International Standard

ISO/IEC 18031

Information technology — Security techniques — Random bit generation

Technologies de l'information — Techniques de sécurité — Génération de bits aléatoires

Third edition
2025-02

Reference number
ISO/IEC 18031:2025(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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols **7**
5 Properties and requirements of a random bit generator **8**
5.1 Properties of arandom bit generator 8
5.2 Requirements of an RBG 9
5.3 Additional information for an RBG 10
6 RBG model **10**
6.1 Conceptual functional model for random bit generation 10
6.2 RBG basic components 11
6.2.1 Introduction to the RBG basic components 11
6.2.2 Randomness source 11
6.2.3 Additional inputs 12
6.2.4 Internal state 12
6.2.5 Internal state transition functions 13
6.2.6 Output generation function 14
6.2.7 Health test 15
7 Types of RBGs **15**
7.1 Introduction to the types of RBGs 15
7.2 Non-deterministic random bit generators 16
7.3 Deterministic random bit generators 17
7.4 The RBG spectrum 17
8 Overview and requirements for an NRBG **17**
8.1 NRBG overview 17
8.2 Functional model of an NRBG 18
8.3 NRBG entropy sources 20
8.3.1 General 20
8.3.2 Primary entropy source for an NRBG 20
8.3.3 Physical entropy sources for an NRBG 22
8.3.4 NRBG non-physical entropy sources 22
8.3.5 NRBG additional entropy sources 23
8.3.6 Hybrid NRBGs 24
8.4 NRBG additional inputs 24
8.4.1 NRBG additional inputs overview 24
8.4.2 Requirements for NRBG additional inputs 24
8.5 NRBG internal state 25
8.5.1 NRBG internal state overview 25
8.5.2 Requirements for the NRBG internal state 25
8.5.3 Additional information for the NRBG internal state 26
8.6 NRBG internal state transition functions 26
8.6.1 NRBG internal state transition functions overview 26
8.6.2 Requirements for the NRBG internal state transition functions 27
8.6.3 Recommendations for the NRBG internal state transition functions 27
8.7 NRBG output generation function 27
8.7.1 NRBG output generation function overview 27
8.7.2 Requirements for the NRBG output generation function 28
8.8 NRBG health tests 28
8.8.1 NRBG health tests overview 28
8.8.2 General NRBG health test requirements 29

© ISO/IEC 2025 – All rights reserved

8.8.3 NRBG health test on deterministic components 29
8.8.4 NRBG health tests within entropy sources 30
8.8.5 NRBG health tests on random output 31
8.9 NRBG component interaction 32
8.9.1 NRBG component interaction overview 32
8.9.2 Requirements for NRBG component interaction 32
8.9.3 Recommendations for NRBG component interaction 33
9 Overview and requirements for a DRBG 33
9.1 DRBG overview 33
9.2 Functional model of a DRBG 33
9.3 DRBG randomness source 36
9.3.1 Primary randomness source for a DRBG 36
9.3.2 Generating seed values for a DRBG 37
9.3.3 Additional randomness sources for a DRBG 38
9.3.4 Hybrid DRBGs 38
9.4 Additional inputs for a DRBG 38
9.5 Internal state for a DRBG 39
9.6 Internal state transition function for a DRBG 39
9.7 Output generation function for a DRBG 40
9.8 Health tests for a DRBG 40
9.8.1 DRBG health tests overview 40
9.8.2 DRBG health test 41
9.8.3 DRBG deterministic algorithm test 41
9.8.4 DRBG software/firmware integrity test 41
9.8.5 DRBG critical functions test 41
9.8.6 DRBG software/firmware load test 41
9.8.7 DRBG manual key entry test 42
9.8.8 Continuous tests on noise sources in entropy sources 42
9.9 Additional requirements for DRBG keys 42
Annex A (normative) **Combining RBGs 44**
Annex B (normative) **Conversion methods for random number generation 45**
Annex C (informative) **Deterministic random bit generators 48**
Annex D (informative) **NRBG examples 75**
Annex E (informative) **Security considerations 84**
Annex F (informative) **Discussion on the estimation of entropy 88**
Annex G (informative) **RBG assurance 89**
Annex H (normative) **RBG boundaries 90**
Annex I (informative) **Rationale for the design of statistical tests 92**
Bibliography 93

© ISO/IEC 2025 – All rights reserved

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC 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 and https://patents.iec.ch. ISO and IEC 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. 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 third edition cancels and replaces the second edition (ISO/IEC 18031:2011), which has been technically revised. It also incorporates the Amendment ISO/IEC 18031:2011/Amd 1:2017 and the Technical Corrigendum ISO/IEC 18031:2011/Cor 1:2014.

The main changes are as follows:

— removal of the MQ_DRBG, Micali-Schnorr DRBG, Dual_EC_DRBG and SHA-1;

— addition and harmonization of the terms and definitions in Clause 3;

— addition of conversion methods for random number generation;

— update of the requirements for DRBGs and NRBGs.

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 2025 – All rights reserved

Introduction

This document sets out specific requirements that, when met, will result in the development of a random bit generator that can be applicable to cryptographic applications.

Numerous cryptographic applications involve the use of random bits. These cryptographic applications include the following:

— random keys and initialization values (*IVs*) for encryption,

— random keys for keyed MAC algorithms,

— random private keys for digital signature algorithms,

— random values to be used in entity authentication mechanisms,

— random values to be used in key-establishment protocols,

— random PINs and passwords,

— nonces.

The purpose of this document is to establish a conceptual model, terminology and requirements related to the building blocks and properties of systems used for random bit generation in or for cryptographic applications.

It is possible to categorize random bit generators into two types, namely, non-deterministic and deterministic random bit generators.

A non-deterministic random bit generator can be defined as a random bit generating mechanism that continuously uses a source of entropy to generate a random bit stream.

A deterministic random bit generator can be defined as a bit generating mechanism that uses deterministic mechanisms such as cryptographic algorithms to generate a random bit stream. In this type of bit stream generation, there is a specific input (normally called a seed) and perhaps some optional input, which, depending on its application, can either be publicly available or not. The seed is processed by a function which provides an output.

NOTE This document also discusses hybrid random bit generators, which incorporate elements of both non-deterministic and deterministic generators.

In this document, variable symbols and variable descriptive terms are given in italic font.

© ISO/IEC 2025 – All rights reserved

Information technology — Security techniques — Random bit generation

1 Scope

This document specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model.

This document specifies the characteristics of the main elements required for both non-deterministic and deterministic random bit generators. It also establishes the security requirements for both non-deterministic and deterministic random bit generators.

Techniques for statistical testing of random bit generators for the purposes of independent verification or validation and detailed designs for such generators are outside the scope of 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 9797-2, *Information security — Message authentication codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*

ISO/IEC 10118-3, *IT Security techniques — Hash-functions — Part 3: Dedicated hash-functions*

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

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

ISO/IEC 29192-5, *Information technology — Security techniques — Lightweight cryptography — Part 5: Hash-functions*

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
algorithm
clearly specified mathematical process for the computation of a set of rules that, if followed, will give a prescribed result

3.2
backward secrecy
assurance that previous *random bit generator (RBG)* (3.40) output values cannot be determined with practical computational effort from knowledge of current or subsequent (future) output values

© ISO/IEC 2025 – All rights reserved