Authorisation	P M Seeviour Senior Executive UK ITSEC Scheme
Date authorised	31 March 1999

(This page is intentionally left blank)

TABLE OF CONTENTS

CERTIFICATION STATEMENT iii

TABLE OF CONTENTS v

ABBREVIATIONS vii

REFERENCES ix

I. EXECUTIVE SUMMARY 1

 Introduction 1

 Evaluated Product 1

 Product Environment 4

 Protection Profile Conformance 6

 Evaluation 6

 General Points 7

II. EVALUATION OUTCOME 9

 Certification Result 9

 Unresolved Issues 9

 Recommendations 9

ANNEX A: EVALUATED CONFIGURATION 11

ANNEX B: PRODUCT SECURITY ARCHITECTURE 13

(This page is intentionally left blank)

ABBREVIATIONS

ADM	ADMinistration
API	Application Programming Interface
AS	Administration Services
BIF	Bulk Input File
CA	Certificate Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CLEF	Commercial Evaluation Facility
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
NIST	National Institute of Standards and Technology
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
SFR	Security Functional Requirement
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/Admin,
Entrust Technologies Limited,
Version 1.3, 3 February 1999.
- d. Security Target - Entrust/Authority,
Entrust Technologies Limited,
Version 1.4, 24 February 1999.
- e. Common Criteria Part 1,
Common Criteria Implementation Board,
CCIB-98-026, Version 2.0, May 1998.
- f. Common Criteria Part 2,
Common Criteria Implementation Board,
CCIB-98-027, Version 2.0, May 1998.
- g. Common Criteria Part 3,
Common Criteria Implementation Board,
CCIB-98-028, Version 2.0, May 1998.
- h. Evaluation Technical Report,
Common Criteria EAL3 Augmented Evaluation of Entrust /Admin and Entrust/Authority
v.4.0a,
Syntegra CLEF,
LFS/T251/ETR, Issue 1.1, 3 March 1999.
- i. 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.
- j. Common Methodology for Information Technology Security Evaluation,
Part II: Evaluation Methodology,
Common Evaluation Methodology Editorial Board,
Version 0.6, CEM-99/008, January 1999.
- k. Harmonised Information Technology Security Evaluation Criteria,

Commission of the European Communities,
CD-71-91-502-EN-C, Version 1.2, June 1991.

- l. Interim CC Evaluation Manual,
Common Evaluation Methodology UK Support Group,
UKSP05.CCINT, Version 2.0, 19 June 1998.
- m. Information Technology Security Evaluation Manual,
Commission of the European Communities,
Version 1.0, 10 September 1993.
- n. Manual of Computer Security Evaluation, Part I, Evaluation Procedures,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 3.0, October 1994.
- o. Manual of Computer Security Evaluation, Part III, Evaluation Techniques and Tools,
UK IT Security Evaluation and Certification Scheme,
UKSP 05, Issue 2.0, 30 July 1997.
- p. Entrust Cryptographic Kernel Version 4.0 FIPS 140-1 Validation Report,
Domus Software IT Security Laboratory,
7 July 1998.
- q. Emails from Communications Security Establishment to Certifier,
Communications Security Establishment,
8:19pm 17 December 1998, 6:26pm 20 January 1999, 6:23pm 5 February 1999.
- r. Entrust/PKI 4.0 Administration Guide,
Entrust Technologies Limited,
Version 4.0, 1998.
- s. Entrust/PKI 4.0 NT Installation Guide,
Entrust Technologies Limited,
Version 4.0, 1998.
- t. Manager Core R4.0 Full Test Case Suite,
Entrust Technologies Limited,
Version 1.1, 5 March 1998.
- u. Entrust/Admin R4.0 Full Test Case Suite,
Entrust Technologies Limited,
Version 1.1, 6 March 1998.

- v. Enhanced Reporting Capabilities Full Test Case Suite,
Entrust Technologies Limited,
Version 1.1, 6 March 1998.
- w. Entrust/Directory Browser R4.0 Full Test Case Suite,
Entrust Technologies Limited,
Version 1.1, 1 March 1998.
- x. Entrust/Admin GUI Full Test Case Suite,
Entrust Technologies Limited,
Version 1.1, 2 November 1998.
- y. R4.0 Full Lake Louise Password Rules Tests,
Entrust Technologies Limited,
Version 1.1, March 1998.
- z. Informal Correspondence Demonstration,
Entrust Technologies Limited,
Version 1.7, 3 February 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/Admin and Entrust/Authority from Entrust/PKI 4.0a 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 Product

3. The product evaluated was:

Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a.

