TECHNICAL SPECIFICATION

**ISO/IEC TS 23078-3**

First edition
2021-03

# Information technology — Specification of DRM technology for digital publications —

## Part 3: Device key-based protection

*Technologies de l'information — Spécification de la technologie de gestion des droits numériques (DRM) pour les publications numériques —*

*Partie 3: Protection par clé matériel*

Reference number
ISO/IEC TS 23078-3:2021(E)

© ISO/IEC 2021



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2021

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 ..... 7
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 ..... 8
5.5.4 Register device certificate and update license document ..... 9
**6 License document** ..... **10**
6.1 General ..... 10
6.2 Content conformance ..... 10
6.3 License information ..... 10
6.3.1 General ..... 10
6.3.2 Encryption (transmitting keys) ..... 10
6.3.3 Links (pointing to external resources) ..... 12
6.3.4 Rights (identifying rights and restrictions) ..... 13
6.3.5 User (identifying the user) ..... 13
6.3.6 Signature (signing the license) ..... 13
6.4 User key ..... 13
6.4.1 General ..... 13
6.4.2 Calculating the user key ..... 14
6.4.3 Hints ..... 14
6.4.4 Requirements for the user key and user passphrase ..... 14
6.5 Signature and public key infrastructure ..... 14
6.5.1 General ..... 14
6.5.2 Certificates ..... 14
6.5.3 Canonical form of the license document ..... 15
6.5.4 Generating the signature ..... 15
6.5.5 Validating the certificate and signature ..... 15
6.6 Device key ..... 15
6.6.1 General ..... 15
6.6.2 Generating the device key ..... 16
6.6.3 Recommendations for the device private key protection ..... 16
**7 License status document** ..... **16**
7.1 General ..... 16
7.2 Content conformance ..... 16
7.3 License status information ..... 17
7.3.1 General ..... 17
7.3.2 Status ..... 17
7.3.3 Updated ..... 17

© ISO/IEC 2021 – All rights reserved

7.3.4 Links ... 17
7.3.5 Potential rights ... 18
7.3.6 Events ... 18
7.4 Interactions ... 18
7.4.1 General ... 18
7.4.2 Handling errors ... 18
7.4.3 Checking the status of a license ... 18
7.4.4 Registering a device ... 18
7.4.5 Returning a publication ... 20
7.4.6 Renewing a license ... 21
**8 Encryption profiles ... 21**
8.1 General ... 21
8.2 Encryption profile requirements ... 21
8.3 Basic encryption profile ... 21
**9 Integration in EPUB ... 22**
**10 Reading system behaviours ... 22**
10.1 Detecting protected publications ... 22
10.2 License document processing ... 22
10.3 User key processing ... 22
10.4 Signature processing ... 22
10.5 Publication processing ... 22
10.6 Device key processing ... 22
**Annex A** (informative) **Examples ... 23**
**Annex B** (informative) **Schema of license document ... 25**
**Bibliography ... 30**


© ISO/IEC 2021 – 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).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

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.

This document was prepared by Joint Technical Committee ISO/IEC JTC1, *Information technology,* Subcommittee SC 34, *Document description and processing languages*.

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.

© ISO/IEC 2021 – 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 TS 23078-2, is a protection technology for EPUB publication with which transferring of the publication to multiple devices can be limited in accordance with providers' policies.


© ISO/IEC 2021 – All rights reserved

# Information technology — Specification of DRM technology for digital publications —

# Part 3: Device key-based protection

## 1 Scope

This document defines a technical solution for encrypting resources of EPUB publications, 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 TS 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 TS 23078-2:2020, *Information Technology — Specification of DRM technology for digital publications—Part2: User key-based protection*

RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group, available at https://tools.ietf.org/html/rfc5280

## 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 http://www.electropedia.org/

**3.1**
**content key**
symmetric key used to encrypt and decrypt *publication resources* (3.16)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.2]

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

[SOURCE: ISO/IEC TS 23078-2:2020, 3.4]

**3.3**
**device key**
public key in a *device certificate* (3.4) that is used to encrypt the *content key* (3.1)

© ISO/IEC 2021 – All rights reserved

**3.4**
**device certificate**
certificate which is issued for a given *reading system* (3.13) and is signed by the *reading system developer* (3.14)

**3.5**
**device private key**
private key embedded securely in a *reading system* (3.13), paired with a *device key* (3.3) and used to decrypt the *content key* (3.1)

**3.6**
**encryption profile**
set of encryption algorithms used in a specific *protected publication* (3.9) and associated *license document* (3.8)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.3]

**3.7**
**license authority**
entity which delivers *provider certificates* (3.11) to *content providers* (3.10) and *reading system developer certificates* (3.15) to *reading system* (3.13)

Note 1 to entry: License authority in this document has an additional role to deliver reading system developer certificates.

