

ISO/IEC ~~DIS~~ 18031:2023(E)2024(en)
ISO/IEC JTC 1/SC 27/WG 2
Secretariat: DIN
Date: ~~2023-11-20~~2024-12-10
Information security — Random bit generation
Technologies de l'information — Techniques de sécurité — Génération de bits aléatoires

Formatted: Centered

Style Definition: Heading 1

Style Definition: Heading 2

Style Definition: Heading 3

Style Definition: Heading 4

Style Definition: Heading 5

Style Definition: Heading 6

Style Definition: Default Paragraph Font

Style Definition: ANNEX

Style Definition: 変更箇所1: No widow/orphan control, Don't hyphenate

Style Definition: Base_Heading: Font:

Style Definition: Base_Text: Font:

Style Definition: AMEND Terms Heading

Style Definition: AMEND Heading 1 Unnumbered

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

iTech Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC 18031

<https://standards.iteh.ai/catalog/standards/iso/a4e9e433-3dc9-4d7f-8777-fdf8614c2a4c/iso-iec-18031>

Formatted: Centered

Edited DIS - MUST BE USED FOR FINAL DRAFT

© ~~ISO/IEC 2023~~ 2024

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~~ISO's member body in the country of the requester.

ISO ~~copyright office~~Copyright Office

Formatted: Indent: Left: 0.5 cm, Right: 0.5 cm, Space Before: 0 pt, No page break before, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Default Paragraph Font

CP 401 • ~~Ch. de Blandonnet 8~~

CH-1214 Vernier, Geneva

Phone: +41 22 749 01 11

Formatted: Indent: Left: 0.5 cm, First line: 0 cm, Right: 0.5 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Email: ~~copyright@iso.org~~

Email: ~~copyright@iso.org~~

Website: ~~www.iso.org~~www.iso.org

Published in Switzerland.

Formatted: Indent: Left: 0.5 cm, First line: 0 cm, Right: 0.5 cm, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 18031
https://standards.iteh.ai/catalog/standards/iso/a4e9e433-3dc9-4d7f-8777-fdf8614c2a4c/iso-iec-18031

Contents

Foreword	vii
Introduction	viii
1 Scope	9
2 Normative references	9
3 Terms and definitions	9
4 Symbols	17
5 Properties and requirements of an RBG	18
5.1 Properties of an RBG	18
5.2 Requirements of an RBG	19
5.3 Recommendations for an RBG	20
6 RBG model	21
6.1 Conceptual functional model for random bit generation	21
6.2 RBG basic components	21
6.2.1 Introduction to the RBG basic components	21
6.2.2 Randomness source	22
6.2.3 Additional inputs	23
6.2.4 Internal state	23
6.2.5 Internal state transition functions	25
6.2.6 Output generation function	26
6.2.7 Health test	27
7 Types of RBGs	27
7.1 Introduction to the types of RBGs	27
7.2 Non-deterministic random bit generators	28
7.3 Deterministic random bit generators	29
7.4 The RBG spectrum	29
8 Overview and requirements for an NRBG	30
8.1 NRBG overview	30
8.2 Functional model of an NRBG	30
8.3 NRBG entropy sources	33
8.3.1 General	33
8.3.2 Primary entropy source for an NRBG	33
8.3.3 Physical entropy sources for an NRBG	35
8.3.4 NRBG non-physical entropy sources	36
8.3.5 NRBG additional entropy sources	36
8.3.6 Hybrid NRBGs	38
8.4 NRBG additional inputs	38
8.4.1 NRBG additional inputs overview	38
8.4.2 Requirements for NRBG additional inputs	38
8.5 NRBG internal state	39
8.5.1 NRBG internal state overview	39
8.5.2 Requirements for the NRBG internal state	39
8.5.3 Recommendations for the NRBG internal state	40
8.6 NRBG internal state transition functions	41
8.6.1 NRBG internal state transition functions overview	41

