INTERNATIONAL STANDARD

ISO/IEC 29128-1

Second edition
2023-03

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

Part 1: **Framework**

Reference number
ISO/IEC 29128-1:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

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

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Formal verification of cryptographic protocols ... **2**
4.1 Methods for modelling cryptographic protocols ... 2
4.2 Verification requirements ... 3
4.2.1 Methods of verification ... 3
4.2.2 Verification tools ... 3
4.2.3 Bounded vs unbounded verification ... 3
4.3 Cryptographic protocol model ... 4
4.3.1 Description of a model ... 4
4.3.2 Formal specification ... 4
4.3.3 Adversarial model ... 5
4.3.4 Submitting a model ... 5
4.3.5 Security properties ... 5
4.3.6 Self-assessment evidence ... 6
5 Verification process ... **6**
5.1 General ... 6
5.2 Duties of the submitter ... 6
5.3 Duties of the evaluator ... 6
5.3.1 Main duties ... 6
5.3.2 Evaluating the prover ... 6
5.3.3 Evaluating the model ... 6
5.3.4 Evaluating the evidence ... 7
5.3.5 Example evaluation ... 7
Annex A (informative) **The Needham-Schroeder-Lowe public key protocol** ... **8**
Annex B (informative) **Example submission** ... **9**
Annex C (informative) **Example evaluation** ... **10**
Annex D (informative) **Dolev-Yao model** ... **11**
Annex E (informative) **Security properties** ... **12**
Bibliography ... **14**

© ISO/IEC 2023 – 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 or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

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 29128:2011), which has been technically revised.

The main changes are as follows:

— removal of informal and paper-and-pencil proofs;

— deprecation of PAL levels;

— streamlining of technical requirements and explanations;

— minor editorial changes to bring the document in line with the ISO/IEC Directives Part 2, 2021.

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 2023 – All rights reserved

Introduction

Many cryptographic protocols have failed to achieve their stated security goals because they are complicated and difficult to design correctly in order to achieve the desired functional and security requirements. This inherent difficulty means that protocols need to be rigorously analysed in order to find errors in their design. The goal of this document is to standardize a method for analysing protocols by proposing a clearly defined verification framework based on well-founded scientific methods.

This document proposes a standardization procedure analogous to what exists for cryptographic algorithms. National and international bodies have evaluation processes that instil a high degree of confidence that a standardized cryptographic algorithm meets the specific security requirements it was designed for. A similar process for cryptographic protocols would provide confidence that a verified protocol meets its stated security properties and can be used in security-critical systems.

The proposed verification process is based on state-of-the-art protocol modelling techniques using rigorous logic, mathematics, and computer science. It is designed to provide objective evidence that a protocol satisfies its stated security goals. Verification is not a guarantee of security; as with any modelling, the results are constrained by the scope and quality of the model and tools used.

© ISO/IEC 2023 – All rights reserved

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

Part 1: Framework

1 Scope

This document establishes a framework for the verification of cryptographic protocol specifications according to academic and industry best practices.

2 Normative references

There are no normative references in this document.

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
adversarial model
capabilities an *adversary* (3.2) has when attempting to attack a *cryptographic protocol* (3.4)

3.2
adversary
party attempting to disrupt the secure operation of a *cryptographic protocol* (3.4), with abilities defined by the *adversarial model* (3.1)

3.3
automated prover
tool used for evaluating the *security properties* (3.9) of a *cryptographic protocol model* (3.5)

3.4
cryptographic protocol
communication protocol which uses cryptography to perform security-related functions

3.5
cryptographic protocol model
formal cryptographic protocol specification (3.8) combined with an *adversarial model* (3.1) and a set of *security properties* (3.9)

3.6
cryptographic protocol specification
human-readable document which defines the functionality of a *cryptographic protocol* (3.4)

© ISO/IEC 2023 – All rights reserved

3.7
evaluator
party in the verification process defined by this document who evaluates a submitted protocol

3.8
formal cryptographic protocol specification
model of a *cryptographic protocol specification* (3.6) written in a machine-readable language

3.9
security property
security goal which a *cryptographic protocol* (3.4) is designed to guarantee, transcribed into a machine-readable language

3.10
soundness
property of a mathematical system in which every statement that can be proved is true

3.11
self-assessment evidence
proofs of *security properties* (3.9) produced by an automated prover run on a *cryptographic protocol model* (3.5)

3.12
submitter
party in the verification process defined by this document who submits a protocol for evaluation

4 Formal verification of cryptographic protocols

4.1 Methods for modelling cryptographic protocols

The goal of the formal verification of a cryptographic protocol is to obtain a formal proof that the protocol, as defined in a protocol specification, meets its security properties and objectives within a specified adversarial framework. Achieving this goal requires the construction of a protocol model. There are two common paradigms for defining a protocol model - the symbolic model and the computational model.[11] The standardization process in this document considers only the symbolic model, however both models are reviewed here for completeness.

In the symbolic model, aspects of cryptography are abstracted out of the model, so cryptographic primitives are represented as black box functions and cryptography is assumed to be perfect. The adversary is restricted to computations and algebraic operations that are part of the given primitives, such as encrypting a message using a key, verifying a signature on a message, or computing the Diffie-Hellman public value from a known private value. In particular, this means that if an adversary knows some encrypted text, the only way they can learn the plain text from it is if they also possess the relevant key. Abstracting away from purely cryptographic attacks allows for the construction of a simple protocol model which is focused on the security of the protocol rather than the underlying cryptography.

In the computational model, the cryptographic aspects are an integral part of the model. The method of showing security in the protocol is to prove that attacking the protocol is at least as difficult as breaking one of the hard problems that the cryptographic primitives are based on. The adversary may do any computations on values they know, provided the computations run in polynomial time.

Automated tools for the computational model are limited and much less mature than for the symbolic model. As such, proofs in the computational model are generally hand-written rather than automated. Once tooling for computational models evolves, verification of protocols using those proofs can be incorporated into this document.

Another paradigm for proving protocol security, known as composition, involves proving statements about small parts of protocols and then combining those pieces together to prove statements about

© ISO/IEC 2023 – All rights reserved