

~~FDIS~~ ISO/IEC ~~FDIS~~ 19790 (E:2024(en)
ISO/IEC JTC 1/SC 27/WG 3
Secretariat: DIN
Date: 2024-06-01-12
Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

Formatted: Centered

Style Definition

Formatted: zzCover, Left

Formatted: Different first page header

Formatted

Formatted

Formatted: Font: Not Bold

Formatted: zzCover, Left, Space After: 0 pt

Formatted: Font: 11 pt

Formatted: zzCover, Line spacing: single

~~FDIS~~ stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

A model document of an International Standard (the Model International Standard) is available at: <https://www.iso.org/drafting-standards.htm>

Formatted: Centered

© ISO 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office Copyright Office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland

- Formatted: Font: 11 pt
- Formatted: Font: 11 pt
- Formatted: Font: 11 pt
- Formatted: Space After: 0 pt, Line spacing: single
- Formatted: Font: 10 pt, Font color: Black, English (United States)
- Formatted: Indent: Left: 0 cm, Right: 0 cm, Space Before: 0 pt, No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Top: (No border), Left: (No border), Right: (No border)
- Formatted: Font color: Blue
- Formatted: Font color: Black, English (United States)
- Formatted: Font color: Black, English (United States)
- Formatted: Font: 11 pt, Font color: Blue
- Formatted: Font color: Black, English (United States)
- Formatted: Font: 11 pt, Font color: Blue
- Formatted: Font color: Black, English (United States)
- Formatted: Font color: Black, English (United States)
- Formatted: Font: 11 pt, Font color: Blue
- Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Left: (No border), Right: (No border)
- Formatted: Font color: Black, English (United States)
- Formatted: Font color: Black, English (United States)
- Formatted: Font: 11 pt, Font color: Blue
- Formatted: Font color: Black, English (United Kingdom)
- Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers, Border: Bottom: (No border), Left: (No border), Right: (No border)
- Formatted: Font color: Black, English (United Kingdom)
- Formatted: Font color: Black, English (United States)
- Formatted: Font color: Black, English (United States)

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC FDIS 19790
<https://standards.itih.ai/catalog/standards/iso/74c98368-c9c5-4a2c-bcdb-2b33>

Contents

Foreword	viii
Introduction	x
1 — Scope	1
2 — Normative references	1
3 — Terms and definitions	1
4 — Abbreviated terms	21
5 — Cryptographic module security levels	21
5.1 — General	21
5.2 — Security level 1	22
5.3 — Security level 2	22
5.4 — Security level 3	22
5.5 — Security level 4	23
6 — Functional security objectives	24
7 — Security requirements	24
7.1 — General	24
7.2 — Cryptographic module specification	28
7.2.1 — Cryptographic module specification general requirements	28
7.2.2 — Types of cryptographic modules	28
7.2.3 — Cryptographic boundary	28
7.2.4 — Module operations	29
7.3 — Cryptographic module interfaces	31
7.3.1 — Cryptographic module interfaces general requirements	31
7.3.2 — Types of interfaces	31
7.3.3 — Categories of interfaces	31
7.3.4 — Plaintext trusted path	32
7.3.5 — Protected internal paths	33
7.4 — Roles, services, and authentication	33
7.4.1 — Roles, services, and authentication general requirements	33
7.4.2 — Roles	33
7.4.3 — Services	34
7.4.4 — Authentication	35
7.5 — Software/firmware security	37
7.5.1 — Software/firmware security general requirements	37
7.5.2 — Security level 1	38
7.5.3 — Security level 2	39
7.5.4 — Security levels 3 and 4	39
7.6 — Operational environment	39
7.6.1 — Operational environment general requirements	39
7.6.2 — Clause applicability	41
7.6.3 — Operating system requirements for modifiable operational environments	41
7.7 — Physical security	43
7.7.1 — Physical security embodiments	43
7.7.2 — Physical security general requirements	45
7.7.3 — Physical security requirements for each physical security embodiment	47
7.7.4 — Environmental failure protection/testing	48
7.7.5 — Environmental failure protection features	49
7.7.6 — Environmental failure testing procedures	49

