This is a free page sample. Access the full version online.

NSAI Standards

Irish Standard
I.S. EN ISO/IEC 19790:2020&LC:2020

Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

© CEN 2021 No copying without NSAI permission except as permitted by copyright law.

This is a free page sample. Access the full version online.

I.S. EN ISO/IEC 19790:2020&LC:2020

Incorporating amendments/corrigenda/National Annexes issued since publication:

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):

NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.

This document is based on: *Published:*

This document was published under the authority of the NSAI and comes into effect on: 2021-01-27	ICS number: 35.030 NOTE: If blank see CEN/CENELEC cover page

NSAI 1 Swift Square, Northwood, Santry Dublin 9	T +353 1 807 3800 F +353 1 807 3838 E standards@nsai.ie W NSAI.ie	Sales: T +353 1 857 6730 F +353 1 857 6729 W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

This is a free page sample. Access the full version online.

National Foreword

I.S. EN ISO/IEC 19790:2020&LC:2020 is the adopted Irish version of the European Document EN ISO/IEC 19790:2020, Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

Compliance with this document does not of itself confer immunity from legal obligations.

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.

This is a free page sample. Access the full version online.

This page is intentionally left blank

This is a free page sample. Access the full version online.

Correction Notice

Reference: **EN ISO/IEC 19790:2020**

Title: Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

Work Item: JT013014

Brussels, 2020-12-09

Please include the following minor editorial correction(s) in the document related to:

the following language version(s) :
- ☒ English
- ☒ French
- ☐ German

for the following procedure :
- ☐ PQ/UQ
- ☐ Enquiry
- ☐ 2nd Enquiry
- ☐ Parallel Enquiry
- ☐ 2nd Parallel Enquiry
- ☐ Formal Vote
- ☐ 2nd Formal Vote
- ☐ Parallel Formal Vote
- ☐ 2nd Parallel Formal Vote
- ☐ UAP
- ☐ TC Approval
- ☐ 2nd TC Approval
- ☒ Publication
- ☐ Parallel Publication

It has been brought to our attention that this document, issued on 2020-03-18, requires modification.

Titles have been modified by adding "including corrected version 2015-12" in English and "y compris version corrigée 2015-11" in French.

Titles and Forewords have been updated accordingly for English and French versions.

We apologise for any inconvenience this may cause.

Rue de la Science, 23 • 1040 Bruxelles
Tel : +32 2 550 08 11 • Fax : +32 2 550 08 19

This is a free page sample. Access the full version online.

This page is intentionally left BLANK.

This is a free page sample. Access the full version online.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 19790

March 2020

ICS 35.030

English version

Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012, including corrected version 2015-12)

Technologies de l'information - Techniques de sécurité - Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012, y compris version corrigée 2015-11)

Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012, einschließlich korrigierte Fassung 2015-12)

This European Standard was approved by CEN on 2 March 2020.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 09 December 2020.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2020 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

This is a free page sample. Access the full version online.

Contents

Page

European foreword **3**

This is a free page sample. Access the full version online.

European foreword

The text of ISO/IEC 19790:2012, including corrected version 2015-12 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 19790:2020 by Technical Committee CEN/CLC/JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2020, and conflicting national standards shall be withdrawn at the latest by September 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/IEC 19790:2012, including corrected version 2015-12 has been approved by CEN as EN ISO/IEC 19790:2020 without any modification.

This is a free page sample. Access the full version online.

This page is intentionally left blank

This is a free page sample. Access the full version online.

INTERNATIONAL STANDARD

ISO/IEC 19790

Second edition
2012-08-15

Corrected version
2015-12-15

Information technology — Security techniques — Security requirements for cryptographic modules

Technologies de l'information — Techniques de sécurité — Exigences de sécurité pour les modules cryptographiques

Reference number
ISO/IEC 19790:2012(E)

© ISO/IEC 2012

This is a free page sample. Access the full version online.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

This is a free page sample. Access the full version online.

Contents

Page

1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Abbreviated terms 15
5 Cryptographic module security levels 15
5.1 Security Level 1 15
5.2 Security Level 2 16
5.3 Security Level 3 16
5.4 Security Level 4 17
6 Functional security objectives 17
7 Security requirements 18
7.1 General 18
7.2 Cryptographic module specification 20
7.2.1 Cryptographic module specification general requirements 20
7.2.2 Types of cryptographic modules 20
7.2.3 Cryptographic boundary 21
7.2.4 Modes of operations 22
7.3 Cryptographic module interfaces 23
7.3.1 Cryptographic module interfaces general requirements 23
7.3.2 Types of interfaces 24
7.3.3 Definition of interfaces 24
7.3.4 Trusted channel 25
7.4 Roles, services, and authentication 25
7.4.1 Roles, services, and authentication general requirements 25
7.4.2 Roles 26
7.4.3 Services 26
7.4.4 Authentication 28
7.5 Software/Firmware security 29
7.6 Operational environment 31
7.6.1 Operational environment general requirements 31
7.6.2 Operating system requirements for limited or non-modifiable operational environments 33
7.6.3 Operating system requirements for modifiable operational environments 33
7.7 Physical security 35
7.7.1 Physical security embodiments 35
7.7.2 Physical security general requirements 37
7.7.3 Physical security requirements for each physical security embodiment 39
7.7.4 Environmental failure protection/testing 42
7.8 Non-invasive security 43
7.9 Sensitive security parameter management 44
7.9.1 Sensitive security parameter management general requirements 44
7.9.2 Random bit generators 44
7.9.3 Sensitive security parameter generation 44
7.9.4 Sensitive security parameter establishment 45
7.9.5 Sensitive security parameter entry and output 45
7.9.6 Sensitive security parameter storage 46

© ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

7.9.7 Sensitive security parameter zeroisation 46
7.10 Self-tests 47
7.10.1 Self-test general requirements 47
7.10.2 Pre-operational self-tests 47
7.10.3 Conditional self-tests 48
7.11 Life-cycle assurance 50
7.11.1 Life-cycle assurance general requirements 50
7.11.2 Configuration management 51
7.11.3 Design 51
7.11.4 Finite state model 51
7.11.5 Development 52
7.11.6 Vendor testing 53
7.11.7 Delivery and operation 54
7.11.8 End of life 54
7.11.9 Guidance documents 54
7.12 Mitigation of other attacks 55

Annex A (normative) Documentation requirements 56
A.1 Purpose 56
A.2 Items 56
A.2.1 General 56
A.2.2 Cryptographic module specification 56
A.2.3 Cryptographic module interfaces 57
A.2.4 Roles, services, and authentication 57
A.2.5 Software/Firmware security 57
A.2.6 Operational environment 58
A.2.7 Physical security 58
A.2.8 Non-invasive security 58
A.2.9 Sensitive security parameter management 58
A.2.10 Self-tests 59
A.2.11 Life-cycle assurance 60
A.2.12 Mitigation of other attacks 61

Annex B (normative) Cryptographic module security policy 62
B.1 General 62
B.2 Items 62
B.2.1 General 62
B.2.2 Cryptographic module specification 62
B.2.3 Cryptographic module interfaces 63
B.2.4 Roles, services, and authentication 63
B.2.5 Software/Firmware security 64
B.2.6 Operational environment 64
B.2.7 Physical security 64
B.2.8 Non-invasive security 65
B.2.9 Sensitive security parameters management 65
B.2.10 Self-tests 66
B.2.11 Life-cycle assurance 66
B.2.12 Mitigation of other attacks 66

Annex C (normative) Approved security functions 67
C.1 Purpose 67
C.1.1 Block ciphers 67
C.1.2 Stream ciphers 67
C.1.3 Asymmetric algorithms and techniques 67
C.1.4 Message authentication codes 67
C.1.5 Hash functions 67
C.1.6 Entity authentication 68

 © ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

C.1.7 Key management 68
C.1.8 Random bit generation 68

Annex D (normative) Approved sensitive security parameter generation and establishment methods 69
D.1 Purpose 69
D.1.1 Sensitive security parameter generation 69
D.1.2 Sensitive security parameter establishment methods 69

Annex E (normative) Approved authentication mechanisms 70
E.1 Purpose 70
E.1.1 Authentication mechanisms 70

Annex F (normative) Approved non-invasive attack mitigation test metrics 71
F.1 Purpose 71
F.1.1 Non-invasive attack mitigation test metrics 71

© ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

Technical corrigendum 1 to ISO/IEC 19790:2012 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This corrected version of Technical corrigendum 1 to ISO/IEC 19790:2012 cancels and replaces the first edition (ISO/IEC 19790:2012/Cor 1:2015), incorporating the same technical revisions and miscellaneous editorial corrections showing in **red** text instead of black underlining:

— 3.21: The term "cryptographic boundary" is corrected;

— 3.80: The term "non-security relevant" is corrected;

— 3.108: The term "self-test" is corrected;

— 7.2.2: The requirements **[02.04]**, **[02.05]** and **[02.06]** are corrected;

— 7.2.4.3: The requirement **[02.31]** is corrected;

— 7.3.3: The requirement **[03.14]** is corrected;

— 7.5: The requirements **[05.06]** and **[05.07]** are added. The requirements **[05.08]**, **[05.13]** and **[05.17]** through **[05.23]** are corrected;

— 7.6.3: The requirement **[06.06]** is corrected;

© ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

- 7.8: The requirement **[08.04]** is corrected;
- 7.9.1: The requirement **[09.04]** is corrected;
- 7.9.7: The requirement **[09.37]** is corrected;
- 7.10.2.2: The requirement **[10.17]** is corrected;
- 7.11.5: The requirement **[11.26]** is corrected;
- 7.11.7: The requirement **[11.35]** is corrected;
- 7.11.9: The requirement **[11.38]** is corrected;
- A.2.5: The requirements of the 1st and 2nd bullets are corrected;
- A.2.7: The requirement of the 3rd bullet is corrected;
- A.2.10: The requirement of the 4th bullet is corrected;
- B.2.4: The requirement of the 9th bullet is corrected;
- B.2.5: The requirement of the 1st bullet is corrected;
- B.2.7: The requirement of the 2nd level 6th bullet is corrected;
- D.1: Duplicate text is removed;
- D.1.2: The reference to ISO/IEC 15946-3 is removed;
- E.1: Duplicate text is removed; and
- F.1: Duplicate text is removed.

© ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

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 cryptographic techniques are identical over the four security levels. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include 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 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 utilised 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 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;

— access 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.

© ISO/IEC 2012 – All rights reserved

This is a free page sample. Access the full version online.

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

This International Standard specifies the security requirements for a cryptographic module utilised 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, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

This International Standard specifies security requirements specified intended to maintain the security provided by a cryptographic module and 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.

The documents listed in ISO/IEC 19790 Annexes C, D, E and F *Information technology – Security techniques – Security requirements for cryptographic modules.*

3 Terms and definitions

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

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 the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module

3.3
automated
without manual intervention or input (e.g. electronic means such as through a computer network)

© ISO/IEC 2012 – All rights reserved

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation