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

ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

Date: 2024-~~06-01~~11-12

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

~~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.html~~

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

Formatted: Centered

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)

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

Contents

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

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

~~List of tables~~

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~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~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.~~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.~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~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~~ — Clauses 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~~ — Annexes A ~~has~~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

~~— 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.~~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

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

— 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

Formatted: Font: 11 pt

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

Formatted: Font: 11 pt

Formatted: Font: 11 pt

- 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.

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

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 modules~~its strengths and limitations, ~~and~~ is expected to be followed for any given deployment.

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 Technologies~~communication technologies (ICT). ~~This document~~It 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.

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/

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)

3.4

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

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

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

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

Formatted: Font: 9 pt

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),~~*digital signature* (3.43), approved ~~*message authentication code* (3.83)~~*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* (3.83) or a *digital signature* (3.43)~~*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 ...