International Standard

ISO/IEC 23078-3

First edition
2024-06

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

Part 3: Device key-based protection

Reference number
ISO/IEC 23078-3:2024(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 **1**
4 Abbreviated terms **4**
5 Overview **4**
5.1 General 4
5.2 Protecting the publication 5
5.3 Licensing the publication 5
5.4 Reading the publication 6
5.4.1 General 6
5.4.2 Registering a device 6
5.4.3 Acquiring a device key-based license document 6
5.4.4 Decrypting a resource 6
5.5 Licensing workflows 7
5.5.1 General 7
5.5.2 Getting a protected publication 7
5.5.3 Transferring a protected publication 7
5.5.4 Register device certificate and update license document 8
6 License document **9**
6.1 General 9
6.2 Content conformance 9
6.3 License information 9
6.3.1 General 9
6.3.2 Encryption (transmitting keys) 9
6.3.3 Links (pointing to external resources) 11
6.3.4 Rights (identifying rights and restrictions) 12
6.3.5 User (identifying the user) 12
6.3.6 Signature (signing the license) 12
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 12
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 14
6.5.5 Validating the certificate and signature 14
6.6 Device key 14
6.6.1 General 14
6.6.2 Generating the device key 14
6.6.3 Recommendations for the device private key protection 15
7 License status document **15**
7.1 General 15
7.2 Content conformance 15
7.3 License status information 15
7.3.1 General 15
7.3.2 Status 15
7.3.3 Updated 15

© ISO/IEC 2024 – All rights reserved

7.3.4 Links 15
7.3.5 Potential rights 16
7.3.6 Events 16
7.4 Interactions 16
7.4.1 General 16
7.4.2 Handling errors 17
7.4.3 Checking the status of a license 17
7.4.4 Registering a device 17
7.4.5 Returning a publication 19
7.4.6 Renewing a license 19
8 Encryption profiles 19
8.1 General 19
8.2 Encryption profile requirements 19
8.3 Basic encryption profile 20
9 Integration in EPUB 20
10 Reading system behaviours 20
10.1 Detecting protected publications 20
10.2 License document processing 20
10.3 User key processing 20
10.4 Signature processing 20
10.5 Publication processing 20
10.6 Device key processing 20
Annex A (informative) **Examples 22**
Annex B (informative) **Schema of license document 24**
Annex C (informative) **An extension of the ISO/IEC 23078-3 specification for PDF 29**
Bibliography 31

© 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 JTC1, *Information technology,* Subcommittee SC 34, *Document description and processing languages*.

This document cancels and replaces ISO/IEC TS 23078-3:2021, which has been technically revised.

The main changes are as follows:

— 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 or software applications (a retailer "lock-in" syndrome); ebooks 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 they have acquired. However, in certain use cases, publishers require a stronger protection measure, which limits the capability for users to transfer publications from one device to another.

This document, as a variation of the ISO/IEC 23078-2, is a protection technology for digital publication[1)] with which transferring of the publication to multiple devices can be limited in accordance with providers' policies.

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 3:
Device key-based protection

1 Scope

This document defines a technical solution for encrypting resources in digital publications (especially EPUB), effectively registering a device certificate to providers and securely delivering decryption keys to reading systems included in licenses tailored to specific devices. This technical solution uses the passphrase-based authentication method defined in ISO/IEC 23078-2 for reading systems to receive 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.

ISO/IEC 23078-2:2024, *Information Technology — Specification of DRM technology for digital publications— Part 2: User key-based protection*

RFC 5280[2)], *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group*

3 Terms and definitions

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

ISO and IEC maintain terminology 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
content key
symmetric key used to encrypt and decrypt *publication resources* (3.16)

[SOURCE: ISO/IEC 23078-2:2024, 3.2]

3.2
container
EPUB container
zip-based packaging and distribution format for *EPUB publications* (3.12)

[SOURCE: ISO/IEC 23078-2:2024, 3.4]

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

© ISO/IEC 2024 – All rights reserved