ISO/IEC ~~DIS~~ PRF 23078-3~~: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 3: Device 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

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~~— No technical change.~~

— 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.

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]~~[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.~~

[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 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~~:—~~:—, *Information Technology — Specification of DRM technology for digital publications—* ~~*Part2*~~*Part 2*: *User key-based protection*

RFC 5280~~[2],~~[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~~(3.16)~~)

[SOURCE: ISO/IEC 23078-2:—, 3.2]

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

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

[SOURCE: ISO/IEC 23078-2:—, 3.4]

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

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

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

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

[SOURCE: ISO/IEC 23078-2:—, 3.3]

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

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

[SOURCE: ISO/IEC 23078-2:—, 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~~(3.9),~~), and *user* (3.19~~(3.19)~~) information

[SOURCE: ISO/IEC 23078-2:—, 3.6]

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

[SOURCE: ISO/IEC 23078-2:—, 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~~(3.9)~~) to *users* (3.19~~(3.19)~~)

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

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

[SOURCE: ISO/IEC 23078-2:—, 3.12]

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

[SOURCE: ISO/IEC 23078-2:—, 3.13]

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

[SOURCE: ISO/IEC 23078-2:—, 3.14]

3.14
reading system developer
developer
EPUB reading system developer
entity which signs the *device certificate* (3.4~~(3.4)~~) associated with a *reading system* (3.13~~(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~~(3.13)~~) in order to confirm that the *device certificate* (3.4~~(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~~(3.12)~~)

[SOURCE: ISO/IEC 23078-2:—, 3.15]

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

[SOURCE: ISO/IEC 23078-2:—, 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~~(3.8),~~), along with historical information

[SOURCE: ISO/IEC 23078-2:—, 3.17]

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

[SOURCE: ISO/IEC 23078-2:—, 3.18]

3.20
user key
hash value of the *user passphrase* (3.21~~(3.21),~~), used to authenticate a *reading system* (3.13~~(3.13)~~) to be able to access a *protected publication* (3.9~~(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 23078-2:—, 3.19, modified — The decryption role has been removed; the authentication role and Note 1 to entry have been added.]

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

[SOURCE: ISO/IEC 23078-2:—, 3.20]

4 Abbreviated terms

DRM	digital rights management
LCP	licensed content protection

5 Overview

5.1 General

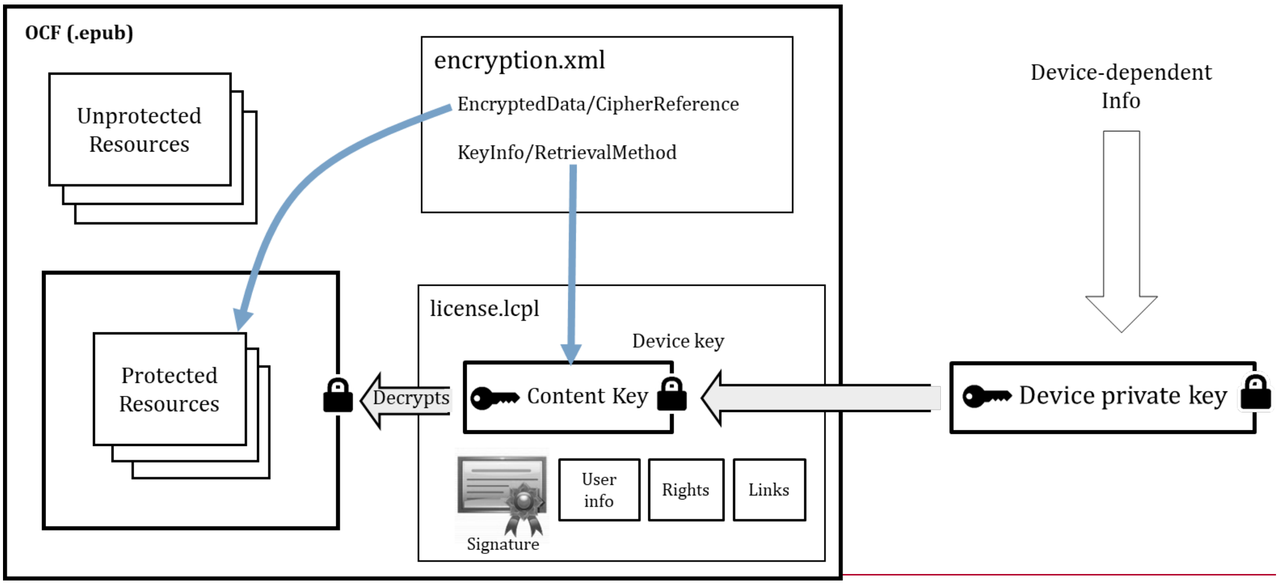
In order to deliver a publication to users without risk of indiscriminate redistribution, most publication resources are encrypted; and a license document is generated.