[SOURCE: ISO/IEC TS 23078-2:2020, 3.5, modified — Additional role and Note 1 to entry have been added.]

**3.8**
**license document**
document which contains references to the various keys, links to related external resources, rights and restrictions that are applied to *protected publication* (3.9), and *user* (3.19) information

[SOURCE: ISO/IEC TS 23078-2:2020, 3.6]

**3.9**
**protected publication**
*publication* (3.12) in which *resources* (3.16) have been encrypted according to this document

[SOURCE: ISO/IEC TS 23078-2:2020, 3.10, modified — The preferred term "LCP-protected publication" has been removed.]

**3.10**
**provider**
**content provider**
entity that delivers licenses for *protected publications* (3.9) to *users* (3.19)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.11, modified — "LCP" before "licenses" has been removed.]

**3.11**
**provider certificate**
certificate that is included in the *license document* (3.8) to identify the *content provider* (3.10) and validate the signature of the license document

[SOURCE: ISO/IEC TS 23078-2:2020, 3.12]

**3.12**
**publication**
**EPUB publication**
logical document entity consisting of a set of interrelated *resources* (3.16) and packaged in an *EPUB container* (3.2)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.13]


© ISO/IEC 2021 – All rights reserved

**3.13**
**reading system**
system which processes *EPUB publications* (3.12) and presents them to *users* (3.19)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.14]

**3.14**
**reading system developer**
**developer**
EPUB reading system developer
entity which signs the *device certificate* (3.4) associated with a *reading system* (3.13)

**3.15**
**reading system developer certificate**
**developer certificate**
EPUB reading system developer certificate
certificate which is embedded in the *reading system* (3.13) in order to confirm that the *device certificate* (3.4) is valid

**3.16**
**resource**
**publication resource**
content or instructions that contribute to the logic and rendering of an *EPUB publication* (3.12)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.15]

**3.17**
**root certificate**
certificate possessed by the *license authority* (3.7) and embedded in each EPUB *reading system* (3.13) in order to confirm that the *provider certificate* (3.11) or *reading system developer* (3.14) is valid

[SOURCE: ISO/IEC TS 23078-2:2020, 3.16, modified — "or reading system developer" has been added.]

**3.18**
**status document**
**license status document**
document that contains the current status and possible interactions with a *license document* (3.8), along with historical information

[SOURCE: ISO/IEC TS 23078-2:2020, 3.17]

**3.19**
**user**
individual who consumes an *EPUB publication* (3.12) using an EPUB *reading system* (3.13)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.18]

**3.20**
**user key**
hash value of the *user passphrase* (3.21), used to authenticate a *reading system* (3.13) to be able to access a *protected publication* (3.9)

Note 1 to entry: User key in this document is only used for authentication purpose to access a protection publication.

[SOURCE: ISO/IEC TS 23078-2:2020, 3.19, modified — The decryption role has been removed; the authentication role and Note 1 to entry have been added.]

© ISO/IEC 2021 – All rights reserved

**3.21**
**user passphrase**
string of text entered by the *user* (3.19) for obtaining access to the *protected publication* (3.9)

[SOURCE: ISO/IEC TS 23078-2:2020, 3.20]

# 4 Abbreviated terms

DRM digital rights management

LCP licensed content protection

# 5 Overview

## 5.1 General

In order to deliver a publication to users without risk of indiscriminate redistribution, most publication resources are encrypted; and a license document is generated.

The license document can be transmitted outside an EPUB container or be embedded inside it. Following the EPUB OCF 3.2 specification, META-INF/encryption.xml identifies all encrypted publication resources and points to the content key needed to decrypt them. This content key is located inside the license document and is itself encrypted using the device key. The device key is a public key whose paired device private key is present in the device. It is used to decrypt the content key, which in turn is used to decrypt the publication resources.

The license document may also contain links to external resources, information identifying the user, and information about what rights are conveyed to the user and which are not. Rights information may include things like the time during which the license is valid, or whether the publication may be printed or copied, etc. Finally, the license document always includes a digital signature to prevent modification of any of its components.

NOTE This subclause has been modified from ISO/IEC TS 23078-2:2020, 5.1. The role of user key has been removed and device key has been added.

Figure 1 shows the relationships among the various components of device key-based protection.


© ISO/IEC 2021 – All rights reserved