ISO/IEC ~~DIS~~PRF 23078-2~~:2024(E)~~

ISO/IEC JTC 1/SC 34~~/JWG 7~~

Secretariat: JISC

Date: 2024-~~01-22~~04-18

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

Part 2:
User key-based protection

PRF stage

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: + 41 22 749 01 11

~~Fax: +41 22 749 09 47~~

~~Email~~E-mail: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

~~© 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~~four sentences which mentions the 'LCP related registries' in 6.3.3.3~~6.3.3.3(Link~~ (link relationships), 6.3.4 ~~6.3.4~~(rights), 6.3.5 ~~6.3.5~~(user) and 8.1 ~~8.1~~(encryption profile) ~~are~~have been changed into NOTE~~.~~;
- ~~Four~~four information references (RFC 6901, RFC 6570, XML Signature Syntax and Processing Version 1.1 and XML Encryption Syntax and Processing Version 1.1) ~~described in the bibliography clause, are moved into Normative clause.~~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)].

~~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~~

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

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],~~[2)] *The application/json Media Type for JavaScript Object Notation (JSON), The Internet Society*

RFC 5280~~[3],~~[3)] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group*

RFC 6570~~[4],~~[4)] *URI Template, Internet Engineering Task Force (IETF)*

RFC 6901~~[5],~~[5)] *JavaScript Object Notation (JSON) Pointer, Internet Engineering Task Force (IETF)*

RFC 7807~~[6],~~[6)] *Problem Details for HTTP APIs, The Internet Engineering Task Force*

~~[2] Available at https://www.ietf.org/rfc/rfc4627.~~
[2)] Available at https://www.ietf.org/rfc/rfc4627.
~~[3] Available at https://tools.ietf.org/html/rfc5280.~~
[3)] Available at https://tools.ietf.org/html/rfc5280.
~~[4] Available at https://tools.ietf.org/html/rfc6570.~~
[4)] Available at https://tools.ietf.org/html/rfc6570.
~~[5] Available at https://tools.ietf.org/html/rfc6901.~~
[5)] Available at https://tools.ietf.org/html/rfc6901.
~~[6] Available at https://tools.ietf.org/html/rfc7807.~~
[6)] Available at https://tools.ietf.org/html/rfc7807.

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/

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~~(3.15)~~)

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

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

[SOURCE: EPUB 3.3, clause 4]

3.5
license authority
entity which delivers *provider certificates* (3.12~~(3.12)~~) to *content providers* (3.11~~(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~~(3.10),~~), and *user* (3.18~~(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 (~~for example~~e.g. HTML, CSS~~, etc.~~))

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

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

3.11
provider
content provider
entity that delivers LCP licenses for *protected publications* (3.10~~(3.10)~~) to *users* (3.18~~(3.18)~~)

3.12
provider certificate
certificate that is included in the *license document* (3.6~~(3.6)~~) to identify the *content provider* (3.11~~(3.11)~~) and validate the signature of the license document

3.13
publication
EPUB publication
logical document entity consisting of a set of interrelated *resources* (3.15~~(3.15)~~) and packaged in an *EPUB container* (3.4~~(3.4)~~)

[SOURCE: EPUB 3.3]

3.14
reading system
system that processes *EPUB publications* (3.13~~(3.13)~~) and presents them to *users* (3.18~~(3.18)~~)

[SOURCE: EPUB Reading Systems 3.3]

3.15
resource
publication resource
content or instructions that contribute to the logic and rendering of an *EPUB publication* (3.13~~(3.13)~~)

3.16
root certificate
certificate possessed by the *license authority* (3.5~~(3.5)~~) and embedded in each EPUB *reading system* (3.14~~(3.14)~~) in order to confirm that the *provider certificate* (3.12~~(3.12)~~) is valid

3.17
status document
license status document
document that contains the current status and possible interactions with a *license document* (3.6~~(3.6),~~), along with historical information

3.18
user
individual that consumes an *EPUB publication* (3.13~~(3.13)~~) using an EPUB *reading system* (3.14~~(3.14)~~)

3.19
user key
hash value of the *user passphrase* (3.20~~(3.20),~~) used to decrypt the *content key* (3.2~~(3.2)~~) and any encrypted *user* (3.18~~(3.18)~~) information embedded in a *license document* (3.6~~(3.6)~~)

3.20
user passphrase
string of text entered by the *user* (3.18~~(3.18)~~) for obtaining access to the *protected publication* (3.10~~(3.10)~~)

4 Abbreviated terms

DRM digital rights management

IANA Internet Assigned Number Authority

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 3.3 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 user key. The user key is generated by calculating a hash of a user passphrase. It is used to decrypt the content key, which in turn is used to decrypt the publication resources.

