Cryptographic Modules

Cryptography and Exchange Services

Draft
Version 1.0e
July 1993

Canadian System Security Centre
Communications Security Establishment
Government of Canada

Acknowledgments

Special recognition is extended to the principal authors of the Cryptographic Modules document: Paul Cormier, CSE; Ken Donaldson, CSE; Albert Pereira, CSE; and William Brierley, AEPOS Technologies Corporation. Also due acknowledgment for their input and contributions to this document are: Steve Booth, CSE; Steve Harrison, CSE; Barry Madill, CSE; and Andrew Robison, CSE.

Summary Table of Contents

Table of Contents

Table of Contents

List of Figures

List of Tables

Foreword

This document represents the current state of the Cryptographic Modules Criteria. The purpose of this document is to present a set of technical hardware/firmware/software criteria for trusted products incorporating cryptography which is consistent with the Security Policy of the Government of Canada, the Information Technology Security Standards under development by the Government of Canada and takes into account reciprocity issues with technical criteria of other nations strategically allied with the Government of Canada. Development of the Cryptographic Modules Criteria has progressed through workshops and discussions with government and industry.

Review, revision and further development, as appropriate, will be on a continuing basis with reissuance of a revised Cryptographic Modules document on an as needed basis.

Comments and recommendations for further development and revision of this document are welcomed and should be directed to:

Criteria Coordinator
S5B InfoSec Standards and Evaluations
Communications Security Establishment
P. O. Pox 9703 Terminal
Ottawa, Canada
K1G 3Z4
phone: (613) 991-7331
fax: (613) 991-7323
net: criteria@manitou.cse.dnd.ca

Requests for further hardcopies of this document can be directed to the Head, INFOSEC Client Support Services, at (613) 991–7543. Electronic copies of the Cryptographic Modules document may be acquired by anonymous `FTP` from:

ftp.cse.dnd.ca

Login as “anonymous” and supply “userName@site” as the password.

Introduction

In January 1993, Version 3.0 of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC or Canadian Criteria) was released. The CTCPEC, separates out Functionality and Assurance criteria.

The Functionality criteria are divided into four criteria: Confidentiality, Integrity, Availability, and Accountability. Within each functionality criteria, security services are defined to counter assumed threats. A level of service is defined as a measurable requirement in terms of granularity of application and strength of mechanism.

The Assurance criteria are divided into seven hierarchical levels representing successively increasing confidence that the product security policy is correctly implemented. All security services provided by a trusted product are evaluated to the same assurance level.

The CTCPEC discusses the use of cryptography in the implementation of specific security services. However, two issues are not discussed in the CTCPEC. The first issue deals with the proper implementation of a cryptographic module and its integration into a trusted product. The second issue deals with the transmission of protected objects between trusted products.

Scope

The Cryptographic Modules document was developed to complement the CTCPEC in the following areas:

1. **functionality criteria:** to provide security services which would cover threats to protected objects transmitted over or stored on unprotected media;
2. **cryptographic modules:** to provide the assurance and functionality requirements for the implementation of commercial grade cryptographic modules, and to define any constraints between the cryptographic module and the host TCB; and
3. **integration:** to provide a framework for the development and evaluation of trusted products incorporating cryptography.

In addition to the goals stated above, the Cryptographic Modules document was developed under the following constraints:

1. to minimize the discrepancy between the requirements for a cryptographic module endorsement as specified under the Cryptographic Endorsement and Assessment Program (CEAP) and the Cryptographic Modules Criteria; and

2. to accept the results of a previous endorsement or validation of a cryptographic module without requiring additional work from the Vendor.

Functionality

The Cryptographic Modules document introduces an additional functionality criteria: Exchange. The Exchange security services counter threats centered around TCB objects transmitted over or stored on unprotected media. Such threats could include the disclosure of protected objects during transmission, the modification of protected objects during transmission, or the authenticity of the trusted products involved in the transmission of protected objects.

Exchange services facilitate the rating and specification of services which support distributed computing environments over unprotected media. By providing Exchange services as distinct criteria it is possible to distinguish between products which have been evaluated to operate in a protected environment and one suitable for an unprotected distributed environment. Products rated for a protected environment do not have rated Exchange services and the evaluation does not take communications functionality into account. Products suitable for an unprotected distributed environment do have rated Exchange services which support an appropriate security policy.

The Exchange services defined in these criteria complement the functionality criteria defined in the CTCPEC. A product under evaluation may target any combination of functionality services defined in either the CTCPEC or the Cryptographic Modules document. However, a single level of assurance is applied globally to all security services.

Cryptographic Modules

The Cryptographic Modules Criteria defined in this document specify the implementation requirements for commercial grade cryptographic modules. Included in the implementation requirements are:

1. **functionality requirements:** the functionality that must be implemented as part of the cryptographic module;
2. **assurance requirements:** the requirements for assurance which contribute to the overall confidence that the cryptographic module has been implemented correctly; and
3. **integration requirements:** the security services and assurance level that must be achieved by the trusted product. The integration requirements appear in the Cryptographic Modules Criteria as constraints to other security services and assurance levels.

If the cryptographic module is embedded within a product (i.e., the product provides the control and status interface for the cryptographic module), then additional security requirements are placed on the trusted product. The requirements are defined in the Cryptographic Module Criteria as constraints to security services which must be provided by the trusted product. These services are required in order to provide sufficient functionality to maintain a trusted interface between the cryptographic module and the host TCB during critical security operations.

Integration

In order to satisfy the constraints defined above, the following approach is taken in writing the Criteria for trusted products incorporating cryptography:

- The cryptographic module is evaluated against the Cryptographic Module Criteria and receives a rating corresponding to the level at which all of the requirements have been satisfied or exceeded.
- For the remainder of the evaluation, the cryptographic module is viewed as a black-box component (i.e., only the interface to the cryptographic module is considered). The internal functionality and the assurance documentation of the cryptographic module is not re-examined.
- The trusted product (i.e., all security services provided by the product) is evaluated to one of the CTCPEC assurance levels. The cryptographic module is considered a configuration item and all assurance requirements are applied to the cryptographic module interface. The trusted product must support all security services which are listed in the constraints section of the Cryptographic Module Criteria.
- The trusted product receives: a rating for each security service provided (e.g., CD-2, CR-1, XC-2, IS-1, WI-1), an assurance rating corresponding to the assurance achieved by all security services (e.g., T-2), and a rating for the cryptographic module (e.g., FL-2).

Under certain conditions, the assurance requirements as specified in the Cryptographic Module Criteria do not apply. An assumption made thus far was not to place any additional requirements on the evaluation of the cryptographic module other than those defined in the Cryptographic Modules Criteria (e.g., the CTCPEC assurance requirements are not directly applied to the internal components of the cryptographic module). This assumption made it necessary to specify, for each cryptographic module rating, the maximum assurance level which may be obtained by the composite trusted product. However, if a Vendor chooses to have the cryptographic module's internal components also meet the CTCPEC assurance requirements (in addition to the Cryptographic Modules Criteria), then the maximum assurance level constraints may not apply to the composite trusted product.

The cryptographic module and the host TCB can be viewed as two distinct entities if:

1. the cryptographic module is a stand-alone, inline module;
2. cryptography is used only to provide Exchange services (non-Exchange services are not provided through the use of cryptography via this cryptographic module); and
3. the host TCB and the cryptographic module cannot interfere with one another in any way.

In such cases, neither the minimum nor the maximum assurance constraints apply to the composite trusted product.

The presence of cryptography in a trusted product does not imply that it is sufficient or acceptable for use in any specific environment or application. A threat/risk analysis will identify the cryptographic module rating and the overall assurance rating required for use in a particular environment.

