DRAFT International Standard

ISO/IEC DIS 29128-3

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

Part 3: Evaluation methods and activities for protocol implementation verification

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2025-12-31

Voting terminates on:
2026-03-25

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 29128-3:2025(en)

© ISO/IEC 2025



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
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 Overview ... **2**
5 Formal evaluation methods and activities for cryptographic protocol implementation ... **3**
5.1 General ... 3
5.2 Evaluation method ... 3
5.2.1 General ... 3
5.2.2 Required inputs ... 4
5.2.3 Cryptographic Protocol Implementation Model ... 4
5.2.4 Adversarial Model ... 5
5.2.5 Scope of cryptographic protocol implementation evaluation methodology ... 5
5.2.6 Pass/Fail Criteria of theoretical proof ... 5
5.2.7 Pass/Fail Criteria of Vulnerability Analysis ... 5
5.2.8 Analysis of the Attack Scenarios ... 6
5.2.9 Attack feasibility ... 6
5.2.10 Security coverage ... 6
5.3 Evaluation Activities ... 6
5.3.1 General ... 6
5.3.2 Identification of evaluation activities ... 7
5.3.3 Objective of evaluation activities ... 7
5.3.4 Required developer inputs ... 8
5.3.5 Required Evaluator Activities ... 8
6 Implementation Assurance Levels ... **8**
6.1 General ... 8
6.2 IAL 1 ... 8
6.2.1 Requirements ... 8
6.3 IAL 2 ... 8
6.3.1 Requirements ... 9
6.4 IAL 3 ... 9
6.4.1 Requirements ... 9
6.5 IAL 4 ... 9
6.5.1 Requirements ... 9
6.6 IAL 5 ... 9
6.6.1 Requirements ... 9
6.7 IAL 6 ... 10
6.7.1 Requirements ... 10
6.8 IAL 7 ... 10
6.8.1 Requirements ... 10
6.9 Additional information on combined assurance and confidence levels ... 11
7 Vulnerability Assessment ... **11**
Annex A (informative) **Example of Known Attacks** ... **12**
Annex B (informative) **Example Evaluation based on Common Criteria CEM** ... **13**
Annex C (informative) **Example of Testing Tools** ... **14**
Bibliography ... **15**

© ISO/IEC 2025 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 *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. ISO 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.

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 website.

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.

© ISO/IEC 2025 – All rights reserved

Introduction

The assurance in a cryptographic protocol implementation is key to a secure cryptographic application. This assurance requires a thorough evaluation to ensure correct functionality and security principles. ISO/IEC 29128-1 highlights the importance of the formal verification of cryptographic protocols.

In ISO/IEC 29128-2 a framework of evaluation methods and evaluation activities for verifying cryptographic protocols derived from ISO/IEC 15408-4 is presented which contain four different assurance levels and three different confidence levels in a two-dimensional score matrix. These levels are based on the theoretical proof obtained from evaluations using automated provers.

In this document, the next step in cryptographic protocol evaluation is provided, working at the implementation level. The provided methods and activities can be utilized to evaluate any cryptographic protocol implementation at a hardware level, and determine its associated assurance level, in this document defined as an Implementation Assurance Level (IAL). The IAL is based on the combination of the theoretical proof obtained when the method or activity as specified in ISO/IEC 29218-2 is applied to the cryptographic protocol, and the vulnerability analysis in terms of security is obtained by performing AVA_VAN evaluation of the implementation.

This document aims at providing the developer and implementer of a cryptographic protocol with a framework to estimate the security capabilities of the cryptographic protocol and its implementation in a generic manner and therefore provide a basis for improvement in terms of security. Additionally, it provides a means to generalize the security evaluation process of different cryptographic protocols and their implementations with an implementation assurance level framework.

© ISO/IEC 2025 – All rights reserved

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

Part 3:
Evaluation methods and activities for protocol implementation verification

1 Scope

This document explains how to conduct an evaluation of a cryptographic protocol implementation based on the method framework provided in ISO/IEC 15408-4.

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, *Information security, cybersecurity and privacy protection — Verification of cryptographic protocols — Part 1: Framework*

ISO/IEC 29218-2, *Verification of cryptographic protocols — Part 2: Evaluation methods and activities for cryptographic protocols*

ISO/IEC 15408-4:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the following terms and definitions 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
attack scenario
adversarial setting that an evaluator identifies in which an underlying asset can be exploited by performing an attack

3.2
attack feasibility
degree of complexity of performing an attack with respect to an identified attack path pertaining to an *attack scenario* (3.1)

© ISO/IEC 2025 – All rights reserved

3.3
cryptographic protocol implementation under test
cryptographic protocol implementation model in *cryptographic protocol implementation submission package* (3.4) provided by a submitter to the evaluator to perform *security evaluation* (3.8) based on the evaluation method provided in this document

3.4
cryptographic protocol implementation submission package
formally verified cryptographic protocol specification from ISO/IEC 29128-2 and finite state model (FSM) representation of the cryptographic protocol implementation, and implementation of the cryptographic protocol combined with the evaluator capabilities (following 3.5) and a set of security properties that the evaluator must test the implementation for

3.5
common evaluation methodology (CEM)
evaluation methodology framework provided by Common Criteria standard scheme as ISO/IEC 18045:2022

3.6
implementation assurance level (IAL)
assurance metric denoting the security of the *cryptographic protocol implementation under test* (3.3) by the combination of the prover assurance level evaluated of the cryptographic protocol from the evaluation activity based on ISO/IEC 29128-2 and the prover assurance achieved by performing the evaluation activity based on this document.

3.7
security coverage
rationale indicating full coverage of the evaluation activity performed by the evaluator describing how all threat/attack scenarios applicable to the *cryptographic protocol implementation under test* (3.3) are covered

3.8
security evaluation
evaluation of the security strength and robustness of a cryptographic protocol implementation model by performing *vulnerability assessment* (3.9)

3.9
vulnerability assessment
security verification performed to measure the security robustness of a *cryptographic protocol implementation model* (3.4) following the *CEM* (3.5) within the scope of this document to prove the correctness of the *cryptographic protocol implementation under test* (3.3) and the security robustness of the design and implementation

4 Overview

The fundamental relationship between the three parts of the ISO/IEC 29128 is shown in Figure 1. This document provides evaluation methods and activities dedicated to evaluating the cryptographic protocol implementation. Combining the theoretical proof obtained as a result of applying the ISO/IEC 29128-2 framework with the result of applying the methods described in this document will lead to the determination of the Implementation Assurance Level (IAL) of the cryptographic protocol as described in clause 6.

© ISO/IEC 2025 – All rights reserved