White Paper: What PDF Security options are available?

Please see our PDF web page for more details on many aspects of publishing PDF files.

When choosing PDF security solutions there are several key questions to ask. However, there is no perfect and universal solution to all requirements, so please don't expect one!

For example, if physical printing is permitted the end user can always scan in the printout and screens can be photographed, scanned or captured and used to create a new PDF without security enabled – "intelligent watermarking" can help discourage and protect against this problem.

Every protection scheme has its limitations, and the more sophisticated it is the more obtrusive and difficult it typically becomes for the end user, so there is always a trade-off between simplicity and security. Corporate and Social pressure and international copyright law are a publisher's ultimate forms of protection – coupled with the best PDF security solutions that strongly discourage abuse of copyright and protect against the most obvious forms of piracy and copyright abuse.

The question we are most often asked is "what is the difference between providing security for a standard Adobe-style PDF and Digital Rights Management (DRM) based security?". This is perhaps best answered by highlighting a few key things to know about PDF security:

1. Adobe permissioning security is easily removed by many software packages and free online services, so has very little protective value. Even when implemented and not removed, non-Adobe PDF readers can simply ignore it and continue to allow printing, for example, without regard to the settings you have made.
2. A file that has been "secured" by any system (from Adobe or anyone else), cannot be protected against the whole file being copied any number of times to any number of people without a Digital Rights Management (DRM) facility in place. Essentially a DRM system is a mechanism to ensure that a specific device and optionally a specific user has the right to view (and maybe print) the document in question. There is only ONE way in which such a system can be implemented, and that is for the end user device (PC, Mac, tablet device or phone) to communicate directly with a central DRM server. This is how all true DRM systems work.
3. DRM service providers deliver security through a range of measures, both the obvious ones: e.g. encryption of the document; permissioning controls that cannot be tampered with; in-network DRM services; but also by less obvious measures, such as usage tracking; intelligent dynamic watermarking, sophisticated end user software implementation (e.g. never decrypting and saving the file at the user end)
4. DRM services vary hugely in the pricing and range of facilities and services provided. We aim to be the most secure and high quality service, and yet the most cost effective. We do not charge for our software, focusing on service provision, so there are no licensing fees
5. A number of providers, including ourselves, offer the option of both offline and online (web-based) PDF security, depending on the requirements you have and likely audience – some publishers prefer one approach over the other, whereas a few use both mechanisms to reach the widest possible audience

Some things to consider that you may wish discuss with us for your own project include:

1. How large is your expected audience for publications in year 1?
2. Geographically where are they located?
3. How large (pages, Mbytes) are your publications?
4. Is your target audience "sophisticated" or are they computer/IT novices?
5. Is your target audience mainly private individuals, or corporates/government agencies, i.e. large organizations with complex rules about software usage and network controls?
6. Do you need to price your items in local currencies, if sold via an ecommerce platform?
7. Are you happy to run a free test using a sample document you can provide?
8. What are your target devices? i.e. what technology platforms do you need to deliver to?

These questions will help you determine the best approach or approaches, to providing the digital distribution you require, at an affordable price, with the level of security you require.

We are also often asked about augmenting/editing a document that has been protected with strong encryption and DRM facilities. The brief answer is that a full protected document cannot be edited if it has the level of protection one expects – however, with some providers mark-up and annotation of documents is possible, so notes can be added and "overlaid' where the user wishes.

In the sections below we pose 12 questions and provide brief answers. We also provide more details on the product and services options available from a range of providers, including those using Adobe software and from ourselves: https://www.drumlinsecurity.com. Please also see our PDF web page for more details plus news and views on many aspects of publishing PDF files.

For Adobe's security advisory notices (breaches of the Adobe PDF offerings and updates to try and fix these) see: http://www.adobe.com/support/security/index.html - scroll down this page to see the notices for Adobe Digital Editions, Adobe Reader and Adobe Acrobat

---

CONTENTS

Note: The opinions expressed in this document are personal and readers should carry out their own reviews and investigations before making decisions on PDF security. All trade names and trademarks of software and service suppliers, including those belonging to Drumlin Security, Adobe, LockLizard and FileOpen amongst others remain the exclusive property of these organizations

Question 1: Who will be the end users of your document(s)?