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Space Before: 48 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

7.8	Non-invasive security	49
7.8.1	Non-invasive security general requirements	49
7.8.2	Security levels 1 and 2	50
7.8.3	Security level 3	50
7.8.4	Security level 4	50
7.9	Sensitive security parameter management	50
7.9.1	Sensitive security parameter management general requirements	50
7.9.2	Random bit generators	51
7.9.3	Sensitive security parameter generation	51
7.9.4	Automated sensitive security parameter establishment	51
7.9.5	Sensitive security parameter entry and output	51
7.9.6	Sensitive security parameter storage	52
7.9.7	Sensitive security parameter zeroization	52
7.10	Self-tests	54
7.10.1	Self-test general requirements	54
7.10.2	Security levels 3 and 4	55
7.10.3	Pre-operational self-tests	55
7.10.4	Conditional self-tests	56
7.11	Life-cycle assurance	58
7.11.1	Life-cycle assurance general requirements	58
7.11.2	Configuration management	59
7.11.3	Design	59
7.11.4	Finite state model	59
7.11.5	Development	60
7.11.6	Vendor testing	62
7.11.7	Delivery and operation	62
7.11.8	Guidance documents	63
7.12	Mitigation of other attacks	64
7.12.1	Mitigation of other attacks general requirements	64
7.12.2	Security levels 1, 2 and 3	64
7.12.3	Security level 4	64
Annex A (normative)	Documentation requirements	65
A.1	Purpose	65
A.2	Items	65
A.2.1	Cryptographic module specification	65
A.2.2	Cryptographic module interfaces	66
A.2.3	Roles, services, and authentication	66
A.2.4	Software/Firmware security	66
A.2.5	Operational environment	67
A.2.6	Physical security	67
A.2.7	Non-invasive security	67
A.2.8	Sensitive security parameter management	68
A.2.9	Self-tests	68
A.2.10	Life-cycle assurance	69
A.2.11	Mitigation of other attacks	70
Annex B (normative)	Cryptographic module security policy	71

B.1	General	71
B.2	Items	71
B.2.1	General	71
B.2.2	Cryptographic module specification	71
B.2.3	Cryptographic module interfaces	72
B.2.4	Roles, services, and authentication	72
B.2.5	Software/Firmware security	73
B.2.6	Operational environment	73
B.2.7	Physical security	73
B.2.8	Non-invasive security	74
B.2.9	Sensitive security parameters management	74
B.2.10	Self-tests	75
B.2.11	Life-cycle assurance	75
B.2.12	Mitigation of other attacks	75
Annex C (normative)	Approved security functions	76
C.1	Purpose	76
C.2	Cryptographic algorithms	76
C.2.1	Block ciphers and operation modes	76
C.2.2	Stream ciphers	76
C.2.3	Asymmetric algorithms and techniques	76
C.2.4	Other encryption techniques	76
C.2.5	Message authentication codes	76
C.2.6	Hash functions	77
C.2.7	Random bit generation	77
C.3	Other security functions	77
Annex D (normative)	Approved sensitive security parameter generation and establishment methods	78
D.1	Purpose	78
D.2	Sensitive security parameter generation	78
D.3	Key establishment methods	78
Annex E (normative)	Approved authentication mechanisms	79
E.1	Purpose	79
E.2	Entity authentication standards	79
E.3	Authentication strength and rate limiting methods	79
E.3.1	Approved authentication strength and rate limiting methods	79
E.4	Password protection methods	79
Annex F (normative)	Approved non-invasive attack mitigation test metrics	80

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

F.1 Purpose 80

F.2 Non-invasive attack mitigation test metrics 80

Annex G (normative) Module secure development, manufacturing and operation 81

G.1 Purpose 81

G.2 Secure Development 81

G.2.1 Hardware secure development 81

G.2.2 Firmware secure development 81

G.2.3 Software secure development 81

G.3 Manufacturing Security 81

G.4 Operations Security 81

G.4.1 Attestation 81

Bibliography 82

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC FDIS 19790

https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790

List of tables

Table 1 — Summary of security requirements	25
Table 2 — Examples of operational environments	40
Table 3 — Summary of physical security requirements for cryptographic modules	44

