INTERNATIONAL STANDARD

ISO/IEC 18014-2

Third edition
2021-09

Information security — Time-stamping services —

Part 2: Mechanisms producing independent tokens

Sécurité de l'information — Services d'horodatage —

Partie 2: Mécanismes produisant des jetons indépendants

Reference number
ISO/IEC 18014-2:2021(E)

COPYRIGHT PROTECTED DOCUMENT

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

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).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

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 18014-2:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

— updated the definition of a hash function to a collision-resistant hash-function;

— application of style and editorial changes.

A list of all parts in the ISO/IEC 18014 series can be found on the ISO and IEC websites.

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.

Information security — Time-stamping services —

Part 2:
Mechanisms producing independent tokens

1 Scope

This document specifies mechanisms that generate, renew, and verify independent time-stamps. In order to verify an independent time-stamp token, time-stamp verifiers do not need access to any other time-stamp tokens. That is, such time-stamp tokens are not linked.

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 18014-1, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
time-stamp token
TST
data structure containing a verifiable binding between a data items' representation and a time-value

[SOURCE: ISO/IEC 18014-1:2008, 3.15, modified – Note to entry has been removed.]

3.2
time-stamping service
TSS
service providing evidence that a data item existed before a certain point in time

[SOURCE: ISO/IEC 18014-1:2008, 3.18]

3.3
time-stamping policy
set of rules that indicates the applicability of a *time-stamp token* (3.1) to a particular community and/or class of application with common security requirements

[SOURCE: ISO/IEC 18014-1:2008, 3.23]