INTERNATIONAL STANDARD

ISO/IEC 18014-1

First edition
2002-10-01

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

Reference number
ISO/IEC 18014-1:2002(E)

© ISO/IEC 2002

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

© ISO/IEC 2002

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing 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.ch
Web www.iso.ch

Printed in Switzerland

© ISO/IEC 2002 – All rights reserved

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

© ISO/IEC 2002 – 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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 part of ISO/IEC 18014 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*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

— *Part 1: Framework*

— *Part 2: Mechanisms producing independent tokens*

— *Part 3: Mechanisms producing linked tokens*

Further parts may follow.

Annexes A and B form a normative part of this part of ISO/IEC 18014.

© ISO/IEC 2002 – All rights reserved

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 this patent right.

The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

© ISO/IEC 2002 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

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

1 Scope

This part of ISO/IEC 18014:

1. identifies the objective of a time-stamping authority;
2. describes a general model on which time-stamping services are based;
3. defines time-stamping services;
4. defines the basic protocols of time-stamping;
5. specifies the protocols between the involved entities.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 18014. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 18014 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c262200f7-ee14-427e-924b-
iso-iec-18014-1-2002

ISO 8601:2000, Data elements and interchange formats – Information interchange – Representation of dates and times

ISO/IEC 8824-1: 1998 | X.680: ITU-T Recommendation X. 680 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation

ISO/IEC 8824-2: 1998 | X.681: ITU-T Recommendation X. 681 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Information object specification

ISO/IEC 8824-3: 1998 | X.682: ITU-T Recommendation X. 682 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification

ISO/IEC 8824-4: 1998 | X.683: ITU-T Recommendation X. 683 (1997), Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications

ISO/IEC 8825-1: 1998 | X.690: ITU-T Recommendation X. 690 (1997), Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

ISO/IEC 9798-1: 1997 Information technology – Security techniques – Entity authentication – Part 1: General

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

ISO/IEC 11770-1: 1996 Information technology – Security techniques – Key management – Part 1: Framework

ISO/IEC 11770-3: 1999 Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques

ISO/IEC 14888-2: 1999 Information technology – Security techniques - Digital signatures with appendix – Part 2: Identity-based mechanisms

ISO/IEC 14888-3: 1999 Information technology – Security techniques - Digital signatures with appendix – Part 3: Certificate-based mechanisms

ISO/IEC 15946-2, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures

3 Terms and Definitions

The following term is used as defined in ISO/IEC 9798-1:

entity authentication: the corroboration that an entity is the one claimed.

The following terms are used as defined in ISO/IEC 10118-1:

collision-resistant hash-function: a hash-function satisfying the following property:

- it is computationally infeasible to find any two distinct inputs which map to the same output.

hash-function: a function which maps strings of bits to fixed-length strings of bits, satisfying two important properties. The first property states that for a given output, it is computationally infeasible to find an input which map to this output. The second property states

© ISO/IEC 2002 - All rights reserved

that, for a given output, it is computationally infeasible to find a second input which map to the same output.

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

The following terms are used as defined in ISO/IEC 11770-1:

certification authority (CA): a centre trusted to create and assign public key certificates. Optionally, the certification authority may create and assign keys to the entities.

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

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

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

sequence number: a time variant parameter whose value is taken from a specified sequence which is non-repeating within a certain time period.

time-stamp: a time variant parameter which denotes a point in time with respect to a common time reference.

time-variant parameter: a 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.

The following terms are used as defined in ISO/IEC 11770-3:

digital signature: a 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.

trusted third party (TTP): a security authority, or its agent, trusted by other entities with respect to security related activities.

For the purposes of this standard, the following definitions apply.

3.1 data items' representation: a data item or some representation thereof such as a cryptographic hash value.

3.2 time-stamping authority (TSA): a trusted third party trusted to provide a time-stamping service.

3.3 time-stamping service: a service providing evidence that a data item existed before a certain point in time.

Note: An example is given by adding a time-stamp to a data items representation and signing the result.

3.4 time-stamp requester: an entity which possesses data it wants to be time-stamped.

Note: A requester may also be a Trusted Third Party including a time-stamping authority.

3.5 time-stamp token: a data structure containing a verifiable cryptographic binding between a data items' representation and a time-value. A time-stamp token may also include additional data items in the binding.

