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

© ISO/IEC 2021 – All rights reserved