

Information technology — Security techniques — Time-stamping services —

Part 3: Mechanisms producing linked tokens

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC 18014-3:2004 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to v, a blank page, pages 1 to 28, an inside back cover and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 19 February 2004

© BSI 19 February 2004

INTERNATIONAL STANDARD

ISO/IEC 18014-3

First edition
2004-02-15

Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens

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

Partie 3: Mécanismes produisant des jetons liés



Reference number
ISO/IEC 18014-3:2004(E)

AVA Documents
Document Sharing Hub

Contents

Page

Foreword.....	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	1
4 General discussion.....	3
5 Operations	3
5.1 Linking	3
5.2 Aggregation	3
5.3 Publishing.....	3
6 Data structures.....	4
6.1 Object identifiers.....	4
6.2 Node	4
6.3 Link.....	4
6.4 Chain	5
6.5 BindingInfo	5
6.6 Extensions.....	6
6.6.1 Request and Token extensions	7
6.6.2 BindingInfo extensions	8
7 Time-stamp request.....	9
8 Time-stamp response.....	9
8.1 DigestedData encapsulation.....	10
8.2 SignedData encapsulation	11
9 Time-stamp verification.....	12
Annex A (normative) ASN.1 Module for time-stamping.....	13
Annex B (normative) Additional Discussion	20
B.1 Discussion	20
B.2 Linking	20
B.2.1 Linear chain linking	20
B.2.2 Anti-monotone binary linking	21
B.2.3 Threaded tree linking.....	21
B.3 Aggregation	21
B.3.1 Unity aggregation	21
B.3.2 Merkle tree aggregation	22
B.3.3 One-way accumulator aggregation.....	22
B.4 Publishing.....	23
B.4.1 No publishing	23
B.4.2 Single link publishing.....	23
B.4.3 Merkle tree publishing.....	23
Annex C (informative) Data structures	24
C.1 Time-stamps using DigestedData encapsulation.....	24
C.2 Time-stamps using SignedData encapsulation	25
C.3 Linear Chain Linking with Merkle Tree Aggregation.....	26
Bibliography	28

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 18014-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 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*

Further parts may follow.

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.

The 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.ni.din.de/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 3: Mechanisms producing linked tokens

1 Scope

This part of ISO/IEC 18014

- describes a general model for time-stamping services producing linked tokens;
- describes the basic components used to construct a time-stamping service of this type;
- defines the data structures used to interact with a time-stamping service of this type;
- describes specific instances of such time-stamping services.

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/IEC 9594-8:2001, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

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

ISO/IEC 18014-1:2002, *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.

3.1

aggregation

the process of generating a proxy data item for a group of data items that are linked together at once, producing a verifiable cryptographic link between each data item and the rest of the group.

3.2

chain

a verifiable cryptographic binding between a data item and the rest of the data items participating in an aggregation. A chain consists of a sequence of operations that authenticate the participation of the selected data item in the aggregation.

3.3

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. [ISO/IEC 9796-3: 2000]

3.4

data items' representation

a data item or its respective hash value. [ISO/IEC 18014-1: 2002]

3.5

hash-function

a 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. [ISO/IEC 9796-3: 2000]

3.6

hash value

the string of bits which is the output of a hash-function. [ISO/IEC 9796-3: 2000]

3.7

link

a data item providing an irreversible and collision-resistant cryptographic statement attesting to the existence of at least two other data items.

3.8

node

a data item representing input data or a previously computed link.

3.9

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.

3.10

time-stamping authority (TSA)

a trusted third party trusted to provide a time-stamping service. [ISO/IEC 18014-1: 2002]

3.11

time-stamping service

a service providing evidence that a data item existed before a certain point in time. [ISO/IEC 18014-1: 2002]

3.12

trusted third party (TTP)

a security authority, or its agent, trusted by other entities with respect to security related activities. [ISO/IEC 11770-3: 1999]

4 General discussion

This part of ISO/IEC 18014 describes methods and processes used to form time-stamp tokens that are related, or “linked”, to other tokens produced by those methods and processes. A time stamping authority (TSA) utilises these methods and processes to provide a secure, verifiable cryptographic binding between a certain point in time and data values, and to enhance the security of the resulting tokens by reducing the trust level required in the TSA. The trustworthiness of the tokens computed in this scheme depends on the integrity of the repository of previously linked tokens maintained by the TSA. The integrity of the repository and of the linking operations performed by the TSA can be verified algorithmically, and do not depend on the trustworthiness of a PKI, nor require trusting that a particular private key has not been compromised.