3.6 time-stamp verifier: an entity which possesses data and wants to verify that it has a valid time-stamp bound to it. The verification process may be performed by the verifier itself or by a Trusted Third Party.

4 General Discussion on Time-stamping

The use of digital data that may be provided on easily modifiable media raises the issue of how to certify when these data were created or last changed. Digital time-stamping shall provide help to achieve a proof of timeliness. Digital time-stamping must fulfil the following requirements:

- A time variant parameter must 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 may be provided in a way that it is not disclosed.

The time-stamping methods in use solve these requirements by time-stamping the hash value of data, which allows for the control of integrity and confidentiality. The data themselves are not exposed. The data's hash will be cryptographically 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, for proof that the data was available in a timely manner after the other included data hash. The publication of the consecutive hash 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/e2620617-ee14-4278-9246-bf4d0619175e/iso-iec-18014-1-2002

© ISO/IEC 2002 - All rights reserved

4.1 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 their existence at a certain point in time. This time it acts as the *requester* of a time-stamp. An entity may also get a proof that the time-stamped data received has a valid time-stamp and acts as the *verifier* of a time-stamp.

A *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 in a two-way handshake protocol. That means, an entity sends a request to the TSA and gets 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.

4.2 Time-Stamps

Time-stamps are used to give proof of the existence of data at a specific point in time. This may be done by cryptographically binding a time-stamp to a data items representation.

Time-stamped data may be time-stamped again at a later time. This may be necessary for example for the following reasons:

1. The cryptographic primitive used to bind the time value to the data will be near its end of its operational life cycle (e.g.: the TSA's signature key is about to expire).
2. The TSA may soon be replaced by another TSA.
3. The requester's hash algorithm may come into question.

Therefore those data time-stamped by the respective TSA may get a time-stamp re-issue prior to reaching any of the above conditions. This way the validity period of an existing time-stamp is extended.

Data may be re-time-stamped before a cryptographic primitive used to bind the time, hash values and other optional parameters together has reached the end of its operational lifetime. The time-stamp generated then is a new time-stamp that has no connection to former time-stamps associated with the data and is called time-stamp re-issue.

A time-stamp re-issue may also be necessary when the hash-function used to form the hash value from the original data is called into question. In this case, both the old time-stamp token and the original data must be included in the newly calculated hash value submitted for time-stamp reissue.

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

4.3 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 cryptographically binds a time value to the hash of the signed document.

The only proof 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 in time when 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c2620057-ee14-427e-924b-8f4b06b1756f/iso-iec-18014-1-2002

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

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.

© ISO/IEC 2002 - All rights reserved

4.4 Verification of a Time-Stamp Token

When verifying a time-stamp token, first the time value included in the time-stamp is evaluated, then the validity of the Time-Stamp Token containing the time parameter is verified. The validity of a time-stamp is verified by evaluating the correctness of the Time-Stamp Token. Alternately, the evaluation of the correctness of the Time-Stamp Token may be delegated to a trusted third party (TTP).

4.5 Services involved in Time-stamping

There are two basic operations involved with time-stamping:

- A time-stamping process, which cryptographically binds time values to data values, and
- a time-stamp verification process, which evaluates the correctness of those cryptographic bindings.

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/26200f7a-14-425-92db-bf4d06f9175e/iso-iec-18014-1-2002

5 Communications between entities involved

The entities involved in the time-stamping process are an entity, either requesting a time-stamp or verifying a time-stamp on the one side and one or more TSA on the other side. The transactions between these entities will be introduced in the following clauses.

5.1 Time-Stamp Request Transaction

The communication between an entity (requester) and the TSA when requesting a time-stamp consists of the following steps:

The requester generates the hash value for the data to be time-stamped. For the hash generation mechanisms as provided in ISO/IEC 10118-2: 1997 Information technology – Security techniques - Hash-functions – Part 2: *Hash functions using an n-bit block cipher algorithm*, as provided in Part 3: *Dedicated hash-functions* or as in Part 4: *Hash functions using modular arithmetic* may be used

1. A time-stamp request message is sent to the TSA including the following data:
   - Hash value,
   - Hash algorithm used, and
   - a nonce.

