# Authorization, Authentication, and Rights Specifications (collectively, 'DRM') on Electronic Books

## A Position Paper for the W3C Workshop on Electronic Books and the Open Web Platform

Jim Dovey, Kobo Inc.

December 10, 2012

**Abstract**

This paper outlines the ideas behind an interoperable form of DRM for eBooks, originally drafted in response to a Request for Proposals from the IDPF in October 2012. It outlines methods of authenticating both content and reader, and for authorizing individual actions ('rights') which may be performed by the user, including extraction of content and book lending.

The proposal is based entirely upon open standards already published by the IDPF and the W3C, supplementing them where necessary with new XML-based data structures.

## Background

There are a variety of competing DRM methods in use today, all of which are mandated by content owners but developed separately by different providers of reading systems. The closest we have to an ad-hoc standard in the area is that used by Adobe's eReader software and the Adobe Content Server. It is our belief that this is not an ideal standard due to its requirement of online fulfilment and its tightly-managed, non-extensible formats.

It would be ideal to have a standard way of specifying the *components* of a DRM system independently: a means for digitally signing the publication, of encrypting it, of

specifying rights and capabilities, and of providing an authentication/unlocking mechanism. All of these can be specified in multiple ways, given an appropriate method of doing so, and any existing DRM scheme can be adapted to the terms of such a system.

# Proposed Solution

The system proposed by Kobo offers a means of describing these four key elements in an extensible fashion using XML.

1. **Digital Signatures**
   The W3C already has a standard for describing digital signatures and their verification using an XML schema: XML-DSIG. This has also been adopted by the IDPF for ePub3. We use it as-is, although we provide additional means of specifying key information for HMAC purposes. Specifically, we allow for the input of a key based on user and/or device authentication.

2. **Encryption**
   Both ePub3 and our proposed standard make use of the XML-ENC specification from the W3C for describing encryption information. Our system adds to this some new means of locating encryption keys through our proposed authentication schema.

3. **Authentication**
   We suggest a new XML schema for the purposes of providing authentication facilities. This provides the following features which we believe make it suitable as a replacement for any more narrowly-defined authentication system.

   - Three classes of authentication: device-based, account-based, and user-input.
   - Fallback support: each method can specify a fallback method to be used should the current method fail. This allows for chaining of methods which would produce the same output key value, i.e. if account-based authentication fails, fall back to user-input, requesting the same account information.
   - Methods are identified using URIs in a manner similar to that employed by XML-DSIG and XML-ENC. This makes the standard extensible by third-parties, as an authentication method 'kobo-user-key' might be employed by Kobo and understood by its own apps and devices, but ignored by non-Kobo reading systems.

4. **Rights Authorization**
   We suggest a new XML schema for the specification of rights. The schema provides an action-oriented lookup with URI-based action identifiers, a number of which (ideally all those that are applicable to reading systems in general) are pre-defined. Our system provides the following features:

   - Three forms of grant: *Permitted*, where the right is unrestricted, *Denied*, where the right is unconditionally prohibited, and *Audited*, where the right is allowed subject to certain limitations.
   - Auditing of rights' use: audited rights have their audit trail built in, protected by digital signature. This allows the audit trail to be used as the basis for accounting of a rights' use, allowing the details of the original grant to be retained unmolested.
   - Explicit authentication: A right may be protected by authentication, by referencing any authentication mechanism from the authentication file described above. This may apply to any *Permitted* or *Audited* right.
   - Ranged application of rights: a right may be constrained to a particular area of an eBook. For example, a user may perhaps only lend the first 5 chapters of a book, or a user might be permitted to quote passages using social media *except* for any in the last chapter. Ranges are specified ruing ePub3 CFIs, and thus can refer to entire spine items (or multiples thereof) or content within a single spine item.
   - A time/date mechanism: rights may be denied or permitted based on the current date: a library might make a book's *read-right* available only for a certain two-week window, or a review copy could enforce a publicity embargo by limiting copying or sharing until a given 'street date.'
   - Specific handling for lending of content between individual readers. This allows for the specification of maximum and minimum loan periods and the number of times a given book may be lent out at a single time. It also enables a publisher to decide whether lending is *exclusive*, meaning that the owner of an eBook loses access to it while it is lent to another reader.

# Position

It is Kobo's position that the system described above (and which can be read in full at `https://dl.dropbox.com/u/896638/Kobo-EPUB-LCP.pdf`) provides a good basis for

the creation of a truly interoperable and extensible DRM system for eBooks. We further take the position that the chaining form of authentication should always be utilized in such a way that at the very least the book may be authenticated and thus unlocked using user-input.

For example, a Key Encryption Key might be obtained using authentication based on predetermined user account details. An app or device might have that data available and thus be able to generate the key, thus authenticating the user, in an entirely transparent manner. If it does not, it can fall back to requesting that the user enter their account details manually, thus generating the same key. The value of this is that the user has a better experience when sticking to the eBook providers' own applications, but that they are not tied to that provider in the future— they are ultimately free to take their eBook to another reader, albeit with the minor nuisance of entering a username/password when they wish to open the book.