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)

Contents

Page

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.

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.

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*

Bibliography

[1] ISO/IEC 29128 (all parts), *Information security, cybersecurity and privacy protection — Verification of cryptographic protocols*

[2] ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

[3] ISO/IEC 15408-5, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

[4] ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Requirements and methodology for IT security evaluation*

[5] Protection Profile BSI-CC-PP-0117 – *Secure Sub-System in System-on-Chip (3S in SoC)*

[6] Goldwasser, S.; Micali, S. *Probabilistic Encryption*. Journal of Computer and System Sciences 28(2): 270–299, April 1984.

[7] Bana, G.; Comon-Lundh, H. Towards Unconditional Soundness: Computationally Complete Symbolic Attacker. In: POST 2012, LNCS 7215, pp. 189–208.

[8] EasyCrypt team. EasyCrypt: Computer-Aided Cryptographic Proofs https://www.easycrypt.info/

[9] Bruno Blanchet. *CryptoVerif: Cryptographic Protocol Verifier in the Computational Model*. https://prosecco.gforge.inria.fr/personal/bblanche/cryptoverif/

[10] Tamarin Prover Team. *The Tamarin Prover: Symbolic verification (proving) and falsification (attack finding) for security protocol*http://tamarin-prover.github.io/

[11] Bruno Blanchet. *ProVerif: Cryptographic Protocol Verifier in the Symbolic Model.*https://bblanche.gitlabpages.inria.fr/proverif/

[12] F* Team. *F*: A Proof-Oriented Programming Language.*https://www.fstar-lang.org/