8.6.2	Requirements for the NRBG internal state transition functions	42
8.6.3	Recommendations for the NRBG internal state transition functions	42
8.7	NRBG output generation function	42
8.7.1	NRBG output generation function overview	42
8.7.2	Requirements for the NRBG output generation function	42
8.8	NRBG health tests	43
8.8.1	NRBG health tests overview	43
8.8.2	General NRBG health test requirements	44
8.8.3	NRBG health test on deterministic components	45
8.8.4	NRBG health tests within entropy sources	46
8.8.5	NRBG health tests on random output	47
8.9	NRBG component interaction	48
8.9.1	NRBG component interaction overview	48
8.9.2	Requirements for NRBG component interaction	49
8.9.3	Recommendations for NRBG component interaction	49
9	Overview and requirements for a DRBG	49
9.1	DRBG overview	49
9.2	Functional model of a DRBG	50
9.3	DRBG randomness source	53
9.3.1	Primary randomness source for a DRBG	53
9.3.2	Generating seed values for a DRBG	55
9.3.3	Additional randomness sources for a DRBG	56
9.3.4	Hybrid DRBGs	56
9.4	Additional inputs for a DRBG	56
9.5	Internal state for a DRBG	57
9.6	Internal state transition function for a DRBG	58
9.7	Output generation function for a DRBG	59
9.8	Health tests for a DRBG	59
9.8.1	DRBG health tests overview	59
9.8.2	DRBG health test	60
9.8.3	DRBG deterministic algorithm test	60
9.8.4	DRBG software/firmware integrity test	60
9.8.5	DRBG critical functions test	60
9.8.6	DRBG software/firmware load test	60
9.8.7	DRBG manual key entry test	61
9.8.8	Continuous Tests on Noise Sources in Entropy Sources	61
9.9	Additional requirements for DRBG keys	61
Annex A (normative)	Combining RBGs	64
Annex B (normative)	Conversion methods for random number generation	65
B.1	Techniques for generating random numbers	65
B.2	The simple discard method	65
B.3	The complex discard method	65
B.4	The simple modular method	66
B.5	The complex modular method	66
B.6	The simple partial discard method	66
B.7	The complex partial discard method	67
Annex C (informative)	DRBGs	68

<u>C.1</u>	<u>DRBG mechanism examples</u>	<u>68</u>
<u>C.2</u>	<u>DRBGs based on hash functions</u>	<u>68</u>
<u>C.2.1</u>	<u>Introduction to DRBGs based on hash functions</u>	<u>68</u>
<u>C.2.2</u>	<u>Hash DRBG</u>	<u>68</u>
<u>C.2.2.1</u>	<u>Discussion</u>	<u>68</u>
<u>C.2.2.2</u>	<u>Description</u>	<u>69</u>

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO/IEC 18031

<https://standards.iteh.ai/catalog/standards/iso/a4e9e433-3dc9-4d7f-8777-fdf8614c2a4c/iso-iec-18031>

6.2.2.2.1 Contents

Foreword	10
Introduction	12
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Symbols	9
5 Properties and requirements of a random bit generator	9
5.1 Properties of a random bit generator	9
5.2 Requirements of an RBG	10
5.3 Additional information for an RBG	12
6 RBG model	12
6.1 Conceptual functional model for random bit generation	12
6.2 RBG basic components	12
6.2.1 Introduction to the RBG basic components	12
6.2.2 Randomness source	14
6.2.3 Additional inputs	15
6.2.4 Internal state	15
6.2.5 Internal state transition functions	17
6.2.6 Output generation function	18
6.2.7 Health test	18
7 Types of RBGs	19
7.1 Introduction to the types of RBGs	19
7.2 Non-deterministic random bit generators	19
7.3 Deterministic random bit generators	20
7.4 The RBG spectrum	20
8 Overview and requirements for an NRBG	21
8.1 NRBG overview	21
8.2 Functional model of an NRBG	22
8.3 NRBG entropy sources	25
8.3.1 General	25
8.3.2 Primary entropy source for an NRBG	25
8.3.3 Physical entropy sources for an NRBG	27
8.3.4 NRBG non-physical entropy sources	28
8.3.5 NRBG additional entropy sources	28
8.3.6 Hybrid NRBGs	29
8.4 NRBG additional inputs	30
8.4.1 NRBG additional inputs overview	30
8.4.2 Requirements for NRBG additional inputs	30
8.5 NRBG internal state	30
8.5.1 NRBG internal state overview	30
8.5.2 Requirements for the NRBG internal state	31
8.5.3 Additional information for the NRBG internal state	32
8.6 NRBG internal state transition functions	32
8.6.1 NRBG internal state transition functions overview	32
8.6.2 Requirements for the NRBG internal state transition functions	33

