

FileOpen for Publishing E-commerce

Nowhere is the need for DRM more pressing than in the online sale of high-value documents. While there may be legitimate debate over the merit of DRM schemes for consumer products -- music, movies, eBooks, etc. -- DRM for documents is an essential component of a reciprocal relationship between publishers and select recipients. For example, a Wall St. analyst who pays \$10,000 per year for a financial newsletter to gain a competitive advantage in the market will be cheated if someone else could receive the same information without paying. In some markets, publishers can consider it a *responsibility* to impose DRM.

Unique Requirements of DRM for Ecommerce

The DRM that is imposed, however, must be properly designed and implemented to enhance, not hinder, the commercial relationship between publisher and user. Any DRM system for valuable documents should:

- Maintain the integrity of the original document by preserving the standard file format (i.e. PDF).
- Be easily integrated into the publisher's existing document creation workflow, ecommerce, and subscription management systems.
- Be as unobtrusive as possible for the end-user. The use of standard formats, viewers and communication ports is critical, as end-users will often lack the authority to install new applications or modify firewall policies in their computing environment. Any inconvenience DRM creates for the end-user is likely to result in frustration and abandonment of the product.
- The DRM vendor should not insert itself between the publisher and end-user, force publishers to upload their content to the DRM vendor's server, have access to the customer's identity or usage data, or charge royalties based on the publisher's revenues.

The FileOpen Approach to DRM for Ecommerce

FileOpen software was designed from the outset to enable the commercial distribution of digital documents, according to the above requirements. While many DRM vendors have approached the problem in different ways, with proprietary file formats and viewers, royalty-based business models, etc., FileOpen's original architecture based on standard formats and open protocols has most effectively matched the demands of online publishers.

A key aspect of the FileOpen approach is the independence it affords publishers and content distributors. Publishers for whom DRM is a strategic necessity typically prefer that the DRM software be implemented entirely in their own environment, on their own hardware. Such publishers also typically insist that the DRM be licensed on a flat-rate basis, independent of usage, whether measured by the number of documents delivered or of users supported.

Other publishers may prefer to use the DRM software as a hosted service, but here too it remains critical that the underlying software be designed for independent operation. There is a difference between employing a vendor to host a DRM server and using a DRM solution that is designed around a cloud-based model. In the first case the publisher retains control over the content and the user data – i.e. can move the application to another location, or take it in-house – while in the second that publisher's content and usage data is tied to the DRM provider, and extraction of that data for transfer to another solution may be limited by technical hurdles, service agreements, or both.

Case Study: FileOpen Hosted™ for Retail eBooks

In 2008 FileOpen Systems contributed to the development of an online bookstore for a provider of technical information. This system was implemented as an add-on to an existing webstore, and required no substantial changes to either the user interface of the store or the underlying hardware/software environment.

The publisher sought to increase the security of their current eBook fulfillment system, in which the customer was supplied with a specific URL pointing to an unencrypted PDF eBook. Although the customer's link to the eBook would expire after two weeks, there was no system in place to stop copying and forwarding of the actual eBooks. Furthermore, the unencrypted eBooks were being stored on the site of the website vendor hosting the shopping cart.

Using the FileOpen Hosted™ system locally on a desktop computer, the publisher made a set of encrypted PDF files matching the original unencrypted set and uploaded these to a new folder on the website. A new set of SKUs were created in the shopping cart system to correspond to the encrypted PDFs, and a new cgi file was loaded to the server to handle purchases of the encrypted files.

Now when a customer buys an encrypted eBook, the link points to a folder containing the encrypted PDF, and the email contains a Username/Password pair unique to that customer generated by the Publisher3 server. When the customer attempts to open the encrypted PDF, the FileOpen plug-in is automatically installed either by Adobe's plug-in finder or by FileOpen's installer site. The Adobe Reader then requests the customer's login, which if accepted, displays the PDF with Offline Permission, so that no further internet access is required to use the content. The eBook is now locked to the user's computer, with one or more backup copies allowed at the discretion of the publisher. Subsequent viewings of the eBook by the end-user do not require any password entry.

By logging in to the FileOpen Hosted™ dashboard, the publisher can see a record of which customers opened eBooks on which machines, and can easily manage customer service requests (transfer from one machine to another, revocation in the case of refund, etc.). The same

interface enables the publisher to impose access restrictions on their eBooks such as expiration and printing restrictions.

While this implementation uses the FileOpen Hosted™ solution (invisibly to the customer, for back-end processing), the publisher could at any time migrate that server to a hosting provider other than FileOpen, or take it in-house. No usage data would be lost and the only interruption in functionality would be the time required to migrate a DNS entry from one IP address to another.

The Result: using FileOpen Hosted™, the Ebook publisher was able to place DRM on their eBooks without major changes to their existing ecommerce system. As an added benefit, the publisher now retains complete control over unencrypted copies of eBooks within their firewall, as well as usage data about their customers.

A Growth Model for E-publishing

As more and more formerly print publications go online, deploying effective DRM will be a critical factor in their online survival. FileOpen's DRM solutions give publishers the autonomy and flexibility they need to determine the right mix of security and usability for their valuable documents. From rendering documents viewable only online for complete piracy prevention, to experimenting with viral "superdistribution," in which recipients of locked documents are invited to purchase them legitimately, FileOpen offers proven solutions for ecommerce-strength DRM.