INTERNATIONAL STANDARD

ISO/IEC 18014-1

Second edition
2008-09-01

Information technology — Security techniques — Time-stamping services —

Part 1: **Framework**

Technologies de l'information — Techniques de sécurité — Services d'estampillage de temps —

Partie 1: Cadre général

Reference number
ISO/IEC 18014-1:2008(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

Page

Foreword ... iv

Introduction ... v

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Symbols and abbreviated terms ... 4

5 General ... 4
5.1 Background and Summary ... 4
5.2 Services involved in Time-stamping ... 5
5.3 Entities of the Time-Stamping Process ... 5
5.4 Use of Time-Stamps ... 5
5.5 Generation of a Time-Stamp Token ... 6
5.6 Verification of a Time-Stamp Token ... 6
5.7 Time-Stamp renewal ... 6

6 Communications between entities involved ... 7
6.1 Time-Stamp Request Transaction ... 7
6.2 Time-Stamp Verification Transaction ... 8

7 Message Formats ... 8
7.1 Time-stamp request ... 9
7.2 Time-stamp response ... 10
7.3 Time-stamp verification ... 12
7.4 Extension fields ... 12
7.4.1 ExtHash extension ... 12
7.4.2 ExtMethod extension ... 13
7.4.3 ExtRenewal extension ... 13

Annex A (normative) **ASN.1 Module for time-stamping** ... 14

Annex B (normative) **Excerpt of the Cryptographic Message Syntax** ... 20
B.1 Introduction ... 20
B.2 General Overview ... 20
B.3 General Syntax ... 20
B.4 Data Content Type ... 21
B.5 Signed-data Content Type ... 21
B.5.1 SignedData Type ... 22
B.5.2 EncapsulatedContentInfo Type ... 23
B.5.3 SignerInfo Type ... 23
B.5.4 Message Digest Calculation Process ... 25
B.5.5 Signature Generation Process ... 25
B.5.6 Signature Verification Process ... 25
B.6 Useful Attributes ... 26
B.6.1 Content Type ... 26
B.6.2 Message Digest ... 26
B.6.3 Countersignature ... 27

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

This second edition cancels and replaces the first edition (ISO/IEC 18014-1:2002), which has been technically revised.

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*

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.

ISO and IEC take no position concerning the evidence, validity and scope of these patent rights.

The holders of these patent rights have assured ISO and IEC that they are willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statements of the holders of these patent rights are registered with 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 1: Framework

1 Scope

This part of ISO/IEC 18014:

— identifies the objective of a time-stamping authority;

— describes a general model on which time-stamping services are based;

— defines time-stamping services;

— defines the basic protocols between the involved entities.

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 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

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