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

Figure 1~~Figure 1~~ shows the relationships among the various components of LCP.

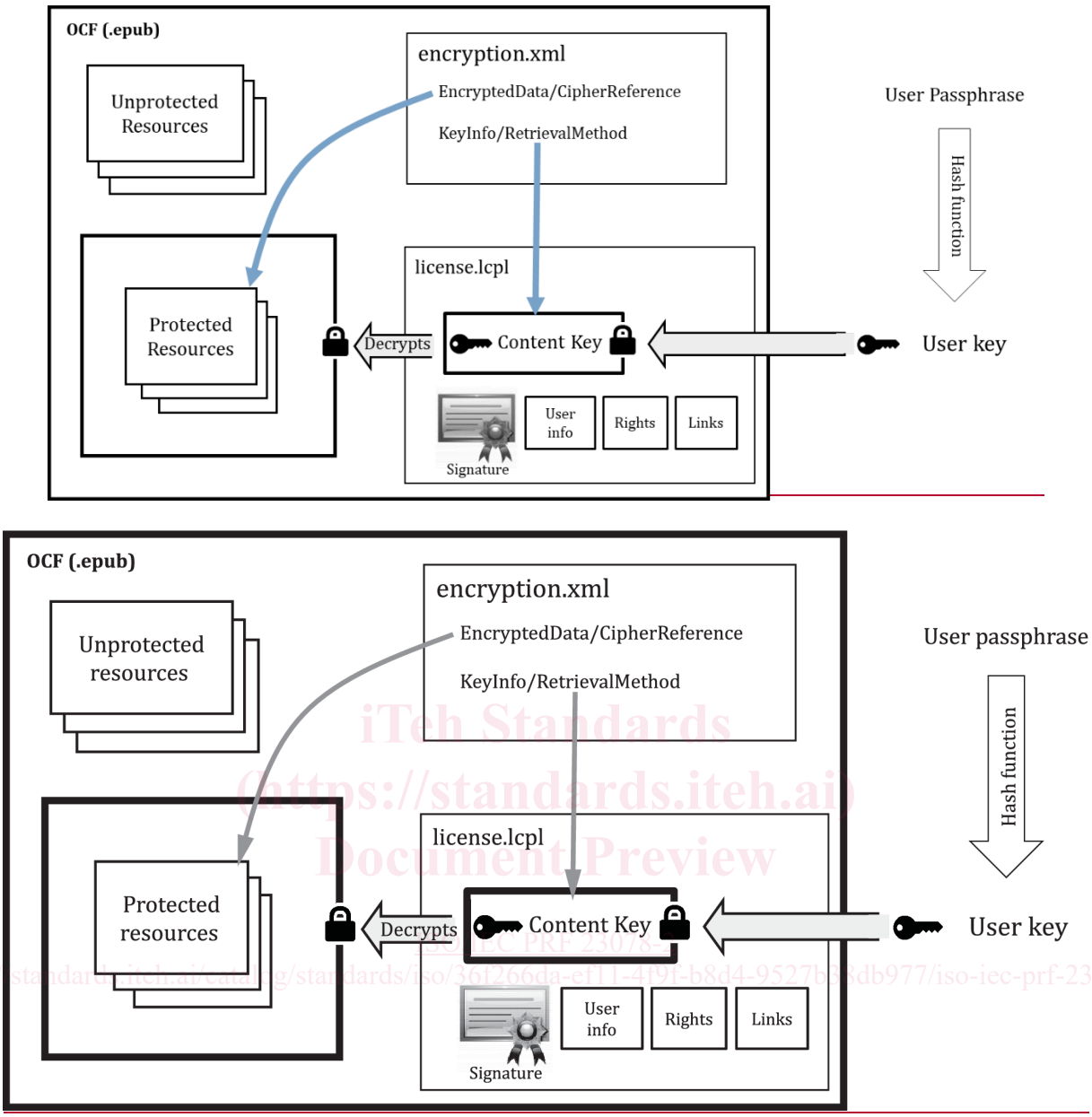

Figure 1 — Protected publication with a license document

5.2 Protecting the publication

To protect a publication, a content provider follows these steps.

a) ~~a)~~ Generate a unique content key for the publication.

b) ~~b)~~ Store this content key for future use in licensing the publication.

c) ~~c)~~ Encrypt each protected resource using that key, after compression if applicable.

d) ~~d)~~ Add these protected resources to the container, replacing unprotected versions.

e) ~~e)~~ Create a META-INF/encryption.xml document (as described in 9.3~~9.3)~~) which includes an EncryptedData element for each protected resource, that contains:

1) ~~1)~~ an EncryptionMethod element that lists the algorithm used;

2) ~~2)~~ a KeyInfo element with a RetrievalMethod child that points to the content key in the license document;

3) ~~3)~~ a CipherData element that identifies the protected resource.

f) ~~f)~~ Add META-INF/encryption.xml to the container.

