INTERNATIONAL STANDARD

ISO/IEC 18014-3

Second edition
2009-12-15

Information technology — Security techniques — Time-stamping services —

Part 3: Mechanisms producing linked tokens

Technologies de l'information — Techniques de sécurité — Services d'horodatage —

Partie 3: Mécanismes produisant des jetons liés

Reference number
ISO/IEC 18014-3:2009(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

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member 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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 18014-3 was prepared by Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition replaces and cancels the first edition (ISO/IEC 18014-3:2004), which has been technically revised. New message formats and data types are defined to support a protocol for extending an existing linked token with data items referring to a published value issued by the TSA. The data type clauses have been expanded and re-ordered, and the ASN.1 definitions in Annex A have been updated and reordered in line with the contents of the clauses in the main body of this International Standard. Annexes B and C have been updated.

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

ISO/IEC 18014-1 provides a general framework for the provision of time-stamping services. This part of ISO/IEC 18014 specifies mechanisms producing linked tokens, that is, time-stamp tokens that are related, or "linked", to other time-stamp tokens produced by the methods and processes described in this document. A time stamping authority (TSA) can utilise the methods and processes described within this document to provide a secure, verifiable cryptographic binding between a certain point in time and data values, in a way that enhances the security of the resulting token.

Information technology — Security techniques — Time-stamping services —

Part 3:
Mechanisms producing linked tokens

1 Scope

This part of ISO/IEC 18014

— describes a general model for time-stamping services producing linked tokens,

— describes the basic components used to construct a time-stamping service producing linked tokens,

— defines the data structures used to interact with a time-stamping service producing linked tokens,

— describes specific instances of time-stamping services producing linked tokens, and

— defines a protocol to be utilized by time-stamping services producing linked tokens for the purpose of extending linked tokens to published values.

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

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
aggregation
process of generating a proxy data item for a group of data items that are linked together, producing a verifiable cryptographic link between each data item and the rest of the group

3.2
collision-resistant hash-function
hash-function satisfying the following property: it is computationally infeasible to find any two distinct inputs which map to the same output

[ISO/IEC 10118-1:2000, definition 3.2]