8.6.3	Recommendations for the NRBG internal state transition functions.....	34
8.7	NRBG output generation function	34
8.7.1	NRBG output generation function overview.....	34
8.7.2	Requirements for the NRBG output generation function.....	34
8.8	NRBG health tests	35
8.8.1	NRBG health tests overview.....	35
8.8.2	General NRBG health test requirements.....	36
8.8.3	NRBG health test on deterministic components	36
8.8.4	NRBG health tests within entropy sources	37
8.8.5	NRBG health tests on random output.....	38
8.9	NRBG component interaction.....	40
8.9.1	NRBG component interaction overview	40
8.9.2	Requirements for NRBG component interaction	40
8.9.3	Recommendations for NRBG component interaction	40
9	Overview and requirements for a DRBG.....	40
9.1	DRBG overview.....	40
9.2	Functional model of a DRBG	41
9.3	DRBG randomness source	44
9.3.1	Primary randomness source for a DRBG	44
9.3.2	Generating seed values for a DRBG.....	46
9.3.3	Additional randomness sources for a DRBG.....	47
9.3.4	Hybrid DRBGs	47
9.4	Additional inputs for a DRBG	47
9.5	Internal state for a DRBG	48
9.6	Internal state transition function for a DRBG	49
9.7	Output generation function for a DRBG.....	49
9.8	Health tests for a DRBG	50
9.8.1	DRBG health tests overview.....	50
9.8.2	DRBG health test	50
9.8.3	DRBG deterministic algorithm test.....	51
9.8.4	DRBG software/firmware integrity test.....	51
9.8.5	DRBG critical functions test	51
9.8.6	DRBG software/firmware load test.....	51
9.8.7	DRBG manual key entry test.....	51
9.8.8	Continuous tests on noise sources in entropy sources	51
9.9	Additional requirements for DRBG keys.....	52
Annex A (normative)	Combining RBGs	54
Annex B (normative)	Conversion methods for random number generation.....	55
Annex C (informative)	Deterministic random bit generators	59
Annex D (informative)	NRBG examples.....	88
Annex E (informative)	Security considerations.....	100
Annex F (informative)	Discussion on the estimation of entropy.....	104
Annex G (informative)	RBG assurance	105
Annex H (normative)	RBG boundaries.....	106
Annex I (informative)	Rationale for the design of statistical tests	109
Bibliography	111

