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 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

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.

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.

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)

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]

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.]

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

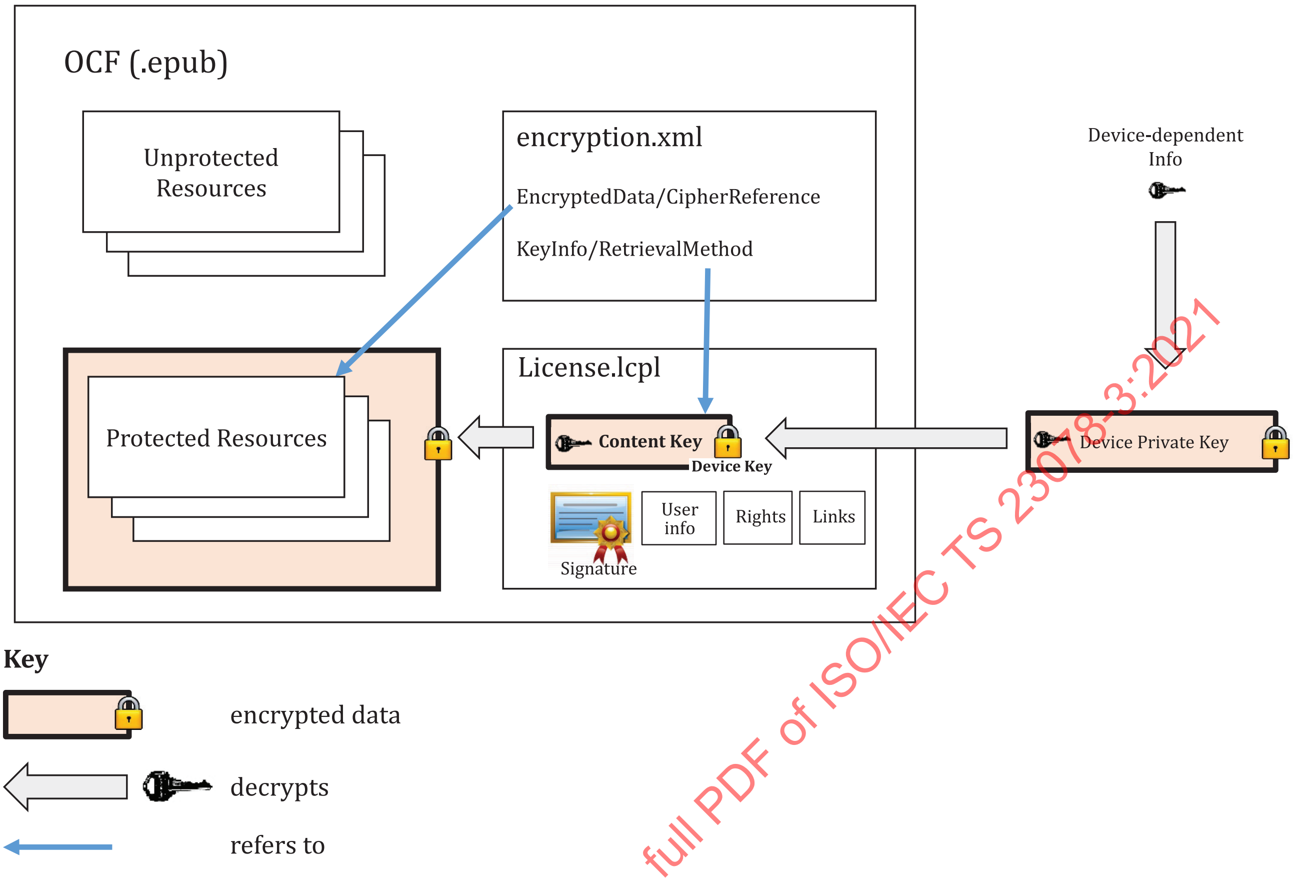
In order to deliver a publication to users without risk of indiscriminate redistribution, most publication resources are encrypted; and a license document is generated.

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.



NOTE 1 This figure has been modified from ISO/IEC TS 23078-2:2020, 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 TS 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 TS 23078-2:2020, 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) Generate the user key by hashing the user passphrase (as described in 6.4.2). It is assumed that the user and associated user passphrase are already known to the provider.

b) Store this user key for future use.

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).

d) Create a device key-based license document (META-INF/license.lcpl) with the following contents:

    1) a unique ID for this license;

2) the date the license was issued;

3) the URI that identifies the content provider;

4) the encrypted content key;

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

6) information relative to the device key;

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

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

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

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 TS 23078-2:2020, 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, 5.4.3 and 5.4.4.

NOTE This subclause has been extended from ISO/IEC TS 23078-2:2020, 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-base 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 with the provider, get the associated device-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) Verify the signature for the license document.

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

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

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 TS 23078-2:2020 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 TS 23078-2:2020. 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.

The provider therefore issues a license document whose content key is encrypted using a device key defined by the provider itself. The reading system does not possess the matching device private key and therefore cannot process this version of the license document. It can still retrieve the license status document, register the device, retrieve an updated license status document and then fetch the device key-based license document tied to the reading system.

The corresponding workflow is illustrated in Figure 2:

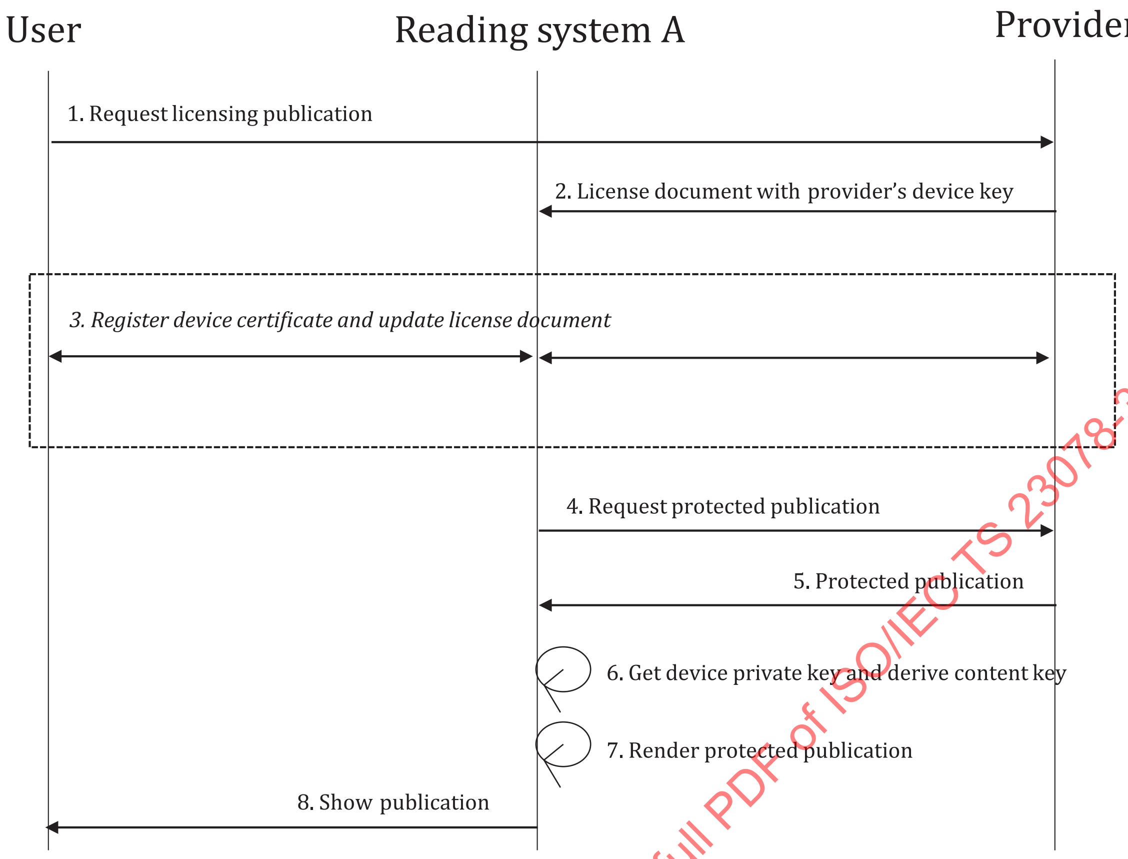

User
Reading system A
Provider
1. Request licensing publication
2. License document with provider's device key
3. Register device certificate and update license document
4. Request protected publication
5. Protected publication
6. Get device private key and derive content key
7. Render protected publication
8. Show publication

Figure 2 — Workflow of licensing for getting a protected publication

5.5.3 Transferring a protected publication

After successfully opening a protected publication on a device, a user may export this protected publication and try to open it on another device. In such a case the second reading system, even if compliant with this document, is not able to decrypt the content key because its device private key does not match the device key of the first device.

Such reading system therefore has to register the new device in order to get a new license document generated with the proper device key information.

The corresponding workflow is illustrated in Figure 3:

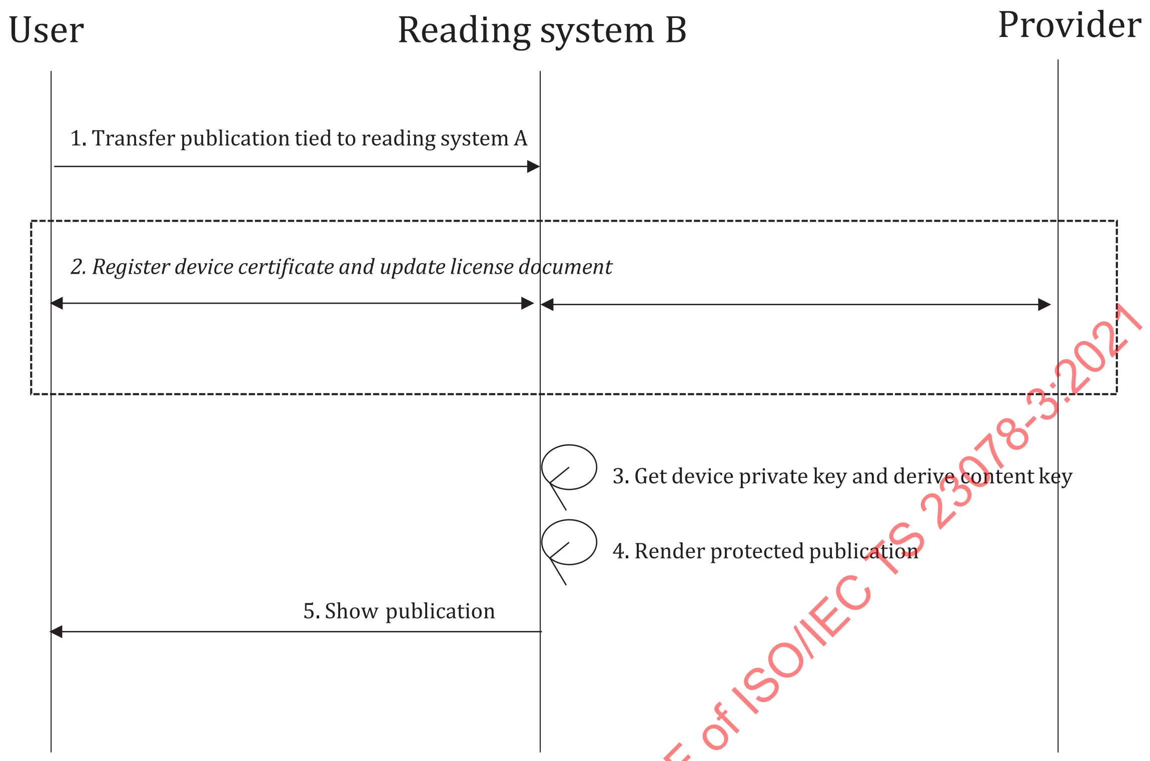

User
Reading system B
Provider
1. Transfer publication tied to reading system A
2. Register device certificate and update license document
3. Get device private key and derive content key
4. Render protected publication
5. Show publication

Figure 3 — Workflow of licensing for transferring a protected publication

5.5.4 Register device certificate and update license document

The two previous processes share the same registration and license acquisition process between the reading system and the provider:

a) The reading system gets a license status document.

b) The reading system gets the user key (if it has previously stored it) or generates it by hashing the user passphrase.

c) The reading system gets the developer certificate and device certificate (assuming that these have already been generated and installed during the installation of the reading system).

d) The reading system registers the device using the register link found in the license status document, with the user key, developer certificate and device certificate as parameters (see 7.4.4).

e) The provider server verifies that the user key matches the value associated with the owner of the license. An error is returned if it is not the case.

f) The provider validates the device registration, as long as the user key is correct and the limit on the number of allowed registrations has not been reached for the current license. An error is returned if it is not the case.

g) The provider returns an updated license status document.

h) The reading system requests an updated license document (see 7.3.4.3 and 7.4.3).

i) The provider server issues a device key-based license document.

