INTERNATIONAL STANDARD

ISO/IEC 18014-1

Second edition
2008-09-01

Information technology — Security techniques — Time-stamping services —

Part 1: Framework

Technologies de l'information — Techniques de sécurité — Services d'estampillage de temps —

Partie 1: Cadre général

Reference number
ISO/IEC 18014-1:2008(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.

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 18014-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 18014-1:2002), which has been technically revised.

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*

Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with ISO and IEC. Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) "*Patent Information*"

SD 8 is publicly available at: http://www.din.de/ni/sc27

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Information technology — Security techniques — Time-stamping services —

Part 1: Framework

1 Scope

This part of ISO/IEC 18014:

— identifies the objective of a time-stamping authority;

— describes a general model on which time-stamping services are based;

— defines time-stamping services;

— defines the basic protocols between the involved entities.

2 Normative references

The following referenced documents are indispensable for the application 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 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash-functions*

3 Terms and definitions

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

3.1
certification authority
CA
centre trusted to create and assign public key certificates

NOTE Optionally, the certification authority can create and assign keys to the entities.

[ISO/IEC 11770-1:1996]

3.2
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000]

3.3
data items' representation
data item or some representation thereof such as a cryptographic hash value

3.4
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protect the sender and the recipient of the data unit against forgery by third parties and sender against forgery by the recipient

[ISO/IEC 11770-3:1999]

3.5
entity authentication
corroboration that an entity is the one claimed

[ISO/IEC 9798-1:1997]

3.6
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties:

— it is computationally infeasible to find for a given output, an input which maps to this output;

— it is computationally infeasible to find for a given input, a second input which maps to the same output

NOTE Computational feasibility depends on the specific security requirements and environment.

[ISO/IEC 10118-1:2000]

3.7
hash value
string of bits which is the output of a hash-function

NOTE Identical to the definition of hash-code in ISO/IEC 10118-1:2000.

3.8
private key
that key of an entity's asymmetric key pair which should only be used by that entity

[ISO/IEC 11770-1:1996]

3.9
public key
that key of an entity's asymmetric key pair which can be made public

[ISO/IEC 11770-1:1996]

3.10
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[ISO/IEC 11770-1:1996]

3.11
sequence number
time variant parameter whose value is taken from a specified sequence which is nonrepeating within a certain time period

[ISO/IEC 11770-1:1996]

3.12
time stamp
time variant parameter which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-1:1996]

3.13
time-stamp renewal
process of issuing a new time-stamp token to extend the validity period of an earlier time-stamp token

3.14
time-stamp requester
entity which possesses data it wants to be time-stamped

NOTE A requester can also be a trusted third party including a time-stamping authority.

3.15
time-stamp token
TST
data structure containing a verifiable binding between a data items' representation and a time-value

NOTE A time-stamp token can also include additional data items in the binding.

3.16
time-stamp verifier
entity which possesses data and wants to verify that it has a valid time stamp bound to it

NOTE The verification process can be performed by the verifier itself or by a trusted third party.

3.17
time-stamping authority
TSA
trusted third party trusted to provide a time-stamping service

3.18
time-stamping service
TSS
service providing evidence that a data item existed before a certain point in time

3.19
time variant parameter
data item used by an entity to verify that a message is not a replay, such as a random number, a sequence number, or a time stamp

[ISO/IEC 11770-1:1996]

3.20
trusted third party
TTP
security authority, or its agent, trusted by other entities with respect to security-related activities

[ISO/IEC 11770-3:1999]

3.21
time referencing scheme
concepts for describing temporal characteristics of geographic information, about the use of an atomic clock, the clock of the GPS signal, etc.

NOTE See ISO 19108:2002.

3.22
time-signal emission
standard time signals are emitted with reference to UTC according to standard schemes

[ITU-R TF.460-6]

3.23
time-stamping policy
set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements

4 Symbols and abbreviated terms

TS (x_1, x_2, …, x_n)	generation of time-stamp token for the data x_1, x_2, …, x_n
D	data to be time-stamped
other info	information used to generate the time-stamp token, and which equals "TSTInfo" less the hash value of the data to be time-stamped
T_0, T_1, …T_n,	the point in time to be time-stamped
t_0, t_1, t_2, … t_n,	the point in time to be time-stamped
S	the point in time at which the end entity's digital signature is generated

5 General

5.1 Background and Summary

The use of digital data that may be provided on easily modifiable media raises the issue of how to certify when this data was created or last changed. Digital time-stamping shall provide evidence of timeliness. Digital time-stamping shall fulfill the following requirements:

— A time variant parameter shall be bound to the data in a non-forgeable way to provide evidence that the data existed prior to a certain point in time.