Foreword	ix
Introduction	xi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	23
5 Cryptographic module security levels	25
5.1 General	25
5.2 Security level 1	25
5.3 Security level 2	25
5.4 Security level 3	26
5.5 Security level 4	26
6 Functional security objectives	27
7 Security requirements	28
7.1 General	28
7.2 Cryptographic module specification	31
7.2.1 Cryptographic module specification general requirements	31
7.2.2 Types of cryptographic modules	31
7.2.3 Cryptographic boundary	31
7.2.4 Module operations	33
7.3 Cryptographic module interfaces	34
7.3.1 Cryptographic module interfaces general requirements	34
7.3.2 Types of interfaces	35
7.3.3 Categories of interfaces	35
7.3.4 Plaintext trusted path	36
7.3.5 Protected internal paths	37
7.4 Roles, services, and authentication	37
7.4.1 Roles, services, and authentication general requirements	37
7.4.2 Roles	37
7.4.3 Services	38
7.4.4 Authentication	40
7.5 Software/firmware security	42
7.5.1 Software/firmware security general requirements	42
7.5.2 Security level 1	42
7.5.3 Security level 2	43
7.5.4 Security levels 3 and 4	44
7.6 Operational environment	44
7.6.1 Operational environment general requirements	44
7.6.2 Clause applicability	46
7.6.3 Operating system requirements for modifiable operational environments	46
7.7 Physical security	48
7.7.1 Physical security embodiments	48
7.7.2 Physical security general requirements	50

7.7.3 Physical security requirements for each physical security embodiment.....	52
7.7.4 Environmental failure protection/testing.....	53
7.7.5 Environmental failure protection features.....	54
7.7.6 Environmental failure testing procedures.....	54
7.8 Non-invasive security.....	55
7.8.1 Non-invasive security general requirements.....	55
7.8.2 Security levels 1 and 2.....	55
7.8.3 Security level 3.....	55
7.8.4 Security level 4.....	55
7.9 Sensitive security parameter management.....	56
7.9.1 Sensitive security parameter management general requirements.....	56
7.9.2 Random bit generators.....	56
7.9.3 Sensitive security parameter generation.....	56
7.9.4 Automated sensitive security parameter establishment.....	57
7.9.5 Sensitive security parameter entry and output.....	57
7.9.6 Sensitive security parameter storage.....	58
7.9.7 Sensitive security parameter zeroization.....	58
7.10 Self-tests.....	59
7.10.1 Self-test general requirements.....	59
7.10.2 Security levels 3 and 4.....	60
7.10.3 Pre-operational self-tests.....	60
7.10.4 Conditional self-tests.....	61
7.11 Life-cycle assurance.....	64
7.11.1 Life-cycle assurance general requirements.....	64
7.11.2 Configuration management.....	65
7.11.3 Design.....	65
7.11.4 Finite state model.....	65
7.11.5 Development.....	66
7.11.6 Vendor testing.....	68
7.11.7 Delivery and operation.....	68
7.11.8 Guidance documents.....	69
7.12 Mitigation of other attacks.....	70
7.12.1 Mitigation of other attacks general requirements.....	70
7.12.2 Security levels 1, 2 and 3.....	70
7.12.3 Security level 4.....	70
Annex A (normative) Documentation requirements.....	72
Annex B (normative) Cryptographic module security policy.....	79
Annex C (normative) Approved security functions.....	85
Annex D (normative) Approved sensitive security parameter generation and establishment methods.....	88
Annex E (normative) Approved authentication mechanisms.....	90
Annex F (normative) Approved non-invasive attack mitigation test metrics.....	92
Annex G (normative) Module secure development, manufacturing and operation.....	93
Bibliography.....	94

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 19790:2012), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 19790:2012/Cor 1:2015.