If cryptography is to be used for secure communications within the Government of Canada, it will require endorsement under the Cryptographic Endorsement and Assessment Program (CEAP). The Vendor is encouraged to contact the Industrial InfoSec Programs manager for further program information at:

Communications Security Establishment
Manager, Industrial InfoSec Programs
P.O. Box 9703 Terminal
Ottawa, Canada
K1G 3Z4
Telephone: (613) 991–7520

Export Controls

Depending upon the cryptographic implementation, export control restrictions may be placed on the product. This will have to be explored separately by contacting the Department of External Affairs:

Department of External Affairs
International Trade Canada
Export Control Division (ESE)
Lester B. Pearson Building
125 Sussex Drive, C-4
Ottawa, Canada
K1A 0G2
Telephone: (613) 996–2387

Advice concerning the technical aspects relating to export may be acquired by contacting the Communications Security Establishment, Director, Evaluation and Engineering Group:

Communications Security Establishment
Director, InfoSec Evaluation and Engineering Group
P.O. Box 9703 Terminal
Ottawa, Canada
K1G 3Z4
Telephone: (613) 991–7174

Structure of the Criteria

The Cryptographic Modules Criteria were developed to be consistent with the structure, format, and style of the CTCPEC. A complete description of the structure of the criteria may be found in the CTCPEC section "Structure of the Criteria."

Letter Codes

Each service is denoted by a two letter code followed by a dash and finally the service level. Unfortunately, it was not possible to come up with matching French equivalents to all the service level letter codes. Therefore, to maintain commonality and to minimize confusion, the French and English codes are identical.

Table 1 contains all the two letter level codes defined in these criteria.

Criteria	Letter Codes	Full Rating Title	Range		
Data Exchange	**XC**	Data Exchange **C**onfidentiality	XC-0	–	XC-4
	XI	Data Exchange **I**ntegrity	XI-0	–	XI-3
	XW	Data Exchange Authentication (**W**ho)	XW-0	–	XW-3
Cryptographic Modules	**FL**	**F**IPS 140-1 **L**evel	FL-1	–	FL-4

Table 1: Criteria Letter Codes

Constraints

As in the CTCPEC, constraints are used to indicate that other security services are required in order for a given security service to perform properly. The constraint list is a *minimal* list, therefore, the services listed may also be constrained by another service which may not be directly required.

Security services defined in the Cryptographic Modules Criteria may also be constrained by the functionality and assurance criteria defined in the CTCPEC.

Exchange Criteria

A product which is rated against the Exchange Criteria must provide services capable of exporting and importing TCB objects to or from unprotected external media. Exchange may be provided in a product through the use of *exchange confidentiality* services, *exchange integrity* services, and *exchange authentication* services.

Exchange Confidentiality

Exchange confidentiality services allow TCB objects to be exported to and imported from unprotected external media in a manner which protects against the unauthorized disclosure of information. Exchange confidentiality services provide protection against the disclosure of information from objects communicated between multiple TCBs or objects stored in external storage. The exchange confidentiality levels of service rate these services based on the strength of the mechanism and the granularity of control.

The application of an exchange confidentiality service to a TCB object exports an "encapsulated TCB object." The exchange criteria refer to two attributes of an encapsulated TCB object: information content, and representation.

Appendix A provides guidance on meeting the exchange confidentiality criteria.

XC–0
Non-compliant

This level is reserved for those products which have been evaluated under the Exchange Confidentiality service and have failed to meet the requirements of a higher level of service.

XC–1
Basic Exchange Confidentiality

The TCB shall enforce an approved exchange confidentiality policy to protect against information disclosure from encapsulated TCB objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection.

CONSTRAINT: FL-1

XC–2
Broadcast Exchange Confidentiality

The TCB shall enforce an approved exchange confidentiality policy to protect against information disclosure from encapsulated TCB objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection.

Requests to import an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process. Requests to export an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process.

Requests to assign or change an object's grade of protection shall be mediated by the TCB based upon the user tag of the requesting user or process and shall only be serviced for administrators or users to whom the required authority has been delegated by the system administrator.

CONSTRAINT: FL-1, **IS-1**

XC–3
Point-to-Point Exchange Confidentiality

The TCB shall enforce an approved exchange confidentiality policy to protect against information disclosure from encapsulated TCB objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection.

Requests to import an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process, **and upon the source of the encapsulated object**. Requests to export an object shall be mediated by the TCB based upon the tag of the interface process, **and upon the destination of the encapsulated object**.

The representation of an encapsulated TCB object shall be a function of the tag of the interface process, the tag of the TCB object which is encapsulated, and the source and destination of the encapsulated object.

Requests to assign or change an object's grade of protection shall be mediated by the TCB based upon the user tag of the requesting user or process and shall only be serviced for administrators or users to whom the required authority has been delegated by the system administrator.

CONSTRAINT: FL-1, IS-1, **XW-1**

XC–4
Channel Exchange Confidentiality

The TCB shall enforce an approved exchange confidentiality policy to protect against information disclosure from encapsulated TCB objects **and to protect against information disclosure by the observation or manipulation of the representations of encapsulated TCB objects or aggregations of encapsulated TCB objects**. The approved policy shall **apply to all TCB objects** and shall define the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection to TCB objects. **The policy shall include objects formed from the aggregation of encapsulated TCB objects.**

Requests to import an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process, and upon the source of the encapsulated object. Requests to export an object shall be mediated by the TCB based upon the tag of the interface process, and upon the destination of the encapsulated object.

The representation of an encapsulated TCB object shall be a function of the tag of the interface process, the tag of the TCB object which is encapsulated and the source and destination of the encapsulated object.

Requests to assign or change an object's grade of protection shall be mediated by the TCB based upon the user tag of the requesting user or process and shall only be serviced for administrators or users to whom the required authority has been delegated by the system administrator.

An analysis shall be conducted to identify covert communication channels. The maximum bandwidth (determined by actual measurement or by engineering estimate) of each covert communication channel shall be documented. Approved subsets of the covert channels shall be audited, reduced, or eliminated.

CONSTRAINT: FL-1, IS-1, XW-1, **WA-1**, **T-3**

Exchange Integrity

Exchange integrity services allow TCB objects to be exported to and imported from unprotected external media in a manner which protects against the unauthorized modification of information. Exchange integrity services provide protection against the modification of information in objects communicated between multiple TCBs or objects stored in external storage. The exchange integrity levels of service rate these services based on the strength of the mechanism and the granularity of control.

The application of an exchange integrity service to a TCB object exports an "encapsulated TCB object". The exchange criteria refer to two attributes of an encapsulated TCB object: information content, and representation.

Appendix A provides guidance on meeting the exchange integrity criteria.

XI–0
Non-compliant

This level is reserved for those products which have been evaluated under the Exchange Integrity service and have failed to meet the requirements of a higher level of service.

XI–1
Basic Exchange Integrity

The TCB shall enforce an approved exchange integrity policy to detect the modification of encapsulated TCB objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection.

CONSTRAINT: FL-1

XI–2
Broadcast Exchange Integrity

The TCB shall enforce an approved exchange integrity policy to detect the modification, **deletion, and replication** of encapsulated TCB objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, the objects to which grades of protection may be associated, and the abilities of users and/or processes to assign grades of protection.

Requests to import an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process. Requests to export an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process.

Requests to assign or change a TCB object's grade of protection shall be mediated by the TCB based upon the user tag of the requesting user or process and shall only be serviced for administrators or users to whom the required authority has been delegated by the system administrator.

CONSTRAINT: FL-1, **IS-1**

XI–3
Point-to-Point Exchange Integrity

The TCB shall enforce an approved exchange integrity policy to detect the modification, deletion, and replication of encapsulated objects. The approved policy shall define the set of objects and interface processes to which the policy applies, the grade or grades of protection provided by the encapsulation mechanism, and the abilities of users and/or processes to assign grades of protection to objects.

Requests to import an encapsulated TCB object shall be mediated by the TCB based upon the tag of the interface process, **and upon the source of the encapsulated object**. Requests to export an object shall be mediated by the TCB based upon the tag of the interface process, **and upon the destination of the encapsulated object**.

The representation of an encapsulated TCB object shall be a function of the tag of the interface process, the tag of the TCB object which is encapsulated and the source and destination of the encapsulated object.

Requests to assign or change an object's grade of protection shall be mediated by the TCB based upon the user tag of the requesting user or process and shall only be serviced for administrators or users to whom the required authority has been delegated by the system administrator.

