BRITISH STANDARD

BS ISO/IEC 18014-3:2009

Information technology — Security techniques — Time-stamping services

Part 3: Mechanisms producing linked tokens

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Documents
Document Sharing Hub
British Standards

Full document details: BS ISO/IEC 18014-3:2009

National foreword

This British Standard is the UK implementation of ISO/IEC 18014-3:2009. It supersedes BS ISO/IEC 18014-3:2004 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

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

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 cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2010.

© BSI 2010

ISBN 978 0 580 66953 8

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18014-3:2009

INTERNATIONAL STANDARD

ISO/IEC 18014-3

Second edition
2009-12-15

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 18014-3:2009(E)

Documents
Document Sharing Hub
© ISO/IEC 2009

Full document details: BS ISO/IEC 18014-3:2009

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.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

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.org
Web www.iso.org

Published in Switzerland

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18014-3:2009

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 General discussion 3
5 Operations specific to TSAs producing linked tokens 3
5.1 Linking operation 3
5.2 Aggregation operation 4
5.3 Publishing operation 5
5.4 Extend operation 5
6 Message formats 5
6.1 Time-stamp request 5
6.2 Time-stamp response 6
6.3 Verify request 6
6.4 Verify response 7
6.5 Extend request 7
6.6 Extend response 7
7 Data types 8
7.1 Object identifiers 8
7.2 TSTInfo 8
7.3 TimeStampToken 9
7.4 BindingInfo 10
7.5 Chain 11
7.6 Link 11
7.7 Node 12
7.8 PublicationInfo 12
7.9 Extensions 13
8 Generating a time-stamp token 15
8.1 General 15
8.2 DigestedData encapsulation 16
8.3 SignedData encapsulation 16
8.4 Security considerations 17
9 Verifying a time-stamp token 17
9.1 General 17
9.2 DigestedData encapsulation 18
9.3 SignedData encapsulation 18
9.4 Security considerations 18
10 Extending a time-stamp token 18
11 Renewing a time-stamp token 19
11.1 General 19
11.2 Renewal and verify operation 19
11.3 Renewal and extend operation 19
Annex A (normative) **ASN.1 Module for time-stamping** 21
Annex B (informative) **Additional discussion** 29
Annex C (informative) **Data structures** 33
Bibliography 37

Documents
Document Sharing Hub

© ISO/IEC 2009 – All rights reserved

Full document details: BS ISO/IEC 18014-3:2009

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18014-3 was prepared by Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition replaces and cancels the first edition (ISO/IEC 18014-3:2004), which has been technically revised. New message formats and data types are defined to support a protocol for extending an existing linked token with data items referring to a published value issued by the TSA. The data type clauses have been expanded and re-ordered, and the ASN.1 definitions in Annex A have been updated and reordered in line with the contents of the clauses in the main body of this International Standard. Annexes B and C have been updated.

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*

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

Introduction

ISO/IEC 18014-1 provides a general framework for the provision of time-stamping services. This part of ISO/IEC 18014 specifies mechanisms producing linked tokens, that is, time-stamp tokens that are related, or "linked", to other time-stamp tokens produced by the methods and processes described in this document. A time stamping authority (TSA) can utilise the methods and processes described within this document to provide a secure, verifiable cryptographic binding between a certain point in time and data values, in a way that enhances the security of the resulting token.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18014-3:2009

INTERNATIONAL STANDARD ISO/IEC 18014-3:2009(E)

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 producing linked tokens,

— defines the data structures used to interact with a time-stamping service producing linked tokens,

— describes specific instances of time-stamping services producing linked tokens, and

— defines a protocol to be utilized by time-stamping services producing linked tokens for the purpose of extending linked tokens to published values.

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

ISO/IEC 18014-1:2008, *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
process of generating a proxy data item for a group of data items that are linked together, producing a verifiable cryptographic link between each data item and the rest of the group

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

[ISO/IEC 10118-1:2000, definition 3.2]

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

3.3
data items' representation
data item or its respective hash value

[ISO/IEC 18014-1: 2008]

3.4
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

[ISO/IEC 10118-1:2000, definition 3.5]

3.5
hash value
string of bits which is the output of a hash-function

NOTE See ISO/IEC 10118-1:2000, 3.4.

3.6
link
data item attesting to the existence of at least two other data items through the use of collision-resistant hash functions

3.7
time-stamping authority
TSA
trusted third party trusted to provide a time-stamping service

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

3.8
time-stamping service
TSS
service providing evidence that a data item existed before a certain point in time

[ISO/IEC 18014-1: 2008, definition 3.18]

3.9
time-stamp token
TST
data structure containing a verifiable cryptographic binding between a data items' representation and a time-value

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

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

3.10
trusted third party
TTP
security authority, or its agent, trusted by other entities with respect to security related activities

[ISO/IEC 10181-1:1996, definition 3.3.30]

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

4 General discussion

This part of ISO/IEC 18014 describes methods and processes to form time-stamp tokens that are related, or "linked", to other time-stamp tokens produced using methods and processes described within this document. A time-stamping authority (TSA) uses 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 level of assurance required in TSA operations. The trustworthiness of the time-stamp tokens computed using these methods and processes depends on the integrity of the TSA-maintained repository of previously computed results of linking operations. The integrity of the repository of links and of the linking operations performed by the TSA can be verified cryptographically, and does not depend on the trustworthiness of a Public Key Infrastructure (PKI) or require trusting that a particular private key has not been compromised.

This part of ISO/IEC 18014 additionally:

- describes methods and processes that a TSA producing linked tokens may utilise to generate values derived from its linking operations with the intent of making them widely available in online or offline media; and

- defines a request-response protocol that allows for time-stamp tokens issued by the TSA to be extended with data items that refer to the values published by the TSA.

Time-stamping services conforming to this part of ISO/IEC 18014 may interoperate through the use of standard tokens, operations, and data formats. In general, a TSA producing linked tokens uses the cryptographic properties of hash-functions to "link" a time-stamp token to other time-stamp tokens previously generated by the TSA. A recommended means of computing a value linking an event with a previously generated link is to concatenate a data representation of the event with the link and use the resulting concatenation as input to a hash-function. The resulting hash value provides a verifiable cryptographic link between the event and the previously generated link. Collision-resistant hash-functions defined in ISO/IEC 10118 are suitable for use in forming linked tokens: pre-image resistance helps to conceal 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.

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 specific to TSAs producing linked tokens

5.1 Linking operation

The linking operation involves forming a verifiable binding between the time-stamp token and links previously produced by the TSA through the use of collision-resistant hash-functions. The value of the most recently produced such link provides a cryptographic summary of all time-stamp tokens that have ever been involved in the linking process.

A conformant TSA producing linked tokens shall perform linking operations using one of the following methods:

- linear chain linking;

- anti-monotone binary linking;

- threaded tree linking.

Linear chain linking involves creating links in the following way: the value of the most recently generated link shall be concatenated with the hash-value of a representation of the most recent event, and a collision-resistant hash-function shall then be applied.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

Anti-monotone binary linking involves creating links in the following way: the value of two previously generated links shall be concatenated with the hash-value of a representation of the most recent event, and a collision-resistant hash-function shall then be applied. One of the two input links shall be the most recently generated link, and the precise identity of the other link will be determined by a data structure, maintained by the TSA, that shall take the form of an acyclic directed graph (see Annex B.2.3).

Threaded tree linking involves creating links in the following way: the value of some number of previously generated links shall be concatenated with the hash-value of a representation of the most recent event, and a collision-resistant hash-function shall then be applied. One of the input links shall be the most recently generated link, and the precise identity of the other links will be determined by a data structure, maintained by the TSA, that shall take the form of a threaded tree (see Annex B.2.4).

In every case, other data items may be concatenated to the input to the collision-resistant hash function prior to generating the new link (for example, time-variant parameters). Additionally, multiple collision-resistant hash-functions may be used concurrently on the same input for the purpose of generating a new link, and, in such a case, the new link is generated by concatenating the resulting hash values.

The values of the previous links used as input to the collision resistant hash-function(s) shall be included in the time-stamp token(s) associated with the most recent event and returned to the requesters within the ‘links’ field of the ‘BindingInfo’ structure (see Clause 7.4).

If hash-functions are used in linking operations, those specified in ISO/IEC 10118 shall be used.

Annex B.2 contains additional discussion regarding the algorithms that may be used in linking operations.

5.2 Aggregation operation

The aggregation operation involves forming a verifiable binding amongst a group of time-stamp tokens that are to be assigned the same time value through the use of a cryptographic function that is both pre-image resistant and collision-resistant, such as a collision-resistant hash-function. An aggregation scheme takes a group of time-stamp tokens as inputs and produces a single aggregate value, as well as verifiable cryptographic data linking together each time-stamp token with the rest of the group. The aggregate value associated with the aggregation operation is further used as an input to a linking operation by the TSA, in a way similar to the case of the linking operation for a single time-stamp token. A conformant TSA may thus perform linking operations for 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.

A conformant TSA producing linked tokens that supports aggregation shall perform aggregation operations using one of the following methods:

- Merkle-tree aggregation;
- one-way accumulator aggregation.

All forms of aggregation involve first applying collision-resistant hash-function(s) to the encapsulated 'TSTInfo' data structures of the time-stamp tokens to be aggregated. We refer to the resulting hash-values as the ‘hash-values to be aggregated’.

Merkle tree aggregation involves arranging the hash-values to be aggregated as the leaves of a tree structure (see Annex B.3.3). A value is then assigned to each non-leaf node of the tree by concatenating the hash-values assigned to its child nodes and then applying a collision-resistant hash-function, until all nodes of the tree structure have been assigned values. The value assigned to the root of the tree is the aggregate value. Multiple collision-resistant hash-functions may be used concurrently in this process, and, in such a case, the value assigned to each non-leaf node is computed by concatenating the hash values generated by each hash-function.

One-way accumulator aggregation involves computing an aggregate value in such a way that verification of the aggregate value for any of the participating hash-values may be done in constant time, regardless of the number of hash-values to be aggregated. Precisely how this is achieved is outside the scope of this part of ISO/IEC 18014; an example of a possible technique is outlined in Annex B.3.4.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

If hash-functions are used in aggregation operations, those specified in ISO/IEC 10118 shall be used.

