

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)



This is a preview of "ISO/IEC 18014-2:2009". [Click here to purchase the full version from the ANSI store.](#)

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.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2009

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of "ISO/IEC 18014-2:2009". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Notation, symbols and abbreviated terms	5
5 Time-stamping services	5
6 Time-stamp tokens	6
6.1 Contents	6
6.2 Notation	7
6.3 Verification	7
6.4 Renewal	8
6.5 Renewal verification	8
7 Protection mechanisms	9
8 Independent time-stamp tokens	10
8.1 Core structure	10
8.2 Extensions	10
8.3 Protection mechanisms	11
8.3.1 Digital signatures using SignedData	11
8.3.2 Message authentication codes using AuthenticatedData	11
8.3.3 Archival	13
8.3.4 Digital signatures using SignerInfo	13
8.4 Protocols	15
Annex A (normative) ASN.1 Module for Time-Stamping	16
Annex B (informative) Cryptographic Syntax	22
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 18014-2 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*