Technical

ISO/IEC TS 20540

Information security, cybersecurity and privacy protection — Testing cryptographic modules in their field

Sécurité de l'information, cybersécurité et protection de la vie privée — Test de modules cryptographiques dans leur domaine

Second edition
2025-05

Reference number
ISO/IEC TS 20540:2025(en)

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

Published in Switzerland

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 second edition cancels and replaces the first edition (ISO/IEC TS 20540:2018), which has been technically revised.

The main changes are as follows:

— the document has been restructured:

  — 7.3 and 7.4 have been moved to 8.2;

  — new Annex B has been created;

— technical changes have been introduced:

  — reviewed and added terminology;

  — aligned terminology with ISO/IEC 19790:2025;

  — introduced security requirements for attestation, backdoor of the components and supply chain in the field;

— introduced metaverse, IoT, big data and AI for the application environment.

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.

In information technology, there is an ever-increasing need to use cryptographic mechanisms, such as the protection of data against 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. Cryptographic modules are utilized within a security system to protect sensitive information in their application environment.

The purpose of this document is to describe the recommendations, requirements and checklists which help in the selection of cryptographic modules for deployment in a diversity of application environments. This document is helpful for the user and the field tester to verify correct deployment in the application environment.

Field testers determine the suitability and proper usage of a cryptographic module in its application environment.

Cryptographic modules and their application environments are generally complex and complicated. When cryptographic modules are deployed in an application environment and a field, a minor error or mistake can affect the security of the whole field and application environment. It is important to perform the field testing to ensure the proper usage of a cryptographic module in their field. This document identifies the field testing by providing:

— a secure assessment of the cryptographic module installation, configuration and operation;

— inspecting the key management system, protection of authentication credentials, and public and critical security parameters in the field;

— identifying cryptographic module vulnerabilities;

— checklists for the cryptographic algorithm policy, security guidance and regulation, security manager requirements, security level for each of the 11 requirement areas, the strength of the security function, etc.;

— inspecting that the cryptographic module's deployment satisfies the security requirements; and

— inspecting security toolkit for application system to help the user select security service in the field.

When using this document for field testing, it can be necessary to consult ISO/IEC 19790:2025; and ISO/IEC 24759:2025.