CONSTRAINT: FL-1, IS-1, **XW-1**

Exchange Authentication

Exchange authentication services allow a TCB to provide proof of its identity to and to verify proofs of identity from other TCBs. TCBs which have exchanged and verified proof of identity will be said to have established a security association. The exchange authentication levels of service rate the services based upon the strength of the authentication mechanism.

Appendix A provides guidance on meeting the exchange authentication criteria.

XW–0
Non-compliant

This level is reserved for those products which have been evaluated under the Exchange Authentication service and have failed to meet the requirements of a higher level of service.

Exchange Criteria

XW–1
Peer-Entity Exchange Authentication

The TCB shall enforce an approved exchange authentication policy. The policy shall identify the attributes associated with a TCB necessary to establish a security association with another TCB.

The TCB shall use a protected mechanism to establish a security association with a TCB before communicating with that TCB.

Proof of identity shall be communicated using an approved authentication protocol.

CONSTRAINT: FL-1

XW–2
Data Origin Exchange Authentication

The TCB shall enforce an approved exchange authentication policy. The policy shall identify the attributes associated with a TCB necessary to establish a security association with another TCB.

The TCB shall use a protected mechanism to establish a security association with a TCB before communicating with that TCB. **The TCB shall employ a protected mechanism to associate a proof of origin with each encapsulated object. The TCB shall use a protected mechanism to verify that each encapsulated object imported to the TCB originated from a TCB with which a security association has been established.**

Proof of identity shall be communicated using an approved authentication protocol.

CONSTRAINT: FL-1

XW–3
Non-Repudiatable Exchange Authentication

The TCB shall enforce an approved exchange authentication policy. The policy shall identify the attributes associated with a TCB necessary to establish a security association with another TCB . **The policy shall also identify those circumstances under which an independent certification of a proof of identity is required.**

The TCB shall use a protected mechanism to establish a security association with a TCB before communicating with that TCB. The TCB shall employ a protected mechanism to associate a proof of origin with each encapsulated object. The TCB shall use a protected mechanism to verify that each encapsulated object imported to the TCB originated from a TCB with which a security association has been established.

Proof of identity shall be communicated using an approved authentication protocol. **The authentication protocol must permit proofs of identity to be certified by an independent third party.**

CONSTRAINT: FL-1

Cryptographic Module Criteria

A product under evaluation which uses cryptography to provide security services must have the cryptographic module evaluated against the Cryptographic Module Criteria. These Criteria provide both the *implementation* requirements for the cryptographic module and the *integration* requirements for embedding cryptographic modules in a trusted product. The integration requirements are presented as constraints to security services and to an appropriate level of assurance which is consistent with the cryptographic requirements.

Appendix B provides guidance on meeting the Cryptographic Module criteria.

Cryptographic Module Implementation

The cryptographic module implementation requirements reference the FIPS 140–1 (CDN) standard. This standard specifies the general security requirements that must be satisfied by a cryptographic module and includes functionality as well as assurance requirements.

FL-1

The cryptographic module shall meet the security level 1 requirements of FIPS 140–1 (CDN) with the exception of the "Operating System Security" requirements.

CONSTRAINT:

TCB requirements for all cryptographic modules:

T-1: The trusted product shall receive a T-1 assurance rating.

Additional host TCB requirements for embedded cryptographic modules:

IT-2: The TCB shall run a suite of self tests during initial start up and on demand in order to validate the correct operation of the critical portions of its interface to the cryptographic module.

Note: The composite TCB shall not receive an assurance rating of greater than T-1.

FL–2

The cryptographic module shall meet the security level **2** requirements of FIPS 140–1 (CDN) with the exception of the "Operating System Security" requirements.

CONSTRAINT:

TCB requirements for all cryptographic modules:

IB-2: The TCB shall be tamperproof and always invoked. The TCB shall protect from interference and tampering all critical cryptographic components and information under its control.

T-1: At a minimum, the trusted product shall receive a T-1 assurance rating.

Additional host TCB requirements for embedded cryptographic modules:

IT-2: The TCB shall run a suite of self tests during initial start up and on demand in order to validate the correct operation of the critical portions of its interface to the cryptographic module.

WI-1: The TCB shall be capable of associating an identity with each user of the product.

Note: The composite TCB shall not receive an assurance rating of greater than **T-2**.

FL–3

The cryptographic module shall meet the security level **3** requirements of FIPS 140–1 (CDN) with the exception of the "Operating System Security" requirements.

CONSTRAINT:

TCB requirements for all cryptographic modules:

IB-2: The TCB shall be tamperproof and always invoked. The TCB shall protect from interference and tampering all critical cryptographic components and information under its control.

T-2: At a minimum, the trusted product shall receive a T-2 assurance rating.

Additional host TCB requirements for embedded cryptographic modules:

IT-2: The TCB shall run a suite of self tests during initial start up and on demand in order to validate the correct operation of the critical portions of its interface to the cryptographic module.

WI-2: The TCB shall identify and authenticate each user of the product.

WT-2: At a minimum, there must be a trusted path to the cryptographic module for identification and authentication data and for key variable entry.

Note: The composite TCB shall not receive an assurance rating of greater than **T-4**.

FL–4

The cryptographic module shall meet the security level **4** requirements of FIPS 140–1 (CDN) with the exception of the “Operating System Security” requirements.

CONSTRAINT:

TCB requirements for all cryptographic modules:

IB-2: The TCB shall be tamperproof and always invoked. The TCB shall protect from interference and tampering all critical cryptographic components and information under its control.

T-3: At a minimum, the trusted product shall receive a T-3 assurance rating.

Additional host TCB requirements for embedded cryptographic modules:

IT-2: The TCB shall run a suite of self tests during initial start up and on demand in order to validate the correct operation of the critical portions of its interface to the cryptographic module.

WI-2: The TCB shall identify and authenticate each user of the product.

WT-2: At a minimum, there must be a trusted path to the cryptographic module for identification and authentication data and for key variable entry.

Note: The composite TCB shall not receive an assurance rating of greater than **T-5**.

Definitions

This list is to be used in association with the Definitions section of the CTCPEC Version 3.0e and the Definitions section of FIPS 140–1 (CDN). The terms listed in this section are only specific to this document.

A

There are no defined terms that begin with A.

B

There are no defined terms that begin with B.

C

Composite Trusted Product

The trusted product which includes the cryptographic module and the host TCB.

Control Information

Information that is entered into a cryptographic module for the purposes of controlling the operation of the module.

Critical Security Parameters

Security-related information (e.g., plaintext cryptographic keys, seed keys) whose disclosure and/or modification can compromise the security of a cryptographic module.

Cryptographic Boundary

An explicitly defined physical and logical contiguous perimeter that establishes the bounds of a cryptographic module.

Cryptographic Implementation Requirements

The functionality requirements which the cryptographic module must provide and the assurance requirements which the cryptographic module must satisfy.

Cryptographic Integration Requirements

The functionality requirements which the host TCB must provide and the assurance requirements which the host TCB must satisfy. These requirements are necessary in order for the host TCB to support the integration of cryptography with the product.

Cryptographic Key (Key)

A parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature, or
- a message authentication code (MAC).

Cryptographic Module

The set of hardware, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

D

There are no defined terms that begin with D.

E

Embedded Cryptographic Module

A cryptographic module for which interaction between the module and a user for the purpose of controlling are mediated by a host TCB.

Encapsulated TCB Object

A TCB object upon which an exchange service has been applied.

F

FIPS 140–1 (CDN)

The acronym used to refer to the Canadian equivalent to the *FIPS PUB 140–1: Security Requirements for Cryptographic Modules* published by the National Institute of Standards and Technology.

G

Grade of Protection

The protection provided by a cryptographic algorithm or other mechanism used to encapsulate TCB objects.

H

Host TCB

That part of the TCB which excludes the cryptographic module.

I

Inline Cryptographic Module

A cryptographic module in which the ciphertext interface communicates exclusively with external communications media (e.g. disk and tape drives, networks, modems, etc.)

Interface

A logical section of a cryptographic module that provides access to the module, including information flow and/or physical access.

Input Data

Information that is entered into a cryptographic module for the purposes of transformation or computation.

Interface Process

The program, process, or component which controls a particular unprotected export or import medium.

J

There are no defined terms that begin with J.

K

Key Management

The activities involving the handling of cryptographic keys during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archival.

L

There are no defined terms that begin with L.

M

There are no defined terms that begin with M.

N

There are no defined terms that begin with N.

O

Offline Cryptographic Module

A cryptographic module which acts as a cryptographic service provider to a host product; in particular, an offline cryptographic module may send encrypted text back to the host for further processing.

Output Data

Information that is to be output from a cryptographic module that has resulted from a transformation or computation in the module.

P

PIN

Personal Identification Number consisting of an alphanumeric code or password used to authenticate an identity.

Pin

A physical and electrical contact point of a port.

Private Key

A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Protected Media

A medium which is under control of the TCB or which must be placed under procedural safeguards.

Public Key

A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and possibly made public.

Public Key Certificate

Digitally signed information associated with an entity and that contains the entity's public key and unambiguously identifies the entity.

Q

There are no defined terms that begin with Q.

R

There are no defined terms that begin with R.

S

Security Association

A state in which multiple TCBs have exchanged and verified proof of identity.

Services

Shall refer to all of the services, operations or functions that can be performed by a cryptographic module. Each service shall result in a service output.

Secret Key

A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and not made public.

Stand-alone Cryptographic Module

A cryptographic module which interacts directly with a user for the purpose of controlling the module.

Status Information

Information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.

T

There are no defined terms that begin with T.

U

There are no defined terms that begin with U.

V

There are no defined terms that begin with V.

W

There are no defined terms that begin with W.

X

There are no defined terms that begin with X.

Y

There are no defined terms that begin with Y.

Z

There are no defined terms that begin with Z.

Bibliography

- Canadian System Security Centre *The Canadian Trusted Computer Product Evaluation Critiera.* Version 3.0e, January 1993.
- Canadian System Security Centre *The Canadian Trusted Computer Product Evaluation Critiera.* Draft Version 3.0e, April 1992.
- Canadian System Security Centre *Proceedings from the Canadian Trusted Computer Product Evaluation Criteria Workshop.* August 4 – 5, 1988.
- Canadian System Security Centre *Proceedings of the 1990 CTCPEC Availability Workshop.* February 6 – 7, 1990.
- Computer Systems Research Institute, University of Toronto *Composability of Trusted Systems.* Reports 1 – 5 [October 16, 1989, January 31, 1990, May 31, 1990, September 31, 1990, January 31, 1991]. B. Thompson, R. Soper, P.I.P. Boulton, E.S. Lee, authors.
- Department of Defense *Trusted Computer System Evaluation Criteria.* DoD 5200.28–STD, December 1985.
- Department of Defense *Magnetic Remanence Security Guideline.* DoD CSC-STD-005–85, November 15, 1985.
- National Computer Security Center *A Guide to Understanding Audit in Trusted Systems.* NCSC-TG-001, Version-2, June 1, 1988.
- National Computer Security Center *A Guide to Understanding Discretionary Access Control in Trusted Systems.* NCSC-TG-003, Version-1, September 30, 1987.
- National Computer Security Center *Trusted Network Interpretation.* NCSC-TG-005, Version-1, July 31, 1987.
- National Computer Security Center *A Guide to Understanding Configuration Management in Trusted Systems.* NCSC-TG-006, Version-1, March 28, 1988.
- National Computer Security Center *A Guide to Understanding Design Documentation in Trusted Systems.* NCSC-TG-007, Version-1, October 2, 1988.
- National Computer Security Center *Computer Security Subsystem Interpretation.* NCSC-TG-009, Version-1, September 16, 1988.

Bibliography

- ☐ National Computer Security Center *Rating Maintenance Phase Program Document.* NCSC-TG-013, Version-1, June 23, 1989.
- ☐ National Computer Security Center *A Guide to Understanding Object Reuse in Trusted Systems (Draft).* NCSC-TG-018, Version-1, September 15, 1989.
- ☐ National Computer Security Center *Trusted Database Management System Interpretation.* NCSC-TG-021, Version-1, April 1991.
- ☐ *Information Technology Security Evaluation Criteria.* Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom. Version 1, May 2, 1990
- ☐ Zentralstelle für Sicherheit in der Informationstechnik (ZSI)*IT – Security Criteria.* Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems. Version 1, 1989.
- ☐ U.S. Department of Commerce/National Institute of Standards and Technology *Security Requirements for Cryptographic Modules (Draft).* Federal Information Processing Standards Publication (FIPS) 140–1, July 13, 1990.
- ☐ IEEE *Proceedings of the Security and Privacy Symposium.* Oakland, California. 1980 – 1991, inclusive.
- ☐ IEEE *Proceedings of the Computer Security Applications Conference (original title: Aerospace Computer Security Applications Conference).* 1985 – 1989, inclusive.
- ☐ National Insitute of Standards and Technology *National Computer Security Conference.* 1984, 1988, 1989.
- ☐ National Institute of Standards and Technology *Report on the Invitational Workshop on Data Integrity.* NIST Special Publication 500–168, September 1989. Zella G. Ruthberg, William T. Polk editors.

APPENDICES

APPENDIX A A Guide to Exchange

Introduction

This appendix provides a general guide to understanding data exchange services in the criteria. Data exchange services apply to the communication of TCB objects between TCBs over unprotected media. TCB objects are encapsulations of computing resources which may be activated, manipulated and exported.

Scope

The guidelines established in this appendix apply to products under evaluation with the intention of meeting the Exchange Confidentiality criteria (XC-1 to XC-4), Exchange Integrity criteria (XI-1 to XI-3), or Exchange Authentication criteria (XW-1 to XW-3).

This appendix is intended as guidance only, and neither replaces nor supersedes the requirements expressed in the Criteria. Examples are given for illustrative purposes only and do not represent the only acceptable approach to satisfying the criteria.

The Role of Data Exchange Criteria

In a distributed environment, multiple TCBs (or TCB subsets [5]) may exist with the possibility of each TCB enforcing a different policy with different classes of objects. (See figure 1.) Criteria for data exchange services apply to the exchange of TCB objects between possibly diverse TCBs over unprotected media. Criteria for data exchange services do not address the coordination of the various TCBs into a useful whole; instead, exchange criteria provide necessary building blocks for the integration of evaluated components into a useful whole.

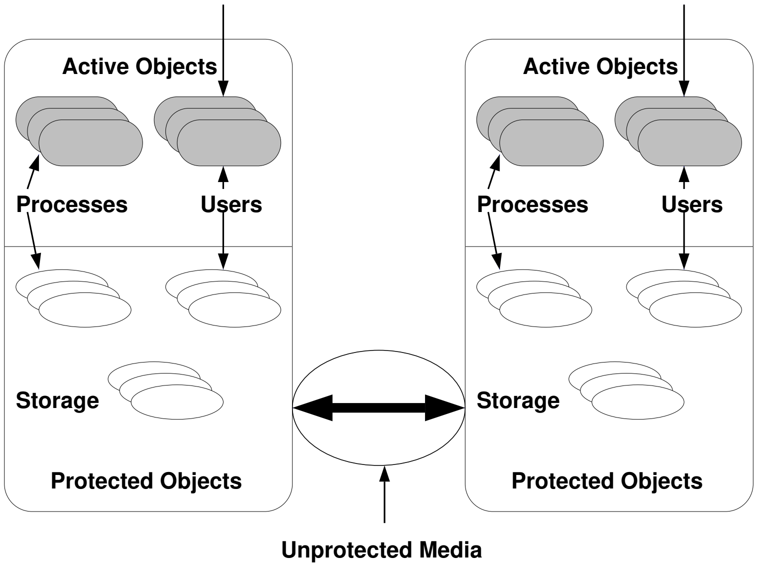

Figure 1: Trusted Distributed Environment

Many of the security concerns addressed by the data exchange services can be addressed by applying the requirements of the Criteria (e.g., architectural requirements of the Assurance Criteria, an interpretation of the IB requirements) to the unprotected distributed environment. The advantage of distinguishing data exchange services as distinct criteria is manifest in the expressive power of the criteria. Issues addressed by data exchange services are explicitly declared in the rating rather than buried in a final evaluation report. By explicitly rating the data exchange service, it is possible to distinguish between a product which has been evaluated for a protected environment and one which has been evaluated for an unprotected distributed environment. For example, an operating system can be evaluated for a protected environment (that is, data exchange services are not supported in the evaluated product) or the evaluation may take account of communications security features as done in a TNI type evaluation. The use of data exchange criteria permits one to more precisely characterize these differences between such products.

The criteria are intended to be policy independent. Consequently they do not reflect constraints imposed by other standards or policy documents within the government of Canada. However, the criteria have been designed to co-exist with the OSI security architecture [2].

The Trusted Distributed Environment

A trusted computing base encapsulates computing resources in the form of objects and manages the interaction of these objects in accordance with a given security policy. Computing resources include volatile and persistent storage, processors, and communications equipment and infrastructure. When encapsulated as a TCB object, a computing resource has two aspects: one logical and the other physical. The logical aspect of an object captures the information content of the object; that is, it provides semantics or meaning. The physical aspect of an object is its representation or syntax.

An object is an encapsulation of a computing resource; that is, an object encapsulates state (or information content) and behaviour. An object's visible or exportable state is characterized by its attributes. An object's behaviour defines the manner in which an object's state may change. An object is active if it is able to respond to stimuli and change state; otherwise an object is passive. An object requires the support of some form of a computational engine to become active, consequently, objects are exported from the TCB in a passive state.

A stand-alone trusted operating system manages the logical aspect of its objects. The physical representation of objects is protected against manipulation by internal objects only. An object's representation is not protected against manipulation by entities external to the system; for example, a file may be tampered with offline. It is assumed that the system administrators will enforce procedural safeguards to protect against manipulation of this kind. (Note, some protections, such as trusted distribution and generation, are afforded at the higher assurance levels.) Volatile storage objects such as random access memory and inter-process communications are not considered vulnerable since they are present only during the operation of the system.

In a distributed environment, one cannot necessarily assume that external entities will not have access to the physical representations of TCB objects. This is particularly true of communications between distributed components. In many circumstances it may also apply to persistent storage objects as well. In fact, in a distributed environment, the line between volatile and persistent storage becomes blurred. Consequently, TCB objects must be protected whenever they are exported from a physically secure environment.

Data Exchange and Network Security

Data exchange criteria facilitate the evaluation of network components. The security policy for data exchange services establishes the objects which are imported to and exported from the TCB and specifies the protection afforded to these objects. For example, an exported user object may have USER_ID, PASSWORD, and PRIVILEGES as attributes; the security policy for the Exchange Confidentiality and Exchange Integrity services specifies the users and processes allowed to export or import a user object, the interfaces through which an object may be imported or exported, and the grade of protection (e.g., a one-way algorithm for password protection or DES) afforded the object by the encapsulation mechanism. An exported file object may have ACCESS_MODES, OWNER, and DATA as attributes, where OWNER is a user object; the security policy for Exchange Confidentiality services may specify, among other things, that the DATA attribute must be protected by encryption suitable for designated information; the security policy for Exchange Integrity requirements may specify that all attributes must be protected by a commercial grade digital signature. If these services are intended for a wide area network, the security policy may require that the Exchange Confidentiality and integrity services be supported by an Exchange Authentication service. As a result, the data exchange services may be used to specify both the communication and composability requirements found in [4].

Data Exchange and Distributed Operating Systems

TCB objects are not restricted to files, network connections, and user identities. For example, a process consisting of identifying attributes and its current state of computation may be an exportable object. It may be protected by a broadcast Exchange Integrity and confidentiality services supported by peer-entity Exchange Authentication. In this way one can specify the security requirements for a redundant cluster or a distributed network operating system supporting load balancing.

Data Exchange and Data Base Security

A distributed data base management system often requires TCBs (called TCB subsets in [5]) to enforce different security policies. The security policy for a product with rated data exchange services will specify the objects and their attributes which will be exported from a TCB. By designing exported objects to be common to all TCB (subsets), the interactions of the diverse policies can be managed.

Alternately, an integrator can introduce components which provide the required translations between objects exported from TCBs (or TCB subsets). The presence of rated data exchange services provides the integrator with the knowledge that the TCBs have been evaluated to properly import and export certain types of objects; that the TCB perform certain types of object mediation upon import and export; and that the encapsulated objects are afforded the specified protection.

Exchange Confidentiality

Exchange Confidentiality criteria provide a rating scale for security mechanisms which protect against unauthorized disclosure. Each level of the Exchange Confidentiality criteria characterize a class of services which provide safeguards against a set of vulnerabilities. The ordering of the criteria is based on the inclusion relation between the sets of vulnerabilities countered; that is, services satisfying a higher rating class safeguard against a larger set of vulnerabilities than services in a lower rating class.

The criteria are intended to be policy independent. The precise specification of a service satisfying any of these criteria is determined by its policy model (or simply policy for T1 level assurance). This policy model will address issues such as the granularity of protection, the strength of the cryptographic or other mechanisms (referred to as the grade of protection in the criteria), key management, acceptable covert channel bandwidth and the definition of traffic flow information.

Encryption is the most common mechanism used to implement Exchange Confidentiality services. In all cases the cryptographic algorithm used and its implementation must be approved by CSE. The choice of algorithm and implementation may also limit the applications to which the product may be applied. It is also recognized that in some products there may be more that one encryption algorithm available. The protection provide by a particular algorithm is referred to as "the grade of protection" in the criteria.

Table 2 provides a summary of the Exchange Confidentiality services.

	Exchange Confidentiality Service			
Safeguard Against	XC-1	XC-2	XC-3	XC-4
Passive Eaves Dropping	X	X	X	X
User Error		X	X	X
Intentional Policy Bypass		X	X	X
Cross Talk			X	X
Covert Channels				X
Traffic Flow Analysis				X

Table 2 Threats Countered by Exchange Confidentiality

Meeting The Criteria

XC-1: Basic Data Confidentiality This level is intended to provide basic data confidentiality. Services rated at this level are suitable for an environment in which the host provides little or no internal security functionality. A personal computer employing an encrypted file system is a candidate for an XC-1 rating. Another application which is a candidate for an XC-1 rating is an e-mail package providing users with the option to encrypt their messages.

Services satisfying XC-1 counter vulnerabilities arising from passive eavesdropping on communication links or scavenging from external storage. Services satisfying XC-1 do not in general provide safeguards against user error, or overt intentional disclosure of information.

It is possible for a product to receive an XC-1 rating by using software cryptography meeting FL-1 running over an untrusted operating system. In this situation, one cannot assume that either the XC-1 service or the cryptography on which it is based is protected from tampering; that is, the product is unlikely to receive an IB-1 rating.

An example of a more secure implementation of an XC-1 service is provided by an hardware based encryption device which directs its output directly to the target storage or communications media. An XC-1 service implemented in this manner is likely immune to tampering; that is the service is supported by an IB-1 rating. However, since access to the target media relies on untrusted software, one cannot assume that the service cannot be bypassed.

A third implementation of an XC-1 service which is both tamper-proof and complete (not by-passable) is a hardware based inline cryptographic module. An inline cryptographic module controls the interface to the communication or storage media which is to be protected. As such, it is not possible to bypass the protection mechanism unless authorized to do so. An implementation of this type is likely to be supported by an IB-1 rating.

It is possible for a security policy for XC-1 to specify a different grade of protection for certain objects. For an XC-1 service, it is most likely that a grade of protection will be assigned to a device. For example, a workstation may protect its communications ports with DES encryption, use a weaker encryption for certain sensitive files, such as the password file, and use triple DES to exchange key information.

XC-2: Broadcast Exchange Confidentiality This level is intended to provide basic data confidentiality and control over the manner in which objects are imported and exported. Services satisfying XC-2 are best suited for "system high" type environments in which the dominant threat to information comes from agents without authorization to access the system, as would be the case in which two dedicated LANs share a common backbone. XC-2 services assume the host TCB is capable of performing mediation based on process tags. However, they do not assume facilities for object labelling.

Services satisfying XC-2 counter vulnerabilities arising from passive eaves dropping, scavenging through storage media, user error, and overt intentional disclosure of information. Services satisfying XC-2 do not provide community-of-interest separation, nor cryptographic separation between classes of objects. Consequently services satisfying XC-2 are not suitable for a system with TCBs supporting different security policies or TCBs with different privileges.

A service rated against the XC-2 level must provide a basic level of protection for TCB objects designated for protection. The protection afforded encapsulated TCB objects may be universal. For example, a single cryptographic key may be used to conceal the information in all encapsulated objects.

A service rated at XC-2 must mediate access to communications. This mediation must, at a minimum, be based on the identity of the protocol or interface process controlling the communications and must be defined by the system administrators. The access mediation need not be restricted to the identity interface process, it may extended to include attributes of users or objects as well. For example, an XC-2 may allow all users to export objects to a back-up device, but allow only system administrators to restore objects from the back-up device. An XC-2 service may permit TCBs to communicate via a messaging package, but deny all other communications.

The introduction of limited access mediation is the primary difference between XC-1 and XC-2. Services rated at XC-2 require the TCB to provide finer control over communications than XC-1 rated services, while still assuming minimum TCB functionality and simple key management schemes.

XC-3: Point-to-Point Exchange Confidentiality This level is intended to provide fine grained data confidentiality, control over the manner in which objects are imported and exported, and cryptographic separation between communication channels. Services at this level are motivated by the confidentiality requirements of multi-level and compartmented mode systems.

Services satisfying XC-3 counter vulnerabilities arising from passive eaves dropping, user error, overt intentional disclosure of information, and TCBs supporting varying degrees of privilege or different policies. Services at XC-3 do not safeguard against sensitive information being deduced from the communications traffic (i.e., traffic analysis), nor do they protect against covert communications channels.

A service rated against the XC-3 level must provide separation between groups of users and categories of information. For example, a unique cryptographic key is assigned to each classification level in a multi-level system to provide cryptographic separation between levels. Cryptographic separation may also be used to separate communities of interest.

In addition to providing access mediation to interface processes, a service rated at XC-3 must represent an encapsulated object in such a manner that the representation is a function of the object tag and the tag of the interface process. At XC-2, an encapsulated object is a function solely of the exported data. A service rated at XC-3 may compute the representation of encapsulated objects based on other aspects of the system state in addition to the object tag and the interface process tag.

The introduction of fine grained cryptographic separation and mediation based upon the source and destination distinguish services at XC-3 from those at XC-2. As a result services at XC-3 must be supported by peer-entity authentication and by sophisticated key management schemes.

XC-4: Channel Exchange Confidentiality This level is intended for an environment in which all data communicated between TCBs requires protection from eaves-dropping and in which secondary aspects of communications must be protected from disclosure. Services at this level are motivated by the confidentiality requirements of multi-level systems in which covert communication channels are an issue and in which traffic flow information must be protected.

Services satisfying XC-4 counter vulnerabilities arising from passive eaves dropping, user error, overt intentional disclosure of information, TCBs of varying capabilities, disclosure of sensitive information along covert communications channels, and eaves-droppers deducing sensitive information by observing network traffic (i.e., traffic analysis).

A covert channel analysis must be conducted for services satisfying XC-4. It is recognized that most communications protocols have large covert channels and that their elimination may adversely affect the performance, integrity, and availability of communications. Consequently, one is required first to provide an analysis to identify and measure the covert channels. Those covert channels which can be eliminated in a manner consistent with performance and other security requirements will be included in the approved subset of covert channels to be eliminated. Those which cannot be eliminated but can be reduced in a manner consistent with performance and other requirements will be included in the approved subset of covert channels to be reduced. Those which cannot be eliminated but can be audited will be included in the approved subset of covert channels to be audited. The reader is referred to a Guide to Covert Channels in [1] for further guidance with respect to the analysis, auditing, and elimination of covert channels.

The security policy for an XC-4 service must define "traffic object". These are second order objects which are formed either from secondary attributes of the representation of an encapsulated objects or from aggregations of encapsulated objects. These objects need not be discrete; they may be objects which convey fuzzy or probabilistic information. For example, the level of activity at a particular site may be sensitive information. The associated object may be described as a probability distribution on the volume of communications traffic in a fixed time period. A mechanism which protects this composite object ensures that the actual observed probability distribution differs from the distribution defining the object by an amount which is not statistically significant.

Services rated at XC-4 differ from those at XC-3 in three respects: all exported objects are protected, covert channels are addressed, and traffic flow objects are defined and protected.

Exchange Integrity

Exchange Integrity criteria provide a rating scale for security mechanisms which protect against undetected, unauthorized modification of objects when communicated between TCBs. Each level of the Exchange Integrity criteria characterize a class of services which provide safeguards against a set of vulnerabilities. The ordering of the criteria is based on the inclusion relation between the sets of vulnerabilities countered; that is, services satisfying a higher rating class safeguard against a larger set of vulnerabilities than services in a lower rating class.

The criteria are intended to be policy independent. The precise specification of a service satisfying any of these criteria is determined by its policy model (or simply policy for T1 level assurance). This policy model will address issues such as the granularity of protection, the strength of the cryptographic or other mechanisms (referred to as the grade of protection in the criteria) and key management.

Digital signatures and message authentication codes are the primary mechanisms used to implement Exchange Integrity services. In all cases the cryptographic algorithm used and its implementation must be approved by CSE. The choice of algorithm and implementation may also limit the applications to which the product may be applied. It is also recognized that in some products there may be more that one algorithm available. The protection provide by a particular algorithm is referred to as "the grade of protection" in the criteria.

Table 3 provides a summary of the Exchange Integrity services.

	Exchange Integrity Service		
Safeguard Against	XI-1	XI-2	XI-3
Undetected Unauthorized Modification	X	X	X
User Error		X	X
Intentional Policy Bypass		X	X
Manipulation of Channel (e.g., message sequencing and message replay)		X	X
Undetected Improper Modification			X

Table 3 Threats Countered by Exchange Integrity

Meeting The Criteria

XI-1: Basic Data Integrity This level is intended to provide basic data integrity. Services rated at this level are suitable for an environment in which the host provides little or no internal security functionality. A personal computer with digital signatures on all executables is a candidate for an XI-1 rating. Another application which is a candidate for an XI-1 rating is an e-mail package providing users with the option to digitally sign their messages.

Services satisfying XI-1 counter vulnerabilities arising from non-random manipulation of communicated objects. When used in conjunction with non-repudiation services (XW-3) and user identification and authentication, they provide individuals with a means to deter fraudulent manipulation of individual communications. Services satisfying XI-1 do not safeguard against user error, nor overt attempts to bypass the integrity policy.

It is possible for a product to receive an XI-1 rating by using software cryptography meeting FL-1 running over an untrusted operating system. In this situation, one cannot assume that either the XI-1 service or the cryptography on which it is based is protected from tampering; that is, the product is unlikely to receive an IB-1 rating.

An example of a more secure implementation of an XI-1 service is provided by an hardware based device which directs digitally signed output directly to the target storage or communications media. An XI-1 service implemented in this manner is likely immune to tampering; that is the service is supported by an IB-1 rating. However, since access to the target media relies on untrusted software, one cannot assume that the service cannot be bypassed.

A third implementation of an XI-1 service which is both tamper-proof and complete (not by-passable) is a hardware based inline cryptographic module. An inline cryptographic module controls the interface to the communication or storage media which is to be protected. As such, it is not possible to bypass the protection mechanism unless authorized to do so. An implementation of this type is likely to be supported by an IB-1 rating.

It possible for a security policy for XI-1 to specify a different grade of protection for certain objects. For an XI-1 service, it is most likely, that a grade of protection to be assigned to a device. For example, a workstation may protect its network layer communications with a public key algorithm, use an X9.9 compliant message authentication code for electronic data interchange, and sign executables with a proprietary algorithm.

XI-2: Broadcast Exchange Integrity This level is intended to provide basic data integrity and control over the manner in which objects are imported and exported. Services satisfying XI-2 are best suited for system high type environments in which the dominant threat to information comes from agents without authorization to access the system as would be the case in which two local area networks share a common backbone. XI-2 services assume the host TCB is capable of performing mediation based on process tags, however, they do not assume facilities for object labelling.

Services satisfying XI-2 counter vulnerabilities arising from unauthorized or improper modification of data, manipulation of message sequences, corruption of communication buffers, message replay, user error, and overt attempt to bypass the integrity policy.

A service rated against the XI-2 level must provide a basic level of protection for TCB objects designated for protection. The protection afforded encapsulated TCB objects may be universal. For example, a single cryptographic key may be used to digitally sign the information in all encapsulated objects.

A service rated at XI-2 must mediate access to communications. This mediation must, at a minimum, be based on the identity of the protocol or interface process controlling the communications and must be defined by the system administrators. The access mediation need not be restricted to the identity interface process, it may extended to include attributes of users or objects as well. For example, an XI-2 may allow all users to export objects to a back up device, but allow only system administrators to restore objects from the back up device. An XI-2 service may permit TCBs to communicate via a messaging package, but deny all other communications.

The introduction of limited access mediation is the primary difference between XI-1 and XI-2. Services rated at XI-2 require the TCB to provide finer control over communications than XI-1 rated services, while still assuming minimum TCB functionality and simple key management schemes.

XI-3: Point-to-Point Exchange Integrity This level is intended to provide fine grained data integrity, control over the manner in which objects are imported and exported, and cryptographic separation between communication channels. Services at this level detect modification, deletion and repetition of encapsulated objects. Unlike confidentiality services which prevent the leakage of information or cross-talk between communication channels, integrity service detect interference between communication channels. Services at this level are motivated by the integrity requirements of products which process multiple types of constrained data items [5] and maintain fine grained control over authorizations.

Services satisfying XI-3 counter vulnerabilities arising from non-random manipulation of message sequences, non-random corruption of communication buffers by techniques such as message replay, non-random manipulation of data, user error, and overt attempt to bypass the integrity policy.

A service rated against the XI-3 level must provide separation between groups of users and categories of information. For example, a unique cryptographic is assigned to each type of constrained data item. This allows remote processes to verify the type of imported objects before processing. Cryptographic separation may also be used to separate communities of interest.

In addition to providing access mediation to interface processes, a service rated at XI-3 must represent an encapsulated object in a such a manner that the representation is a function of the object tag and the tag of the interface process. At XI-2, an encapsulated object is a function solely of the exported data. A service rated at XI-3 may compute the representation of an encapsulated objects based on other aspects of the system state in addition to the object tag and the interface process tag.

Protection against replication and deletion and the introduction of fine grained cryptographic separation and mediation based upon the source and destination distinguish services at XC-3 from those at XC-2. As a result services at XI-3 must be supported by peer-entity authentication and by sophisticated key management schemes.

Exchange Authentication

Exchange Authentication criteria are the counterpart to user identification and authentication and trusted path services in [1]. Whereas user identification and authentication, authenticates the identity of a user at the product's interface, Exchange Authentication provides authentication of TCBs. Services rated against Exchange Authentication criteria provide varying degrees of protection against entities masquerading as TCBs. Services rated against these criteria provide necessary support for confidentiality, integrity, and availability policies. The specification of the authentication protocol constitutes the policy for these criteria.

Table 4 provides a summary of the Exchange Integrity services.

	Exchange Authentication Service		
Safeguard Against	XW-1	XW-2	XW-3
Masquerade Attacks	X	X	X
Hijack Attacks		X	X
Deniability			X

Table 4 Threats Countered by Exchange Authentication

Meeting The Criteria

XW-1: Peer-Entity Authentication This level is intended for environments in which a TCB need authenticate itself before communicating with another TCB. A LAN environment in which portable workstations are frequently connected and disconnected is an example of such an environment. Another example of an environment for which services at this level are suitable would be a LAN environment with low to moderate sensitivity supporting remote connections. Services satisfying XW-1 provide a safeguard against a rogue system masquerading as a valid TCB at the establishment of a security association.

Note, this level is analogous to user identification and authentication.

XW-2: Data Origin Authentication This level is intended for environments in which TCBs must provide continual proof of their identity. Such would be the case in a wide area network supporting critical applications. Services satisfying XW-2 safeguard against both masquerade attacks, and hijack attacks (i.e., manipulation of a connection by an unauthorized party after it has been established and authenticated.)

Services at the XW-2 do not provide non-deniability; that is, the proof of authentication is witnessed only by the communicating TCBs and not by an independent third party.

Note, services rated at XW-2 are analogous to trusted path services.

XW-3: Non-Repudiatable Exchange Authentication This level is intended for environments in which TCBs must provide continual proof of their identity and for certain transactions this proof must not be deniable. Electronic data interchange and electronic fund transfer environments often bear this requirement. Services satisfying XW-3 safeguard against masquerade attacks, hijack attacks, and fraudulent behaviour.

Services at the XW-3 do provide non-deniability; that is, the proof of authentication is witnessed by an independent third party. One may implement the third party witness as an authentication server. Another approach to implementing a third party witness is to have a server act as a notarization authority, providing TCBs with credentials in the form of signed certificates. The difference between services at the XW-2 and XW-3 is analogous to the difference between signing a contract and having the contract notarized.

References

[1] Communications Security Establishment, *The Canadian Trusted Computer Product Evaluation Criteria*, January 1993.

[2] International Standards Organization, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*, ISO 7498-2, February, 1989.

[3] U.S. Department of Defense, *Trusted Computer Security Evaluation Criteria*, DOD 5200.28–STD, December 1985.

[4] U.S. National Computer Security Center, *Trusted Network Interpretation (TNI)*, NCSC-TG-005, Version 1, July 1987.

[5] U.S. National Computer Security Center, *Trusted Database Management System Interpretation (TDI)*, NCSC-TG-021, April 1991.

[6] Financial Institution Message Authentication (Wholesale), American National Standard, ANSI X9.9, 1986.

[7] D.D. Clarke and D.R. Wilson, *A Comparison of Commercial and Military Computer Security Policies*, In Proceedings of the IEEE Symposium on Security and Privacy, Oakland CA, 1987.

APPENDIX B A Guide to Cryptographic Modules

Introduction

This appendix provides a general guide to understanding Cryptographic Modules in these Criteria. Cryptographic modules are intended to provide the following classes of service: encryption/decryption; the generation of digital signatures; key distribution; key generation; and/or key management. This appendix discusses considerations for designing mechanisms to meet the Cryptographic Modules Criteria.

The security requirements for Cryptographic Modules have been adopted from the National Institute of Standards and Technology *FIPS PUB 140–1: Security Requirements For Cryptographic Modules (Draft)* [1]. The integration requirements are derived from Appendix I of the CTCPEC Draft Version 3.0 [8].

Scope

The guidelines established in this appendix apply to products under evaluation with the intention of meeting the Cryptographic Modules Implementation requirements (FL-1 to FL-4).

This appendix is intended as guidance only, and does not replace or supercede the requirements expressed in these Criteria. Examples are given as illustration only and are not the only acceptable solution in meeting these Criteria.

Overview

Cryptographic Algorithms

If cryptography is used to provide Exchange services, the cryptographic module must implement a Cryptographic Endorsement and Assessment Program (CEAP) approved algorithm. The security requirements in these Criteria have been designed to minimize the effort required to obtain a CEAP endorsement. The Vendor is encouraged to contact the TPEP manager to discuss the possibility of combining a rating under the TPEP and endorsement under the CEAP with a single submission.

Configurations

The term *configuration* is used to describe a specific implementation of a cryptographic module into a trusted product. Figure 2 illustrates several configurations of a cryptographic module: cryptographic module 1 has been implemented as a trusted application, cryptographic module 2 has been implemented as part of the TCB, and cryptographic module 3 has been implemented as a peer to the TCB. Combinations of these implementations are also possible (e.g., a cryptographic module could for the most part run as an application but have some low-level device drivers as part of the TCB).

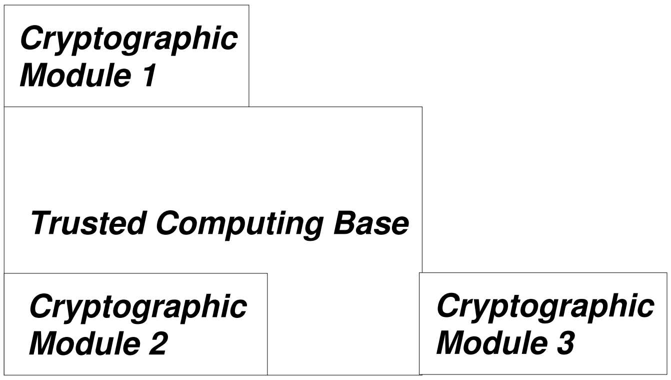

Figure 2: Cryptographic Module Configurations

The configuration of the cryptographic module with respect to the TCB is important in helping to define the dependencies between the cryptographic module and the TCB. For example, since cryptographic module 2 and the TCB are implemented as one entity, it is essential that neither component interfere with the operations of the other component. For these reasons, constraints have been developed which specify the minimum and maximum TCB assurance level required for each cryptographic module implementation level (FL-x levels).

Integration

Four methods of integrating a cryptographic module into a trusted product are identified in this document: stand-alone inline, embedded inline, stand-alone offline, and embedded offline.

Control Interface Implementations A cryptographic module is considered to be **stand-alone** if it provides its own physical security and if all security critical control information (e.g. identification and authentication) is input by an interface which is external to the host TCB; if all security critical status information (e.g., audit and alarms) is output by an interface external to the host; and if key data is input only through an interface external to the host TCB. Critical interaction between a user and a stand-alone cryptographic modules are not mediated by a host TCB system.

A cryptographic module is **embedded** if it is not stand-alone. Embedded cryptographic modules rely on the host TCB to mediate interaction with a user. Figure 3 illustrates the difference between a stand-alone and an embedded cryptographic module.

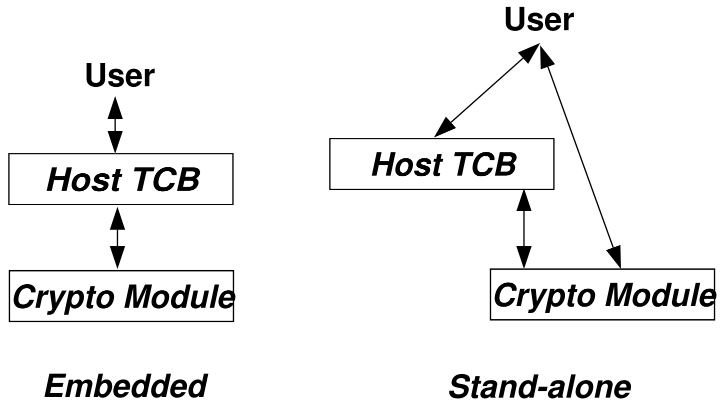

Figure 3: Control Interface Implementations

The control interface implementation is important in determining the security services which must be provided by the host TCB. In a stand-alone configuration, critical security parameters are only entered via the control interface of the cryptographic module. The control interface was examined during the evaluation of the cryptographic module itself. However, in an embedded configuration, critical security parameters must be entered to the host TCB and then passed on to the cryptographic module. Several important security services are therefore required and are included as constraints in the Cryptographic Module Criteria.

Ciphertext Interface Implementations A cryptographic module is considered to be **inline** if the export media can be accessed only through the ciphertext interface of the cryptographic module; for example, a cryptographic module which implements its own communications controller would be considered inline for devices connected to that controller.

A cryptographic module is considered to be **offline** if the ciphertext interface communicates directly with the host TCB. Figure 4 illustrates the difference between a stand-alone and an embedded cryptographic module.

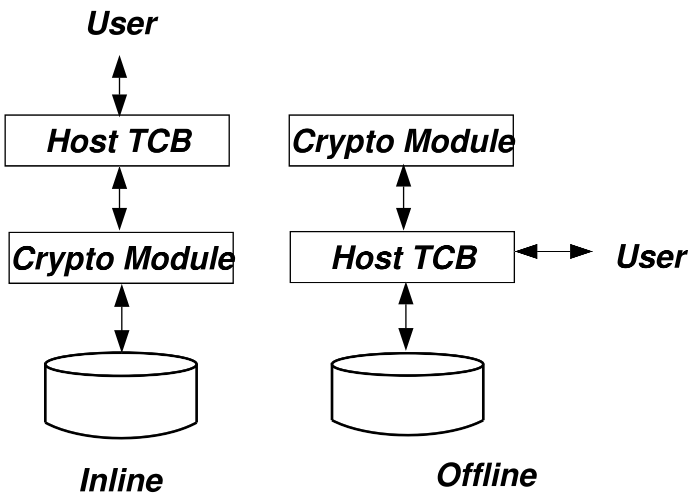

Figure 4: Ciphertext Interface Implementations

Offline cryptographic modules require that the host TCB be capable of maintaining the separation of plaintext and ciphertext. The Crytographic Modules criteria do not specify the specific mechanisms that must be used to enforce this separation. However, it must be clear from the design of the trusted product that the host TCB maintains plaintext and ciphertext separation for all services implemented via cryptography.

TCB Assurance Constraints

Under certain conditions, the assurance requirements as specified in the Cryptographic Module criteria do not apply. An assumption made thus far was not to place any additional requirements on the evaluation of the cryptographic module other than those defined in the Cryptographic Modules criteria (e.g., the CTCPEC assurance requirements are not directly applied to the internal components of the cryptographic module). This assumption made it necessary to specify, for each cryptographic module rating, the maximum assurance level which may be obtained by the composite trusted product. However, if a Vendor chooses to have the cryptographic module's internal components also meet the CTCPEC assurance requirements (in addition to the Cryptographic Modules criteria), then the maximum assurance level constraints do not apply to the composite product.

The cryptographic module and the host TCB can be viewed as two distinct entities if:

1. the cryptographic module is a stand-alone, inline module;
2. cryptography is used only to provide Exchange services (non-Exchange services are not provided through the use of cryptography via this cryptographic module); and
3. the host TCB and the cryptographic module cannot interfere with one another in any way.

In such cases, neither the minimum nor the maximum assurance constraints apply to the composite trusted product.

Meeting the Criteria

The *Validation Requirements for FIPS PUB 140–1: Security Requirements for Cryptographic Modules [7]* document describes the test methods that will be used by validation laboratories to test whether a cryptographic module conforms to the requirements of FIPS 140–1. As such, Vendors are directed to this document in order to obtain an explanation of the FIPS 140–1 requirements and to determine the evidence required to meet these requirements.

References

[1] U.S. Department of Commerce, National Institute of Standards and Technology. *Security Requirements For Cryptographic Modules (Draft)*, Federal Information Processing Standards Publication FIPS PUB 140–1, May 1993

[2] U.S. Department of Commerce, National Institute of Standards and Technology. *General Security Requirements for Equipment Using the Data Encryption Standard*, Federal Information Processing Standards Publication FIPS PUB 1027, April 1982

[3] Communications Security Establishment, *Federal Standard 1027: General Security Requirements for Equipment Using the Data Encryption Standard*, CID 09/11(1) April 1985

[4] National Computer Security Center. *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG 005 version-1, July 1987

[5] Communications Security Establishment, *Cryptographic Endorsement and Assessment Program Standards*, NITSM 10/90, July 27, 1990

[6] William Brierley, *Integrating Cryptography into Trusted Systems: A Criteria Approach*, Proc. 8th IEEE Annual Computer Security Applications Conference, 1992.

[7] William Brierley, *A Comparison of FIPS 140–1 and The CTCPEC Requirements For Cryptography*, Internal Communications Security Establishment Report, May 4, 1992.

[8] Communications Security Establishment, *The Canadian Trusted Computer Product Evaluation Criteria*, Draft Version 3.0, April 1992.