Common Criteria Evaluation for a Trusted Entrust/PKI™

Author: Marc Laroche
Date: March 2000
Version: 2.0

Table of Contents

Introduction 4
Common Criteria 5
  Background to the Common Criteria 5
  Evaluation Process 5
  International Recognition 6
  What does it mean for Entrust? 6
Security Evaluation of Entrust/Authority and Entrust/RA 7
  Delivered Services 7
  Core Services 7
  Support Services 7
  Evaluated Security Functions 8
  Security Assurance 11
  Components excluded 12
References 13

Introduction

The notion of trust is fundamental in public-key infrastructures (PKIs). For PKIs to be valuable, users must be assured that the parties they communicate with are safe, i.e. their identities and keys are valid and trustworthy. To provide this assurance, there must be confidence that the technology involved in binding the names of users to their public keys is trusted. The technology used to create these bindings includes security mechanisms and services that provide the secure generation, destruction, and distribution of cryptographic keys, cryptographic operations, identification and authentication, complete access control, management of security functions and services, roles and separation of duties, audit of security critical events, secure communications, data protection, and more. These mechanisms and services contribute jointly in allowing the Certification Authority (CA) to securely bind together the user identities and public keys in a digital format known as a public-key certificate. In creating these certificates, CAs act as trusted third parties in a PKI. As long as users trust the CA and its business policies for issuing and managing certificates, they can trust the public-key certificates issued by the CA.

Trust is a fundamental requirement for any large-scale implementation of security services based on public key cryptography. Trusting a PKI implies that the people, processes and tools involved in the creation and management of cryptographic keys and certificates ensures an absolute reliable binding between user identities and public keys. Therefore there must be confidence that the technology involved in creating and maintaining the public-key certificates can be trusted to operate with an appropriate level of security. Security evaluations performed by certified third party evaluation facilities against recognized security criteria are instrumental in establishing trust in PKI technology. They allow unbiased security experts to analyze the security functions, interface specifications, guidance documentation and design of the product.

So far, five versions of the Entrust software cryptographic module have been validated against the FIPS 140-1 standard. These validations provide Entrust users with assurance that the cryptographic services delivered by Entrust, i.e. encryption/decryption, digital signature creation/verification, hashing, random number generation, key generation/zeroization, etc., are secure. The Common Criteria Evaluation of Entrust/Authority™ and Entrust/RA™ (previously known as Entrust/Admin™) serves as a fundamental extension to the FIPS 140-1 process in that it extends the security assurance to the services involved in issuing and managing the life cycle of public-key certificates. The certification of these products by the UK Certification Body (CESG) confirms that these products have met the specified ISO 15408-3 (Common Criteria Part 3) Evaluation Assurance Level (EAL) 3 augmented requirements, and can be trusted to reliably and securely deliver CA services.

Common Criteria

Background to the Common Criteria

The Common Criteria (CC), which became ISO standard 15408 in 1999, is an alignment and development of a number of source IT security evaluation criteria including existing European (ITSEC), US (TCSEC - Orange Book) and Canadian (CTCPEC). The CC permits comparability between the results of independent security evaluations. By establishing such a common criteria base, the intent is for the results of an IT security evaluation to be meaningful to a wider audience. It does so by providing a common set of requirements for the security functions of Information Technology (IT) products and for assurance measures applied to them during a security evaluation. The CC describes Security functionality in the form of 11 classes of requirements: Security Audit, Communication, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Privacy, Protection of security Functions, Resource Utilization, Access, and Trusted Path/Channels. The CC also contains a set of defined assurance levels constructed using components from assurance families. The assurance families consist of Configuration Management, Delivery and Operation, Development, Guidance Documents, Life Cycle Support, Test, Vulnerability Assessment and Maintenance of Assurance.

Evaluation Process

The principal inputs to a CC evaluation are the Security Target, the set of evidence documentation about the product under evaluation, and the product itself (referred to as the Target of Evaluation – TOE).

The Security Target is the basis for the agreement between the product vendor, evaluators and certification agencies as to what security functionality the product (TOE) offers and the scope of the evaluation. The Security Target identifies, and refines as appropriate, a set of CC IT security and assurance requirements. It provides a definition of the TOE security functions claimed to meet the functional requirements and the assurance measures taken to meet the assurance requirements. The ST also addresses the organizational security policies with which the TOE must comply and the security aspects for the environment in which the TOE will be used.

The set of evidence documentation includes the documents, which describe the TOE in the form of design description, functional specification, configuration management, delivery and operations, support and maintenance, vulnerability analysis, functional testing and more. These documents, the TOE, the administration and user guides and the Security Target are submitted to a third party certified laboratory that proceeds with the evaluation. Using the procedures and interpretations detailed in the Common Evaluation Methodology (CEM), the certified laboratory facility will evaluate the Security Target for completeness and consistency. The evaluators will then analyze the evidence documentation, and proceed with functional and penetration testing of the TOE, to verify conformance to the CC. The results of the evaluation confirm that the ST is satisfied with the TOE, in other words the functional and assurance security claimed in the ST has been verified. The certified laboratory facility produces a report documenting the findings. The report is submitted to a government agency acting as the Certification Body, which then proceeds with certification/validation of the product (i.e. TOE certification/validation).

The evaluation process establishes a level of confidence that the security functions of a product and the assurance measures applied to it meet the requirements. The evaluation results help consumers gain confidence that the IT product is secure enough for their intended application and that the security risks implicit in its use are tolerable.

International Recognition

The following countries: United States, United Kingdom, Canada, Germany, France, Australia and New Zealand officially signed a Mutual Recognition Arrangement (MRA). The MRA allows IT products that earn a CC certificate to be procured and used in different jurisdictions without the need for them to be evaluated and certified/validated more than once. By recognizing the results of each other' s evaluations, products evaluated in one MRA member nation can be accepted in the other member nations.

What does it mean for Entrust?

Basically, the evaluation and validation of Entrust products allow Entrust to provide "trusted" security solutions to its customers. With FIPS 140-1 validations, the Entrust cryptographic modules have been verified and tested by a third party, and thus can be trusted to provide reliable and well designed cryptographic services. The CC evaluation is a fundamental extension to the FIPS 140-1 validation process; an autonomous third party has examined the cryptography in detail, determined its compliance with strict security requirements, and analyzed the security functions, interface specifications, guidance documentation and design of the product as a whole. Entrust/Authority and Entrust/RA have been successfully "methodically tested and checked", and can be trusted to provide secure and reliable public key management services.

Security Evaluation of Entrust/Authority and Entrust/RA

Delivered Services

Entrust/Authority and Entrust/RA are responsible for creating and issuing end-entity public-key certificates, Certificate Revocation Lists (CRLs), and Authority Revocation Lists (ARLs). In addition, they provide the infrastructure support functions that are expected in a PKI such as

- maintaining end-entity encryption key-pair history and end-entity verification certificate history,
- providing mechanisms for trusted key revocation and trusted recovery of public keys and certificates,
- providing automatic public key and certificate updates,
- auditing security-related events; and
- maintaining CA data confidentiality and integrity in distributed environments.

The functionality that Entrust/Authority and Entrust/RA jointly provide can be categorized in two broad categories of services, namely *Core Services* and *Support Service*s.

Core Services

The Core Services are the basis for Entrust/PKI™ management functionality. These services include CA Key Management, End-entity Management, Operator (i.e. administrative user) Management, and Cross-Certificate Management.

1) CA Key Management Service: This service is responsible for providing secure management of the CA signing key pair and other information, and maintaining CA data integrity.

2) Operator Management Service: This service is responsible for providing the capability (to privileged operators) to manage other operators. Passwords, keys, privileges, and all other operator characteristics are managed through this service.

3) End-entity Management Service: Similar to Operator Management, the End-entity Management Service allows authorized operators to manage End-entities (i.e. end-users) associated with a CA domain. This service allows for creating, initializing, and deleting users, recovering, revoking, and updating keys, and others.

4) Cross-Certificate Management Service: This service manages the generation and maintenance of cross-certificates that allow different CA domains to establish and maintain trustworthy electronic relationships. It provides the ability to support and maintain a strict PKI hierarchy and peer-to-peer relationships with other CAs and provides fine-grained control to limit these relationships.

Support Services

The Support Services consist of a set of services relating to management of Entrust/PKI components. These services include CA Self-Management, Database Management, Audit Trail Management, and management of repository components (i.e. Database and X.500 Directory).

1) Self Management: Services to initialize the CA, start and stop CA services, and validate passwords.

2) Database Management: Services to operate and maintain the repository that stores encryption key pairs for end-entities, user information, and system and security policy data.

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

4) Directory Management: Services to operate and maintain the Directory (e.g., search the directory, create directory entries, etc.).

Evaluated Security Functions

Entrust/Authority and Entrust/RA include security functions that ensure that the CA services described above are delivered in a secure fashion. These functions were assessed as part of the evaluation process, meaning that they have been successfully verified and tested, and therefore trusted. These functions can be grouped in the following categories where TOE refers to Target of Evaluation i.e. Entrust/Authority and Entrust/RA:

1) Identification and Authentication

All individual users (administrative or not) are assigned a unique user identifier. This user identifier supports individual accountability. The TOE authenticates the claimed identity of the user before allowing the user to perform any further actions. The TOE enforces password policies. The authentication data (i.e. passwords and authentication codes) is protected against unauthorized disclosure, and also against re-use for one-time only operations (e.g. initialization of end-users and key recovery). The TOE requires administrative users to re-authenticate or forces multiple-authentication before executing security-critical operations (e.g. security policy change, password change, etc.). The TOE terminates active sessions after a timeout period has lapsed and terminates a login process after three consecutive authentication failures.

2) Access Control

The TOE enforces controls such that access to the data objects (including cryptographic key material and other CA data) and the permitted actions with respect to them including access to the various CA services can only take place in accordance with an access-control policy based on privileges associated with the role and identity of users.

3) Roles and Privileges

The TOE maintains default roles for: management of security policies, management of administrative users, everyday management of end users and key management of end entities, view audit information, and more. The TOE also provides for custom roles to be defined.

Associations between users and roles can only be placed and removed by users operating under a privileged role. Each role can be assigned to more than one user.

4) Audit

The TOE generates an audit record of any security-critical event including, but not limited to password rule changed, password (for privileged user) changed, privileged user login completed/failed, security policy changed, integrity check or encryption failed, backup completed/failed, user permissions modified, key/certificate expire date changed, operation/transaction failed to successfully complete, audit error, cross-certification completed/failed, services started/stopped, key recovery/update completed/failed, end entities added/removed/initialized.

Each audit record includes a log number, the date and time the event occurred, a description of the event, a severity level and an encrypted integrity checksum. The TOE can associate each audit record with the identity of the user that caused the event and can detect modifications to the audit records.

The TOE provides administrative users with the necessary privileges and the capability to read all audit records. Searches of audit data based on ranges of dates can be made.

5) Trusted Communication Path

The TOE ensures that data transmitted between itself and remote administrative users, between itself and other CAs and between itself and end-users is protected against unauthorized disclosure and modification including deletion, insertion and replay. Such data is transferred during normal administrative operations and key management transactions.

6) Non-Repudiation

The TOE enforces proof of origin on any certificate it generates, including end-entity certificates, Certification Revocation Lists (CRLs) and Authorization Revocation Lists (ARLs), as well as on data objects transferred during remote administrative operations and key management transactions. The TOE also provides trusted IT products with the capability to verify the evidence of origin of information.

The TOE enforces the generation of evidence of receipt for received public key certificates and provides a capability to verify the evidence of receipt and exchanges.

7) Data Integrity Monitoring

The TOE monitors the integrity of all data objects it stores and exchanges, including cryptographic keys, cryptographic parameters, authentication information, certificates, security attributes and other security critical information.

8) Cryptographic Operations

The TOE performs encryption/decryption, digital signature generation and verification, hashing, random number generation, and key generation and destruction in accordance with recognized FIPS and ANSI standards. These cryptographic operations are performed by the TOE, or on behalf of the TOE, using a FIPS 140-1 validated cryptographic module or equivalent.

9) Key Storage and Distribution

The cryptographic aspect of the TOE requires that cryptography-related data items and other security critical items be protected. The TOE provides the functions and services to ensure that the following security-critical assets are protected against unauthorized disclosure and/or modification as appropriate:

- Cryptographic variables (including secret keys, public and private keys, public-key certificates, other parameters such initialization vectors, etc.); these are always protected while in storage (as described in Section Access Control) and in transit.
- Input and output data from the cryptographic function (e.g., plain text and cipher text).
- Implementation of the cryptographic services.
- Other critical security parameters (e.g., authentication data).

The TOE provides mechanisms to securely distribute, destruct, recover, revoke and update keys as required in accordance with recognized FIPS and ANSI standards.

10) Protection of Security Functions and Automated Recovery

The TOE ensures that security enforcement functions are invoked and succeed before each function within it is allowed to proceed. Also, a security domain is maintained to protect the execution of TOE' s functions from interference and tampering by untrusted subjects.

Secure functions are provided that ensure the return of the TOE to a secure state after failures or service discontinuities.

A set of security functional components was extracted from the CC to express the security functional requirements within the ST. In other words, the security functions described above are detailed in the form of CC security functional requirements (SFRs) within the ST, which forms the basis for the evaluation.

Entrust/Authority and Entrust/RA, in conjunction with the FIPS 140-1 validated Entrust cryptographic module, have been successfully evaluated against the CC SFRs listed in Table 1.

Table 1 TOE security functional requirements

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

37.	FPT_RVM.1	Non-bypassability of the TSP
38.	FPT_TST.1	TSF testing
39.	FPT_TDC.1	Inter-TSF basic TSF data consistency
40.	FTA_SSL.3	TSF-initiated termination
41.	FTP_ITC.1	Inter-TSF trusted channel
42.	FTP_TRP.1	Trusted path

Security Assurance

Entrust/Authority and Entrust/RA have been evaluated at the CC EAL3 (augmented) assurance level and this evaluation satisfies the U.S. CS2 Protection Profile assurance requirements (EAL-CS2). EAL3 (and EAL-CS2) provide assurance by an analysis of the security functions using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behavior. The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain). EAL3 also provides assurance through the use of development environment controls, TOE configuration management and evidence of secure delivery procedures. The augmentation to EAL3 addresses the area of problem tracking and flaw remediation providing assurance that any problems or flaws that may appear would be effectively remedied. The augmentation also adds the TOE component categorization report that is required for maintaining the assurance rating of the TOE and an informal TOE Security Policy Model.

The CC assurance components included in this evaluation are summarized in Table 2 and those components that augment EAL3 are listed in Table 3.

Table 2 EAL3 assurance components

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

Table 3 Augmentation to EAL3

Component ID	Component title	Note
ACM_SCP.2	Problem Tracking CM Requirements	Upgrade from ACM_SCP.1 TOE CM coverage

Component ID	Component title	Note
AVA_MSU.2	Validation of Analysis	Upgrade from AVA_MSU.1 Examination of Guidance
ADV_SPM.1	Informal TOE Security Policy Model	Addition
ALC_FLR.2	Flaw Remediation requirements	Addition
AMA_CAT.1	Categorization Report	Addition

Components excluded

The Entrust/PKI components excluded from the evaluation, with justification for their exclusion, are given below:

1) Entrust Cryptographic module: The justification for excluding the cryptomodule from the TOE boundary is that the Entrust cryptomodule has been assessed under the FIPS 140-1 validation program.

2) Entrust/Authority database: The justification for excluding the database from the Entrust/Authority TOE boundary is based on the following factor: Database security is provided by Entrust, not the database. As such, all data items stored in the Entrust/Authority database are encrypted and MACs are generated for each data item. Thus, the evaluation makes no claims about database functionality (aside from the inherent, fundamental and basic function of data storage) and database functionality is not mapped to any of the SFRs in the Security Target.

3) Hardware and operating system platform (Abstract Machine): The TOE abstract machine consists of the Windows NT 4.0 operating system and any hardware for which the operating system and TOE configurations are valid. The operating system is trusted to operate correctly, to provide reliable time stamps, to protect stored audit records against unauthorized deletion and to protect the execution of the TOE against interference and tampering by untrusted subjects. The justification for excluding the abstract machine from the Entrust/Authority TOE boundary is based on the following factors: Each security policy is enforced by the TOE only, and the SFRs are completely satisfied by TOE functions. The TOE is hardware independent, as Entrust software does not interact with the hardware platform directly. That is, the Entrust software interacts with the operating system which, in turn, interacts with the hardware platform.

4) Directory: The directory serves as the repository for publicly accessible data, such user certificates, CA certificates, revocation lists and so on. The justification for excluding the directory from the TOE boundary is based on the following factors: Entrust/Authority digitally signs all data it stores on the Directory to allow for verification of authenticity, integrity and origin; security on these data items is provided by Entrust, not the Directory. The evaluation makes no claims about Directory functionality (aside from the inherent, fundamental and basic function of data storage) and Directory functionality is not mapped to any of the SFRs in the Security Target.

References

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

[Reference 2] Information Technology - Security techniques - Evaluation criteria for IT security ISO/IEC 15408-1, 15408-2 and 15408-3, First edition, 1999-12-01.

[Reference 3] FIPS PUB 140-1 (Federal Information Processing Standards Publication), Security Requirements For Cryptographic Modules, National Institute Of Standards And Technology, 1994 January 11.

[Reference 4] UK ITSEC Scheme Certification Report No. P122, Entrust/Authority and Entrust/Admin from Entrust/PKI 4.0a on Microsoft Windows NT 4.0 Service Pack 3, March 1999.

[Reference 5] UK ITSEC Scheme Certification Report No. P141, Entrust/Authority and Entrust/RA from Entrust/PKI 5.0 on Microsoft Windows NT 4.0 Service Pack 3, March 2000.