# ISO/IEC TS 23078-3:2021 (E)

## Information technology — Specification of DRM technology for digital publications — Part 3: Device key-based protection

## Contents


Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Overview

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

6 License document

- 6.1 General
- 6.2 Content conformance
- 6.3 License information
- 6.3.1 General
- 6.3.2 Encryption (transmitting keys)
- 6.3.2.1 General
- 6.3.2.2 Profile
- 6.3.2.3 Content key
- 6.3.2.4 User key
- 6.3.2.5 Device key
- 6.3.3 Links (pointing to external resources)
- 6.3.3.1 General
- 6.3.3.2 Link object
- 6.3.3.3 Link relationships
- 6.3.4 Rights (identifying rights and restrictions)
- 6.3.5 User (identifying the user)
- 6.3.6 Signature (signing the license)
- 6.4 User key
- 6.4.1 General
- 6.4.2 Calculating the user key
- 6.4.3 Hints
- 6.4.4 Requirements for the user key and user passphrase
- 6.5 Signature and public key infrastructure
- 6.5.1 General
- 6.5.1.1 Validity of license document

6.5.1.2 Validity of a device certificate
6.5.2 Certificates
6.5.2.1 Provider certificates
6.5.2.2 Root certificate
6.5.2.3 Developer certificates
6.5.2.4 Device certificates
6.5.3 Canonical form of the license document
6.5.4 Generating the signature
6.5.5 Validating the certificate and signature
6.5.5.1 Validating the certificate
6.5.5.2 Validating the signature
6.6 Device key
6.6.1 General
6.6.2 Generating the device key
6.6.3 Recommendations for the device private key protection

7 License status document

7.1 General
7.2 Content conformance
7.3 License status information
7.3.1 General
7.3.2 Status
7.3.3 Updated
7.3.4 Links
7.3.4.1 General
7.3.4.2 Link object
7.3.4.3 Link relationships
7.3.5 Potential rights
7.3.6 Events
7.4 Interactions
7.4.1 General
7.4.2 Handling errors
7.4.3 Checking the status of a license
7.4.4 Registering a device
7.4.5 Returning a publication
7.4.6 Renewing a license

8 Encryption profiles

8.1 General
8.2 Encryption profile requirements
8.3 Basic encryption profile

9 Integration in EPUB

10 Reading system behaviours

10.1 Detecting protected publications
10.2 License document processing
10.3 User key processing
10.4 Signature processing
10.5 Publication processing
10.6 Device key processing

Annex A (informative) Examples

A.1 Example of a license document
A.2 Example of a license status document

Annex B (informative) Schema of license document

Page count: 30