INTERNATIONAL STANDARD

ISO/IEC 20543

First edition
2019-10

Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

Technologies de l'information — Techniques de sécurité — Méthodes d'essai et d'analyse des générateurs de bits aléatoires dans l'ISO/IEC 19790 et l'ISO/IEC 15408

Reference number
ISO/IEC 20543:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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).

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. 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 http://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.

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

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.

Introduction

Cryptographic applications need random numbers for a wide range of tasks. A strong cryptographic random bit generator that is suitable for general cryptographic applications is expected to provide output bit strings that cannot be distinguished with any potentially practical computational effort and any potentially practical sample sizes from bit strings of the same length drawn uniformly at random. Furthermore, such an RBG is expected to offer enhanced backward secrecy and enhanced forward secrecy.

Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

1 Scope

This document specifies a methodology for the evaluation of non-deterministic or deterministic random bit generators intended to be used for cryptographic applications. The provisions given in this document enable the vendor of an RBG to submit well-defined claims of security to an evaluation authority and shall enable an evaluator or a tester, for instance a validation authority, to evaluate, test, certify or reject these claims.

This document is implementation-agnostic. Hence, it offers no specific guidance on design and implementation decisions for random bit generators. However, design and implementation issues influence the evaluation of an RBG in this document, for instance because it requires the use of a stochastic model of the random source and because any such model is supported by technical arguments pertaining to the design of the device at hand.

Random bit generators as evaluated in this document aim to output bit strings that appear evenly distributed. Depending on the distribution of random numbers required by the consuming application, however, it is worth noting that additional steps can be necessary (and can well be critical to security) for the consuming application to transform the random bit strings produced by the RBG into random numbers of a distribution suitable to the application requirements. Such subsequent transformations are outside the scope of evaluations performed in this document.

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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 17825, *Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*

ISO/IEC 18031:2011, *Information technology — Security techniques — Random bit generation*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*