INTERNATIONAL STANDARD

ISO/IEC 18014-2

First edition
2002-12-15

Information technology — Security techniques — Time-stamping services —

Part 2: Mechanisms producing independent tokens

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

Partie 2: Mécanismes produisant des jetons indépendants

Reference number
ISO/IEC 18014-2:2002(E)

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.

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

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.

ISO/IEC 18014-2 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.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 2: Mechanisms producing independent tokens

1 Scope

A time-stamping service provides evidence that a data item existed before a certain point in time. Time-stamp services produce time-stamp tokens, which are data structures containing a verifiable cryptographic binding between a data item's representation and a time-value. This part of ISO/IEC 18014 defines time-stamping mechanisms that produce independent tokens, which can be verified one by one.

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 7498-2: 1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*

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

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

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

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

ISO/IEC 8825-1: 1998 | 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 9594-8: 2001 | ITU-T Recommendation X.509 (2000), *Information technology – Open Systems Interconnection – The Directory: Public key and attribute certificate frameworks*

ISO/IEC TR 14516: 2002 | ITU-T Recommendation X.842 (2000), *Information technology – Guidelines for the use and management of Trusted Third Party services*

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

ISO/IEC 10181-2: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*

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 13888-1: 1997, *Information technology – Security techniques – Non-repudiation – Part 1: General*

ISO/IEC 14888 (all parts), *Information technology – Security techniques – Digital signatures with appendix*

ISO/IEC 18014-1: 2002, *Information technology – Security techniques – Time-stamping services – Part 1: Framework*

3 Terms and Definitions

The following terms are used as defined in ISO/IEC 7498-2:

Cryptography: the discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use.

Data integrity: the property that data has not been altered or destroyed in an unauthorized manner.

Data origin authentication: the corroboration that the source of data received is as claimed.

Digital signature: data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

The following term is used as defined in ISO/IEC 8825-1:

Distinguished Encoding Rules (DER): encoding rules that may be applied to values of types defined using the ASN.1 notation. Application of these encoding rules produces a transfer syntax for such values. It is implicit that the same rules are also to be used for decoding. The DER is more suitable if the encoded value is small enough to fit into the available memory and there is a need to rapidly skip over some nested values.

The following term is used as defined in ISO/IEC 9594-8:

Certification path: an ordered sequence of certificates of objects in the DIT (directory information tree) which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

The following terms are used as defined in ISO/IEC 9798-1:

Asymmetric key pair: a pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

Asymmetric signature system: a system based on asymmetric techniques whose private transformation is used for signing and whose public transformation is used for verification.

The following term is used as defined in ISO/IEC 10181-2:

Authentication: the provision of assurance of the claimed identity of an entity.

The following term is 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.

The following terms are used as defined in ISO/IEC 13888-1:

Message Authentication Code (MAC): a data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of a message by any entity holding the secret key.

Private key: that key of an entity's asymmetric key pair that is usable only by that entity. In the case of an asymmetric signature system, the private key and the associated algorithms define the signature transformation.

Public key: the key of an entity's asymmetric key pair that can be made public. In the case of an asymmetric signature system, the public key and the associated algorithms define the verification transformation.

Public key certificate: a security certificate which binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key.

The following term is used as defined in ISO/IEC 14888-2:

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

The following terms are used as defined in ISO/IEC 18014-1:

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

Time-stamping service (TSS): a service providing evidence that a data item existed before a certain point in time.

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

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.

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

ISO/IEC 18014-1 presents a general framework for the provision of time-stamping services.

Time-stamping services produce time-stamp tokens. These tokens are associations between data and points in time, and are created in a way that aims to provide evidence that the data existed at the associated date and time. In addition the evidence may be used by non-repudiation services.

This part of ISO/IEC 18014 presents mechanisms to produce time-stamp tokens that are independent: in order to verify a time-stamp token, verifiers do not need access to any other time-stamp token.

Independency means that a verifier just requires one time-stamp token to verify the point in time at which the document existed.

Three mechanisms are presented. The first one is based on digital signatures, and is backwards compatible with the time-stamping protocol defined by IETF [RFC3161]. The second mechanism uses a message authentication code (MAC) to authenticate the binding in a time-stamp token, and the third mechanism is based on TSA archiving of information.

The first mechanism asks the time-stamp service provider to digitally sign the binding of the time to the document so that signature verification sustains the evidence.

The second mechanism asks the time-stamp service provider to use a MAC to sign the binding. The same secret is needed for signature creation and for signature verification, and this secret is kept by the TSA. Therefore, the TSA is required for verification.

The third mechanism asks the time-stamp service provider to archive the evidence, and only publish a reference to the archive. Therefore, the TSA is required for archival and verification.