— Data shall be provided in a way that it is not disclosed.

The time-stamping methods specified in this international standard solve these requirements by time-stamping the hash value of data, which allows for the control of integrity and nondisclosure. The data themselves are not exposed. The hash of the data will be bound to the current time value by the TSA. This binding demonstrates the integrity and authenticity of the time-stamp. A time-stamp token providing these elements will be sent to the requester of the time-stamp.

Time-stamp tokens may also include information relating to previously generated tokens. Here the data's representation and additional information from data time-stamped prior to that time-stamp request are input parameters to the time-stamping process. The TSA may in addition publish various data items relating to the time-stamping process, to provide evidence that the data was available in a timely manner after the other included data hash. The publication of consecutive hashes gives evidence that the related data existed prior to the second published hash. This approach allows the verifier to verify a time-stamp without involving another authority.

5.2 Services involved in Time-stamping

There are two basic operations involved with time-stamping:

— a time-stamping process, which binds time values to data values, and

— a time-stamp verification process, which evaluates the correctness of those cryptographic bindings.

A Time-Stamping Authority (TSA) provides the time-stamping services, whereas the time-stamp verification process may involve other trusted authorities.

The time provided shall fulfill the general requirement of being accurate; the service providing the time for the TSA is outside the scope of this document.

NOTE Time sources are typically dependent on standard time-signal emissions based on standard time referencing schemes.

5.3 Entities of the Time-Stamping Process

The following entities may be involved when a time-stamp is requested:

An *entity* possesses data it wants to be time-stamped; e.g. to have evidence of the data's existence at a certain point in time. In this case it acts as the requester of a time-stamp. An entity may also request evidence that the time-stamped data received has a valid time-stamp, and may act as the *verifier* of a time-stamp.

The *time-stamping authority* (TSA) offers a time-stamping service. The nature of this service is highly sensitive for it helps to identify the validity of data and especially the validity of cryptographic elements related to these data. The TSA offers evidence that data existed at a certain point in time and guarantees the correctness of the time parameter.

All the entities introduced communicate using a two-way handshake protocol. That is, an entity sends a request to the TSA and receives in return a time-stamp (see details in clause 5.1 and clause 5.2). The token contains sufficient information to allow the entity to verify the token at a later point in time.

A time-stamping service may operate online and offline (e.g. using a store-and-forward protocol); the distinction is made at the transport level of the communication protocols between the involved entities.

5.4 Use of Time-Stamps

A time-stamp does not present the exact time when an electronic document was generated, altered or even signed. The entity providing a document for time-stamping may sign the document independently from the TSA, while the TSA binds a time value to the hash of the signed document.

The only evidence available is that a document existed prior to the included time-stamp.

Time-stamps also play an important role for the validity of signed documents. There exist three different possibilities for the time at which time-stamping and signing of data may occur. Data may be time-stamped before the requester of the time-stamp signs it, after the provision of the signature of the document's sender, and before and after the signature. This leads to different results when examining the timely validity of the signature. Table 1 describes these possibilities.

Table 1 —Timely arrangement of signatures and time-stamps

Case 1	t_1	TSA generates a time-stamp
	S	Requester signs data together with the provided time-stamp
Case 2	S	Requester signs data
	t_2	TSA time-stamps signed data
Case 3	t_1	TSA generates a time-stamp
	S	Requester signs data together with the provided time-stamp
	t_2	TSA time-stamps signed data

Technically:

Case 1: (Signature includes time-stamp) does not exactly define the point in time when data was signed. It states that the signature was provided after data was time-stamped.

Case 2: expresses that data was signed prior to the stated point in time.

Case 3: defines an interval during which the document was signed.

5.5 Generation of a Time-Stamp Token

When generating a time-stamp token, first the requester computes the hash value for the data to be time-stamped and sends it to TSA within a time-stamp request message. TSA binds the hash value and the time-stamp request message to the current time value as a Time-Stamp Token and sends it back to the requester.

5.6 Verification of a Time-Stamp Token

When verifying a time-stamp token, the validity of the Time-Stamp Token containing the time parameter is verified. Alternatively, the evaluation of the correctness of the Time-Stamp Token may be delegated to a trusted third party (TTP).

5.7 Time-Stamp renewal

Time-stamped data may be time-stamped again at a later time. This process is called time-stamp renewal and may optionally be implemented by the TSA. This may be necessary for example for the following reasons:

— The mechanism used to bind the time value to the data is near the end of its operational life cycle (e.g.: when using a digital signature and the public key certificate is about to expire).