

# ISO/IEC TS 23078-2:2020 (E)

## Information technology — Specification of DRM technology for digital publications — Part 2: User 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
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
6.3.3	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
6.5.2	Certificates
6.5.2.1	Provider certificates
6.5.2.2	Root certificate
6.5.3	Canonical form of the license document
6.5.3.1	General
6.5.3.2	Example
6.5.4	Generating the signature
6.5.4.1	General
6.5.4.2	Example
6.5.5	Validating the certificate and signature
6.5.5.1	Validating the certificate

	6.5.5.2	Validating the signature
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 (timestamps)
	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 profile
	8.1	General
	8.2	Encryption profile requirements
	8.3	Basic encryption profile 1.0
9		Integration in EPUB
	9.1	General
	9.2	Encrypted resources
	9.3	Using META-INF/encryption.xml for LCP
10		Reading system behavior
	10.1	Detecting LCP protected publication
	10.2	License document processing
	10.2.1	Overall
	10.2.2	Validating the license document
	10.2.3	Acquiring the publication
	10.2.4	License status processing
	10.3	User key processing
	10.4	Signature processing
	10.5	Publication processing
Annex A (informative) Examples		
	A.1	Example of LCP license document
	A.2	Example of LCP license status document
Annex B (informative) Use case scenarios for library lending model		
	B.1	Lending via a library portal/a web site
	B.2	Lending via a reading application
	B.3	Renewing a license
	B.4	Returning a license
	B.5	Expired e-book
	B.6	Fair use
	B.7	User experience
	B.8	Revoked license