INTERNATIONAL STANDARD

ISO/IEC
29128

First edition
2011-12-15

Information technology — Security techniques — Verification of cryptographic protocols

Technologies de l'information — Techniques de sécurité — Vérification des protocoles cryptographiques

Reference number
ISO/IEC 29128:2011(E)

© ISO/IEC 2011

ISO/IEC 29128:2011(E)

Contents

ISO/IEC 29128:2011(E)

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29128 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

The security of digital communications is dependent on a number of aspects, where cryptographic mechanisms play an increasingly important role. When such mechanisms are being used, there are a number of security concerns such as the strength of the cryptographic algorithms, the accuracy and correctness of the implementation, the correct operation and use of cryptographic systems, and the security of the deployed cryptographic protocols.

Standards already exist for the specification of cryptographic algorithms, and for the implementation and test of cryptographic devices and modules. However, there are no standards or generally accepted processes for the assessment of the specification of protocols used in such communication. The goal of this International Standard is to establish means for verification of cryptographic protocol specifications to provide defined levels of confidence concerning the security of the specification of cryptographic protocols.
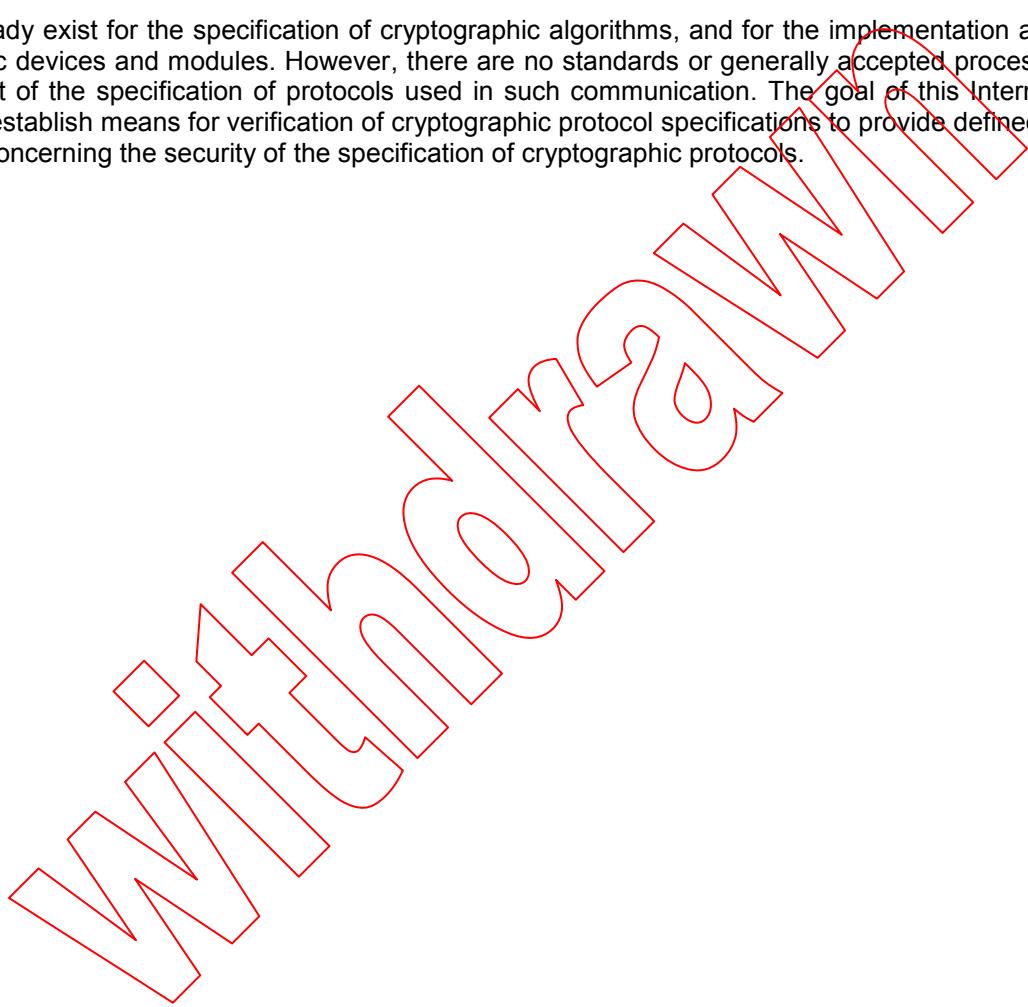
Information technology — Security techniques — Verification of cryptographic protocols

1   Scope

This International Standard establishes a technical base for the security proof of the specification of cryptographic protocols. This International Standard specifies design evaluation criteria for these protocols, as well as methods to be applied in a verification process for such protocols. This International Standard also provides definitions of different protocol assurance levels consistent with evaluation assurance components in ISO/IEC 15408.