If the answer is third party corporate customers in larger organizations, then your choices are:

a) use standard Adobe Acrobat to create PDFs with security features enabled, which will work almost everywhere (but see below for significant security problems with this approach), or

b) use a web-based solution that displays PDFs as HTML5 (with dynamic or static conversion and a security framework added as required – see https://www.pdf2html5.com as an example of such a service) – some standalone and add-in viewers can provide secure viewing but require separate installation and licensing (see Question 11 for more details), or

c) ask customers in such corporates to use their own home/laptop/netbook/mobile computers with a proprietary secure PDF reader – this is often a practical option, depending on the application area

d) most corporate networks are Windows PC based with internet access controlled via firewalls and proxy servers. Software solutions that will work in this environment include the standard Adobe reader and the Javelin3Pro for Windows reader from Drumlin Security. The Javelin3Pro reader is specifically designed for this kind of environment, offering device registration and document security management without requiring an online connection

If you issue standard Adobe-compatible PDFs, but add security features using Adobe Acrobat such as watermarking, password to open, and text copy restrictions, these will be readable by the intended end user in all cases. However, such protection mechanisms are not necessarily implemented by non-Adobe readers and can be removed by widely available software (e.g. see http://elcomsoft.com/products.html) and many free online services. There is also no protection against the PDF being forwarded to someone else - i.e. there is no digital rights management (DRM) system included to protect against such copying. For DRM options Adobe offer their Adobe Content Server (ACS) and Adobe Livecycle solutions.

If the answer is intra-corporate, smaller corporate users, or 'consumers' and home-based business PCs, then a range of options is available. These include solutions based on services and software from Drumlin Security. Drumlin Security's Javelin secure PDF readers are available for PC, Mac, iPAD, iPhone and Android devices, so deliver true cross-platform delivery with a single file format and full DRM-enabled protection. Alternative authorization procedures can be provided, based on commercial and technical requirements, e.g. for specific bespoke apps. If you need to protect a broader range of files, not just PDFs but also Microsoft Office and other files, a solution from FileOpen might be a better option, assuming the cost is acceptable.

Question 2: Do your PDF files need to be read on a wide range of devices, from PCs to Mac computers, portable devices and eBook readers?

If the answer is "yes" then you will need to decide whether you can conveniently convert your PDF or underlying source document to the various formats required by the different platforms or whether to stick with PDF:

a) for PCs, Mac computers, iPADs, iPhones, Android tablets (or similar devices), sticking with pure PDFs is possible and often desirable although they are not secure unless augmented in some way with extra facilities. Not all solutions are available for PC and Mac OS, and/or mobile devices – in fact often the providers of security systems for PDFs are PC/Windows only. For some applications the latest version of Adobe's ePublishing product set may be appropriate. For more details see: http://www.adobe.com/products/digitaleditions/ - several bookstores and Library services use Adobe Content Server as their main platform for selling PDFs and ePUB formatted docs with built-in security – see for example, the ebooks.com website. Drumlin Security's Javelin PDF readers are one of the few full functionality PDF readers that are available across all major technology platforms, free, and providing full DRM-based security for PDF files.

b) For hardware-based portable eBook readers, every one tends to be different although there are some common 'standards'- notably ePUB and MOBI (or Amazon Kindle variants of MOBI, e.g. KF8). In general these do not handle complex formatted PDFs and embedded images in a satisfactory manner – the only way to know is to test converting your source file or PDF to one of these other formats and to view the result on the target device and/or a desktop emulator of that device. Many of these devices are greyscale, so cannot display color, although this is changing rapidly. Services like Lulu and Smashwords provide consolidated distribution for ePUB-based eBooks, but not for PDFs.

   The Amazon Kindle family of devices is designed for a specific file format (see the Kindle page for more details), although it will read standard PDFs also (without security). Protection against screen capture tools such as http://www.ebook-converter.com/ is not provided. The latest addition to Amazon's Kindle range is the Kindle Fire (various models) that run an amended version of Android, and hence the Javelin secure PDF reader can be used in this environment using manual installation.

   Proprietary eBook readers are moving towards Android as a common operating system platform, with Nook being a good example (and now Kindle Fire). PDFs may be read on such devices and products like Javelin for Android (available free from the Google App Store and from our website) runs extremely well on such devices and provides the DRM security that many publishers and training companies are looking for.

c) Dynamically or statically converting a PDF to HTML5 is possible. This is a good option now that HTML5 is widespread as it supports much richer content types and structuring. This is ideal for fast online display of PDFs, subject to the limitations of access via web browsers. For samples of PDFs in HTML5 please see:

   https://www.pdf2html5.com/formats.php

d) converting a PDF to images (typically initially as TIF files, one per page) is standard in Adobe Acrobat and the pages can then be embedded in an viewer, such as Google

Books viewer. These kind of systems also extract the text content and use this for searching and related functionality. In the case of the Google Books viewer and our own online viewer solutions, you can use this within an iframe on any web page with any PDF you already have or simply via a URL (e.g. a link in an email or on a web page). For more on such file conversions please see Question 11

Question 3: Do your PDF files need to be printed on non-standard paper/with no scale distortion?

