ISO/IEC 23078-3:2024-06 (E)

Information technology - Specification of digital rights management (DRM) technology for digital publications - Part 3: Device key-based protection

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Abbreviated terms **4**

5 Overview **4**

5.1 General 4
5.2 Protecting the publication 5
5.3 Licensing the publication 5
5.4 Reading the publication 6
5.4.1 General 6
5.4.2 Registering a device 6
5.4.3 Acquiring a device key-based license document 6
5.4.4 Decrypting a resource 6
5.5 Licensing workflows 7
5.5.1 General 7
5.5.2 Getting a protected publication 7
5.5.3 Transferring a protected publication 7
5.5.4 Register device certificate and update license document 8

6 License document **9**

6.1 General 9
6.2 Content conformance 9
6.3 License information 9
6.3.1 General 9
6.3.2 Encryption (transmitting keys) 9
6.3.3 Links (pointing to external resources) 11
6.3.4 Rights (identifying rights and restrictions) 12
6.3.5 User (identifying the user) 12
6.3.6 Signature (signing the license) 12
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 12
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 14
6.5.5 Validating the certificate and signature 14
6.6 Device key 14
6.6.1 General 14
6.6.2 Generating the device key 14
6.6.3 Recommendations for the device private key protection 15

7 License status document **15**
7.1 General 15
7.2 Content conformance 15
7.3 License status information 15
7.3.1 General 15
7.3.2 Status 15
7.3.3 Updated 15
7.3.4 Links 15
7.3.5 Potential rights 16
7.3.6 Events 16
7.4 Interactions 16
7.4.1 General 16
7.4.2 Handling errors 17
7.4.3 Checking the status of a license 17
7.4.4 Registering a device 17
7.4.5 Returning a publication 19
7.4.6 Renewing a license 19

8 Encryption profiles **19**
8.1 General 19
8.2 Encryption profile requirements 19
8.3 Basic encryption profile 20

9 Integration in EPUB **20**

10 Reading system behaviours **20**
10.1 Detecting protected publications 20
10.2 License document processing 20
10.3 User key processing 20
10.4 Signature processing 20
10.5 Publication processing 20
10.6 Device key processing 20

Annex A (informative) **Examples** **22**

Annex B (informative) **Schema of license document** **24**

Annex C (informative) **An extension of the ISO/IEC 23078-3 specification for PDF** **29**

Bibliography **31**