INTERNATIONAL STANDARD

ISO/IEC 18014-2

Second edition
2009-12-15

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 18014-2:2009(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

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.

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 18014-2 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 18014-2:2002). The text has been revised to clarify the presentation, and a new time-stamping mechanism has been added.

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*

Information technology — Security techniques — Time-stamping services —

Part 2: Mechanisms producing independent tokens

1 Scope

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

Time-stamping services may generate, renew and verify time-stamp tokens.

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 at the associated date and time. In addition, the evidence may be used by non-repudiation services.

This part of ISO/IEC 18014 specifies mechanisms that generate independent time-stamps: in order to verify an independent time-stamp token, verifiers do not need access to any other time-stamp tokens. That is, time-stamp tokens are not linked, as is the case for the token types defined in ISO/IEC 18014-3.

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/IEC 8824-1:1998, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation*

ISO/IEC 9594-8:2005, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 18014-1:2008, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

3 Terms and definitions

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

3.1
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation

NOTE Adapted from ISO/IEC 9798-1.