



BSI Standards Publication

Information technology — Specification of DRM technology for digital publications

Part 2: User key-based protection

National foreword

This Published Document is the UK implementation of ISO/IEC TS 23078-2:2020.

The UK participation in its preparation was entrusted to Technical Committee IST/41, Document description and processing language.

A list of organizations represented on this committee can be obtained on request to its committee manager.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2020
Published by BSI Standards Limited 2020

ISBN 978 0 539 15580 8

ICS 35.240.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 October 2020.

Amendments/corrigenda issued since publication

| Date | Text affected |
|------|---------------|
|------|---------------|

**TECHNICAL
SPECIFICATION**

**ISO/IEC TS
23078-2**

First edition
2020-09

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

**Part 2:
User key-based protection**



Reference number
ISO/IEC TS 23078-2:2020(E)

© ISO/IEC 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2020

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 | 3 |
| 5 Overview | 3 |
| 5.1 General..... | 3 |
| 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..... | 13 |
| 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..... | 14 |
| 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..... | 18 |
| 7.3 License status information..... | 18 |
| 7.3.1 General..... | 18 |
| 7.3.2 Status..... | 18 |
| 7.3.3 Updated (timestamps)..... | 19 |
| 7.3.4 Links..... | 19 |
| 7.3.5 Potential rights..... | 20 |
| 7.3.6 Events..... | 20 |
| 7.4 Interactions..... | 21 |
| 7.4.1 General..... | 21 |
| 7.4.2 Handling errors..... | 21 |
| 7.4.3 Checking the status of a license..... | 21 |
| 7.4.4 Registering a device..... | 21 |
| 7.4.5 Returning a publication..... | 22 |
| 7.4.6 Renewing a license..... | 23 |
| 8 Encryption profile | 25 |
| 8.1 General..... | 25 |

| | | |
|-----------|---|-----------|
| 8.2 | Encryption profile requirements | 25 |
| 8.3 | Basic encryption profile 1.0 | 26 |
| 9 | Integration in EPUB | 26 |
| 9.1 | General | 26 |
| 9.2 | Encrypted resources | 26 |
| 9.3 | Using META-INF/encryption.xml for LCP | 27 |
| 10 | Reading system behavior | 28 |
| 10.1 | Detecting LCP protected publication | 28 |
| 10.2 | License document processing | 28 |
| 10.2.1 | Overall | 28 |
| 10.2.2 | Validating the license document | 28 |
| 10.2.3 | Acquiring the publication | 28 |
| 10.2.4 | License status processing | 28 |
| 10.3 | User key processing | 29 |
| 10.4 | Signature processing | 29 |
| 10.5 | Publication processing | 29 |
| | Annex A (informative) Examples | 30 |
| | Annex B (informative) Use case scenarios for library lending model | 33 |
| | Bibliography | 36 |

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 <http://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 JTC 1, *Information technology*, Subcommittee SC 34, *Document description and processing languages*.

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

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.

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), 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.

Information technology — Specification of 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 publication.

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 Open Container Format (OCF) 3.2, W3C, available at <https://www.w3.org/publishing/epub32/epub-ocf>

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): Specification of basic notation — Part 1:*

RFC 4627, *The application/json Media Type for JavaScript Object Notation (JSON)*, The Internet Society, available at <https://www.ietf.org/rfc/rfc4627>

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>

RFC 7807, *Problem Details for HTTP APIs*, The Internet Engineering Task Force, available at <https://tools.ietf.org/html/rfc7807>

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

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.