Time-stamping service users may select the mechanism to be used by means of the ExtMethod extension specified in ISO/IEC 18014-1. If no mechanism is explicitly selected in a time-stamp request, the digital signature mechanism is assumed.

NOTE: In order to guarantee full interoperability with IETF compliant time-stamping servers, this extension must be omitted in order to force the usage of the digital signature mechanism, which matches the protocol specified in [RFC3161].

5 Entities of the Time-Stamping Process

The following entities (from ISO/IEC 18014-1) may be involved when a time-stamp is requested or verified:

- the time-stamp **requester;**
- the time-stamp **verifier**; and
- the **Time-Stamping Authority (TSA).**

6 Message Formats

This section reproduces some ASN.1 definitions that appear in ISO/IEC 18014-1, and introduces new ones. The complete ASN.1 module can be found Annex A.

The TSA produces the time-stamp information that is defined in ISO/IEC 18014 part 1 as:

```
TSTInfo ::=  SEQUENCE {
      version        Version,
      policy         TSAPolicyId,
      messageImprint    MessageImprint,
      serialNumber      SerialNumber,
      genTime        GeneralizedTime,
      accuracy          Accuracy OPTIONAL,
      ordering          BOOLEAN DEFAULT FALSE,
      nonce             Nonce OPTIONAL,
      tsa            [0] EXPLICIT GeneralName OPTIONAL,
      extensions        [1] Extensions OPTIONAL
}
```

This TSTInfo is wrapped into a time-stamp response, DER-encoded into an OCTET STRING:

```
ETSTInfo ::=
      OCTET STRING (CONTAINING TSTInfo ENCODED BY der)
```

The wrapping depends on the mechanism used.

The time-stamp response returned to the requester is defined as:

```
TimeStampResp ::= SEQUENCE {

      status        PKIStatusInfo,

      timeStampToken    TimeStampToken OPTIONAL

}


PKIStatusInfo ::= SEQUENCE {

      status        PKIStatus,

      statusString      PKIFreeText OPTIONAL,

      failInfo          PKIFailureInfo OPTIONAL

}


TimeStampToken ::= SEQUENCE {

      contentType       CONTENT.&id({Contents}),

      content    [0] EXPLICIT CONTENT.&Type({Contents}{@contentType})

}
```

```
Contents CONTENT ::= {

      time-stamp-mechanism-signature  |

      time-stamp-mechanism-MAC        |

      time-stamp-mechanism-archival,

       --

      ...  -- Expect additional time-stamp mechanisms --

}


time-stamp-mechanism-signature CONTENT ::=

      { SignedData IDENTIFIED BY id-signedData }


time-stamp-mechanism-MAC CONTENT ::=

      { AuthenticatedData IDENTIFIED BY id-ct-authData }
```

```
time-stamp-mechanism-archival CONTENT ::=

      { ETSTInfo IDENTIFIED BY id-data }
```

The value of the contentType component is an OBJECT IDENTIFIER. It is tightly bound to the type of the content component. The Contents information object set is referenced by both components of TimeStampToken. Each object in the Contents set specifies a valid pair of associated contentType and content values. There is one object in the set for each of the time-stamp mechanisms defined in this standard.

6.1 Object Identifiers

A number of OBJECT IDENTIFIERS are required to support the mechanisms defined below. These identifiers are used to uniquely identify specific time-stamping mechanisms. The following root identifier is defined to support allocation of further identifiers for independent token mechanisms:

```
tsp-itm  OBJECT IDENTIFIER::= { iso(1) standard(0) time-stamp(18014) itm(2) }
```

Identifiers defined in this document originate from this root identifier, except where declared otherwise.

6.2 Extension fields

The following extensions fields are identified to be carried either by the TimeStampReq or the TSTInfo. Further extensions may be identified in the future.

6.2.1 ExtHash extension

A requester of time-stamping services may wish to submit for time-stamping more than one hash value derived from a single data item. To enable the submission of multiple hash values the following extension is defined:

```
extHash EXTENSION ::= { SYNTAX ExtHash IDENTIFIED BY tsp-ext-hash }


ExtHash ::= SEQUENCE SIZE(1..MAX) OF MessageImprint


tsp-ext-hash OBJECT IDENTIFIER ::= { tsp-ext 1 }
```

This extension is carried in the "extensions" field of both the TimeStampReq message sent by a requester to a TSA and in the "extensions" field of the resulting TSTInfo structure formed by the TSA and returned to the requester. The TSA reproduces the contents of this extension unmodified.

6.2.2 ExtMethod extension

A requester of time-stamping services may wish to indicate to a specific TSA which time-stamping method to use when forming the eventual time-stamp token. To enable a requester to indicate to a specific TSA which time-stamping method to use in forming the resulting time-stamp token, the following extension is defined:

```
extMethod EXTENSION ::= { SYNTAX ExtMethod IDENTIFIED BY tsp-ext-meth }
```