   Only the first two parameters are mandatory, the third value is optional.
2. The TSA checks the completeness of the received request.
3. The TSA generates a time-stamp (Time-Stamp Token). The time-stamp itself is a data structure containing
   - The time-parameter generated or received from a reliable source,
   - The data delivered by the requester, and
   - Data generated by the TSA to cryptographically bind the time value to the hash value, hash algorithm, and optionally, the nonce.

   If the cryptographic binding uses digital signatures then the TSA may use cryptographic algorithms as provided in standards ISO/IEC FCD 14888-3: Information technology – Security techniques - Digital signatures with appendix – Part 3: Certificate-based mechanisms and ISO/IEC FCD 15946-2: Information technology- Security techniques – Cryptographic techniques based on elliptic curves: *Digital signatures*.
4. The TSA returns the Time-Stamp Token to the requesting entity.
5. The entity may immediately check the completeness and correctness of the received Time-Stamp Token, or allow the eventual relying party to do so.

Figure 1 shows the communications between the requester and the TSA; the numbering refers to the text.

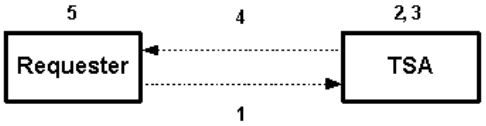

Figure 1 — Communications between Requester and TSA

5.2 Time-Stamp Verification Transactions

Verification of tokens produced using independent token mechanisms makes use of information contained in a single time-stamp token. The verifier may be required to obtain additional information required by the mechanism in order to complete the verification operation; this may be done by the requesting entity or on behalf of the entity by another TTP.

© ISO/IEC 2002 - All rights reserved

Verification of tokens produced using linked token mechanisms makes use of information contained in a single time-stamp token and possibly other tokens produced by the TSA. The verifier may be required to obtain additional information required by the mechanism in order to complete the verification operation; this may be done by the requesting entity or on behalf of the entity by another TTP.

Additional information is provided in part 2 and part 3 of this standard.

6 Message Formats

There are two types of messages that are needed to generate the transactions introduced in Clause 5: Messages between time-stamping requester/verifier and TSA, and messages between TSA and requester/verifier. All messages will be described in the ASN.1 notation. A complete ASN.1 module is provided in annex A. Messages will be distinguished according to the service they represent.

6.1 Time-stamp request

TimeStampReq messages are used by entities to request time-stamping services from time-stamping authorities. A TimeStampReq message is formed as follows:

```
TimeStampReq ::=   SEQUENCE {
      version                  Version,
      messageImprint           MessageImprint,
      reqPolicy                TSAPolicyId OPTIONAL,
      nonce                    INTEGER OPTIONAL,
      certReq                  BOOLEAN DEFAULT FALSE,
      extensions               [0] Extensions OPTIONAL
}
```

The following table explains the variables and their values.

Data field	Description
version	The syntax version number
messageImprint	The MessageImprint to which the service provider is to bind a time value
reqPolicy	Service policy requested from the TSA issuing the Time-Stamp Token
nonce	Identifies the specific request; the purpose of this value is to tie a specific request to the respective reply.
certReq	Signals the TSA to provide certificate information, if present.
extensions	Contains and extensions required to properly fulfill the requested time-stamping operation.

Type *MessageImprint* is used to encapsulate the message imprint data along with an indicator of the algorithm used to generate the message imprint.

```
MessageImprint ::=  SEQUENCE {
      hashAlgorithm      DigestAlgorithmIdentifier,
      hashedMessage      OCTET STRING
}
```

Data field	Description
hashAlgorithm	Hash Algorithm Identifier and parameter value
hashedMessage	The corresponding hash value of a message to be time-stamped, as calculated with the hash-function specified in the **hashAlgorithm** data field.

The hash-function must be a collision-resistant hash-function.

TSAPolicyId is defined as follows:

```
TSAPolicyId ::= POLICY.&id({TSAPolicies})
```

6.2 Time-stamp response

The answer to a time-stamp request is a ***TimeStampResp*** data structure. It has the following form:

```
TimeStampResp ::=                SEQUENCE {
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 18014-1:2002
https://standards.iteh.ai/catalog/standards/sist/c26200f7-ee14-427e-924b-bf4d06f9175e/iso-iec-18014-1-2002

© ISO/IEC 2002 - All rights reserved