The evaluated configuration, including the product's supporting guidance documentation [r, s], is detailed in Annex A. This product is also described in this report as the Target of Evaluation (TOE). The Developer was Entrust Technologies Limited.

4. The Entrust Public Key Infrastructure (PKI) 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 by means of key management transactions, such as the communication of public key certificates to legitimate users of Entrust/PKI, that use the Secure Exchange Protocol. With the exclusion of cryptographic functionality, these key management transactions were within the scope of the evaluation of Entrust/Authority.

6. Entrust/Admin is the administrative client of the Entrust PKI. Entrust/Admin provides a Graphical User Interface (GUI) which is the interface to the Entrust/Authority functionality to enable TOE administrators to set high-level policies and to administer the electronic identities of users and certificate directories. With the exception of some minor certificate directory administration and search functions, which is provided by Entrust/Admin, all of the administration services themselves are provided by Entrust/Authority. However, Entrust/Admin does provide a secure communications channel to Entrust/Authority to ensure that all communications between the 2 products maintain confidentiality and integrity.

7. Entrust/Authority is the management server component of the Entrust PKI and acts as the Certificate Authority (CA) within the 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 provides the CA signing key pair, CA master keys and ensures data integrity.

- b. Entrust/Authority provides end user and administrator 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 administrator management service allows the management of the passwords, keys and privileges of TOE administrators.
 - c. Entrust/Authority provides a cross-certification management service.
 - 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/Admin and Entrust/Authority are administrators. There are no unprivileged users of the TOE. The administrator roles assigned by the TOE are as follows:
- C Master User
 - C Security Officer
 - C Administrator
 - C Directory Administrator
9. The Entrust PKI is used by client applications to ensure secure communications between end users. However, neither the client applications nor end user documentation were examined during this evaluation.
10. The Security Targets [c, d] fully specify the TOE's security objectives, threats and Organisational Security Policies (OSPs) 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 [f]; use of this standard facilitates comparison with other evaluated products. An overview of CC is given in CC Part 1 [e].
11. The TOE Security Policy (TSP) is enforced by the security functions specified in the Security Targets [c, d] and is thus evident from them. However, the OSPs constrain the TSP in the following ways:
- a. Entrust/Authority users must be granted access rights in accordance with the organisational security policy based on object attributes, user attributes and user identity.
 - b. TOE users must be accountable for security relevant actions.

- c. Entrust/Authority and its environment must be resistant to insecurity and provide a means of recovering from insecure states.
- d. TOE cryptographic operations must be performed by a Federal Information Processing Standard (FIPS) 140-1 validated or equivalent module.
- e. Public key certificates, Certification Revocation Lists and Authority Revocation Lists must be electronically bound to the originating CA by digital signature.
- f. Entrust/Authority must distribute and revoke public key certificates as requested by administrators.
- g. Entrust/Authority must recover end user encryption keys as requested by administrators.
- h. Mechanisms must be available to allow for the non-repudiation of origin, confidentiality and integrity of exchanged data.
- i. Entrust/Authority's OSP must remain valid across the network.

12. The TOE did not contain any cryptographic functions provided by the product's cryptomodules. All of the algorithms used to implement cryptographic functions in the product's cryptomodules have been assessed successfully either by the US National Institute of Standards and Technology (NIST) under the US FIPS 140-1 to Security Level 1 (see the validation report [p]) or by the Canadian Communications Security Establishment (CSE) under their Cryptographic Endorsement Program (see the email communications from CSE [q]). Entrust's Entelligence client does implement unassessed algorithms but the algorithms used by default for desk-top encryption and digital signature, CAST5/128 and RSA/DSA both with 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. The current list of unassessed algorithms available in Entelligence or Entrust-ready applications is as follows:

- C CAST (desk-top encryption)
- C CAST3 (desk-top encryption)
- C RC2 (desk-top encryption)
- C HMAC-MD5 (digital signature)
- C HMAC-SHA-1 (digital signature)
- C MD5 (digital signature)

13. It is the responsibility of the potential consumer to ensure that any algorithms used in client applications are suitable and that any unassessed algorithms used are implemented correctly to ensure the confidentiality and integrity of their communications. The potential consumer should also be aware that secure usage assumption A.CRYPTO of the Security Targets [c, d] explicitly requires all cryptographic functions to be performed using FIPS 140-1 validated or equivalent modules.

