TECHNICAL REPORT

ISO/IEC TR 29149

First edition
2012-03-15

Information technology — Security techniques — Best practices for the provision and use of time-stamping services

Technologies de l'information — Techniques de sécurité — Meilleures pratiques pour la fourniture et l'utilisation de services d'horodotage

Reference number
ISO/IEC TR 29149:2012(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

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.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 TR 29149 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide

- timeliness and data integrity services, or
- non-repudiation services (in conjunction with other mechanisms).

ISO/IEC 18014 specifies time-stamping services, explaining how to generate, renew, and verify time-stamp tokens. The goal of a non-repudiation service is to treat evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. Depending on the non-repudiation service which is required, the non-repudiation policy in effect for a specific application, and the legal environment within which the application operates, time-stamp tokens from time-stamping authorities may be required as components of non-repudiation information.

Information technology — Security techniques — Best practices for the provision and use of time-stamping services

1 Scope

This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness, data integrity, and non-repudiation services in conjunction with other mechanisms. It defines:

- how time-stamp requesters should use time-stamp token generation services;
- how TSAs (time-stamping authorities) should provide a service of guaranteed quality;
- how TSAs should deserve trust based on good practices;
- which algorithms and parameters should be used in TST (time-stamp token) generation and TST renewal, so that TSTs resist during the time period during which the TSTs can be verified as being valid;
- how time-stamp verifiers should use the time-stamp token verification services, both when validating individual TSTs, and when validating sequences of renewal TSTs.

2 Terms and definitions

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

2.1
certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

NOTE Optionally, the certification authority may create the users' keys.

[ISO/IEC 9594-8:2005]

2.2
digital signature
data appended to, or a cryptographic transformation 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

[ISO 7498-2:1989]

2.3
evidence
information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

NOTE Evidence does not necessarily prove the truth or existence of something, but can contribute to the establishment of such a proof.

[ISO/IEC 13888-1:2009]

2.4
evidence user
entity that uses non-repudiation evidence

[ISO/IEC 13888-1:2009]

2.5
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]

2.6
hash-value
string of bits which is the output of a hash-function

[ISO/IEC 10118-1:2000, modified — The term "hash-code" is used to represent this concept in ISO/IEC 10118-1:2000.]

2.7
imprint
string of bits, either the hash-value of a data string or the data string itself

[ISO/IEC 13888-1:2009]

2.8
message authentication code
MAC
string of bits which is the output of a MAC algorithm

NOTE A MAC is sometimes called a cryptographic check value (see for example ISO 7498-2).

[ISO/IEC 9797-1:2011]

2.9
non-repudiation
ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

[ISO 7498-2:1989]

2.10
non-repudiation token
special type of security token as defined in ISO/IEC 10181-1, consisting of evidence, and, optionally, of additional data

[ISO/IEC 13888-1:2009]

2.11
object identifier
OID
globally unique value associated with an object to unambiguously identify it

[ISO/IEC 8824-1:2002 | ITU X.680:2002]

2.12
private key
that key of an entity's asymmetric key pair which should only be used by that entity

[ISO/IEC 9798-1:1997]

2.13
public key
that key of an entity's asymmetric key pair which can be made public

NOTE In the case of an asymmetric signature scheme, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.

[ISO/IEC 11770-3:2008]

2.14
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[ISO/IEC 11770-3:2008]

2.15
signer
entity generating a digital signature

[ISO/IEC 13888-1:2009]

2.16
time stamp
data item which denotes a point in time with respect to a common time reference

[ISO/IEC 11770-1:2010]

2.17
time-stamp token renewal
process of issuing a new time stamp token to extend the validity period of an earlier time-stamp token

[ISO/IEC 18014-1:2008, adapted]

2.18
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.

[ISO/IEC 18014-1:2008]

2.19
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.

[ISO/IEC 18014-1:2008]

2.20
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 may be performed by the verifier itself or by a trusted third party.

[ISO/IEC 18014-1:2008]

2.21
time-stamping authority
TSA
trusted third party trusted to provide a time-stamping service

[ISO/IEC 18014-1:2008]

2.22
time-stamping policy
named set of rules that indicates the applicability of a time-stamp token to a particular community or class of application with common security requirements

[ISO/IEC 18014-1:2008]

2.23
time-stamping service
TSS
service providing evidence that a data item existed before a certain point in time

[ISO/IEC 18014-1:2008]

2.24
trusted third party
TTP
security authority, or its agent, trusted by other entities with respect to security related activities

[ISO/IEC 10181-1:1996]

3 Symbols and abbreviated terms

In the remainder of this document the following notation will be used:

HMAC	Hash Message Authentication Code
H(D)	The hash-value of data D, using hash-function H
MAC	Message Authentication Code
OID	Object Identifier
PKI	Public Key Infrastructure
$S_X(y)$	The signature computed on data y using a signature algorithm and the private key of entity X
TSA	Time-Stamping Authority
TSP	Time-Stamp Packet: the combination of the TST and the data upon which the TST is generated

TSS	Time-Stamping Service
TST	Time-Stamp Token
TST(D, t)	time-stamp token on data D, at point in time t

4 Time-stamping services

Time-stamping services include generation, renewal, and verification of time-stamp tokens, as defined in ISO/IEC 18014-1.

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

Time-stamping services involve the following entities (from ISO/IEC 18014-1):

- the time-stamp requester, that has some data (e.g. a document) to time-stamp;
- the Time-Stamping Authority (TSA), that generates time-stamp tokens (TST);
- the time-stamp verifier, that verifies time-stamps bound to data.

Time-stamping services (TSS) provide three specific services:

- time-stamp token generation, where the requester submits data items, and receives a time-stamp token; this service is provided by the TSA;
- time-stamp token renewal, a special case of time-stamp token generation, where the requester submits an existing first time-stamp token and related data items, and receives a new time-stamp token, such that the validity period of the first time-stamp token is extended by the new time-stamp token; this service is provided by the TSA;
- time-stamp token verification, when the verifier validates the time-stamp token; this service may also involve the TSA or other trusted third parties.

Users of the time-stamping services handle time-stamp packets (TSP), encompassing the data plus the time-stamp token (TST).

5 Use cases for non-repudiation

5.1 Introduction

Time-stamping services provide tokens that may be used, in combination with an adequate non-repudiation policy, to support non-repudiation claims.

Non-repudiation services provide a user B with protection against another user A later denying that an action or event has taken place. While these services do not prevent A from trying to repudiate B’s claim, they provide evidence to support the resolution of such disagreement. In general, the evidence needs to be convincing to a third party arbitrator C.

The following clauses present some use cases.