Information technology - Security techniques - Security requirements for cryptographic modules (ISO/IEC 19790:2012)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 19790:2020 sisaldab Euroopa standardi EN ISO/IEC 19790:2020 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 19790:2020 consists of the English text of the European standard EN ISO/IEC 19790:2020.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 18.03.2020.	Date of Availability of the European standard is 18.03.2020.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.030

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)

Technologies de l'information - Techniques de sécurité - Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012)

Informationstechnik - Sicherheitstechniken - Sicherheitsanforderungen für kryptografische Module (ISO/IEC 19790:2012)

This European Standard was approved by CEN on 2 March 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

Ref. No. EN ISO/IEC 19790:2020 E

European foreword

The text of ISO/IEC 19790:2012 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 has been approved by CEN as EN ISO/IEC 19790:2020 without any modification.

Contents

Page

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.

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 Annexes C, D, E and F of this International Standard

3 Terms and definitions

For the purposes of this document, 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)

3.4
approval authority
any national or international organisation/authority mandated to approve and/or evaluate security functions