14. The Entrust cryptomodules of the Entrust/Admin and Entrust/Authority were outside the scope of the evaluation because they have been subject to a separate assessment as detailed above. The

Entrust/Authority database providing a repository of the users' cryptographic key pairs for end users and the X.500 public key certificate directory 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.

15. The Entrust Entelligence user client was also outside the scope of the evaluation, although it was used as a representative client in the functional and penetration testing of the TOE.

16. No security functionality was traced to the Entrust/Database, the X.500 certificate directory product used or to the Entrust Entelligence user client.

17. The product's security architecture is outlined in Annex B.

Product Environment

18. The TOE was evaluated with reference to its specified environment. Secure usage assumptions and environmental objectives for the TOE are specified in the Security Targets [c, d].

19. Entrust/Admin relied on the underlying operating system to enforce TOE Security Functions (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 Security Functional Requirement (SFR) FPT_SEP.1 in the Security Targets [c, d].

20. 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) and to protect audit records from unauthorised deletion (FAU_STG.2.1).

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

22. Entrust/Admin relied on the Entrust/Admin 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).

23. 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).

24. 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 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.

25. The secure usage assumptions of Entrust/Admin were as follows:
- a. the TOE is physically protected from unauthorised modification;
 - b. the cryptographic operations are performed by a FIPS 140-1 validated or equivalent module;
 - c. the TOE operates in a correct and expected manner;
 - d. authorised users recognise the need for a secure IT environment;
 - e. authorised users are trusted to perform discretionary actions in accordance with the security policies and not to interfere with the TOE;
 - f. Entrust/Admin and its environment are competently installed and administered;
 - g. Entrust/Authority is trusted to record security critical events relevant to effective security management (A.RECORD);
 - h. Entrust/Authority is trusted to provide, distribute and revoke certificates as requested by administrators (A.DISTRIBUTE); and
 - i. Entrust/Authority is trusted to recover end user encryption keys as requested by administrators (A.REVOKE).
26. Evaluation of the TOE demonstrated that assumptions A.RECORD, A.DISTRIBUTE and A.REVOKE were met by Entrust/Authority.
27. The secure usage assumptions of Entrust/Authority were as follows:
- a. TOE processing resources will be located within controlled access facilities;
 - b. the TOE is physically protected from unauthorised modification;
 - c. the cryptographic operations are performed by a FIPS 140-1 validated or equivalent module;
 - d. the TOE operates in a correct and expected manner because the TOE is independent of the hardware platform used;
 - e. authorised users recognise the need for a secure IT environment;
 - f. authorised users are trusted to perform discretionary actions in accordance with the security policies and not to interfere with the TOE;
 - g. Entrust/Authority and its environment are competently installed and administered; and

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

Protection Profile Conformance

28. The Security Targets [c, d] did not claim conformance to any Protection Profiles.

Evaluation

29. The evaluation was carried out in accordance with the rules of the UK IT Security Evaluation and Certification Scheme which is 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.

30. 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 were an appropriate baseline for a Common Criteria evaluation, it was first itself evaluated, as outlined in CC Part 3 [g].

31. 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) and AMA_CAT.1 (TOE component categorisation report). CC Part 3 [g] describes the scale of assurance given by predefined Evaluation Assurance Levels EAL0 to EAL7, where EAL0 represents no assurance.

32. 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.

33. 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 but a rating of SoF-Medium was claimed for the operator password verification mechanism.

34. Testing addressed the following to the extent required by the specified assurance requirements:

- a. security functions specified by the Security Target;
- b. potential vulnerabilities of which there is knowledge in the public domain; and
- c. other potential vulnerabilities which became evident during the course of the evaluation.

35. Whilst the TOE was evaluated against criteria taken from those agreed internationally in CC Part 3 [g], the evaluation was performed prior to the finalisation of the Common Evaluation Methodology (CEM). To ensure an appropriate application of the criteria, available drafts of CEM [i, j] 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) [k] in many respects, the UK's Interim CC Evaluation Manual [l] was used, which is based on the IT Security Evaluation Manual (ITSEM) [m] and elaborated in the UK ITSEC Manual of Computer Security Evaluation UKSP 05 [n, o]. 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 [g].

36. The Certification Body monitored the evaluation which was carried out by the Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed in March 1999 when the CLEF submitted the final Evaluation Technical Report (ETR) [h] to the Certification Body which, in turn, produced this Certification Report.

General Points

37. Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities remain undiscovered.

38. The evaluation addressed the security functional requirements and security functions claimed in the Security Targets [c, d], with reference to the assumed environment specified in the Security Targets. The evaluated configuration 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.

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

(This page is intentionally left blank)

II. EVALUATION OUTCOME

Certification Result

40. After due consideration of the ETR [h], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a meet the specified CC Part 3 [g] augmented requirements incorporating Evaluation Assurance Level EAL3 for the specified CC Part 2 [f] conformant functionality in the specified environment.

41. The minimum SoF of the operator password verification mechanism was SoF-Medium as claimed.

Unresolved Issues

42. The Developer's test documentation [t-y] did not identify which security functions were identified by each test. However, the Evaluators were able to use the mapping provided in a separate Developer's test correspondence document [z] to identify the security functions described in [t-y]. To support any future evaluation, the Certification Body recommends that the test documentation is updated to indicate clearly which security functions are tested by particular tests.

43. The Developer's test documentation [t-z] did not clearly identify the TOE test configuration. However, the Evaluators noted during their visit to the development site that any additional requirements to the standard TOE configuration were clearly deducible from the test documentation. To support any future evaluation, the Certification Body recommends that the test documentation is updated to identify clearly the TOE test configuration.

44. The Developer's test documentation [t-z] contained some minor inconsistencies and did not provide tests for a small number of audit events. To support any future evaluation, the Certification Body recommends that the test documentation is updated to address these issues.

45. Although the Evaluators checked the correctness of the Developer's categorisation of the TOE components into TSP-enforcing and non-TSP-enforcing components as part of AMA_CAT, they did not check the correctness of the Developer's categorisation of the TSP-enforcing components into security-critical and security-supporting components. The Evaluators thereby confirmed that the minimum Developer's categorisation requirement for AMA_CAT was met.

Recommendations

46. 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].

47. Only the evaluated product configuration, specified in Annex A, should be installed. The product should only be used in accordance with its guidance documentation.

48. The products should only be used in accordance with the environment and secure usage assumptions outlined in the Security Targets [c, d] and in the "Product Environment" section above.

49. The Developer's test documentation [t-z] should be updated as specified in the "Unresolved Issues" section above.

50. 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:

- C CAST (desk-top encryption)
- C CAST3 (desk-top encryption)
- C RC2 (desk-top encryption)
- C HMAC-MD5 (digital signature)
- C HMAC-SHA-1 (digital signature)
- C MD5 (digital signature)

51. In any future evaluation including AMA_CAT, the Evaluators should check the Developer's categorisation of the TSP-enforcing components into security-critical and security-supporting components.

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely identified as:

Entrust/Admin and Entrust/Authority from Entrust/PKI 4.0a.

2. The supporting guidance documents evaluated were:

- C Administrator's Guide [r]
- C Installation Guide [s]

TOE Configuration

3. The TOE had the following configuration options:

- a. use of the Entrust/Directory or a third party 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/Admin on the same server as Entrust/Authority or on a different platform.

4. 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 [s].

5. 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.

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

Environmental Configuration

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

- C Microsoft Windows NT Server Version 4.0 Service Pack 3 operating system
- C Dell OptiPlex GX Pro with a 200 MHZ Pentium processor
- C 2 x 64 EDO DIMM memory
- C Entrust/Authority database (Informix Online Workgroup Server Version 7.22.TC1 running on Entrust/Authority server)

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

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

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

- C ICL i500 Version 7.0b running on
- C Microsoft Windows NT Server Version 4.0 Service Pack 3 operating system
- C Hewlett Packard NetServer LH Pro SMP with dual 200 MHZ Pentium processors
- C 2 x 64 EDO DIMM memory

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

ANNEX B: PRODUCT SECURITY ARCHITECTURE

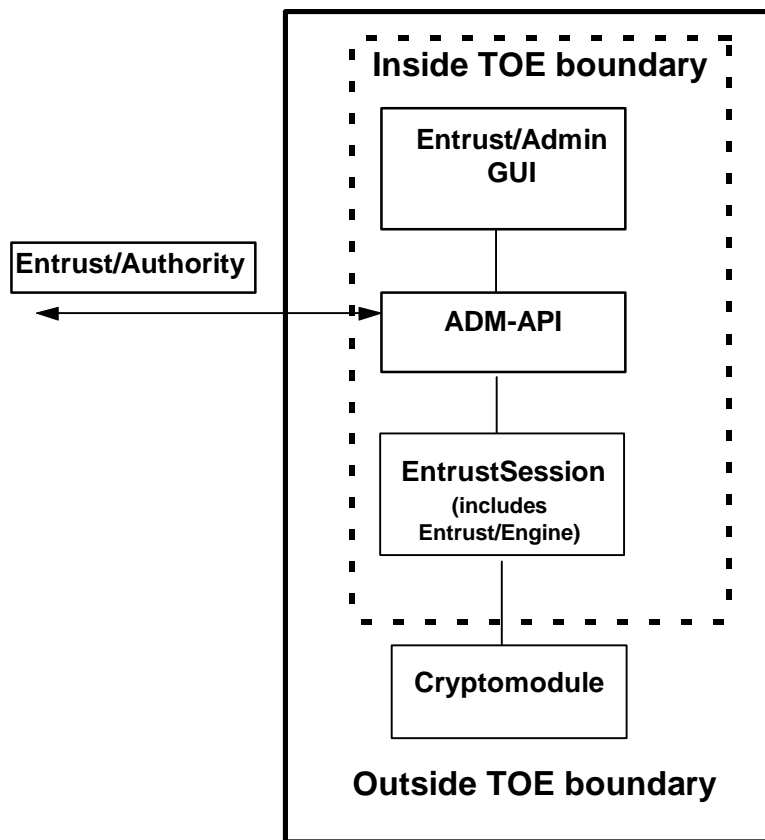
1. Entrust/PKI uses a distributed architecture to deliver PKI services. Entrust/Authority, Entrust/Engine and Entrust/Admin are 3 major components of the Entrust system architecture. Entrust/Engine is encapsulated in Entrust/Session which is part of both the Entrust/Authority and Entrust/Admin.
2. Entrust/Authority is the PKI management server component. It acts as the CA within the PKI, issuing and managing end-entity certificates and the revocation list and controlling PKI policy.
3. Entrust/Engine is the core component of client Entrust-ready applications and is encapsulated within EntrustSession and the other Entrust Toolkits and applications. Entrust/Engine, in conjunction with the services provided by Entrust/Authority, provides user initialisation, automatic key management, signature verification and certificate validation, as well as having integrated encryption and encryption key management capabilities.
4. The third major component of the architecture is the administrative client, Entrust/Admin. Entrust/Admin 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/Admin, Entrust/Engine (encapsulated with EntrustSession) and Entrust/Authority are discussed in the following sections in terms of their high level design components and interfaces.

Entrust/Admin

8. Entrust/Admin 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/Admin is assigned to the following Entrust roles listed below.

- C Master User
- C Security Officer
- C Administrator
- C Directory Administrator

9. The Entrust/Admin architecture is shown below.



10. As illustrated, Entrust/Admin 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/Admin 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/Admin the user's privilege vector.

11. The GUI is the primary interface to Entrust/Admin services. For every service offered by Entrust/Admin, there is at least one corresponding GUI element that enables operators to invoke that service. The other interface to Entrust/Admin services is the Bulk Input Files (BIFs). BIFs are used for batch processing of Entrust/Admin services. They are used to perform either directory management services, such as adding new user entries, or end-entity or operator management services, such as enabling end-entities. BIF processing is initiated via the GUI.

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

13. The Administration Service is a server that listens for and processes requests from Entrust/Admin.

14. The Key Management Service is a server that listens for end-entity requests, ie requests for client initialisation, key update or key recovery from Entrust/Engine and certificate requests from other Entrust/Authority installations for cross certification purposes.

Entrust/Engine

15. 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 communications between 2 points. 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 software with security services. EntrustSession includes the Entrust/Engine that encapsulates the common security services required by all the Entrust/Toolkits and Entrust applications. In the case of Entrust/Admin the toolkit used is the EntrustSession Toolkit.

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/Admin and Entrust/Master Control which is part of the TOE.

