

What is DRM for Documents?

What is a Document?

It used to be a piece of paper. In the digital world, when we speak of documents, we mean information that starts out in office productivity and desktop publishing software and most often ends up in a portable format like PDF. Documents, as opposed to image files (although they may contain images) or HTML content or emails, are in a finished format and intended to be viewed online and/or printed. Some examples of digital documents are financial statements, newsletters, legal contracts, market research papers, and the like.

Challenges of Digital Document Distribution

The reasons to distribute documents in digital form are obvious, however many publishers and business users are understandably reluctant to send high-value or sensitive documents outside the firewall. In unencrypted form, digital documents are easily copied and forwarded with no degradation in quality from the original.

Simply applying passwords to documents doesn't enhance security because the passwords are tied to the document itself, and can be shared along with the copy. Issuing unique passwords to many documents and users is also an administrative headache.

Adding to the concern about security is the increasingly complex landscape of users on the receiving end of documents. Ten years ago, a business publisher could safely assume that the vast majority of its users were on some variant of Windows on a PC. Today, users are demanding access to documents on Mac and Linux platforms, using Safari and Firefox instead of IE, and sometimes need to see documents on their Blackberries (in addition to their laptop at home and their desktop at work). Supporting these cases while maintaining document security is indeed a daunting task.

The good news is that software companies have been working on this problem for a lot longer than there has been a market for a solution, and those on the buying side stand to benefit from many years of development, testing, and real-world implementations by early adopters.

The Solution: DRM for Documents

Digital Rights Management (DRM) is an approach to security in which copying of digital content is prevented by software that in most cases is running on the end-user's computer or device. DRM has been controversial in the context of music files and other mass marketed content in which the end-user has little incentive to cooperate with the publisher's copyright protection

goals. In the case of documents, however, the publisher's and user's goals are most often aligned (e.g. protecting privacy or protecting high-cost content). Moreover, DRM for documents can operate in a way that is invisible to the end-user (in some cases because no software needs to be installed at their end).

DRM for documents works by encrypting the files and then selectively granting access to them based on whatever credentials the publishers uses to authenticate users. This could be a pre-existing login to a website, or a cookie placed in the user's browser at the end of an ecommerce transaction. In some cases, a plug-in will be installed on the end-user's computer or device. The document viewer (e.g. Adobe Reader) displays the document for the end-user with no password entry necessary. The viewer enforces the security settings placed on the document by the DRM software, such as timed expiration or printing restrictions. In most cases the end-user won't know the document is secured unless they send it to a friend (who won't have permission to open it).

Why Standards Are Important

A "standard" is a technology that is architected for universal adoption, and enjoys the lion's share of the market for that technology.¹ Microsoft Word is the standard for authoring business documents; RC4 and AES are standards for data encryption. Adobe's PDF is an "open standard," meaning that its specification is published and that third parties may create their own PDF display mechanisms. PDF became an ISO (International Standards Organization) standard in 2008, officially putting the format under the control of the foremost international standards body.

What does this mean for DRM for documents? It is important for the publishers of documents to choose DRM solutions that are based on standards, because standards-based solutions ensure that their secured documents will work in the broadest range of software and hardware environments. It is tempting for DRM vendors to simply put their own secure wrapper around a file and insist that end-users download that wrapper in order to view the document. This approach is deeply flawed because it changes the native file format of the document, requires the end-user to download and install a large piece of new software (which may not be allowed by their IT department or device), and traps the publisher's content in the proprietary format of a vendor who may not be in business in a few years' time.

The FileOpen Approach

FileOpen Systems has designed its DRM technology around standards from the ground up, beginning with our flagship products for PDF. Rather than write our own secure viewer for PDF, we partnered with Adobe Systems in 1997 to develop a security handler plug-in which is licensed to operate in the free Adobe Reader. We have since extended this approach to the Microsoft

¹ We use the word "standard" in the sense of a *de facto* standard. A "technical standard" refers to a formal document that establishes norms and requirements for engineering and industry, which incidentally is an important market for DRM.

Office formats. Working with the makers of standard document formats has several advantages. First, we are not reinventing the wheel—FileOpen software encrypts documents in their existing format, and the encrypted documents can be opened in their native viewers which end-users already have installed. Second, it offers publishers compatibility with as many platforms and devices as these standard formats provide, along with the assurance of forward compatibility. Third, it allows for a consistent end-user experience, since they are viewing documents in a familiar format and interface.

Security vs. Usability

No software can offer absolute security, only a greater or lesser degree of vulnerability. The old saying that "the only secure computer is one that is in a locked room and switched off" illustrates the challenge: the more secure the system, the less useful it must be.

The goal for DRM is to create a system that is as secure as possible without degrading the experience of the intended user. Of course, there are circumstances in which information must be secured at all costs, irrespective of any reduction in usability. This problem is addressed by "Enterprise Rights Management" (ERM) systems, which uses heavy-duty encryption to keep documents inside the firewall, as distinct from DRM, where products must be accessed by users outside the firewall.

Because FileOpen DRM works from within standard document viewers, we are able to leverage the security frameworks of those applications to achieve a high degree of security, without compromising the end-user experience. FileOpen software uses industry-standard encryption and offers a range of access controls comparable with corporate ERM solutions. Our customers report a dramatic drop in technical support calls from their users upon switching to a FileOpen solution from a competing product.

Benefits of DRM for Documents

As the technology behind DRM for documents improves, the benefits of adopting it overwhelm the drawbacks. For publishers of valuable content, DRM's basic function of preventing copying has made a real impact in preserving their copyright and protecting their revenues. Deploying the more advanced access controls available, such as expiration and printing restrictions, has enabled publishers to manage subscription services online, replacing expensive and complex print-based systems. Publishers can now ensure that users have the authentic and current version of a document. They can also expire and revoke access to users who do not maintain their subscription dues. Finally, using DRM delivers volumes of useful data about how users are viewing and printing documents, when, and from which platforms and devices. Having such an audit trail opens up new business opportunities for publishers, such as entering into cooperative licensing arrangements with authors and other content providers.

The case for DRM for documents is no less compelling to corporate users. While there are many ERM solutions available to keep documents within the corporate firewall, these solutions are not designed for sharing documents with employees, partners, contractors, or other entities out in

the field. Furthermore, large-scale ERM systems are licensed and implemented enterprise-wide, at the highest level of the corporation, with commensurate fees attached. By contrast, a DRM scheme such as FileOpen Server™ may be licensed by a smaller unit within a large enterprise, or by a small or medium-sized business, and complement the existing firewall. Corporate users of FileOpen Server™ can use many of the same fine-tuned access controls available in large-scale ERM systems and apply them to end-users out in the field. At the extreme end of the security spectrum, an end-user may only have access to a document on the corporation's website while logged in, be prohibited from saving a local copy or printing it. Or a more flexible approach may be taken in which usage of a document is simply logged by the server.

Conclusion

Using DRM, document owners can carve out a secure space in the digital world for their content, without having to wait for a more secure Internet infrastructure or license a costly enterprise security solution. By choosing a standards-based DRM solution, publishers can quickly implement a secure document delivery system that leverages their existing assets.