International Standard

ISO/IEC 29128-2

First edition
2026-09

Information security, cybersecurity and privacy protection — Verification of cryptographic protocols —

Part 2: Evaluation methods and activities for cryptographic protocols

Sécurité de l'information, cybersécurité et protection de la vie privée — Vérification des protocoles cryptographiques —

Partie 2: Méthodes et activités d'évaluation pour les protocoles cryptographiques

Reference number
ISO/IEC 29128-2:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Security assessment and verification of cryptographic protocols ... **2**
4.1 Overview ... 2
4.2 Prover ... 4
4.2.1 Prover assurance level ... 4
4.2.2 Prover confidence level ... 4
4.3 Models ... 4
4.3.1 Cryptographic protocol model ... 4
4.3.2 Adversarial model ... 5
4.3.3 Formal protocol specification ... 5
4.3.4 Security properties ... 6

5 Method for cryptographic protocol security evaluation ... **6**
5.1 Overview ... 6
5.2 Scope of cryptographic evaluation method ... 6
5.3 Cryptographic protocol evaluation method ... 7
5.3.1 General ... 7
5.3.2 Prover evaluation method ... 7
5.3.3 Model evaluation method ... 7

6 Activities for cryptographic protocol security evaluation ... **8**

Annex A (informative) **List of tools for automated model verification** ... **10**

Annex B (informative) **Evaluation of the prover** ... **11**

Annex C (informative) **Extension model** ... **12**

Annex D (informative) **Relationship between confidence levels with Implementation Assurance Levels in ISO/IEC 29128-3** ... **13**

Bibliography ... **14**

© ISO/IEC 2026 – All rights reserved

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 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 Technical Committee ISO/IEC/JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 29128 series can be found on the ISO and IEC websites.

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.

© ISO/IEC 2026 – All rights reserved

Introduction

Cryptographic protocols form the basis of secure applications. A thorough evaluation is necessary to confirm their expected behaviour before deployment.

The ISO/IEC 29128 series specifies methods for the verification and evaluation of cryptographic protocols.

ISO/IEC 29128-1 specifies the formal verification process and the evidence produced by this process.

This document (see ISO/IEC 29128-2) specifies the methodology and evaluation activities for collecting and submitting the evidence from the formal verification process to the evaluator and the testing laboratory.

ISO/IEC 29128-3 specifies evaluation methods and activities for assessing a concrete implementation of a cryptographic protocol. It provides an assurance framework based on vulnerability assessment principles derived from the Common Criteria.

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection — Verification of cryptographic protocols —

Part 2: Evaluation methods and activities for cryptographic protocols

1 Scope

This document specifies an extension of evaluation methods and activities for cryptographic protocols based on ISO/IEC 15408-4, which provides a framework for evaluation methods and activities. This document provides a mapping between the work items for cryptographic protocol evaluation and the associated evaluation activities or evaluation methods. Additionally, this document also provides security assurance classification based on the cryptographic assessment performed by automated provers in four different levels of increasing assurance.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 29128-1:2023, *Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, terms and definitions used in ISO/IEC 29128-1 and the following 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

— IEC Electropedia: available at https://www.electropedia.org/

3.1
prover assurance level
level of assurance of the prover output with regards to correctness

3.2
prover confidence level
level of confidence of the prover to verify the security properties with regards to strength of the adversary

3.3
evaluation method
set of one or more *evaluation activities* (3.4) for application in a cryptographic protocol evaluation context

3.4
evaluation activity
specific actions performed by an evaluator as defined in this document

© ISO/IEC 2026 – All rights reserved

3.5
message
communication unit of information exchange between parties in a cryptographic protocol

3.6
model verification
proof of correctness of security properties obtained after an evaluator successfully performs all *evaluation activities* (3.4) for all security properties of the cryptographic protocol

3.7
rationale
evidence or reason for supporting the conformity to expected requirement(s)

3.8
automated prover
tool or set of tools used for evaluation of the security properties of a cryptographic protocol model

4 Security assessment and verification of cryptographic protocols

4.1 Overview

The security assessment and verification of cryptographic protocol performed by using an automated prover is presented in Figure 1, also capturing the submitter's responsibilities as specified in ISO/IEC 29128-1.

© ISO/IEC 2026 – All rights reserved