Annex B.3 contains additional discussion regarding the algorithms that may be used in aggregation operations.

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

5.3 Publishing operation

Values derived from the links produced by a conformant TSA may be published in such a way as to make the linking operations “widely-witnessed.” This can be achieved by periodic publication in widely available media, e.g., web pages or printed publications. The value published should depend on all time-stamp 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 time-stamp token was generated by the system.

A conformant TSA producing linked tokens that supports publishing shall perform publishing operations using one of the following methods:

- single-link publishing;
- Merkle tree publishing.

Single link publishing involves the periodic publication of a single link value. This single link value enables the verification of all link values produced up to the time at which it was generated. For further details see Annex B.4.3.

Merkle tree publishing involves the periodic publication of the Merkle tree aggregation of all links generated since the last publication event. For further details see Annex B.4.4.

If hash-functions are used in publishing operations, those specified in ISO/IEC 10118 shall be used.

Annex B.4 contains additional discussion regarding the publishing operations performed by a conformant TSA.

5.4 Extend operation

If a conformant TSA makes published values available, an entity in possession of a linked token issued by this TSA may carry out a request-response protocol with the issuing TSA or other TTP that has access to the issuing TSA’s links for the purpose of extending this time-stamp token to a published value, using a data integrity and data origin authentication protected channel. This protocol should be carried out once the published value corresponding to this time-stamp token has been issued by the TSA and becomes available, and it results in the generation of a new time-stamp token, containing the same components as the original, as well as additional data items that refer to the published value and bind the linked token to it. The additional data items permit the computation of the corresponding published value without requiring access to the issuing TSA's links. Message formats supporting the extend operation are described in Clauses 6.5 and 6.6.

6 Message formats

6.1 Time-stamp request

A time-stamp request is a message sent by a time-stamp requester to a TSA in order to request that the TSA issue a time-stamp token for the data items in the message. As defined in ISO/IEC 18014-1, the time-stamp request contains the data fields listed in Table 1.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

Table 1 — Time-stamp request

Data field	Description
version	version number of this data structure
messageImprint	message imprint to which the TSA is to bind a time value
reqPolicy	service policy requested from the TSA (optional)
nonce	identifier enabling the request to be matched to the issued time-stamp token (optional)
certReq	requests the TSA to provide certificate information, if present
extensions	additional items required to properly fulfil the requested time-stamp request (optional)

The ASN.1 definition of the time-stamp request is given in Annex A as `TimeStampReq`.

6.2 Time-stamp response

A time-stamp response is a message returned by the TSA in response to a time-stamp request. As defined in ISO/IEC 18014-1, the time-stamp response contains the data fields listed in Table 2.

Table 2 — Time-stamp response

Data field	Description
status	status of the time-stamp operation
timeStampToken	issued time-stamp token, if the time-stamp operation is successful

The ASN.1 definition of the time-stamp response is given in Annex A as `TimeStampResp`.

6.3 Verify request

A verify request is a message sent by a time-stamp verifier to a TSA or other TTP that has access to the issuing TSA's links in order to request the entity receiving the message to verify the validity of the time-stamp token contained in the message. As defined in ISO/IEC 18014-1, the verify request contains the data fields listed in Table 3.

Table 3 — Verify request

Data field	Description
version	version number of this data structure
tst	time-stamp token to be verified
requestID	request identifier (optional)

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009

The ASN.1 definition of the verify request is given in Annex A as `VerifyReq`.

6.4 Verify response

A verify response is a message returned by the TSA or other TTP that has access to the issuing TSA's links in response to a verify request. As defined in ISO/IEC 18014-1, the verify response contains the data fields listed in Table 4.

Table 4 — Verify response

Data field	Description
version	version number of this data structure
status	status of the verify operation
tst	submitted time-stamp token
requestID	response identifier, matches request identifier (optional)

The ASN.1 definition of the verify response is given in Annex A as `VerifyResp`.

6.5 Extend request

An extend request is a message sent by an entity in possession of a linked token to the issuing TSA or other TTP that has access to the issuing TSA's links in order to request the entity receiving the message to extend the time-stamp token contained in the message with additional data items that refer to values published by the issuing TSA. The extend request may be granted once the publishing event for the time-stamp token has taken place, that is, after the TSA has issued a published value for the time interval covering the time value in the time-stamp token. The extend request contains the data fields listed in Table 5.

Table 5 — Extend request

Data field	Description
version	version number of this data structure
tst	time-stamp token to be extended to a published value
requestID	request identifier (optional)

For the purposes of this standard, the 'version' field shall be set to one.

The 'requestID' field binds the extend request to the corresponding extend response.

The ASN.1 definition of the extend request is given in Annex A as `ExtendReq`.

6.6 Extend response

An extend response is a message returned by the TSA or other TTP that has access to the issuing TSA's links in response to an extend request. If the request is granted, a new time-stamp token is returned in the response with additional data items that refer to values published by the issuing TSA. The extend response contains the data fields listed in Table 6.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18014-3:2009