GRAND-DUCHY OF LUXEMBOURG

INCERT

31st May – 1st June 2023

NIST RBG WORKSHOP

New edition of ISO/IEC 18031 on Random Bit Generation

Overview of ISO/IEC 20543 on test and analysis of random bit generators

Gaëtan Pradel, INCERT

Version 1.2

Classification: Unclassified

TABLE OF CONTENTS

INCERT

Introduction

01

Introduction

Background

The International Organization for Standardization (ISO) **develop and publish international standards** on many topics.

The topic discussed in this document is **information security**, more specifically the random generation of bits.

Context

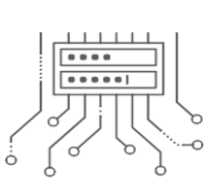
During the last three years, the standard ISO/IEC 18031 on Random Bit Generation (RBG) is going through an extensive revision.

Purpose of this document

In this document, an overview of the changes from the last edition to the (foreseen) new one is presented.

Additionally, a succinct overview of the ISO/IEC 20543 on test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408 is discussed.

– INCERT: who are we?



DEFENDING LUXEMBOURG'S NATIONAL INTERESTS

STATE-OWNED

INCERT

FOUNDED IN 2012

SERVING PUBLIC SECTOR

(HISTORICAL MISSION)

DESIGNING & APPLYING EMERGING TECHNOLOGIES

CREATING DIGITAL ASSETS

(FOR BOTH PUBLIC & PRIVATE SECTORS)

INCERT

How ISO works

02

How ISO works

Participants

Each country has a national body (NB) which has a certain membership to ISO. Based on this membership, NBs have **participation rights or observation rights** for the development of standards.

Experts participating to the development of standards can come from **industry**, **government**, **academia** or **any other relevant sectors**, and **represent the NB** in which they are registered.

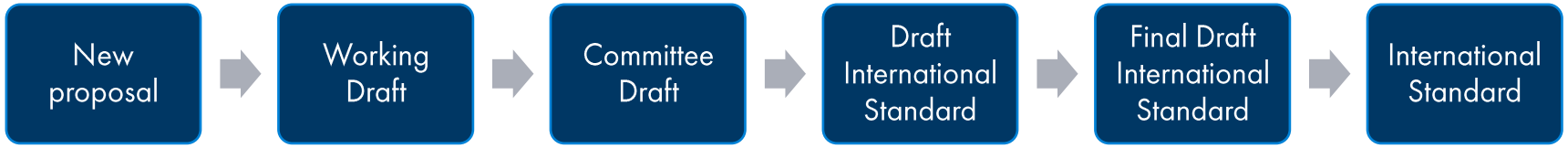
Consensus-based

The voting process is based on **consensus**.

Consensus is typically achieved through discussion, negotiation, and compromise. The goal is to find a balance that reflects the collective expertise and interests of the stakeholders involved. Ultimately, the standard is approved if it receives a two-thirds majority vote from the ISO member bodies.

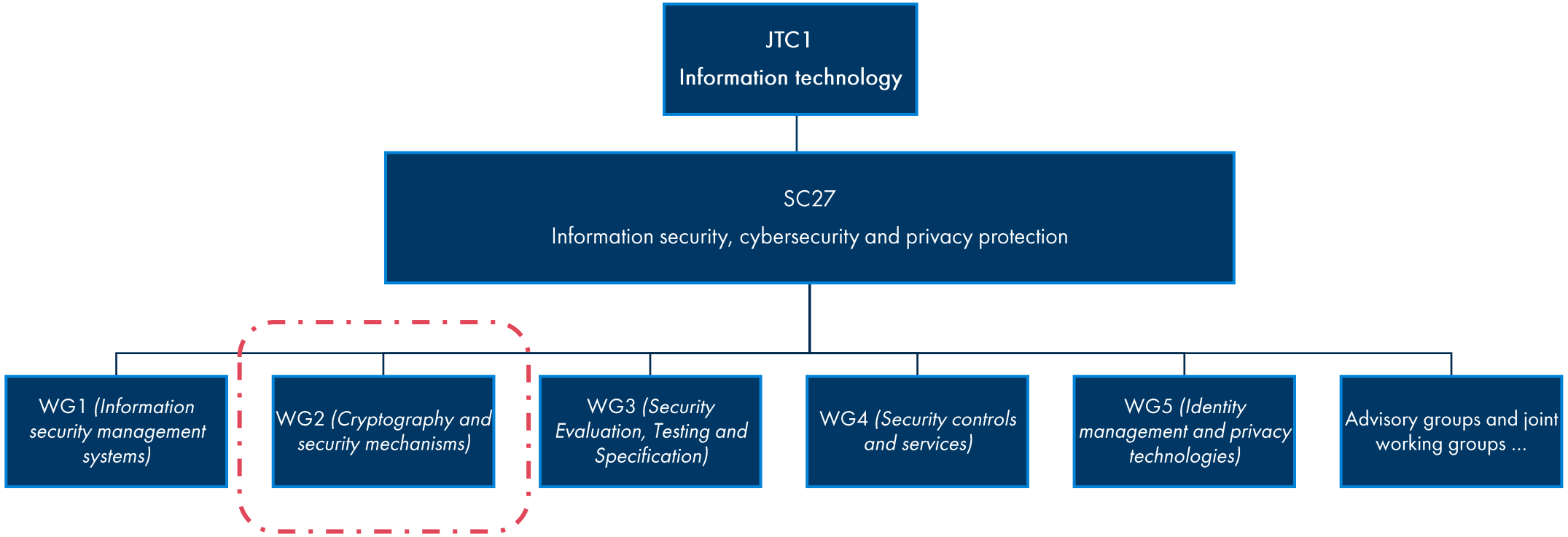
From first proposal to final publication, developing a standard usually takes **about 3 years**. **Every 5 years, a standard is revised**.

