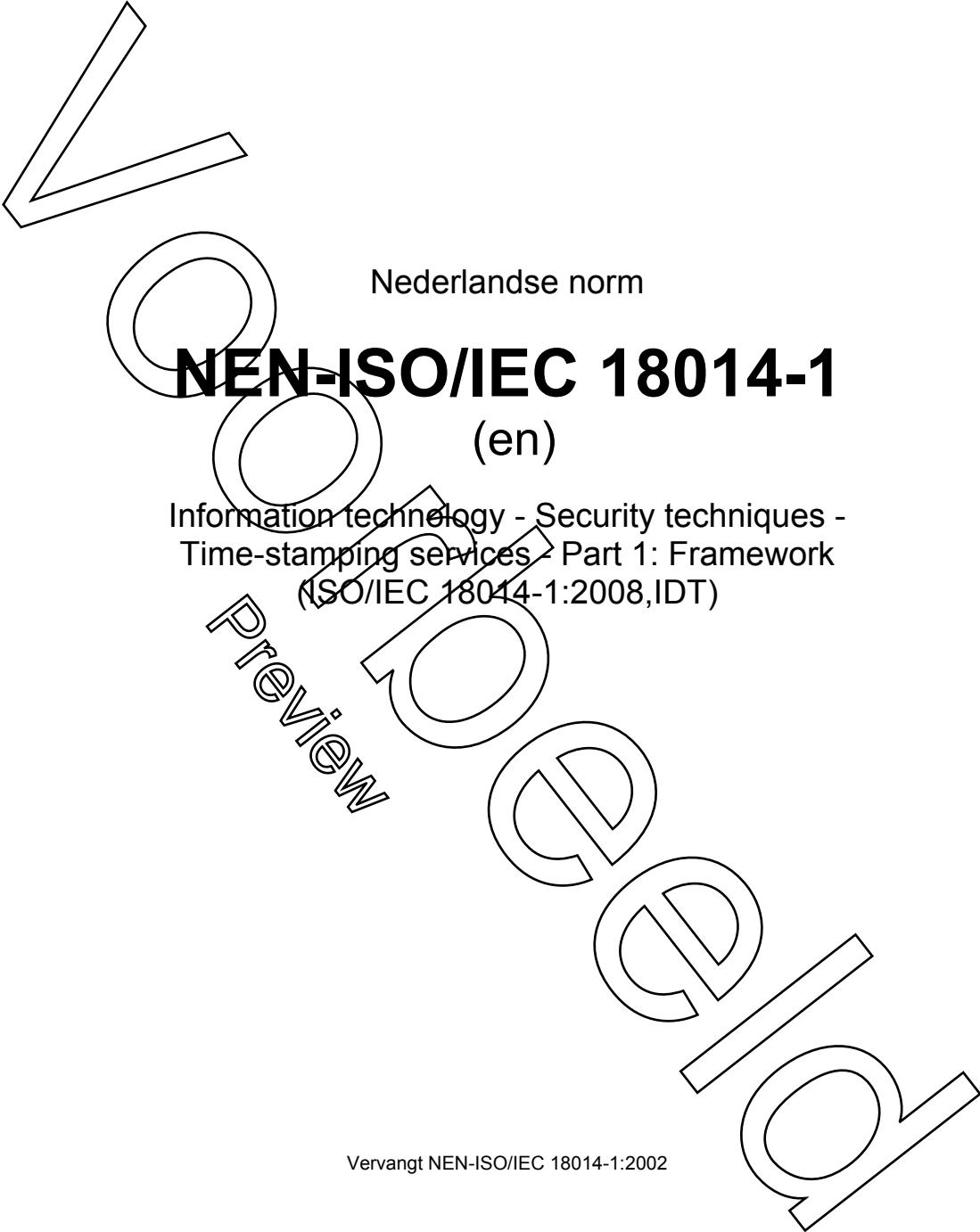


Dit document mag slechts op een stand-alone PC worden geïnstalleerd. Gebruik op een netwerk is alleen toestaan als een aanvullende licentieovereenkomst voor netwerkgebruik met NEN is afgesloten.  
This document may only be used on a stand-alone PC. Use in a network is only permitted when a supplementary license agreement for us in a network with NEN has been concluded.



Nederlandse norm

# **NEN-ISO/IEC 18014-1**

(en)

Information technology - Security techniques -  
Time-stamping services - Part 1: Framework  
(ISO/IEC 18014-1:2008, IDT)

Vervangt NEN-ISO/IEC 18014-1:2002

ICS 35.040  
september 2008

Als Nederlandse norm is aanvaard:

- ISO/IEC 18014-1:2008, IDT

VOORBEELD  
Preview

Normcommissie 381 027 "IT-Beveiligingstechnieken"

---

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Netherlands Standardization Institute.

The Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

---

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Nederlands Normalisatie-instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

---

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Netherlands Standardization Institute.

---

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaardden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Nederlands Normalisatie-instituut gepubliceerde uitgaven.

Preview

---

---

**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*

**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  
Preview

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2008

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](mailto:copyright@iso.org)  
Web [www.iso.org](http://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.

Copyright  
Preview

Voorbeeld  
Preview



# 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*

### 3 Terms and definitions

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

#### 3.1 certification authority

##### CA

centre trusted to create and assign public key certificates

NOTE Optionally, the certification authority can create and assign keys to the entities.

[ISO/IEC 11770-1:1996]

# Bestelformulier

## Stuur naar:

NEN Standards Products & Services  
t.a.v. afdeling Klantenservice  
Antwoordnummer 10214  
2600 WB Delft



**NEN** Standards Products & Services

Postbus 5059  
2600 GB Delft

Vlinderweg 6  
2623 AX Delft

T (015) 2 690 390  
F (015) 2 690 271

[www.nen.nl/normshop](http://www.nen.nl/normshop)

## Ja, ik bestel

\_\_ ex. NEN-ISO/IEC 18014-1:2008 en Information technology - Security techniques - Time-stamping services - Part 1: Framework € 124.99

**Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via [www.nen.nl/normshop](http://www.nen.nl/normshop)**

### Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. [www.nen.nl/nieuwsbrieven](http://www.nen.nl/nieuwsbrieven)

## Gegevens

Bedrijf / Instelling \_\_\_\_\_

T.a.v. \_\_\_\_\_ O M O V

E-mail \_\_\_\_\_

Klantnummer NEN \_\_\_\_\_

Uw ordernummer \_\_\_\_\_ BTW nummer \_\_\_\_\_

Postbus / Adres \_\_\_\_\_

Postcode \_\_\_\_\_ Plaats \_\_\_\_\_

Telefoon \_\_\_\_\_ Fax \_\_\_\_\_

**Factuuradres** (indien dit afwijkt van bovenstaand adres)

Postbus / Adres \_\_\_\_\_

Postcode \_\_\_\_\_ Plaats \_\_\_\_\_

Datum \_\_\_\_\_ Handtekening \_\_\_\_\_

### Retourneren

Fax: 015 2 690 271

E-mail: [klantenservice@nen.nl](mailto:klantenservice@nen.nl)

Post: NEN Standards Products & Services,

t.a.v. afdeling Klantenservice  
Antwoordnummer 10214,  
2600 WB Delft

(geen postzegel nodig).

### Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typfouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: [www.nen.nl/leveringsvoorwaarden](http://www.nen.nl/leveringsvoorwaarden).