General 69

C.2.2.2.2	Instantiation of Hash DRBG (...)	71
C.2.2.2.2	Reseeding Hash DRBG (...) Instantiation	73
C.2.2.2.4	Generating pseudorandom bits using Hash DRBG (...)	74
C.2.2.2.5	Inserting additional entropy into the state of Hash DRBG (...)	76
C.2.3	HMAC DRBG	77
C.2.3.1	Discussion	77
C.2.3.2	Description	77
C.2.3.2.1	General	77
C.2.3.2.2	Internal function: The Update function	79
C.2.3.2.3	Instantiation of HMAC DRBG	79
C.2.3.2.4	Reseeding HMAC DRBG (...) Instantiation	80
C.2.3.2.5	Generating pseudorandom bits using HMAC DRBG (...)	81
C.3	DRBGs based on block ciphers	83
C.3.1	Introduction to DRBGs based on block ciphers	83
C.3.2	CTR DRBG	83
C.3.2.1	Discussion	83
C.3.2.2	Description	84
C.3.2.2.1	General	84
C.3.2.2.2	Instantiation of CTR DRBG (...)	86
C.3.2.2.3	Internal function: The Update function	87
C.3.2.2.4	Derivation function using a block cipher algorithm	88
C.3.2.2.5	CBC MAC function	89
C.3.2.2.6	Reseeding CTR DRBG (...) Instantiation	90
C.3.2.2.7	Generating pseudorandom bits using CTR DRBG (...)	91
C.3.3	OFB DRBG	93
C.3.3.1	Discussion	93
C.3.3.2	Description	93
C.3.3.2.1	General	93
C.3.3.2.2	Internal function: The update function	94
C.3.3.2.3	Instantiation of OFB DRBG (...)	94
C.3.3.2.4	Reseeding OFB DRBG (...) Instantiation	94
C.3.3.2.5	Generating pseudorandom bits using OFB DRBG (...)	94
Annex D (informative)	NRBG examples	97
D.1	Canonical coin tossing example	97
D.1.1	Overview	97

Formatted: Default Paragraph Font, English (United Kingdom)

<u>D.1.2 Description of basic process</u>	<u>97</u>
<u>D.1.3 Relation to standard NRBG components</u>	<u>97</u>
<u>D.1.4 Optional variations</u>	<u>98</u>
<u>D.1.5 Peres unbiasing procedure</u>	<u>99</u>
<u>D.2 Hypothetical noisy diode example</u>	<u>99</u>
<u>D.2.1 Overview</u>	<u>99</u>
<u>D.2.2 General structure</u>	<u>99</u>
<u>D.2.3 Details of operation</u>	<u>100</u>
<u>D.2.3.1 Entropy source</u>	<u>100</u>
<u>D.2.3.2 Primary tasks</u>	<u>101</u>
<u>D.2.3.3 Health tests</u>	<u>102</u>
<u>D.2.3.4 Health test details</u>	<u>103</u>
<u>D.2.4 Failsafe design consequences</u>	<u>104</u>
<u>D.2.5 Modified example</u>	<u>104</u>
<u>D.3 Mouse movement example</u>	<u>105</u>
<u>Annex E (informative) Security considerations</u>	<u>106</u>
<u>E.1 Attack model</u>	<u>106</u>
<u>E.2 The security of hash-functions</u>	<u>106</u>
<u>E.3 Algorithm and key size selection</u>	<u>106</u>
<u>E.3.1 Introduction</u>	<u>106</u>
<u>E.3.2 Equivalent algorithm strengths</u>	<u>107</u>
<u>E.3.3 Selection of appropriate DRBGs</u>	<u>108</u>
<u>E.4 The security of block cipher DRBGs</u>	<u>109</u>
<u>E.5 Conditioned entropy source output and the derivation function for block cipher DRBGs</u>	<u>109</u>
<u>Annex F (informative) Discussion on the estimation of entropy</u>	<u>110</u>
<u>Annex G (informative) RBG assurance</u>	<u>111</u>
<u>Annex H (informative) RBG boundaries</u>	<u>112</u>
<u>Annex I (informative) Rationale for the design of statistical tests</u>	<u>114</u>
<u>I.1 Introduction</u>	<u>114</u>
<u>I.2 Runs test</u>	<u>114</u>
<u>I.3 Long runs test</u>	<u>115</u>
<u>Bibliography</u>	<u>1</u>

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/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.

Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Formatted: Font color: Auto

Formatted: cite_sec

Formatted: cite_sec

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.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC 18031

<https://standards.itih.ai/catalog/standards/iso/a4e9e433-3dc9-4d7f-8777-fdf8614c2a4c/iso-iec-18031>

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 ~~initialisation~~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~~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.

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO/IEC 18031

<https://standards.itih.ai/catalog/standards/iso/a4e9e433-3dc9-4d7f-8777-fdf8614c2a4c/iso-iec-18031>