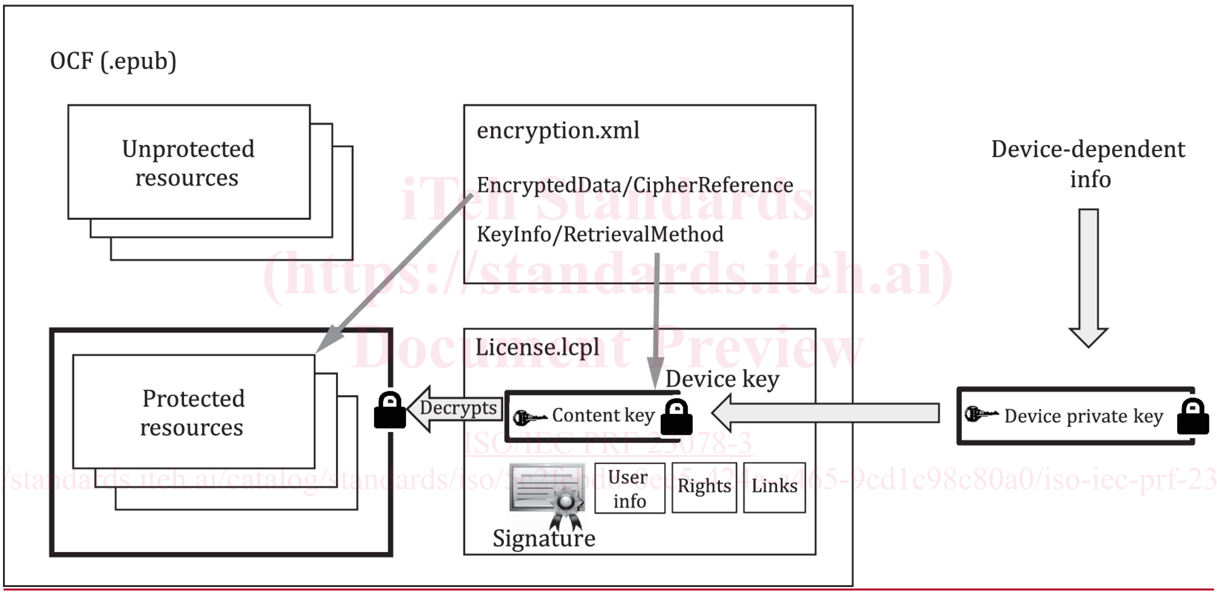
The license document can be transmitted outside an EPUB container or be embedded inside it. Following the EPUB 3.3 specification, META-INF/encryption.xml identifies all encrypted publication resources and points to the content key needed to decrypt them. This content key is located inside the license document and is itself encrypted using the 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 23078-2:—, 5.1. The role of user key has been removed and device key has been added.

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





NOTE 1 This figure has been modified from ISO/IEC 23078-2:—, Figure 1. The user key has been removed, and device key has been added.

NOTE 2 The content key is encrypted using the device key and decrypted using the device private key; the mechanism is different in ISO/IEC 23078-2, where the content key is encrypted and decrypted using the user key.

Figure 1 — Protected publication with a license document

5.2 Protecting the publication

ISO/IEC 23078-2:—, 5.2 shall apply.

5.3 Licensing the publication

After a user has requested 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)~~ Store this user key for future use.

c) ~~c)~~ Encrypt the content key associated with the protected publication using the device key found in the device certificate. The device certificate has been registered by the reading system in advance (as described in 7.4.4~~7.4.4).~~).

d) ~~d)~~ Create a device key-based 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)~~ information relative to the device key;

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

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

   9) ~~9)~~ information identifying the user (optional). Some of the fields in this section may be encrypted using the device key.

e) ~~e)~~ 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 the protected publication: The provider adds the license document to the protected publication's container and delivers this to the user.

— ~~—~~ License document delivered separately: The provider includes a link to the protected publication in the license document, and then delivers just the license document to the user. The reading system processing the license document downloads the protected publication and adds the license document to the container of the protected publication.

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

NOTE This subclause has been modified from ISO/IEC 23078-2:—, 5.3. Step b) and step d) 6) have been added, and user key has been changed with device key in step d) 9).

5.4 Reading the publication

5.4.1 General

In order to decrypt and render a protected publication, the reading system follows the steps specified in 5.4.2~~5.4.2, 5.4.3~~, 5.4.3 and 5.4.4~~5.4.4.~~.

NOTE This subclause has been extended from ISO/IEC 23078-2:—, 5.4 into 5.4.1, 5.4.2, 5.4.3 and 5.4.4.

5.4.2 Registering a device

A device registration is mandatory before a device key-based license is obtained. The register link is obtained from a license status document; and this link is specific to the license to be acquired.

Any user who knows the passphrase of a publication can register the device to the provider, get the associated device key-based license document and open the publication, as long as the accumulated number of registrations does not exceed the limit defined by the provider.

5.4.3 Acquiring a device key-based license document

After having successfully registered the device, a reading system is able to acquire a device key-based license document.

5.4.4 Decrypting a resource

After having successfully acquired the device key-based license document, the reading system follows these steps, in a highly secured manner:

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

b) ~~b)~~ Get the device private key associated with the reading system.

c) ~~c)~~ Decrypt the content key using the device private key.

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

NOTE The acquiring process of the user key in the step b) in the ISO/IEC 23078-2:— has been changed to a process for getting the device private key; and the process using the user key in the step c) has been changed to one using the device private key.

5.5 Licensing workflows

5.5.1 General

Device registration is required by this document before a protected publication can be processed by a reading system, which is a difference compared to ISO/IEC 23078-2:—. Such registration is necessary when a reading system gets a protected publication as well as when a protected publication is transferred from a reading system to another one.

5.5.2 Getting a protected publication

The first time a license document is issued to a user, the provider cannot generate a user-specific device key-based license document because the device is not yet registered for this license and therefore the provider server doesn't know the device key yet.