The publication is now protected (i.e. has become a protected publication) and is ready for licensing to one or more users.

5.3 Licensing the publication

After a user requests a protected publication, the following steps are followed by the content provider to license the protected publication.

a) ~~a)~~ Generate the user key by hashing the user passphrase (as described in 6.4.2~~6.4.2).~~). It is assumed that the user and associated user passphrase are already known to the provider.

b) ~~b)~~ Encrypt the content key for the protected publication using the user key.

c) ~~c)~~ Create a license document (META-INF/license.lcpl) with the following contents:

1) ~~1)~~ a unique ID for this license;

2) ~~2)~~ the date the license was issued;

3) ~~3)~~ the URI that identifies the content provider;

4) ~~4)~~ the encrypted content key;

5) ~~5)~~ information relative to the user passphrase and user key;

6) ~~6)~~ links to additional information stored outside of the protected publication and license document (optional);

7) ~~7)~~ information on specific rights being granted to the user (optional);

8) ~~8)~~ information identifying the user (optional); some of the fields may be encrypted using the user key.

d) ~~d)~~ Generate a digital signature for the license document data and add it to the license document.

There are then two different methods to deliver the license document and protected publication to the user.

— License document included inside protected publication: The content provider adds the license document to the protected publication's container and delivers this to the user.

— License document delivered separately: The content provider includes a link from the license document to the protected publication, and then delivers just the license document to the user. The reading system processing the license document retrieves the protected publication and add the license document to the container of this protected publication.

Whichever method is used, the reading system is presented with an EPUB container that includes the protected publication and the license document.

5.4 Reading the publication

In order to decrypt and render a protected publication, the user's reading system follows these steps.

a) a) Verify the signature for the license document.

b) b) Get the user key (if already stored) or generate it by hashing the user passphrase.

c) c) Decrypt the content key using the user key.

d) d) Decrypt the protected resources using the content key.

6 License document

6.1 General

This clause defines the license document's syntax, its location in the container, its media type, file extension and processing model.

While META-INF/encryption.xml describes how the resources are encrypted and where the encrypted content key is located, every other relevant information for LCP is stored in the license document.

Annex A Annex A shows an example of a license document.

6.2 Content conformance

A license document shall meet all of the following criteria:

Document properties:

— It shall meet the conformance constraints for JSON documents as defined in RFC 4627.

— It shall be encoded using UTF-8.

File properties:

— Its filename shall use the file extension .lcpl.

— Its MIME media type shall be application/vnd.readium.lcp.license.v1.0+json.

— Its location in the container shall be META-INF/license.lcpl.

6.3 License information

6.3.1 General

The license document shall contain id, issued, provider, encryption, links and signature objects and may contain updated, rights and user objects as defined in Table 1~~Table 1~~.

Table 1 — Objects list of license document

Name	Value/Object	Format/data type	Required?
id	Unique identifier for the license	String	Yes
issued	Date and time of first issue of the license	ISO 8601-1 date and time	Yes
updated	Date and time of last update of the license	ISO 8601-1 date and time	No
provider	Identifier for the content provider	URI	Yes
encryption	encryption object	Object as defined in 6.3.2~~6.3.2~~	Yes
links	links object	Object as defined in 6.3.3~~6.3.3~~	Yes
rights	rights object	Object as defined in 6.3.4~~6.3.4~~	No
user	user object	Object as defined in 6.3.5~~6.3.5~~	No
signature	signature object	Object as defined in 6.3.6~~6.3.6~~	Yes

The date and time format shall follow the rules defined in ISO 8601-1.

6.3.2 Encryption (transmitting keys)

6.3.2.1 General

To transmit keys, the encryption object shall contain profile, content_key and user_key objects.

6.3.2.2 Profile

The encryption/profile object shall contain the value defined in Table 2~~Table 2~~.

Table 2 — Profile information in encryption

Name	Value	Format/data type
profile	Identifier for the encryption profile used by this LCP-protected publication	URI

6.3.2.3 Content key

The encryption/content_key object contains the content key (encrypted using the user key) used to encrypt the publication resources. It shall contain the name/value pairs described in Table 3~~Table 3~~.

Table 3 — Content key information in *encryption*

Name	Value	Format/data type
encrypted_value	Encrypted content key	Base 64 encoded octet sequence