This part of ISO/IEC 18014 describes how time-stamping systems utilising linked tokens can interoperate through standard tokens, operations, and data formats.

Note: For a complete treatment of time-stamping with linked tokens, see [HS91], [BHS93], [HS97], [BLLV98], and [BLS00]. For a proof of security of the linking technique, see [HS97] Section 3.1, Theorem 1.

5 Operations

In general, a TSA producing linked tokens uses the cryptographic properties of hash-functions to “link” a time-stamp token to other tokens previously generated by the TSA. Hash-functions defined in ISO/IEC 10118 that are both irreversible and collision-resistant are suitable for use in forming linked tokens: irreversibility conceals the content of the original data item from the TSA, while collision resistance ensures a false token cannot be inserted into an existing collection of linked tokens.

5.1 Linking

The linking operation consists of forming a verifiable, irreversible and collision-resistant binding between the time-stamp token and links previously produced by the TSA. The most recently produced such link provides a cryptographic summary of all time-stamp tokens that ever participated in the linking process. A common algorithm for computing a link between two events is to concatenate the data representation of the events and use the resulting concatenation as input to a hash-function. The resulting hash value provides a verifiable cryptographic link between the two input events due to the collision-resistant nature of the hash-function.

5.2 Aggregation

A conformant TSA may perform linking operations on groups of time-stamp tokens, rather than for each time-stamp token individually, in order to improve computational efficiency or achieve a higher degree of service scalability. Linking multiple events together at once is referred to as “aggregation,” and all time-stamp tokens involved in an aggregation shall be assigned the same time-value. Each aggregation scheme takes a group of events as inputs and produces a verifiable cryptographic link between each event and the rest of the group. The unique resulting value associated with the aggregation is further linked by the TSA, in a way similar to the case of the single time-stamp token.

Note: Common forms of aggregation include Merkle hash trees [M80], one-way accumulators [BD93], or other binary linking schemes [BLLV98].

5.3 Publishing

The links produced by a conformant TSA are published in such a way as to make them “widely-witnessed.” The manner most commonly used is through periodic publication on some well-known media, e.g., web pages or offline media. The value published should depend on all tokens generated by the TSA since the previous publishing event. By linking the tokens to “widely-witnessed” events, the TSA in effect generates verifiable statements of when each token was generated by the system.

6 Data structures

A conformant TSA produces linked time-stamp tokens using linking and aggregation processes that utilise the data types defined in the following sub-clauses.

6.1 Object identifiers

The following root object identifier arc is defined to support allocation of further object identifiers within this standard:

```
tsp-lt ::= OBJECT IDENTIFIER { iso(1) standard(0) time-stamp(18014) lt(3) }
```

Subsequent object identifiers defined in this document originate from this root identifier, except where declared otherwise.

6.2 Node

A single input element to a linking operation or to a step of an aggregation is represented by the following data structure:

```
Imprint ::= OCTET STRING
Imprints ::= SEQUENCE SIZE (1..MAX) OF Imprint
Node ::= CHOICE {
    imprints      [0] Imprints,
    reference     [1] INTEGER
}
Nodes ::= SEQUENCE SIZE (1..MAX) OF Node
```

Data field	Description
imprints	input data items for a link
reference	local identifier of a link from which to obtain input data items

If the 'imprints' field is present, the node contains the actual data items to be used as input to the current operation. If the 'reference' field is present, the node identifies a 'Link' structure (defined below) whose result is to be used as input to the current operation. In this case the value of the 'reference' field corresponds to the value of the 'identifier' field of the 'Link' structure whose results are to be included in the current operation. A value of zero in the 'reference' field indicates the data item to be used as input is obtained from a source external to the local group of links being computed.

6.3 Link

A single linking operation or a single step of an aggregation is represented by the following data structure:

```
Link ::= SEQUENCE {
    algorithm      [0] LinkAlgorithmIdentifier OPTIONAL,
    identifier     [1] INTEGER OPTIONAL,
    members        Nodes
}
Links ::= SEQUENCE SIZE (1..MAX) OF Link
```