The main changes are as follows:

- ~~Clause 3~~ ~~has~~ ~~4 and 5 have~~ been refined and updated to reflect changes in requirements in ~~Clause 7~~;
- ~~Clause 4~~ ~~has been refined and updated to reflect changes in requirements in Clause 7;~~
- ~~Clause 5~~ ~~has been refined and updated to reflect major changes in requirements in Clause 7;~~
- ~~the language in Clause 6~~ has been refined and modernized;
- ~~in Clause 7~~, the requirements have been reworded and rearranged for clarity. ~~New requirements have been added, and redundant or unnecessary requirements removed;~~
- ~~Annex A~~ ~~Annexes A and B~~ have been updated to reflect changes in requirements in ~~Clause 7~~;

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: std_publisher

Formatted: std_docNumber

Formatted: std_publisher

Formatted: std_docNumber

Formatted: std_year

Formatted: std_publisher

Formatted: std_docNumber

Formatted: std_year

Formatted: std_suppl

Formatted: Font: Cambria

Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: cite_sec

Formatted: cite_sec

Formatted: cite_sec

Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: cite_sec

Formatted: cite_sec

Formatted: cite_sec

Formatted: cite_sec

Formatted: cite_app

Formatted: cite_sec

Formatted: cite_sec

FDIS ISO/IEC-FDIS 19790 (E:2024(en)

- ~~Annex B has been updated to reflect changes in requirements in Clause 7;~~
- ~~Annex — Annexes C, has, D and E have~~ been restructured and updated in line with standards published since the previous edition;
- ~~Annex D has been restructured and updated in line with standards published since the previous edition;~~
- ~~Annex E has been updated with standards published since the previous edition,~~ as well as with examples of rate limiting methods;
- ~~Annex F~~ has been updated with the inclusion of ISO/IEC 17825; and
- ~~New — new~~ Annex-G on module secure development, manufacturing and operation has been added.

The catalogue of security requirements defined in this document is provided in machine readable format (XML) at: <https://standards.iso.org/iso-iec/TBD>.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: cite_app

Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: cite_app

Formatted: cite_app

Formatted: std_publisher

Formatted: std_docNumber

Formatted: cite_app

Formatted: cite_app

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC FDIS 19790

<https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>

Introduction

In information technology there is an ever-increasing need to use cryptographic mechanisms, such as for the protection of data against ~~unauthorised~~unauthorized 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 document provides four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels defined in this document. The security requirements cover areas relative to the design and implementation of a cryptographic module. ~~These areas include cryptographic module specification; cryptographic module interfaces; These areas include: roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.~~

— cryptographic module specification;

— cryptographic module interfaces;

— roles, services, and authentication;

— software/firmware security;

— operational environment;

— physical security;

— non-invasive security;

— sensitive security parameter management;

— self-tests;

— life-cycle assurance; and <https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>

— mitigation of other attacks.

The overall security rating or the security level within each area of a cryptographic module is chosen to provide a level of security which is appropriate for the security requirements of the application and environment in which the module is 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 ~~utilise~~utilize cryptographic modules provide an ~~acceptable~~appropriate 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, conformity with this document 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;

— access controls;

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: No page break before, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: List Continue 1, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

- ~~—~~ system security maintenance and patch management;
- ~~—~~ 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.

Conformity with this document is not sufficient to ensure that a 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. Owners of sensitive information are expected to assess the risks to their information and to deploy cryptographic modules as part of their overall risk mitigation plan, in order to mitigate specific identified risks. ~~Guidance contained in the module's~~The security policy ~~of the module, which~~ outlines ~~the module's~~ strengths and limitations, ~~and~~ is expected to be followed for any given deployment.