The corresponding workflow is illustrated in Figure 4:

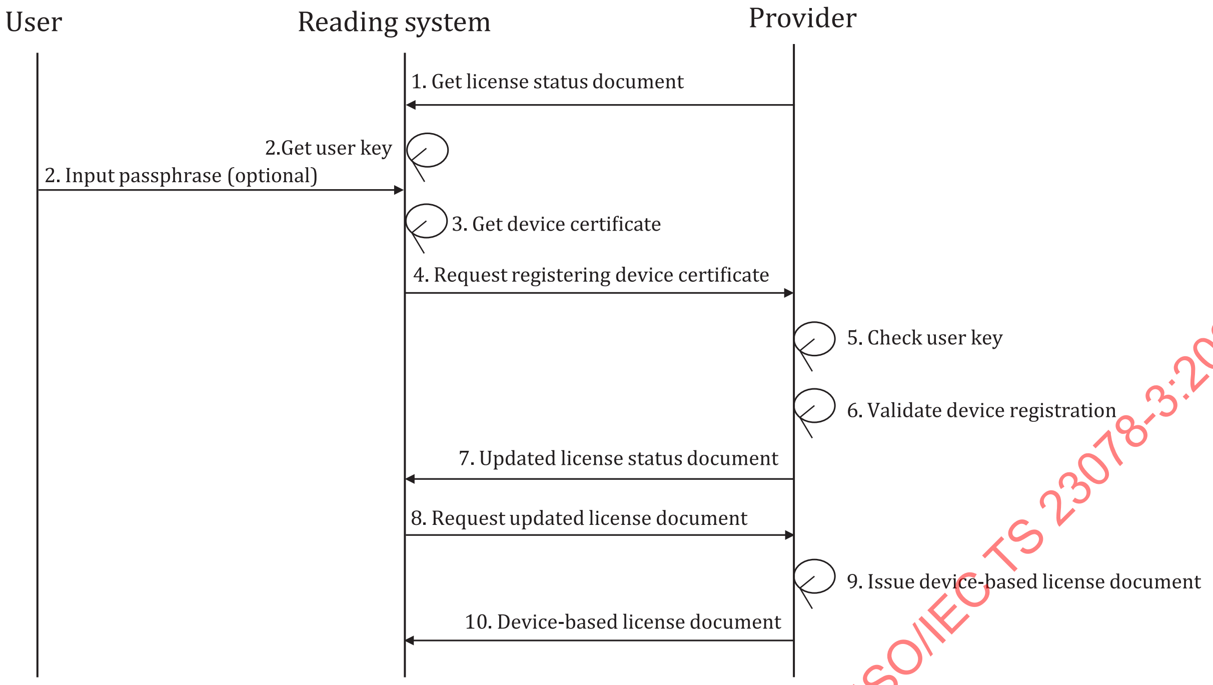

User
Reading system
Provider
1. Get license status document
2.Get user key
2. Input passphrase (optional)
3. Get device certificate
4. Request registering device certificate
5. Check user key
6. Validate device registration
7. Updated license status document
8. Request updated license document
9. Issue device-based license document
10. Device-based license document

Figure 4 — Workflow of registering device certificate and updating license document

6 License document

6.1 General

ISO/IEC TS 23078-2:2020, 6.1 shall apply.

6.2 Content conformance

ISO/IEC TS 23078-2:2020, 6.2 shall apply.

6.3 License information

6.3.1 General

ISO/IEC TS 23078-2:2020, 6.3.1 shall apply.

6.3.2 Encryption (transmitting keys)

6.3.2.1 General

To transmit keys, the encryption object shall contain the profile, content_key, user_key objects and device_key objects in accordance with 6.3.2.5.

NOTE This subclause has been modified from ISO/IEC TS 23078-2:2020, 6.3.2.1. The device key has been added.

6.3.2.2 Profile

The encryption/profile object shall contain the value defined in Table 1.

Table 1 — Profile information in encryption

Name	Value	Format/data type
profile	Identifier for the encryption profile used by this ISO/IEC TS 23078-3 compliant publication.	URI

NOTE Table 1 has been modified from ISO/IEC TS 23078-2:2020, Table 2. The value of profile has been changed.

6.3.2.3 Content key

The encryption/content_key object contains the content key (encrypted using the device key) used to encrypt the publication resources. It shall contain the name/value pairs described in Table 2.

Table 2 — Content key information in encryption

Name	Value	Format/data type
encrypted_value	Encrypted content key.	Base 64 encoded octet sequence
algorithm	Algorithm used to encrypt the content key, identified using the URIs defined in W3C XML Encryption. This shall match the content key encryption algorithm named in the encryption Profile identified in encryption/profile.	URI

NOTE This subclause has been modified from ISO/IEC TS 23078-2:2020, 6.3.2.3. The content key is encrypted using the device key.

6.3.2.4 User key

The encryption/user_key object contains information regarding the user key used to authenticate the user. It shall contain the name/value pairs defined in Table 3.

Table 3 — User key information in encryption

Name	Value	Format/data type
text_hint	Hint to be displayed to the user in order to help him remember the user passphrase.	String
algorithm	Algorithm used to generate the user key from the user passphrase. This URI shall match the user passphrase hash algorithm specified in the encryption profile identified in encryption/profile.	URI

NOTE Table 3 has been modified from ISO/IEC TS 23078-2:2020, Table 4. The key_check property has been removed.

6.3.2.5 Device key

The encryption/device_key object contains information associated with the device key that is used to encrypt the content key. It shall contain the name/value pairs defined in Table 4.

Table 4 — Device key information in encryption

Name	Value	Format/data type
key_name	DN (Distinguished Name in X.509 as defined in RFC 5280) described in the device certificate, which is used for identifying the paired device private key.	String

Table 4 *(continued)*

Name	Value	Format/data type
key_check	Value of the license document's id field, encrypted using the device key and the same algorithm identified for content key encryption in encryption/content_key/algorithm. This is used to verify that the reading system has the correct device private key.	Base 64 encoded octet sequence

EXAMPLE Encryption information for a license document with content key, user key and device key for this document.

```
{
  "id": "ef15e740-697f-11e3-949a-0800200c9a66",
  "issued": "2013-11-04T01:08:15+01:00",
  "updated": "2014-02-21T09:44:17+01:00",
  "provider": "https://www.imaginarybookretailer.com",
  "encryption": {
       "profile": "http://iso.org/ISO-TS-23078-3/basic-profile",
       "content_key": {
          "encrypted_value": "/k8RpXqf4E2WEunCp76E8PjhS051NXwAXeTD1ioazYxCRGvHLAck/KQ3cCh5
JxDmCK0nRLyAxs1X0aA3z55boQ==",
          "algorithm": "http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"
        },
       "user_key": {
           "text_hint": "Enter your email address",
           "algorithm": "http://www.w3.org/2001/04/xmlenc#sha256"
        },
       "device_key": {
          "key_name": "CN=$DEVICE_ID, O=EDRLab",
          "key_check": "ljJEjUDipHK3OjGt6kFq7dcOLZuicQFUYwQ+TYkAIWKm6Xv6kpHFhF7LOkUK/Owww"
       }
  },
  "links": "...",
  "rights": "...",
  "signature": "..."
}
```

6.3.3 Links (pointing to external resources)

6.3.3.1 General

ISO/IEC TS 23078-2:2020, 6.3.3.1 shall apply.

