International Standard

ISO/IEC 23078-2

First edition
2024-06

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

Part 2: User key-based protection

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

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Abbreviated terms **3**
5 Overview **4**
5.1 General 4
5.2 Protecting the publication 4
5.3 Licensing the publication 5
5.4 Reading the publication 5
6 License document **6**
6.1 General 6
6.2 Content conformance 6
6.3 License information 6
6.3.1 General 6
6.3.2 Encryption (transmitting keys) 7
6.3.3 Links (pointing to external resources) 8
6.3.4 Rights (identifying rights and restrictions) 9
6.3.5 User (identifying the user) 10
6.3.6 Signature (signing the license) 11
6.4 User key 12
6.4.1 General 12
6.4.2 Calculating the user key 12
6.4.3 Hints 12
6.4.4 Requirements for the user key and user passphrase 13
6.5 Signature and public key infrastructure 13
6.5.1 General 13
6.5.2 Certificates 13
6.5.3 Canonical form of the license document 14
6.5.4 Generating the signature 15
6.5.5 Validating the certificate and signature 17
7 License status document **17**
7.1 General 17
7.2 Content conformance 17
7.3 License status information 18
7.3.1 General 18
7.3.2 Status 18
7.3.3 Updated (timestamps) 18
7.3.4 Links 19
7.3.5 Potential rights 19
7.3.6 Events 20
7.4 Interactions 20
7.4.1 General 20
7.4.2 Handling errors 20
7.4.3 Checking the status of a license 20
7.4.4 Registering a device 21
7.4.5 Returning a publication 22
7.4.6 Renewing a license 23
8 Encryption profile **24**
8.1 General 24
8.2 Encryption profile requirements 25

© ISO/IEC 2024 – All rights reserved

8.3 Basic encryption profile 1.0 25
9 Integration in EPUB 25
9.1 General 25
9.2 Encrypted resources 25
9.3 Using META-INF/encryption.xml for LCP 26
10 Reading system behaviour 27
10.1 Detecting LCP protected publication 27
10.2 License document processing 27
10.2.1 Overall 27
10.2.2 Validating the license document 27
10.2.3 Acquiring the publication 27
10.2.4 License status processing 28
10.3 User key processing 28
10.4 Signature processing 28
10.5 Publication processing 29
Annex A (informative) **Examples 30**
Annex B (informative) **Use case scenarios for library lending model 33**
Annex C (informative) **An extension of the LCP specification for PDF 36**
Bibliography 38

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

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.

© ISO/IEC 2024 – All rights reserved

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
codec content type
content type that has intrinsic binary format qualities

EXAMPLE Such as video and audio media type.

Note 1 to entry: It is already designed for optimum compression or provides optimized streaming capabilities.

3.2
content key
symmetric key used to encrypt and decrypt *publication resources* (3.15)

3.3
encryption profile
set of encryption algorithms used in a specific *protected publication* (3.10) and associated *license document* (3.6)

3.4
container
EPUB container
zip-based packaging and distribution format for *EPUB publications* (3.13)

[SOURCE: EPUB 3.3, clause 4]

3.5
license authority
entity which delivers *provider certificates* (3.12) to *content providers* (3.11)

3.6
license document
document that contains references to the various keys, links to related external resources, rights and restrictions that are applied to *protected publication* (3.10), and *user* (3.18) information

3.7
licensed content protection
LCP
Readium LCP
DRM technology published by the Readium Foundation

3.8
non-codec content type
content type that benefits from compression due to the nature of its internal data structure

EXAMPLE Such as a file format based on character strings (e.g. HTML, CSS)

3.9
package document
publication resource (3.15) carrying meta information about an *EPUB publication* (3.13)

3.10
protected publication
LCP-protected publication
publication (3.13) in which *resources* (3.15) have been encrypted according to this document

© ISO/IEC 2024 – All rights reserved