INTERNATIONAL ISO/IEC

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 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

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.

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.