6.3.3.2 Link object

ISO/IEC TS 23078-2:2020, 6.3.3.2 shall apply.

6.3.3.3 Link relationships

Link relationships defined in ISO/IEC TS 23078-2:2020, 6.3.3.3 are valid in this document. The specificity of this document is that a license document shall have a status link. Table 5 introduces link relationships for each link object which is used for value of rel.

Table 5 — Link relationships of link

Relation	Semantics	Required?
hint	Location where a reading system can redirect a user looking for additional information about the User Passphrase	Yes
publication	Location where the publication associated with the license document can be downloaded	Yes
self	As defined in the IANA registry of link relations: "Conveys an identifier for the link's context"	No
support	Support resources for the user (either a website, an email or a telephone number)	No

Table 5 *(continued)*

Relation	Semantics	Required?
status	Location of the license status document associated with the license document	Yes

NOTE Table 5 has been modified from ISO/IEC TS 23078-2:2020, Table 6. The 'Required?' field has been changed.

EXAMPLE A license document points to a publication, contains the location of the status document and the location of a hint about the user passphrase.

```
{
  "id": "ef15e740-697f-11e3-949a-0800200c9a66",
  "issued": "2013-11-04T01:08:15+01:00",
  "updated": "2014-02-21T09:44:17+01:00",
  "provider": "https://www.imaginaryebookretailer.com",
  "encryption": "...",
  "links": [
    { "rel": "publication",
      "href": "https://www.example.com/file.epub",
      "type": "application/epub+zip",
      "length": "264929",
      "hash": "8b752f93e5e73a3efff1c706c1c2e267dffc6ec01c382cbe2a6ca9bd57cc8378"
    },
    { "rel": "hint",
      "href": "https://www.example.com/passphraseHint?user_id=1234",
      "type": "text/html"
    },
    { "rel": "status",
      "href": "https://www.example.com/lsd/4d8f5e99-7f18-7ab8/status",
      "type":"application/vnd.readium.license.status.v1.0+json"
    }
  ],
  "rights": "...",
  "signature": "..."
}
```

6.3.4 Rights (identifying rights and restrictions)

ISO/IEC TS 23078-2:2020, 6.3.4 shall apply.

6.3.5 User (identifying the user)

ISO/IEC TS 23078-2:2020, 6.3.5 shall apply.

6.3.6 Signature (signing the license)

ISO/IEC TS 23078-2:2020, 6.3.6 shall apply.

6.4 User key

6.4.1 General

This document uses a passphrase model for authenticating a user. The user passphrase can be anything at all: a user-defined password, a content provider-defined password, an e-mail address, a library card number, etc. The user key is defined as a hash of the user passphrase. A user key is sent to the provider server at the time of registration of a device. The content provider verifies the user key using its own copy of the user passphrase information, stored in the provider server.

When the reading system opens a protected publication for the first time, it prompts the user for a passphrase, generates the corresponding user key and stores this information securely for future use.

6.4.2 Calculating the user key

ISO/IEC TS 23078-2:2020, 6.4.2 shall apply.

6.4.3 Hints

ISO/IEC TS 23078-2:2020, 6.4.3 shall apply.

6.4.4 Requirements for the user key and user passphrase

ISO/IEC TS 23078-2:2020, 6.4.4 shall apply.

6.5 Signature and public key infrastructure

6.5.1 General

6.5.1.1 Validity of license document

ISO/IEC TS 23078-2:2020, 6.5.1 shall apply.

6.5.1.2 Validity of a device certificate

Since this document allows any reading system with a valid device certificate to register the device and get a device key-based license document as long as the user knows the passphrase associated with the license document, it is critical that the provider can verify that the device certificate is authentic and has not been altered.

When requested to register a device, the content provider first validates the developer certificate as well as the device certificate which are sent from the reading system. The validation process is also executed for checking the validity of the certificate chain among the root certificate, developer certificate and device certificate.

To make sure that the developer certificate and the device certificate have not been revoked, the provider also checks a certificate revocation list maintained by the license authority.

NOTE This subclause has been extended from ISO/IEC TS 23078-2:2020, 6.5.1 into 6.5.1.1 and 6.5.1.2. The general explanation on the validation process of device certificate has been added.

6.5.2 Certificates

6.5.2.1 Provider certificates

ISO/IEC TS 23078-2:2020, 6.5.2.1 shall apply.

6.5.2.2 Root certificate

ISO/IEC TS 23078-2:2020, 6.5.2.2 shall apply.

6.5.2.3 Developer certificates

The developer of a reading system shall have a certificate in the [X.509] v3 format, issued and signed by the license authority using the private key paired with the root certificate: this is referred to here as the developer certificate. The subject of the developer certificate should represent the reading system developer.

Reading system developers shall distribute their developer certificates when the reading system is installed.

6.5.2.4 Device certificates

A reading system shall have a certificate in the [X.509] v3 format, issued and signed by the developer of the reading system using the private key paired with its developer certificate: this is referred to here as the device certificate. The subject of the device certificate should represent a reading system; it should not include any user's personal information.

The reading system should obtain a signed device certificate from the reading system developer via a proprietary and secure channel at the time the reading system is installed.

For a device certificate to be considered valid, the developer certificate shall have been valid at the time the device certificate was signed (as indicated by the issued field); and the developer certificate shall not have been revoked.

6.5.3 Canonical form of the license document

ISO/IEC TS 23078-2:2020, 6.5.3 shall apply.

6.5.4 Generating the signature

ISO/IEC TS 23078-2:2020, 6.5.4 shall apply.

6.5.5 Validating the certificate and signature

6.5.5.1 Validating the certificate

a) The reading system shall check the signature of the provider certificate and developer certificate using the root certificate it embeds.

b) The reading system shall check the signature of the device certificate using the developer certificate.

c) If a network connection is available, the reading system shall periodically update its certificate revocation list, as defined in RFC 5280.

d) The reading system shall check that the device certificate, provider certificate, and developer certificate are not revoked, as defined in RFC 5280.

e) The reading system shall check that the provider certificate has not expired when the license document was last updated.

f) The reading system shall check that the developer certificate has not expired when the reading system gets the device certificate.

6.5.5.2 Validating the signature

ISO/IEC TS 23078-2:2020, 6.5.5.2 shall apply.

6.6 Device key

6.6.1 General

To transfer a content key securely from the provider to a reading system using an asymmetric cryptographic key, the provider uses the reading system's public key called the device key, while the reading system uses for decryption the associated private key called as device private key. The key pair is stored in the reading system; and the device certificate, which includes the device key, is sent to the provider before a device key-based license document is acquired.

6.6.2 Generating the device key

A key pair (private and public keys defined in RFC 5280) for a reading system should be generated when the reading system is installed, where the public key is used as device key and the private key is used as device private key. Then the reading system developer shall sign the device key to make a device certificate. No human intervention for authentication between the reading system and reading system developer should be involved for key pair generation and signing.

Here is a possible scenario for key pair generation:

a) The reading system generates a X.509 key pair during installation.

b) The reading system sends the public key to the developer and requests signing via a secure channel.

c) The developer signs the public key with the developer private key.

d) The developer returns the signed device certificate to the reading system.

6.6.3 Recommendations for the device private key protection

Although it is not an interoperability issue, protection measures applicable to the handling of the device private key and the signing process of the device key are very important in this document. It is recommended to follow the security guidelines outlined below:

- The device private key should be stored in an encrypted form in the reading system.
- The cryptographic algorithm used to protect the device private key should be at least as secure as AES-256, defined in FIPS 197.
- The key used for the encryption of the device private key should be unique for every reading system.
- The key used for the encryption of the device private key should be related to the device H/W information of the reading system, so that a copy of the encrypted device private key cannot work on another device.
- A communication protocol used between the reading system and the reading system developer for certificate signing should be at least as secure as SSL, defined in RFC 6101.
- The encryption algorithm used to protect the device private key and the communication protocol used to retrieve the device certificate should not be open to the public.

7 License status document

7.1 General

This clause defines the status of a DRM license along with the interactions that can affect its status. It also contains a history of the events associated with the license.

The interactions defined in this document aim at supporting lending in public libraries, where a user may have the ability to renew a time-limited loan or return one before it expires. And the register interaction is necessarily used for registering the device certificate of the reading system.

A.2 shows an example of a license status document.

7.2 Content conformance

ISO/IEC TS 23078-2:2020, 7.2 shall apply.

7.3 License status information

7.3.1 General

ISO/IEC TS 23078-2:2020, 7.3.1 shall apply.

7.3.2 Status

ISO/IEC TS 23078-2:2020, 7.3.2 shall apply.

7.3.3 Updated

ISO/IEC TS 23078-2:2020, 7.3.3 shall apply.

7.3.4 Links

7.3.4.1 General

ISO/IEC TS 23078-2:2020, 7.3.4.1 shall apply.

7.3.4.2 Link object

Each link object contained in links supports the keys defined in Table 6.

Table 6 — Object list in link

Name	Value	Format/data type	Required?
href	Link location.	URI or URI template	Yes
rel	Link relationship to the document.	List of well-known relation values, URIs for extensions as defined in 7.3.4.3	Yes
title	Title of the link.	String	No
type	Expected MIME media type value for the external resources.	MIME media type	No, but highly recommended
templated	Indicates that the href is a URI template.	Boolean	No, default value is "false"
profile	Expected profile used to identify the external resource.	URI	No, default value is "http://iso.org/ISO-TS-23078-3/basic-profile"

NOTE Table 6 has been modified from ISO/IEC TS 23078-2:2020, Table 13. The 'Required?' field of the profile relation has been changed.

7.3.4.3 Link relationships

This document introduces the link relationships defined in Table 7 for each link object which is used for value of rel.

Table 7 — Allowed value list in rel

Relation	Semantics	Templated?	Required?	HTTP verb
license	Location of the license document associated to the status document.	No	Yes	GET
register	Action to register a device.	Yes	Yes	POST
return	Action to return a license.	Yes	No	PUT

Table 7 *(continued)*

Relation	Semantics	Templated?	Required?	HTTP verb
renew	Action to renew a license.	Yes	No	PUT

NOTE Table 7 has been modified from ISO/IEC TS 23078-2:2020, Table 14. The 'Required?' field of the register relation has been changed.

7.3.5 Potential rights

ISO/IEC TS 23078-2:2020, 7.3.5 shall apply.

7.3.6 Events

ISO/IEC TS 23078-2:2020, 7.3.6 shall apply.

7.4 Interactions

7.4.1 General

ISO/IEC TS 23078-2:2020, 7.4.1 shall apply.

7.4.2 Handling errors

ISO/IEC TS 23078-2:2020, 7.4.2 shall apply.

7.4.3 Checking the status of a license

ISO/IEC TS 23078-2:2020, 7.4.3 shall apply.

7.4.4 Registering a device

Registration of the device is mandatory for every publication before a device key-based license document can be acquired.

When a reading system opens a license document for the first time and gets access to its associated status document:

— it shall attempt to register the device to the provider using the link exposed in the status document;

— it shall block the user from accessing the publication associated with the license document if the registration fails (the reading system cannot decrypt the protected resource if the registration process is not successful);

— it shall attempt to register itself again if it couldn't do so the first time the license document was opened.

NOTE 1 The requirements for a reading system on registering a device have been modified from ISO/IEC TS 23078-2:2020, 7.4.4.

During the registration, a reading system shall always send the same unique identifier for a specific device, no matter which status document it interacts with. Any further interaction with a provider should use the same identifier/name. To consider user privacy and assure the unicity of device ids, the client should generate device unique ids using a hash value of the device key. Table 8 defines a HTTP protocol for the register interaction.

Table 8 — HTTP protocol for register interaction

Relation	Semantics	Templated?	Required?	HTTP verb
register	Associate a new device with the license	Yes	Yes	POST

Parameter*	Format	Semantics	Required?
id	Octet sequence	A unique identifier for the device.	Yes
name	String	A human readable name for the device.	Yes
user_key	Base 64 encoded octet sequence	The user key of the publication, derived from the user passphrase. The algorithm for deriving the user key from the user passphrase is specified in the encryption profile identified in encryption/profile in the license document.	Yes
device_certificate	Base 64 encoded DER certificate	The device certificate: an X.509 certificate containing the device key	No (Yes, if the first time)
developer_certificate	Base 64 encoded DER certificate	The reading system developer certificate: an X.509 certificate used for signing the device certificate	No (Yes, if the first time)

NOTE 2 Table 8 has been extended from ISO/IEC TS 23078-2:2020, Table 18. The user_key, device_certificate and developer_certificate parameters have been added.

All parameters in Table 8 shall be URL encoded.

Table 9 defines the expected behaviour of the server and client on the register interaction.

Table 9 — Expected behaviour of register interaction

Server side behaviour	HTTP status code	Client side behaviour
The server registers the device identified by 'id' if user_key matches the license owner. It then returns an updated status document. The server shall update the timestamp of the status document contained in the status key of the updated object. If the status was previously set to 'ready', it shall be updated by the server to 'active' instead. The server may also add a new event in the events object of the status document.	200	Once the certificate is registered properly, the client may not attempt to register the device again for this license.

NOTE 3 Table 9 has been modified from ISO/IEC TS 23078-2:2020, Table 19.

Table 10 defines expected failures of server response on the register interaction.

Table 10 — Expected failures of register interaction

Type	HTTP Status Code	Title
http://readium.org/license-status-document/error/registration	400	Your device could not be registered properly.
http://readium.org/license-status-document/error/registration/authentication	403	The user key is incorrect.
http://readium.org/license-status-document/error/registration/limit	403	The number of registrations exceeds the limit.
http://readium.org/license-status-document/error/registration/not-acceptable	406	The request does not include a device_certificate or developer_certificate, or there was no registered device certificate associated with the device id in the server.

Table 10 *(continued)*

Type	HTTP Status Code	Title
http://readium.org/license-status-document/error/server	5xx	An unexpected error has occurred.

NOTE 4 Table 10 has been extended from ISO/IEC TS 23078-2:2020, Table 20. Two error types equivalent to HTTP status 403 and 406 are added.

Example 1 A simple license with a registration link.

```
{
  "links": [
     {
       "rel": "register",
         "href": "https://example.org/license/aaa-bbbb-ccc/register{?id,name,user_
key,device_certificate,developer_certificate}",
         "type": "application/vnd.readium.license.status.v1.0+json",
         "templated": true
    }
  ]
}
```

Example 2 A sample for a HTTP request body, in which a device registers the device key.

```
POST /license/aaa-bbbb-ccc/register HTTPS/1.1
Host: example.org

id=B9DA0A331B6A1F1CBE797FB37138586EBB42539C1DCA4FBFD2DD0E68FF59FCC7
&name=eBook%20App%20(Android)
&user_key=qwYXxfNDVt3z0OZyvO10mzL37wLYi986zOR7mU5ZGj4%3D
&device_certificate=MIIESTCCAzGgAwIBAgIDANkyMA0GCSqGSIb3DQEBCwUAMHUxGTAXBgNVBAoTEGNvcHlyaW
dodHMub3Iua3IxGTAXBgNVBAsTEGNvcHlyaWdodHMub3Iua3IxFjAUBgNVBAMTDURSTSBpbnNpZGUgQ0ExJTAjBgNV
BC4THFEyQktabXdpVUZvRXdrUEx3WnpwdjdJTmNzVT0wHhcNMTUwNjA4MDUyMDE1WhcNMjQwODA5MDUyMDE1WjB1MR
kwFwYDVQQKExBjb3B5cmlnaHRzLm9yLmtyMRkwFwYDVQQLExBjb3B5cmlnaHRzLm9yLmtyMRYwFAYDVQQDEw1Cb29r
aW5nU2VydmVyMSUwIwYDVQQuExw0L2FQNEpiUS9mMDdzTk5ueFdqT1BoMkkxWEk9MIIBIjANBgkqhkiG9w0BAQEFAA
OCAQ8AMIIBCgKCAQEAul5CkVsQDxxqTkDc4sClfeI2esChMv0bPjj9pWln3VoBqA6BzEDNYcpnF9Ic5ZdOcBW0egSA
iHb2EcDnzT94FH7SryC97iA%2F9TqRs2pdHQacL9fCOjCrIsmwZ2RmGevft0oLMlKNhePS1E8nvnt852lDpJWDIGV9
rDIVCWXzy6PcylkZYOyXXYJxDa886Vgjpeeg9UKtWTO495aHJdDJ7Iaeokh4bb8CuEI2ro13HXcWiivTdjc7eNK2UF
hyIYecQOiJAV%2FGDjvbLlWnVBUauYqLRwBe3bSeKCDXUGnNWfFl4XKBQ7Oojc3ktaDHbdKmz2XsP1pi16ZZVE7F4B
gUJwIDAQABo4HhMIHeMAsGA1UdDwQEAwIEsDAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTj9o%2FgltD9%2FTuw02f
FaM4%2BHYjVcjCBoQYDVR0jBIGZMIGWgBRDYEpmbCJQWgTCQ8vBnOm%2Fsg1yxaF5pHcwdTEZMBcGA1UEChMQY29we
XJpZ2h0cy5vci5rcjEZMBcGA1UECxMQY29weXJpZ2h0cy5vci5rcjEWMBQGA1UEAxMNRFJNIGluc2lkZSBDQTElMCM
GA1UELhMcUTJCS1ptd2lVRm9Fd2tQTHdaenB2N0lOY3NVPYIDANhpMA0GCSqGSIb3DQEBCwUAA4IBAQCjVTU2JPcY7
lO41h6KcM2%2BLKJE9252%2BfPYk7YzLcxCT3ZZkt44bairKqqHuyNBzCjPLWrHNYaBz%2F5BX1qxyKm6QgFpUDpVB
T2tIDl97%2FmGMiBfCvTxCaRKAipSvzj%2Fif0tZd9n%2BPuBGPZnWibQsg2nH77LGRuGJHBG7O%2BLmpg%2BT2R2l
q2FBOodonMzzmxl6judWhOVzmc1bt7ZtdgHOhfaLwyu2yLrmmByStDlqI7ZBqDg%2BqFXKOOrWc%2F%2BbgESXZ1yi
RmCNGIazrHUcqHQFLaVGbzylI9Qmt5l7zIOuX0N2su1JGMwB7vg%2F9c7d1YP1i1TNvyMS43tnKmhc77BUcCR
&developer_certificate=MIIESTCCAzGgAwIBAgIDANkyMA0GCSqGSIb3DQEBCwUAMHUx
GTAXBgNVBAoTEGNvcHlyaWdodHMub3Iua3IxGTAXBgNVBAsTEGNvcHlyaWdodHMub3Iua3IxFjAUBgNVBAMTDURSTS
BpbnNpZGUgQ0ExJTAjBgNVBC4THFEyQktabXdpVUZvRXdrUEx3WnpwdjdJTmNzVT0wHhcNMTUwNjA4MDUyMDE1WhcN
MjQwODA5MDUyMDE1WjB1MRkwFwYDVQQKExBjb3B5cmlnaHRzLm9yLmtyMRkwFwYDVQQLExBjb3B5cmlnaHRzLm9yL
mtyMRYwFAYDVQQDEw1Cb29raW5nU2VydmVyMSUwIwYDVQQuExw0L2FQNEpiUS9mMDdzTk5ueFdqT1BoMkkxWEk9MI
IBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAul5CkVsQDxxqTkDc4sClfeI2esChMv0bPjj9pWln3VoBqA6
BzEDNYcpnF9Ic5ZdOcBW0egSAiHb2EcDnzT94FH7SryC97iA%2F9TqRs2pdHQacL9fCOjCrIsmwZ2RmGevft0oLMlK
NhePS1E8nvnt852lDpJWDIGV9rDIVCWXzy6PcylkZYOyXXYJxDa886Vgjpeeg9UKtWTO495aHJdDJ7Iaeokh4bb8Cu
EI2ro13HXcWiivTdjc7eNK2UFhyIYecQOiJAV%2FGDjvbLlWnVBUauYqLRwBe3bSeKCDXUGnNWfFl4XKBQ7Oojc3kt
aDHbdKmz2XsP1pi16ZZVE7F4BgUJwIDAQABo4HhMIHeMAsGA1UdDwQEAwIEsDAMBgNVHRMBAf8EAjAAMB0GA1UdDgQ
WBBTj9o%2FgltD9%2FTuw02fFaM4%2BHYjVcjCBoQYDVR0jBIGZMIGWgBRDYEpmbCJQWgTCQ8vBnOm%2Fsg1yxaF5p
HcwdTEZMBcGA1UEChMQY29weXJpZ2h0cy5vci5rcjEZMBcGA1UECxMQY29weXJpZ2h0cy5vci5rcjEWMBQGA1UEAxM
NRFJNIGluc2lkZSBDQTElMCMGA1UELhMcUTJCS1ptd2lVRm9Fd2tQTHdaenB2N0lOY3NVPYIDANhpMA0GCSqGSIb3D
QEBCwUAA4IBAQCjVTU2JPcY7lO41h6KcM2%2BLKJE9252%2BfPYk7YzLcxCT3ZZkt44bairKqqHuyNBzCjPLWrHNYa
Bz%2F5BX1qxyKm6QgFpUDpVBT2tIDl97%2FmGMiBfCvTxCaRKAipSvzj%2Fif0tZd9n%2BPuBGPZnWibQsg2nH77LG
RuGJHBG7O%2BLmpg%2BT2R2lq2FBOodonMzzmxl6judWhOVzmc1bt7ZtdgHOhfaLwyu2yLrmmByStDlqI7ZBqDg%2B
qFXKOOrWc%2F%2BbgESXZ1yiRmCNGIazrHUcqHQFLaVGbzylI9Qmt5l7zIOuX0N2su1JGMwB7vg%2F9c7d1YP1i1TN
vyMS43tnKmhc77BUcCR
```

