AS/NZS ISO/IEC 19790:2006
ISO/IEC 19790:2006

AS/NZS ISO/IEC 19790:2006

Australian/New Zealand Standard™

Information technology—Security techniques—Security requirements for cryptographic modules

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification. It was approved on behalf of the Council of Standards Australia on 23 June 2006 and on behalf of the Council of Standards New Zealand on 30 June 2006.
This Standard was published on 26 July 2006.

The following are represented on Committee IT-012:

Attorney General's Department
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Department of Defence
Department of Social Welfare, NZ
Government Communications Security Bureau, NZ
Internet Industry Association
NSW Police Service
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 06207.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

Australian/New Zealand Standard™

Information technology—Security techniques—Security requirements for cryptographic modules

First published as AS/NZS ISO/IEC 19790:2006.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 7620 5

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification.

The objective of this Standard is to provide informative security practitioner with four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operation environment; cryptographic key management; self-tests; design assurance; and mitigation of other attacks.

This Standard is identical with, and has been reproduced from ISO/IEC 19790:2006, *Information technology—Security techniques—Security requirements for cryptographic modules*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover

(b) In the source text 'this International Standard' should read 'this Australian/New Zealand Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		AS ISO/IEC	
15408	Information technology—Security techniques—Evaluation criteria for IT security	15408	Information technology—Security techniques—Evaluation criteria for IT security
15408.1	Part 1: Introduction and general model	15408.1	Part 1: Introduction and general model
15408.2	Part 2: Security functional requirements	15408.2	Part 2: Security functional requirements
15408.3	Part 3: Security assurance requirements	15408.3	Part 3: Security assurance requirements

Only international references that have been adopted as Australian or Australian/New Zealand Standards have been listed.

The terms 'normative' and 'informative' have been used in this Standard to define the application of the annex to which they apply. A 'normative' annex is an integral part of a Standard, whereas an 'informative' annex is only for information and guidance.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

CONTENTS

Page

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 9

5 Cryptographic module security levels 9
5.1 Security Level 1 10
5.2 Security Level 2 10
5.3 Security Level 3 10
5.4 Security Level 4 11

6 Functional security objectives 11

7 Security requirements 12
7.1 Cryptographic module specification 14
7.2 Cryptographic module ports and interfaces 15
7.3 Roles, services, and authentication 16
7.4 Finite state model 18
7.5 Physical security 19
7.6 Operational environment 26
7.7 Cryptographic key management 29
7.8 Self-tests 31
7.9 Design assurance 34
7.10 Mitigation of other attacks 36

Annex A (normative) **Documentation requirements** 38

Annex B (normative) **Cryptographic module security policy** 42

Annex C (normative) **Approved protection profiles** 44

Annex D (informative) **Approved security functions** 45

Annex E (informative) **Approved key establishment methods** 47

Annex F (informative) **Recommended software development practices** 48

Annex G (informative) **Examples of mitigation of other attacks** 50

Bibliography 51

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

INTRODUCTION

In Information Technology there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorised disclosure or manipulation, for entity authentication and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

This International Standard provides for four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; self-tests; design assurance; and mitigation of other attacks.

The overall security level of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, compliance with this International Standard does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to

- physical and environmental controls;
- software development;
- backup and contingency plans; and
- information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.

This International Standard will be revised later, if a new work item is approved, in order to improve the links with Common Criteria scheme (ISO/IEC 15408).

This International Standard is derived from NIST Federal Information Processing Standard (FIPS) PUB 140-2 (see Bibliography [1]).

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

This International Standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 10 requirement areas. Each security level offers an increase in security over the preceding level.

While the security requirements specified in this International Standard are intended to maintain the security provided by a cryptographic module, compliance to this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
approval authority
any national or international organisation/authority mandated to approve and/or evaluate security functions

3.2
approved
ISO/IEC approved or approval authority approved

3.3
approved mode of operation
mode of the cryptographic module that employs only approved security functions

NOTE Not to be confused with a specific mode of an approved security function, e.g., Cipher Block Chaining (CBC) mode.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.4
approved operating system
any operating system evaluated and approved by an approval authority

3.5
approved protection profile
any protection profile approved by an approval authority

3.6
ISO/IEC approved
security function that is either

- specified in an ISO/IEC standard or
- adopted/recommended in an ISO/IEC standard and specified either in an annex of the ISO/IEC standard or in a document referenced by the ISO/IEC standard

3.7
asymmetric cryptographic technique
cryptographic technique that uses two related transformations — a public transformation (defined by the public key) and a private transformation (defined by the private key) — which have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with a given limited computing power

3.8
authentication code
cryptographic checksum based on an approved security function

NOTE Also known as a Message Authentication Code (MAC).

3.9
certificate
entity's data rendered unforgettable with the private or secret key of a certification authority

3.10
compromise
unauthorised disclosure, modification, substitution, or use of CSPs or the unauthorised modification or substitution of PSPs

3.11
confidentiality
property that information is not made available or disclosed to unauthorised entities

3.12
control information
information that is entered into a cryptographic module for the purposes of directing the operation of the module

3.13
critical security parameter
CSP
secret or private security related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.14
cryptographic boundary
explicitly defined continuous perimeter that establishes the physical and/or logical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module

3.15
cryptographic key
key
sequence of symbols that controls the operation of a cryptographic transformation

NOTE A cryptographic transformation may include but is not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

3.16
cryptographic key component
key component
parameter(s) used in a security function to perform a cryptographic function

3.17
cryptographic module
module
set of hardware, software, and/or firmware that implements security functions and is contained within the cryptographic boundary

3.18
cryptographic module security policy
security policy
precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module

NOTE See Annex B.

3.19
crypto officer
role taken by an individual or a process (i.e., subject) acting on behalf of an individual allowing cryptographic initialisation or management functions of a cryptographic module to be performed

3.20
data path
physical or logical route over which data passes

NOTE A physical data path may be shared by multiple logical data paths.

3.21
differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

3.22
digital signature
data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g., by the recipient)

3.23
electronic key entry
entry of cryptographic keys into a cryptographic module using electronic methods such key loader or on line means

NOTE The operator of the key may have no knowledge of the value of the key being entered.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.24
electronic key transport
transfer of cryptographic keys, usually in encrypted form, using electronic means such as a computer network

3.25
encrypted key
cryptographic key that has been encrypted using an approved security function with a key encryption key

3.26
entity
person, a group, a device or a process

3.27
environmental failure protection
EFP
use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range

3.28
environmental failure testing
EFT
use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range

3.29
error detection code
EDC
value computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data

3.30
finite state model
FSM
mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state

3.31
firmware
programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution

EXAMPLE Storage hardware may include but is not limited to ROM, PROM, EEPROM, or FLASH.

3.32
hardware
physical equipment/components within the cryptographic boundary used to process programs and data

3.33
input data
information that is entered into a cryptographic module and may be used for the purposes of transformation or computation using an approved security function

3.34
integrity
property that sensitive data has not been modified or deleted in an unauthorised and undetected manner

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.35
interface
logical entry or exit point of a cryptographic module that provides access to the module for logical information flows

3.36
key encryption key
KEK
cryptographic key that is used for the encryption or decryption of other keys

3.37
key establishment
process of making available a shared secret key to one or more entities

NOTE Key establishment includes key agreement and key transport.

3.38
key loader
self-contained device that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module

3.39
key management
administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy

3.40
key transport
process of transferring a key from one entity to another entity

3.41
maintenance role
role assumed to perform physical maintenance and/or logical maintenance services

EXAMPLE Maintenance services may include but are not limited to hardware and/or software diagnostics.

3.42
manual key entry
entry of a cryptographic key into a cryptographic module, using a device such as a keyboard

3.43
manual key transport
out of band means of transporting cryptographic keys, such as a key loader

3.44
microcode
processor instructions that correspond to an executable program instruction

EXAMPLE Assembler code.

3.45
operator
individual or a process (subject) operating on behalf of the individual, authorised to assume one or more roles

3.46
output data
information produced by a cryptographic module

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.47
passivation
process in the construction of semiconductor devices in which junctions, surfaces of components and integrated circuits are afforded a means of protection, which may modify circuit behaviour

NOTE 1 Silicon dioxide or phosphorus glass can be used for this purpose.

NOTE 2 Passivation material is technology dependent.

3.48
password
string of characters used to authenticate an identity or to verify access authorisation

EXAMPLE Letters, numbers, and other symbols.

3.49
personal identification number
PIN
numeric code used to authenticate an identity

3.50
physical protection
safeguarding of a cryptographic module, CSPs and PSPs using physical means

3.51
plaintext key
unencrypted cryptographic key

3.52
port
physical/logical input or output point of a cryptographic module that provides access to the module

3.53
private key
that key of an entity's asymmetric key pair which should only be used by that entity

NOTE In the case of an asymmetric signature system the private key defines the signature transformation. In the case of an asymmetric encipherment system the private key defines the decipherment transformation.

3.54
production-grade
product, component or software that has been tested to meet operational specifications

3.55
protection profile
implementation-independent set of security requirements for a category of TOE that meet specific consumer needs

3.56
public key
that key of an entity's asymmetric key pair which can be made public

NOTE In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

3.57
public key certificate
public key information of an entity signed by an appropriate certification authority and thereby rendered unforgeable

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.58
public security parameter
PSP
security related public information whose modification can compromise the security of a cryptographic module

EXAMPLE Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, and one time passwords associated with a counter.

3.59
random bit generator
RBG
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

3.60
removable cover
physical means which permits access to the physical contents of a cryptographic module

3.61
role
security attribute associated with a user defining the user access rights or limitations to services of a cryptographic module

NOTE One or more services may be associated with a role. A role may be associated with one or more users and a user may assume one or more roles.

3.62
secret key
cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public

3.63
security function
cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and key establishment all approved either by ISO/IEC or an approval authority

NOTE See Annex D.

3.64
seed key
secret value used to initialise a cryptographic function or operation

3.65
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys

3.66
software
programs and data components within the cryptographic boundary and usually stored on erasable media which can be dynamically written and modified during execution

EXAMPLE Erasable media may include but are not limited to hard drives.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.67
split knowledge
process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the original key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key

3.68
status information
information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module

3.69
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the encryption and the decryption transformations

3.70
system software
general purpose software within the cryptographic boundary designed to facilitate the operation of the cryptographic module

EXAMPLES Operating system, compilers and utility programs.

3.71
tamper detection
automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module

3.72
tamper evidence
external indication that an attempt has been made to compromise the security of a cryptographic module

NOTE The evidence of the tamper attempt should be observable.

3.73
tamper response
automatic action taken by a cryptographic module when tamper detection has occurred

3.74
target of evaluation
TOE
information technology product or system and associated administrator and user guidance documentation that is the subject of a CC evaluation

3.75
TOE security functions
TSF
subset of the TOE consisting of all hardware, software, and firmware that must be relied upon for the correct enforcement of the TOE security policy

3.76
TOE security policy
TSP
set of rules that regulate how assets are managed, protected, and distributed within a TOE

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

3.77
trust anchor
trusted information, which includes a public key algorithm, a public key value, an issuer name, and optionally, other parameters

NOTE 1 Other parameters may include but are not limited to a validity period.

NOTE 2 A trust anchor may be provided in the form of a self-signed certificate.

3.78
trusted path
means by which a user and a TSF can communicate with necessary confidence to support the TSP

3.79
user
individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services

3.80
zeroisation
method of destruction of stored data and CSPs to prevent retrieval and reuse

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

API	Application Program Interface
CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
EAL	Evaluation Assurance Level
EDC	Error Detection Code
HDL	Hardware Description Language
IC	Integrated Circuit
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read-Only Memory

5 Cryptographic module security levels

The following sub-clauses provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive. Within this document, references to a *module* shall be interpreted as a *cryptographic module*.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

5.1 Security Level 1

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one approved algorithm or approved security function shall be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computer system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

5.2 Security Level 2

Security Level 2 enhances the physical security mechanisms of Security Level 1 by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals or pick-resistant locks on removable covers or doors.

Tamper-evident coatings or seals are placed on a module so that the coating or seal must be broken to attain physical access to Critical Security Parameters (CSPs) and/or Public Security Parameters (PSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorised physical access.

Security Level 2 requires, at a minimum, role-based authentication in which a cryptographic module authenticates the authorisation of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified in an approved protection profile (Annex C); and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL2 (or higher).

An approved evaluated operating system may be used. It provides a level of trust so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

5.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs and/or PSPs held within the module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroise all CSPs when the removable covers/doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorised to assume a specific role and perform a corresponding set of services.

Security Level 3 requires the entry or output of CSPs (including the entry or output of CSPs using split-knowledge techniques) to be performed using ports that are physically separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. CSPs may be entered into or

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

Security Level 3 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified in an approved protection profile (Annex C) with the additional functional requirement of a Trusted Path (FTP_TRP.1); and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL3 (or higher) with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An approved evaluated trusted operating system may be used. The implementation of a trusted path protects CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the system.

5.4 Security Level 4

Security Level 4 provides the highest level of security defined in this International Standard. At this level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorised attempts at physical access when CSPs and/or PSPs are contained in the module whether external power is applied or not. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate zeroisation of all CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defences. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroise CSPs, or to undergo rigorous environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified for Security Level 3; and
- is evaluated at the ISO/IEC 15408 evaluation assurance level EAL4 (or higher).

An approved evaluated trusted operating system may be used.

6 Functional security objectives

The security requirements specified in this International Standard relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module to:

- employ and correctly implement the approved security functions for the protection of sensitive information;
- protect a cryptographic module from unauthorised operation or use;
- prevent the unauthorised disclosure of the contents of the cryptographic module, including CSPs;

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

- prevent the unauthorised and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorised modification, substitution, insertion, and deletion of CSPs and/or PSPs;
- provide indications of the operational state of the cryptographic module;
- ensure that the cryptographic module performs properly when operating in an approved mode of operation; and
- detect errors in the operation of the module and to prevent the compromise of CSPs and/or PSPs resulting from these errors.

7 Security requirements

This clause specifies the security requirements that shall be satisfied by cryptographic module's compliance to this International Standard. The security requirements cover areas related to the design and implementation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; self-tests; and design assurance.

An additional area concerned with the mitigation of other attacks is currently not tested except at Security Level 4, but it is required to document implemented controls (e.g., DPA). Table 1 summarizes the security requirements in each of these areas.

A module shall be tested against the requirements of each area addressed in this clause. The cryptographic module shall be independently rated in each area. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module will receive a rating that reflects the maximum-security level for which the module fulfils all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the cryptographic module will receive a rating commensurate with the overall level of security.

In addition to receiving independent ratings for each of the security areas, a cryptographic module will also receive an overall rating. The overall rating will indicate the minimum of the independent ratings received in the areas.

Many of the security requirements of this International Standard include specific documentation requirements that are summarized at Annex A. All documentation, including copies of the user and installation manuals, shall be provided for evaluation.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006

Table 1 — Summary of security requirements

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved algorithms, and approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for critical security parameters logically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production-grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modelling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random bit and key generation, key establishment, key distribution key entry/output, key storage and key zeroisation.			
	Secret and private keys transported using manual transport methods may be entered or output in plaintext form.		Secret and private keys transported using manual transport methods shall be entered or output either encrypted or using split knowledge procedures.	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, and critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and post conditions.
Mitigation of other attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			Specification of mitigation of attacks with testable requirements.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 19790-2006