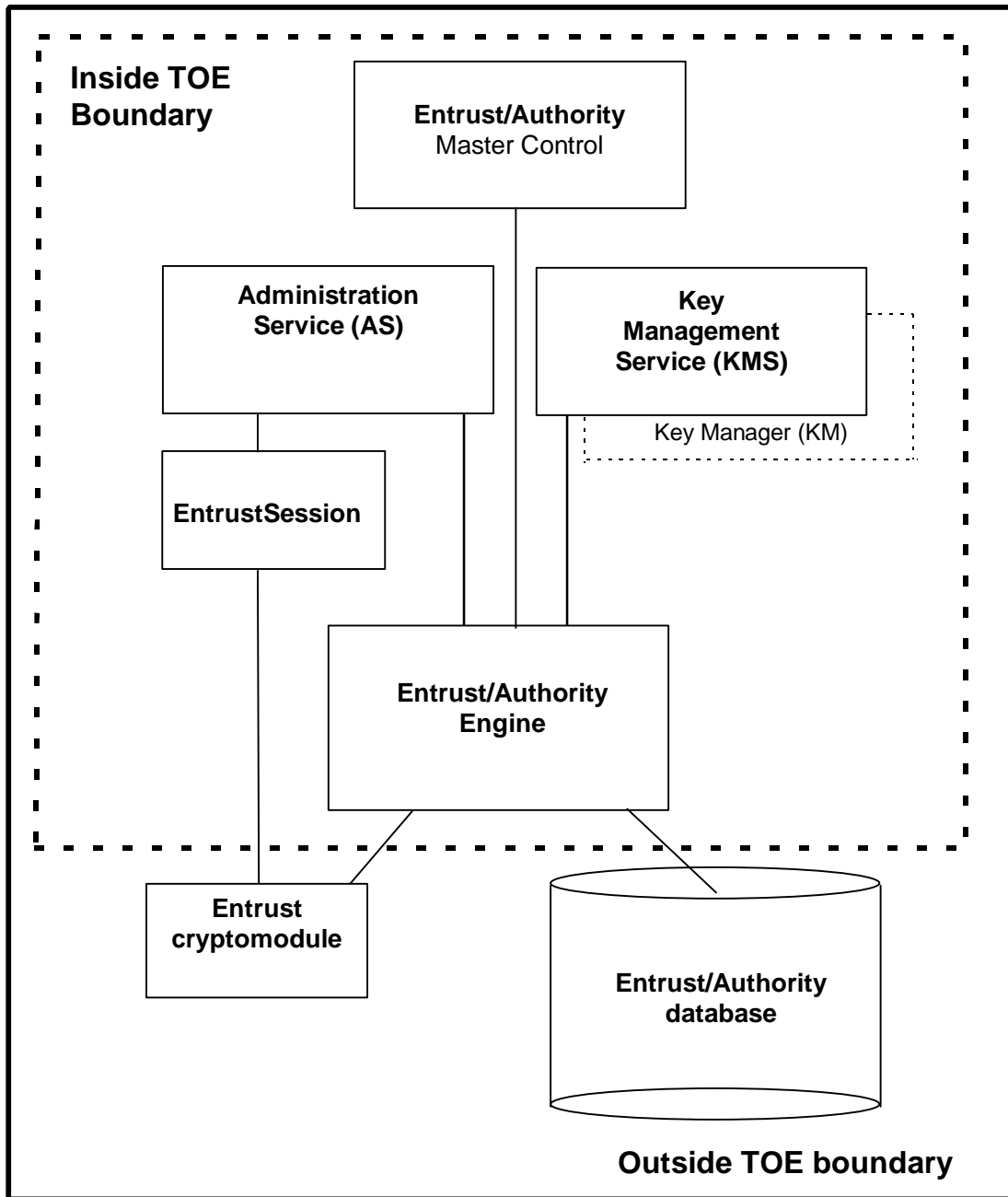
17. Entrust/Master Control is the part of Entrust/Authority which is used to manage Entrust/Authority itself. The functions available through Entrust/Master Control include:

- 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/Admin 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:

- C Master User
- C Security Officer
- C Administrator
- C Directory Administrator

19. The Entrust/Authority architecture is shown below.



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

- C Entrust/Authority Engine
- C Key Management Service
- C Administration Service
- C EntrustSession
- C Master Control

21. The Key Management Service, the Administration Service, EntrustSession and Master Control have been discussed above. 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.

(This page is intentionally left blank)