ICS 35.040 SLOVENSKÁ TECHNICKÁ NORMA Júl 2021

| STN | Informačné technológie<br>Bezpečnostné metódy<br>Ľahká kryptografia<br>Časť 1: Všeobecne | STN<br>ISO/IEC 29192-1<br><br>97 4136 |
|---|---|---|

Information technology
Security techniques
Lightweight cryptography
Part 1: General

Technologies de l’information
Techniques de sécurité
Cryptographie pour environnements contraints
Partie 1: Généralités

Informationstechnologie
Sicherheitstechniken
Lightweight cryptography
Teil 1: Allgemeines

Táto norma obsahuje anglickú verziu ISO/IEC 29192-1: 2012.

This standard includes the English version of ISO/IEC 29192-1: 2012.

**132969**

## Anotácia

Táto časť ISO/IEC 29192 poskytuje termíny a definície, ktoré sa uplatňujú v nasledujúcich častiach ISO/ IEC 29192. Táto časť ISO/IEC 29192 stanovuje bezpečnostné požiadavky, požiadavky na klasifikáciu a implementačné požiadavky pre mechanizmy, ktoré sú navrhnuté na zahrnutie do ďalších častí tejto normy.

## Národný predhovor

### Normatívne referenčné dokumenty

V tomto dokumente sa nenachádzajú žiadne normatívne referenčné dokumenty.

### Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

# 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 29192-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 29192 consists of the following parts, under the general title *Information technology — Security techniques — Lightweight cryptography*:

- *Part 1: General*
- *Part 2: Block ciphers*
- *Part 3: Stream ciphers*
- *Part 4: Mechanisms using asymmetric techniques*

Further parts may follow.

# Introduction

ISO/IEC 29192 is a multi-part International Standard that specifies lightweight cryptography for the purposes of data confidentiality, authentication, identification, non-repudiation, and key exchange. Lightweight cryptography is suitable in particular for constrained environments. The constraints normally encountered can be any of the following:

- chip area;
- energy consumption;
- program code size and RAM size;
- communication bandwidth;
- execution time.

The purpose of ISO/IEC 29192 is to specify standardized mechanisms which are suitable for lightweight cryptographic applications, including radiofrequency identification (RFID) tags, smart cards (e.g. contactless applications), secure batteries, health-care systems (e.g. Body Area Networks), sensor networks, etc.

This part of ISO/IEC 29192 sets the security requirements, classification requirements and implementation requirements of mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.

Lightweight cryptography delivers adequate security in the context for which it is intended. The cryptographic mechanisms standardized in ISO/IEC 29192 provide their full security strength if they are used within the limitations of the mechanisms as specified.

EXAMPLE For a block cipher with a block size of n bits and a key size of k bits, when limiting the use of the block cipher to encrypting no more than 2n/2 blocks of plaintext under a single key in say counter mode, it will provide k-bit security. The security degrades with more than 2n/2 blocks.

There are overlaps in some security techniques between ISO/IEC 29192 and existing standards such as ISO/IEC 18033, ISO/IEC 9798, and ISO/IEC 11770. The exclusion of particular mechanisms does not imply that these mechanisms are not suitable for lightweight cryptography. The criteria used to select the cryptographic mechanisms specified in subsequent parts of ISO/IEC 29192 are described in Annex A.

# Information technology — Security techniques — Lightweight cryptography —

# Part 1: General

## 1 Scope

This part of ISO/IEC 29192 provides terms and definitions that apply in subsequent parts of ISO/IEC 29192. This part of ISO/IEC 29192 sets the security requirements, classification requirements and implementation requirements for mechanisms that are proposed for inclusion in subsequent parts of ISO/IEC 29192.