INTERNATIONAL STANDARD

**ISO/IEC 18014-1**

First edition
2002-10-01

# 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 18014-1:2002(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.ch
Web www.iso.ch

Printed 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 3.

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 part of ISO/IEC 18014 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*.

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.

Annexes A and B form a normative part of this part of ISO/IEC 18014.

# 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 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 1:
# Framework



## 1 Scope

This part of ISO/IEC 18014:

1. identifies the objective of a time-stamping authority;
2. describes a general model on which time-stamping services are based;
3. defines time-stamping services;
4. defines the basic protocols of time-stamping;
5. specifies the protocols between the involved entities.

## 2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 18014 . For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 18014 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 8601:2000, Data elements and interchange formats – Information interchange – Representation of dates and times

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

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

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

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

ISO/IEC 8825-1: 1998 | X.690: 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 9798-1: 1997 Information technology – Security techniques – Entity authentication – Part 1: General

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

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 14888-2: 1999 Information technology – Security techniques - Digital signatures with appendix – Part 2: Identity-based mechanisms

ISO/IEC 14888-3: 1999 Information technology – Security techniques - Digital signatures with appendix – Part 3: Certificate-based mechanisms

ISO/IEC 15946-2, Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures

## 3 Terms and Definitions

The following term is used as defined in ISO/IEC 9798-1:

**entity authentication:** the corroboration that an entity is the one claimed.

The following terms are used as defined in ISO/IEC 10118-1:

**collision-resistant hash-function:** a hash-function satisfying the following property:

- it is computationally infeasible to find any two distinct inputs which map to the same output.

**hash-function:** a function which maps strings of bits to fixed-length strings of bits, satisfying two important properties. The first property states that for a given output, it is computationally infeasible to find an input which map to this output. The second property states