

This is a preview of ISO/IEC TS 20540:2025. [Click here to purchase the full version from the ANSI store.](#)

**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**

This is a preview of ISO/IEC TS 20540:2025. Click here to purchase the full version from the ANSI store.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2025

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  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of ISO/IEC TS 20540:2025. [Click here to purchase the full version from the ANSI store.](#)

<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Abbreviated terms</b> .....	<b>5</b>
<b>5 Document organization</b> .....	<b>5</b>
<b>6 Developing, validating and field testing</b> .....	<b>6</b>
<b>7 Cryptographic modules</b> .....	<b>7</b>
7.1 General.....	7
7.2 Types of cryptographic modules.....	7
7.2.1 General.....	7
7.2.2 Software module.....	8
7.2.3 Firmware module.....	8
7.2.4 Hardware module.....	8
7.2.5 Hybrid software module.....	8
7.2.6 Hybrid firmware module.....	8
7.3 Security requirements for cryptographic modules.....	9
7.3.1 General.....	9
7.3.2 Security level 1.....	9
7.3.3 Security level 2.....	10
7.3.4 Security level 3.....	10
7.3.5 Security level 4.....	11
7.4 Life-cycle assurance of cryptographic modules.....	11
7.5 Security policy of the module.....	12
7.5.1 General.....	12
7.5.2 Cryptographic module specification.....	12
7.5.3 Cryptographic module interfaces.....	12
7.5.4 Roles, services, and authentication.....	12
7.5.5 Software/firmware security.....	13
7.5.6 Operational environment.....	13
7.5.7 Physical security.....	13
7.5.8 Non-invasive security.....	13
7.5.9 Sensitive security parameters management.....	14
7.5.10 Self-tests.....	14
7.5.11 Life-cycle assurance.....	14
7.5.12 Mitigation of other attacks.....	14
7.6 Intended purpose or use of the validated cryptographic modules.....	15
<b>8 Application environment</b> .....	<b>15</b>
8.1 Organizational security.....	15
8.2 Architecture of the application environment.....	16
8.3 Application environments for the cryptographic modules.....	16
8.4 Security products with cryptographic modules.....	17
<b>9 Field</b> .....	<b>18</b>
9.1 Security requirements related to cryptographic modules for their field.....	18
9.1.1 General.....	18
9.1.2 Entropy sources.....	19
9.1.3 Audit mechanism.....	19
9.1.4 Physically unclonable function.....	19
9.2 Security assumptions for the field.....	19
9.2.1 General.....	19

This is a preview of ISO/IEC TS 20540:2025. [Click here to purchase the full version from the ANSI store.](#)

	9.2.4	Security level 3.....	21
	9.2.5	Security level 4.....	21
<b>10</b>		<b>How to select cryptographic modules.....</b>	<b>22</b>
	10.1	General.....	22
	10.2	Use policy.....	23
	10.3	Cryptographic module assurance.....	24
	10.4	Interoperability.....	24
	10.5	Selection of security rating for SSP protection.....	24
<b>11</b>		<b>Principles for field testing.....</b>	<b>25</b>
	11.1	General.....	25
	11.2	Assumptions.....	26
	11.3	Field testing activities.....	26
	11.4	Competence for field testers.....	27
	11.5	Use of validated evidence.....	27
	11.6	Documentations.....	27
	11.7	Field testing procedure.....	27
<b>12</b>		<b>Recommendations for field testing.....</b>	<b>28</b>
	12.1	General.....	28
	12.2	Installation, configuration, and operation of the cryptographic module.....	28
	12.2.1	General.....	28
	12.2.2	Assessing installation of the cryptographic module.....	28
	12.2.3	Assessing the configuration of the cryptographic module.....	29
	12.2.4	Assessing the correct operation of the cryptographic module.....	30
	12.3	Key management system.....	30
	12.4	Security requirements of authentication credentials.....	31
	12.5	Availability of cryptographic modules.....	32
	12.6	Potential residual vulnerabilities of cryptographic modules.....	32
	12.7	Security toolkit for the application system of cryptographic modules.....	33
	12.8	Organization's security policies.....	33
<b>13</b>		<b>Reporting the results of field testing.....</b>	<b>34</b>
		<b>Annex A (informative) Examples of validated cryptographic modules lists.....</b>	<b>35</b>
		<b>Annex B (informative) Security toolkit for application system of cryptographic modules in their field.....</b>	<b>36</b>
		<b>Annex C (informative) Checklist for field testing of cryptographic modules.....</b>	<b>40</b>
		<b>Bibliography.....</b>	<b>44</b>

This is a preview of ISO/IEC TS 20540:2025. [Click here to purchase the full version from the ANSI store.](#)

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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

This is a preview of ISO/IEC TS 20540:2025. [Click here to purchase the full version from the ANSI store.](#)

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.