Formatted: Font: 11 pt

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Font: 11 pt

Formatted: Font: 11 pt

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

iTech Standards (<https://standards.iteh.ai>) Document Preview

ISO/IEC FDIS 19790

<https://standards.iteh.ai/catalog/standards/iso/74e98368-c9c5-4a2c-bcdb-2b336c93c703/iso-iec-fdis-19790>

Formatted: Centered

Formatted: Different first page header

Formatted: zzSTDTitle, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules

1 Scope

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in Information information and Communication Technologiescommunication technologies (ICT). ~~This document~~ defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. ~~Data sensitivity covers, for example, low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government.~~ This document specifies up to four security levels for each of the 11 requirement areas with each security level increasing security over the preceding level.

Formatted: Body Text

Formatted: English (United States)

Formatted: Font: 12 pt, English (United States)

Formatted: English (United States)

Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Tab stops: Not at 1.42 cm

Formatted: English (United States)

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Term(s), Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at <https://www.iso.org/obp><https://www.iso.org/obp>

— IEC Electropedia: available at <https://www.electropedia.org/><https://www.electropedia.org/>

Formatted: Font: Bold

Formatted: Admitted Term, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Term(s), Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Term(s), Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

3.1 access control list

ACL
list of permissions to grant access to an object

3.2 administrator guidance

written material that is used by either the crypto officer (3.30)crypto officer (3.30) or any other administrative role (3.120)role (3.119) for the correct configuration, maintenance, and administration of the cryptographic module (3.35)cryptographic module (3.35)

3.3 automated

without manual (3.82)manual (3.81) intervention or input (e.g. electronic means such as through a computer network)

Formatted: Normal, Centered, Space After: 24 pt, Line spacing: Exactly 12 pt, Tab stops: 17.2 cm, Right

Formatted: Font: 9 pt

3.4

approved data authentication technique

approved method providing assurance that the originator of the data is as claimed

Note 1 to entry: Approved data authentication techniques can include the use of an approved [digital signature \(3.43\)](#), approved [message authentication code \(3.82\)](#) or approved keyed hash. Approved data authentication techniques are specified in [Annex C, Annex C](#).

3.5

approved integrity technique

approved method of verifying whether or not data has been corrupted or modified

Note 1 to entry: Approved integrity techniques can be keyed, and can include an approved hash, a [message authentication code \(3.82\)](#) or a [digital signature \(3.43\)](#) algorithm.

Note 2 to entry: Approved integrity techniques are specified in [Annex C, Annex C](#).

3.6

approved process

set of interrelated functions that includes at least one [approved security function \(3.8\)](#), [approved security function \(3.8\)](#), and can include a non-cryptographic function or non-approved [security function \(3.127\)](#) [security function \(3.126\)](#) which are not security relevant to the process's operation

Note 1 to entry: A banking transaction, a compression service that includes encryption, etc.

3.7

approved service

[service \(3.133\)](#) [service \(3.136\)](#) which includes at least one [approved security function \(3.8\)](#) [approved security function \(3.8\)](#) or process, and can include [non security relevant \(3.92\)](#) [non security relevant \(3.91\)](#) functions or processes

Note 1 to entry: Any [security relevant \(3.129\)](#) [security relevant \(3.128\)](#) but non-approved security functions or processes are excluded from approved services.

3.8

approved security function

[security function \(3.127\)](#) [security function \(3.126\)](#) that is [permitted for use in an approved service \(3.7\)](#)

Note 1 to entry: Approved security functions are referenced in [Annex C, Annex C](#), which references [Annex D, Annex D](#) and [Annex E, Annex E](#).

3.9

asymmetric algorithm

asymmetric technique

[cryptographic algorithm \(3.31\)](#) [cryptographic algorithm \(3.31\)](#) or technique that uses two related transformations: a public transformation (defined by the [public key \(3.114\)](#) [public key \(3.113\)](#)) and a private transformation (defined by the [private key \(3.111\)](#) [private key \(3.110\)](#))

Note 1 to entry: The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with given computational resources.

3.10

attestation

Formatted: Font: 12 pt, Bold

Formatted: Normal, Centered, Space After: 36 pt, Line spacing: Exactly 12 pt, Tab stops: 0.71 cm, Left

Formatted: Term(s), Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Note, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Term(s), Don't keep with next, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers

Formatted: Note, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted: Note

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted