# ISO/IEC 23078-2:2024-06 (E)

## Information technology - Specification of digital rights management (DRM) technology for digital publications - Part 2: User key-based protection

## Contents

Page


**Foreword** ..... **v**

**Introduction** ..... **vi**

**1 Scope** ..... **1**

**2 Normative references** ..... **1**

**3 Terms and definitions** ..... **2**

**4 Abbreviated terms** ..... **3**

**5 Overview** ..... **4**
5.1 General ..... 4
5.2 Protecting the publication ..... 4
5.3 Licensing the publication ..... 5
5.4 Reading the publication ..... 5

**6 License document** ..... **6**
6.1 General ..... 6
6.2 Content conformance ..... 6
6.3 License information ..... 6
6.3.1 General ..... 6
6.3.2 Encryption (transmitting keys) ..... 7
6.3.3 Links (pointing to external resources) ..... 8
6.3.4 Rights (identifying rights and restrictions) ..... 9
6.3.5 User (identifying the user) ..... 10
6.3.6 Signature (signing the license) ..... 11
6.4 User key ..... 12
6.4.1 General ..... 12
6.4.2 Calculating the user key ..... 12
6.4.3 Hints ..... 12
6.4.4 Requirements for the user key and user passphrase ..... 13
6.5 Signature and public key infrastructure ..... 13
6.5.1 General ..... 13
6.5.2 Certificates ..... 13
6.5.3 Canonical form of the license document ..... 14
6.5.4 Generating the signature ..... 15
6.5.5 Validating the certificate and signature ..... 17

**7 License status document** ..... **17**
7.1 General ..... 17
7.2 Content conformance ..... 17
7.3 License status information ..... 18
7.3.1 General ..... 18
7.3.2 Status ..... 18
7.3.3 Updated (timestamps) ..... 18
7.3.4 Links ..... 19
7.3.5 Potential rights ..... 19
7.3.6 Events ..... 20
7.4 Interactions ..... 20
7.4.1 General ..... 20
7.4.2 Handling errors ..... 20
7.4.3 Checking the status of a license ..... 20

7.4.4 Registering a device ..... 21
7.4.5 Returning a publication ..... 22
7.4.6 Renewing a license ..... 23

**8 Encryption profile ..... 24**
8.1 General ..... 24
8.2 Encryption profile requirements ..... 25
8.3 Basic encryption profile 1.0 ..... 25

**9 Integration in EPUB ..... 25**
9.1 General ..... 25
9.2 Encrypted resources ..... 25
9.3 Using META-INF/encryption.xml for LCP ..... 26

**10 Reading system behaviour ..... 27**
10.1 Detecting LCP protected publication ..... 27
10.2 License document processing ..... 27
10.2.1 Overall ..... 27
10.2.2 Validating the license document ..... 27
10.2.3 Acquiring the publication ..... 27
10.2.4 License status processing ..... 28
10.3 User key processing ..... 28
10.4 Signature processing ..... 28
10.5 Publication processing ..... 29

**Annex A** (informative) **Examples ..... 30**

**Annex B** (informative) **Use case scenarios for library lending model ..... 33**

**Annex C** (informative) **An extension of the LCP specification for PDF ..... 36**

**Bibliography ..... 38**