INTERNATIONAL STANDARD

ISO/IEC 18014-4

First edition
2015-04-15

Information technology — Security techniques — Time-stamping services —

Part 4: Traceability of time sources

Technologies de l'information — Techniques de sécurité — Services d'horodatage —

Partie 4: Traçabilité des sources du temps

Reference number
ISO/IEC 18014-4:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015

All rights reserved. Unless otherwise specified, 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 member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **3**
5 General ... **4**
6 Time traceability chains and certification of traceability ... **4**
6.1 Time dissemination and traceability chains ... 4
6.2 Time auditing of TSA clock by TAA ... 4
7 Technical requirements for TAA ... **5**
7.1 Policy on requirements for TAA ... 5
7.2 Requirements for TAA clock ... 5
7.2.1 General ... 5
7.2.2 Configuration of TAA clock ... 5
7.2.3 Time synchronization with UTC(***k***) ... 6
7.2.4 Accuracy of TAA clock ... 6
7.2.5 Time offset measurements and retention of data ... 6
7.2.6 Records of instrument manipulation and their retention ... 6
7.3 Requirements for time audit ... 6
7.3.1 General ... 6
7.3.2 Time audit policy ... 6
7.3.3 Authentication of TSA clock ... 6
7.3.4 Measurements of time offset ... 7
7.3.5 Time offset certificates ... 7
7.3.6 Retention of records ... 7
7.3.7 Measures against extraordinary time discrepancy of TSA clock ... 7
7.4 Requirements for time dissemination ... 7
7.4.1 General ... 7
7.4.2 Time dissemination policy ... 8
7.4.3 Authentication of TSA clock ... 8
7.4.4 Time dissemination control ... 8
7.4.5 Measures against falsification of disseminated time ... 8
7.5 Other requirement ... 8
Annex A (informative) **Relation between time offset certificate and existing national standards** ... **9**
Annex B (informative) **Traceability chains and required accuracy** ... **10**
Annex C (informative) **Examples of TAA-based trusted time source schemes from ITU-R TF.1876** ... **12**
Annex D (informative) **Required accuracy and frequency stability of the reference clock** ... **13**
Bibliography ... **14**

© ISO/IEC 2015 – All rights reserved

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.

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).

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).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

ISO/IEC 18014 consists of the following parts, under the general title *Information technology — Security techniques — Time-stamping services*:

— *Part 1: Framework*

— *Part 2: Mechanisms producing independent tokens*

— *Part 3: Mechanisms producing linked tokens*

— *Part 4: Traceability of time sources*

© ISO/IEC 2015 – All rights reserved

Introduction

ISO/IEC 18014-1, ISO/IEC 18014-2, and ISO/IEC 18014-3 provide a general framework and specify time-stamping methods for time-stamping services offered by the time-stamping authority (TSA). This part of ISO/IEC 18014 describes an overall architecture for providing trusted time to the TSA and specifies technical guidelines to guarantee its correctness through the use of the time assessment authority (TAA).

© ISO/IEC 2015 – All rights reserved

Information technology — Security techniques — Time-stamping services —

Part 4: Traceability of time sources

1 Scope

This part of ISO/IEC 18014

— defines the functionality of the time assessment authority (TAA),

— describes an overall architecture for providing the time to the time-stamping authority (TSA) and to guarantee the correctness of it through the use of the TAA, and

— gives technical guidelines for the TAA to provide, and to provide assurance in, a trusted time source to the TSA.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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*

ITU-R TF.1876, *Trusted time source for Time Stamp Authority*

3 Terms and definitions

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

3.1
accuracy
closeness of the agreement between the result of a measurement and the true value of the measurand

Note 1 to entry: Accuracy is generally characterized by the overall uncertainty of a measured value.

[SOURCE: ITU-R TF.686-3:2013, Annex 1]

3.2
leap second
intentional time step of one second used to adjust UTC to ensure approximate agreement with UT1

[SOURCE: ISO 8601:2004, 2.2.2]

3.3
measurement
process of experimentally obtaining one or more quantity values that can be reasonably attributed to a quantity

[SOURCE: ISO/IEC GUIDE 99:2007, 2.1]

© ISO/IEC ISO pub-date year – All rights reserved

3.4
second
basic unit of time or time interval that is equal to the duration of 9 192 631 770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of caesium-133

[SOURCE: ISO 80000-3:2006, 3.13.a]

3.5
time assessment authority
TAA
entity which audits the time of the TSA clock and may also disseminate time to the TSA

3.6
time assessment authority clock
TAA clock
clock system of the TAA, used for time audit and time dissemination

Note 1 to entry: In the actual implementations, each TAA has more than one TAA clock for back up purposes.

3.7
time audit
audit of the time of downstream clocks in time traceability chains in order to check that it is consistent within the required accuracies

3.8
time dissemination
distribution of a time signal from one location to another

3.9
time offset certificate
certificate issued by a TAA to certify the measured time offset of a TSA clock with respect to the TAA clock

3.10
time scale
system of ordered marks which can be attributed to instants on the time axis, one instant being chosen as the origin

[SOURCE: ISO 8601:2004, 2.1.4]

3.11
time-stamping authority
TSA
trusted third party trusted to provide a time-stamping service

[SOURCE: ISO/IEC 18014-1:2008, 3.17]

3.12
time-stamp token
TST
data structure containing a verifiable cryptographic binding between a data item's representation and a time-value

Note 1 to entry: A time-stamp token can also include additional data items in the binding.

[SOURCE: ISO/IEC 18014-1:2008, 3.15]

3.13
time traceability chain
chain consisting of a sequence of reference clocks starting with UTC(*k*), used to relate the time from an end user to a timing centre

© ISO/IEC 2015 – All rights reserved

3.14
timing centre
organization with the means to disseminate the UTC(*k*) time to a TSA with the required accuracy

Note 1 to entry: The UTC(*k*) generated by the timing centre can be used in real time and its time difference from UTC is regularly published by the BIPM (the Bureau International des Poids et Measures).

3.15
traceability
property of the result of a measurement or the value of a standard whereby it can be related to stated references, usually national or international standards, through an unbroken chain of comparisons all having stated uncertainties

[SOURCE: ITU-R TF.686-3:2013, ANNEX 1]

3.16
TSA clock
clock of the TSA, which generates the time information included in the TST

Note 1 to entry: In the actual implementations, each TSA has more than one TSA clock for back up purpose.

3.17
UTC
time scale maintained by the Bureau International des Poids et Measures (BIPM) and the International Earth Rotation Service (IERS) that forms the basis of a coordinated dissemination of standard frequencies and time signals

Note 1 to entry: UTC is Coordinated Universal Time defined by ITU-R.

[SOURCE: ISO 19108:2002, 4.1.3]

3.18
UTC(*k*)
time scale realized by institute "*k*" and kept in close agreement with UTC, with the goal to be within ±100 ns, according to Recommendation S5 (1993) of the Consultative Committee for the Definition of the Second

[SOURCE: ITU-R TF.536-2:2003, 2]

4 Symbols and abbreviated terms

For the purpose of this document, the following abbreviations apply:

GNSS Global Navigation Satellite System

GPS Global Positioning System

NMI National Measurement Institute

NTP Network Time Protocol

OID Object Identifier

TTP Trusted Third Party

URL Uniform Resource Locator

© ISO/IEC 2015 – All rights reserved