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 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

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*

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).

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]

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

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

5 General

In time-stamping services, the TSA clock used to create time-stamp tokens is required to be synchronized with UTC within the declared accuracy, and shall be managed so as to guarantee the correctness of the time parameter included in the time-stamp token. The TAA certifies the traceability of the time reference of the TSA to the time scale of UTC(*k*) provided by a timing centre and may, optionally, distribute time information to the TSA. The function of the TAA may be performed by a timing centre or by a TTP.

As for time-stamping services, those specified in ISO/IEC 18014-1 shall be referred to. As for functionalities of the TAA, those defined in ITU-R TF.1876 shall be referred to.

This part of ISO/IEC 18014 describes an overall architecture for providing accurate and traceable time to the TSA and for certifying the traceability of the time of the TSA to UTC(*k*). It also addresses technical requirements for the TAA:

a) to provide certification to the TSA by auditing that the time used in the TSA is within the required accuracy, and

b) to distribute time information to the TSA if the TAA operates in time dissemination mode.

NOTE This part of ISO/IEC 18014 is based partly on JIS X 5094.[11]

6 Time traceability chains and certification of traceability

6.1 Time dissemination and traceability chains

Timing centres can disseminate their UTC time scale by broadcast over a radio, telephone or network path as services to end users. These services allow end users to connect to a timing centre and to establish a time traceability chain.[12] The TSA, as an end user, uses time signals from the clock located upstream in the chain as a reference signal. The chain thus enables traceability of a time signal to UTC(*k*).

The TSA clock and the TAA clock are located downstream from the timing centre on such time traceability chains, and the TAA clock is located upstream from the TSA clock when the TAA operates in time dissemination mode, as described in 6.2.

Traceability chains can also be established through time signals not controlled by a timing centre, provided that an NMI monitors and compares these signals to its UTC time scale.[12] This type of traceability chain is realized by using a certified GNSS timing receiver. The TSA can use a local oscillator controlled via the timing signal from the receiver as a traceable reference time source for the TSA clock. In this case, the timing centre referred to by the TAA is usually different from the NMI associated with the GNSS, as shown in case d) of Figure C.1.

The type of broadcast services used depends on the required accuracy for downstream clocks in the chain.

The NTP[2] can be used to synchronize clocks over computer networks.

6.2 Time auditing of TSA clock by TAA

The role of the TAA is to audit that the TSA clock synchronized with UTC(*k*) is traceable to UTC(*k*) within the required accuracy and to provide a time offset certificate (see 7.3.5) asserting traceability to the TSA. The architecture specified in this part of ISO/IEC 18014 provides time auditing by using the TAA in the following way.

The TAA maintains synchronization of its clock with UTC(*k*) by using disseminated time from a timing centre as described in 6.1. Alternatively, the TAA clock can be directly controlled by a timing centre if the TAA is operated by the timing centre. The TAA provides assurance of traceability chains by periodically measuring the time offset between UTC(*k*) and the TAA clock, and between the TAA clock and the TSA clock. The TAA records the measured time offset and issues a time offset certificate to the TSA.

The TAA may distribute time information to the TSA using this synchronized TAA clock, and such an arrangement can also be classified into one of the time traceability chains, as described in 6.1.

A block diagram of the architecture is given in B.1.

NOTE Examples of TAA-based trusted time source schemes specified in ITU-R TF.1876 are given in Annex C.

7 Technical requirements for TAA

7.1 Policy on requirements for TAA

This part of ISO/IEC 18014 stipulates the minimum necessary requirements to make it possible for the TAA to certify that time values in the TST issued by the TSA should be accurate to within ± 1 s of UTC(*k*). The permitted margin of error of ± 1 s allows for problems that might arise from the introduction of a leap second.

Clause 7 provides requirements for the TAA that also disseminates time to the TSA. Requirements related to time dissemination given in 7.4 are not applicable to the TAA operating in time auditing mode only.

The accuracy required for the TAA clock and the TSA clock with respect to UTC(*k*) and the accuracy required for time offset measurement of the TSA clock are defined and quantified in this part of ISO/IEC 18014. The TAA clock comprises a reference clock, a time auditing unit and an optional time dissemination unit. The time source used by both units is the reference clock. The accuracy of the TAA clock refers to the accuracy of the time value output at the interface point of the time auditing unit and the time dissemination unit, and this output time is referred to as the disseminated time of the TAA clock. Similarly, the accuracy of the TSA clock refers to the accuracy of the time value output at its interface point (see Figure B.2).

The required accuracy of the disseminated time of the TAA clock is determined so as to make its time offset to UTC(*k*) negligible. For the permitted margin of error of ± 1 s, the required accuracy of the disseminated time of the TAA clock is determined to be one tenth of the average accuracy error of ± 500 ms of the TSA clock. Both the required accuracy of time offset measurement and the required accuracy of the reference clock are determined in the same way.

The clock time error of the TAA caused by the reference clock frequency instability over the time offset measurement interval of the TSA clock shall be negligible compared to the accuracy of the reference clock. Specifically the time error of the TAA shall be less than one tenth of the accuracy of the reference clock.

NOTE 1 An atomic clock or an oven crystal clock is commonly used as a reference oscillator in actual services to meet the accuracy required of the TSA clock.

NOTE 2 The accuracy required for the TAA clock and the TSA clock and the accuracy required for time offset measurement in this part of ISO/IEC 18014 are shown in B.2.

7.2 Requirements for TAA clock

7.2.1 General

The requirements specified in 7.2.2 to 7.2.6 apply to both time auditing and time distributing.

7.2.2 Configuration of TAA clock

The configuration of the TAA clock shall meet the following requirements.

a) The TAA clock shall consist of a reference clock, a time auditing unit, and optionally a time dissemination unit. The time auditing unit and time dissemination unit shall use the reference clock as a time source.

b) The TAA shall employ a redundant configuration for the implementation of the reference clock, incorporating two or more clocks.