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)

COPYRIGHT PROTECTED DOCUMENT

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

Page

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.