7.4.5 Returning a publication

ISO/IEC TS 23078-2:2020, 7.4.5 shall apply.

7.4.6 Renewing a license

ISO/IEC TS 23078-2:2020, 7.4.6 shall apply.

8 Encryption profiles

8.1 General

In order to maintain maximum flexibility, no specific algorithms are mandated by this document. Instead, the design of both encryption.xml and the license document allow for the identification of encryption algorithms to be discovered by reading systems when presented with a protected publication.

In order to simplify the discovery process, this document defines the notion of encryption profile, which is the set of encryption algorithms used in a specific protected publication and associated license document. Reading systems that implement the algorithms identified in the encryption profile are able to decrypt protected publications encoded using such encryption profile. The identification of the encryption profile in the license document eases the discovery of these requirements by reading systems.

This document defines the basic encryption profile 1.0, composed from a set of associated algorithms extracted from W3C XML Encryption or W3C XML Signature.

Other encryption profiles are (or will be) defined for use in production; these profiles are referenced in the ISO-TS-23078-3 encryption profiles registry. Such profiles may use algorithms which are not directly extracted from W3C XML Encryption or W3C XML Signature.

NOTE This subclause has been modified from ISO/IEC TS 23078-2:2020, 8.1. Identifier of the specification has been changed as ISO-TS-23078-3.

8.2 Encryption profile requirements

ISO/IEC TS 23078-2:2020, 8.2 shall apply.

8.3 Basic encryption profile

The basic encryption profile 1.0 for this specification is officially identified by the URI http://iso.org/ISO-TS-23078-3/basic-profile.

The algorithms defined in Table 11 are associated to the basic encryption profile 1.0.

Table 11 — Algorithm list for the basic encryption profile 1.0

Encryption target	Algorithm (name)	Algorithm (URI)	Identified in
publication resources	AES 256 bits CBC	http://www.w3.org/2001/04/xmlenc#aes256-cbc	encryption.xml
Content key, user fields (if encrypted)	RSA-OAEP	http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p	License document
User Passphrase	SHA-256	http:// www.w3.org/2001/04/xmlenc#sha256	License document
Signature	ECDSA with SHA-256	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256	License document

NOTE Table 11 has been modified from ISO/IEC TS 23078-2:2020, Table 28. Encryption algorithms for content key and signature have been changed.

9 Integration in EPUB

ISO/IEC TS 23078-2:2020, Clause 9 shall apply.

10 Reading system behaviours

10.1 Detecting protected publications

ISO/IEC TS 23078-2:2020, 10.1 shall apply.

10.2 License document processing

ISO/IEC TS 23078-2:2020, 10.2 shall apply.

10.3 User key processing

ISO/IEC TS 23078-2:2020, 10.3 shall apply.

10.4 Signature processing

ISO/IEC TS 23078-2:2020, 10.4 shall apply.

10.5 Publication processing

ISO/IEC TS 23078-2:2020, 10.5 shall apply.

10.6 Device key processing

Reading systems shall:

- have a device certificate and a paired device private key;
- have a developer certificate used to verify the device certificate;
- register the device when opening a license document for the first time.

Reading systems should:

- store the device private key in a secure manner;
- get the device private key associated with the value of device_key/key_name property in the license document in a secure manner.

Reading systems shall not:

- transfer the device private key in any form outside of the reading system.

Annex A
(informative)

Examples

A.1 Example of a license document

In the following example, the license document contains the following information:

- Profile name: http://iso.org/ISO-TS-23078-3/basic-profile
- Rights: no print, allowing copy as much as 2048 words at once, with starting and expiration date
- URL of the publication: https://www.example.com/file.epub
- URL of the status document: https://example.org/license/status/aaa-bbbb-ccc

```
{
"id": "ef15e740-697f-11e3-949a-0800200c9a66",
  "issued": "2013-11-04T01:08:15+01:00",
  "encryption": {
    "content_key": {
      "algorithm": "http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p ",
      "encrypted_value": "/k8RpXqf4E2WEunCp76E8PjhS051NXwAXeTD1ioazYxCRGvHLAck/KQ3cCh5JxDm
CK0nRLyAxs1X0aA3z55boQ=="
    },
    "profile": "http://iso.org/ISO-TS-23078-3/basic-profile",
    "user_key": {
      "algorithm": "http://www.w3.org/2001/04/xmlenc#sha256",
      "text_hint": "Enter your email address"
    },
    "device_key": {
      "key_name": "CN=709e1380-3528-11e5-a2cb-0800200c9a66, O=DRMinside",
      "key_check": "ljJEjUDipHK3OjGt6kFq7dcOLZuicQFUYwQ+TYkAIWKm6Xv6kpHFhF7LOkUK/Owww"
    }
  },
"rights": {
       "print": 0,
       "copy": 2048,
       "start": "2020-01-01T00:00:00+01:00",
       "end": "2030-12-31T23:59:59+01:00",
       "https://www.imaginaryebookretailer.com/lcp/rights/tweet": true
  },
  "links": [
    { "rel": "hint",
      "href": "https://www.imaginaryebookretailer.com/lcp/hint",
      "type": "text/html"
    },
    { "rel": "status",
      "href": "https://example.org/license/status/aaa-bbbb-ccc",
      "type": "application/vnd.readium.license.status.v1.0+json"
    },
   { "rel": "publication",
      "href": "https://www.example.com/file.epub",
      "type": "application/epub+zip",
      "length": "264929",
      "hash": "8b752f93e5e73a3efff1c706c1c2e267dffc6ec01c382cbe2a6ca9bd57cc8378"
    }
  ],
  "user": {"id": "d9f298a7-7f34-49e7-8aae-4378ecb1d597"},
  "signature": {
    "algorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
    "certificate": "MIIDEjCCAfoCCQDwMOjkYYOjPjANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzETMB
EGA1UECBMKQ2FsaWZvcm5pYTETMBEGA1UEBxMKRXZlcnl3aGVyZTESMBAGA1UEAxMJbG9jYWxob3N0MB4XDTE0MDEw
MjIxMjYxNloXDTE1MDEwMjIxMjYxNlowSzELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExEzARBgNVBA
cTCkV2ZXJ5d2hlcmUxEjAQBgNVBAMTCWxvY2FsaG9zdDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOpC
RECG7icpf0H37kuAM7s42oqggBoikoTpo5yapy+s5eFSp8HSqwhIYgZ4SghNLkj3e652SALav7chyZ2vWvitZycY+a
q50n5UTTxDvdwsC5ZNeTycuzVWZALKGhV7VUPEhtWZNm0gruntronNa8l2WS0aF7P5SbhJ65SDQGprFFaYOSyN6550
P3kqaAO7tDddcA1cmuIIDRf8tOIIeMkBFk1Qf+lh+3uRP2wztOTECSMRxX/hIkCe5DRFDK2MuDUyc/iY8IbY0hMFFG
w5J7MWOwZLBOaZHX+Lf5lOYByPbMH78O0dda6T+tLYAVzsmJdHJFtaRguCaJVtSXKQUAMCAwEAATANBgkqhkiG9w0B
AQUFAAOCAQEAi9HIM+FMfqXsRUY0rGxLlw403f3YtAG/ohzt5i8DKiKUG3YAnwRbL/VzXLZaHru7XBC40wmKefKqoA
0RHyNEddXgtY/aXzOlfTvp+xirop+D4DwJIbaj8/wHKWYGBucA/VgGY7JeSYYTUSuz2RoYtjPNRELIXN8A+D+nkJ3d
xdFQ6jFfVfahN3nCIgRqRIOt1KaNI39CShccCaWJ5DeSASLXLPcEjrTi/pyDzC4kLF0VjHYlKT7lq5RkMO6GeC+7YF
vJtAyssM2nqunA2lUgyQHb1q4Ih/dcYOACubtBwW0ITpHz8N7eO+r1dtH/BF4yxeWl6p5kGLvuPXNU21ThgA==",
    "value": "q/3IInic9c/EaJHyG1Kkqk5v1zlJNsiQBmxz4lykhyD3dA2jg2ZzrOenYU9GxP/xhe5H5Kt2WaJ/
hnt8+GWrEx1QOwnNEij5CmIpZ63yRNKnFS5rSRnDMYmQT/fkUYco7BUi7MPPU6OFf4+kaToNWl8m/ZlMxDcS3BZnVh
SEKzUNQn1f2y3sUcXjes7wHbImDc6dRthbL/E+assh5HEqakrDuA4lM8XNfukEYQJnivqhqMLOGM33RnS5nZKrPPK/
c2F/vGjJffSrlX3W3Jlds0/MZ6wtVeKIugR06c56V6+qKsnMLAQJaeOxxBXmbFdAEyplP9irn4D9tQZKqbbMIw=="
  }
}
```

A.2 Example of a license status document

In the following example, the status document indicates that the license has been registered for a single device and may be renewed or returned.

```
{
  "id": "234-5435-3453-345354",
  "status": "active",
  "message": "Your license is currently active and has been used on one device.",
  "updated": {
    "license": "2020-08-05T00:00:00Z",
    "status": "2020-08-08T00:00:00Z"
  },
  "links": [
    {
      "rel": "license",
      "href": "https://example.org/license/35d9b2d6",
      "type": "application/vnd.readium.lcp.license.v1.0+json",
      "profile": "http://iso.org/ISO-TS-23078-3/basic-profile"
    },
    {
      "rel": "register",
      "href": "https://example.org/license/35d9b2d6/register{?id,name,user_key,device_
certificate,developer_certificate}",
      "type": "application/vnd.readium.license.status.v1.0+json",
      "templated": true
    },
    {
      "rel": "return",
      "href": "https://example.org/license/35d9b2d6/return{?id,name}",
      "type": "application/vnd.readium.license.status.v1.0+json",
      "templated": true
    },
{
      "rel": "renew",
      "href": "https://example.org/license/35d9b2d6/renew{?end,id,name}",
      "type": "application/vnd.readium.license.status.v1.0+json",
      "templated": true
    }
  ],
  "potential_rights": {
    "end": "2020-09-13T00:00:00Z"
  },
  "events": [
    {
      "type": "register",
      "name": "eBook App (Android)",
      "timestamp": "2016-07-14T00:00:00Z",
      "id": "709e1380-3528-11e5-a2cb-0800200c9a66"
    }
  ]
}
```