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)

Formatted: Centered

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

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

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

Contents

~~C.2.2.2.1~~ Contents

Formatted: Default Paragraph Font, English (United Kingdom)

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~~www.iso.org/directives or ~~www.iec.ch/members_experts/refdocs~~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~~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~~www.iso.org/iso/foreword.html. In the IEC, see ~~www.iec.ch/understanding-standards~~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~~.www.iso.org/members.html and www.iec.ch/national-committees.

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.

