International Standard

ISO/IEC 23078-2

Information technology — Specification of digital rights management (DRM) technology for digital publications —

Part 2: User key-based protection

First edition
2024-06

Reference number
ISO/IEC 23078-2:2024(en)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 34, *Document description and processing languages*.

This document cancels and replaces ISO/IEC TS 23078-2:2020, which has been technically revised.

The main changes are as follows:

— four sentences which mentions the ‘LCP related registries’ in 6.3.3.3 (link relationships), 6.3.4 (rights), 6.3.5 (user) and 8.1 (encryption profile) have been changed into NOTE;

— four information references (RFC 6901, RFC 6570, XML Signature Syntax and Processing Version 1.1 and XML Encryption Syntax and Processing Version 1.1) have been changed into normative references;

— Annex C has been added.

A list of all parts in the ISO/IEC 23078 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Ever since ebooks have grown in popularity, copyright protection has been an important issue for authors and publishers.

While the distribution of ebooks around the world is mostly based on the open EPUB standard, most ebook retailers are using proprietary technologies to enforce usage constraints on digital publications in order to impede oversharing of copyrighted content. The high level of interoperability and accessibility gained by the use of a standard publishing format is therefore cancelled by the use of proprietary and closed technologies: ebooks are only readable on specific devices of software applications (a retailer "lock-in" syndrome), cannot be accessed anymore if the ebook distributor which protected the publication goes out of business or if the DRM technology evolves drastically. As a result, users are deprived of any control over their ebooks.

Requirements related to security levels differ depending on which part of the digital publishing market is addressed. In many situations, publishers require a solution which technically enforces the digital rights they provide to their users; most publishers are happy to adopt a DRM solution which guarantees an easy transfer of publications between devices, a certain level of fair-use and provides permanent access to the publications acquired by their customers.

This is where this document comes into play[1)].

1) Although this document is primarily intended for the protection of EPUB publications, it can also protect digital publications in other formats, provided that the publication format supports the encryption of resources and the embedding of a license. This is especially the case for PDF documents contained in a Readium Packaging Format, as presented in Annex C. This is important for owners of large PDF collections, who want to apply the same DRM to their EPUB and PDF collections.

Information technology — Specification of digital rights management (DRM) technology for digital publications —

Part 2: User key-based protection

1 Scope

This document defines a technical solution for encrypting resources in digital publications (especially EPUB) and for securely delivering decryption keys to reading systems, included in licenses tailored to specific users. It also defines a simple passphrase-based authentication method for reading systems to verify the license and access the encrypted resources of such digital publications.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

EPUB 3.3, W3C, available at https://www.w3.org/TR/epub-33/

ISO 8601-1, *Date and time — Representations for information interchange — Part 1: Basic rules*

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

RFC 4627[2], *The application/json Media Type for JavaScript Object Notation (JSON), The Internet Society*

RFC 5280[3], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group*

RFC 6570[4], *URI Template, Internet Engineering Task Force (IETF)*

RFC 6901[5], *JavaScript Object Notation (JSON) Pointer, Internet Engineering Task Force (IETF)*

RFC 7807[6], *Problem Details for HTTP APIs, The Internet Engineering Task Force*

XML Encryption Syntax and Processing Version 1.1, W3C, available at https://www.w3.org/TR/xmlenc-core1/

XML Signature Syntax and Processing Version 1.1, W3C, available at https://www.w3.org/TR/xmldsig-core1/

2) Available at https://www.ietf.org/rfc/rfc4627.

3) Available at https://tools.ietf.org/html/rfc5280.

4) Available at https://tools.ietf.org/html/rfc6570.

5) Available at https://tools.ietf.org/html/rfc6901.

6) Available at https://tools.ietf.org/html/rfc7807.