Standard Development stages



ISO/IEC JTC1 SC27

Structure



INCERT

INCERT

ISO/IEC 18031

03

ISO/IEC 18031

Several editions

The editions of the ISO/IEC 18031 standard are as follows:

1. First edition in **2005**
2. Second edition in **2011**
3. Third edition is currently ongoing (more on this later)

Scope from the third edition

*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**, and establishes the **security requirements** for both non-deterministic and deterministic random bit generators.*

Where there is a requirement to produce sequences of random numbers from random bit-strings, the guidelines in Annex B on how this can be performed shall be followed.

***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**.*

GRAND-DUCHY OF LUXEMBOURG

INCERT

2011 Edition

04

Classification: Unclassified

2011 Edition

Contents

Main Body:

1. Properties and requirements of an Random Bit Generator (RBG)
2. RBG model
3. Types of RBGs
4. Overview and requirements for an Non-Deterministic Random Bit Generator (NRBG)
5. Overview and requirements for a Deterministic Random Bit Generator (DRBG)

Annexes:

1. Combining RBGs and conversion methods
2. DRBGs
3. Application specific constants
4. NRBG examples
5. Security considerations
6. Estimation of entropy, RBG assurance and boundaries
7. Rational for the design of statistical tests

2011 Edition

Defect report on ISO/IEC 18031

- Submitted by a RU expert on the 7th October 2019
- The standard describes the MQ_DRBG mechanism (Annex C), and it has been shown that it is possible to **construct weak instances** of this mechanism (with lower security than claimed by the standard).
- Possible **security problems** with **real-life implementations** of MQ_DRBG.
- The conclusion of the associated meeting is that the security of MQ_DRBG, including the implications on ISO/IEC 18031, will be evaluated in the ISO process called "Study Period".

Revision of ISO/IEC 18031:2011

In April 2020, it has been agreed in the ISO/IEC JTC1 SC27 WG2 meetings to revise ISO/IEC 18031.

- Target date for the International Standard publication: **October 2023**
- Editors: **Gaëtan Pradel (LU)** and **Chris Mitchell (GB)**

INCERT

Main incoming changes

05

Main incoming changes

General information

- Currently at DIS stage
- Three Working Drafts and two Committee Drafts
- Participation of several national bodies, in particular the NIST **(thank you!)**
- Overall, **a total of more than 1,000 comments** (so far!)

Main incoming changes

Details

- **Removal of mechanisms:**
  - MQ_DRBG
  - Micali-Schnorr DRBG
  - Dual_EC_DRBG
  - SHA-1
- **Addition of definitions and terms** such as
  - (enhanced) forward and backward secrecy
  - Hybrid/pure DRBGs and NRBGs
- **Harmonisation of definitions and terms** used in the text such as:
  - (physical) noise source
  - randomness source
  - entropy source
  - seed / seed value
  - secret parameter

- **Addition of conversion methods for random number generation:**
  - The simple partial discard method
  - The complex partial discard method
- Update on the **requirements for DRBGS and NRBGS**, for example adding forward secrecy or backward secrecy if necessary.
- (Many!) **editorial updates** for a clearer text.

INCERT

Main incoming changes

Contents of the new edition (subject to small updates)

Main Body:

1. Properties and requirements of an RBG
2. RBG model
3. Types of RBGs
4. Overview and requirements for an NRBG
5. Overview and requirements for a DRBG

Annexes:

1. Combining RBGs and conversion methods
2. DRBGs (removal of mechanisms)
3. ~~Application specific constants~~
4. NRBG examples
5. Security considerations
6. Estimation of entropy, RBG assurance and boundaries
7. Rational for the design of statistical tests

INCERT

ISO/IEC 20543

06

ISO/IEC 20543:2019

Title and scope

ISO/IEC 20543:2019 *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

→ methodology for the evaluation of NRBGs and DRBGs intended to be used for cryptographic applications.

Working Group involved

ISO/IEC JTC1 SC27 **WG3**

Key points

- The **standard does not provide methodologies or implementation requirements/recommendations for implementing an RBG**, but rather methodologies to evaluate the security claims of an RBG.
- The standard focuses on testing and evaluation activities for RBGs for a conformance scheme using **ISO/IEC 19790** (security requirements for security modules) and an evaluation scheme using the **ISO/IEC 15408 series** (common criteria).
- **Transformation of random bits to random numbers** are outside of the scope of this document.

Contents

Main body:

- Overview of NRBGs and conformance testing
- Overview of DRBGs and conformance testing
- Testing methodology

Annexes:

- General statistical methodology
- Test files

INCERT

INCERT

Conclusion

07

Conclusion

- The third edition of ISO/IEC 18031 on Random Bit Generation is expected to be **published end of 2023 or during 2024.**
- This new edition has been through **an extensive review** (few working drafts, few committee drafts).
- **More than 1,000 comments** were provided by experts in almost three years of work!
- The main changes include
  - a **removal of some of the DRBGs**,
  - the **addition of conversion methods,** and
  - the **harmonisation of definitions and terms** throughout the document (with consideration of alignment with ISO/IEC 20543).
- Overall, a **higher quality document** on random bit generation will be published by ISO!

THANK YOU

15 rue Léon laval – L3372 Leudelange
+352 621 154 466
contact@incert.lu