If the answer is "yes", for example you need to print on very large sheets for architectural drawings, engineering drawings, or clothing patterns, you have two options:

a) convert the large-format file to "tiles" of standard paper size, e.g. A4 or US Letter – this facility is available in some PDF manipulation software, notably in Adobe Acrobat. Note that tiled documents need to be manually re-assembled once printed, so are best accompanied by a diagram and/or mark-up showing how the pages fit together and providing clear/large numbering of the pages. Note that for scale-specific printouts the PDF reader must be able to reproduce the scale correctly

b) keep to standard Adobe PDF, without security, and permit the end user to take a copy of their file to a digital print shop for output on a large format printer – such print shops do not generally accept formats other than standard PDF and some image formats. There is no doubt that the print functionality of the core Adobe Acrobat reader is the best (most flexible) available from any provider

c) Provide an in-network print service for the files, managed to ensure your document security is maintained

Question 4: Do you need to protect your PDF files from being copied to another computer or user and then read?

If the answer is "yes" you need to use a system (software and service) that provides Digital Rights Management (DRM). A DRM service can be intra-corporate (i.e. you have your own, in-house server and service) or provided as a service by a third party, e.g. Adobe or Amazon or Drumlin.

Many ebook stores provide PDF files (and other file formats) with no DRM, so these do not provide copy protection. If web-based ebookstores offer DRM support for PDFs it tends to be based on the Adobe Content Server solution.

It is important to note that every solution that provides DRM support involves two key components:

a) a PDF reader that is DRM aware and has built-in security features (e.g. Adobe Digital Editions, Drumlin's Javelin readers)

b) a network connection to the DRM service for enabling or "authorizing" the file that the end user wishes to read (this may be direct or indirect)

In addition, the DRM may require unique user and/or device details in order to offer user- or device-specific controls. Alternatively the DRM can provide a one-shot authorization, irrespective of user or device, which greatly simplifies the process for the end user but may reduce the control and tracking information available to the publisher.

Drumlin Security offers multiple solutions with DRM, both online and offline.

Question 5: Do you need to protect your PDF files in other ways, for example to prevent printing or to control the date and time the file is available?

If the answer is "yes" you have two choices:

a) use the facilities provided for security in Adobe's standard PDF offering (Adobe Acrobat/Acrobat Pro can create and manage such files), including disabling the clipboard, password protecting the file, and disabling printing. Note that date/time protection is not provided via this standard mechanism. Also note that such facilities may be ignored by some PDF readers, thereby effectively removing any intended protection, and in many cases protection can be readily removed by widely available third party software, so this provides a disincentive rather than a strong solution. Also note that a secured PDF can still be copied and distributed, unless additional DRM protection is provided.

b) use the facilities provided in a specialized PDF reader that supports such controls within a strongly encrypted framework. Note that readers such as Adobe's Digital editions and LockLizard's PDF reader (which is based on the Foxit reader) require installation and registration to use. Drumlin's offerings, based on the Javelin family of PDF readers, are provided without charge via the main mobile device AppStores, plus Apple's OSX AppStore and for Windows users, via direct download). This family of PDF readers includes protection against copying to the clipboard, start and end date controls, elapsed time control (e.g. can be viewed for 3 days), a range of controls on printing, number of viewings and number of prints control, user-specific watermarking, usage tracking and several other features. Note that for screen capture protection the only real cross-platform option is "intelligent watermarking".

Question 6: Do you require a free or low cost solution?

If the answer is "yes", then the use of a third party service and software is the main choice, unless you plan to develop your own solution set (which can be very expensive).

However, there are a great many services and offerings, most of which operate on a subscription service basis and/or a commission basis to recover their costs and maintain and develop their services. Very few free services exist that are genuinely secure.

Question 7: Do you require a multi-language or specific (non-English) language solution?

If the answer is "yes", then you need to choose a solution that is multi-language enabled. This means that (a) menus and messages are available in the language of your choice or selectable by the end user, and (b) the page display supports the character encoding and display mode appropriate – for example, to support Japanese, Hebrew and Arabic, right-to-left page turning and text searching is required, which may not be available. Many pure PDF readers, such as those from Adobe, Foxit and Drumlin, do offer multi-language support. With Foxit and Drumlin the language files are downloadable and/or coded in XML format, so may be modified and/or new languages supported by end user translation of the English base file. The Javelin family of PDF readers support multiple languages (varying by platform). The Javelin (version 2) readers for Windows provide support a wide range of languages and bespoke versions of the readers, by technology platform, can be provided with branding and language variants.

Question 8: Do you have a large number of documents to secure and manage?

If the answer is "yes", then you need to choose a solution that offers batch processing, especially if files may have to be updated on a regular basis (e.g. time expired files). If, in addition, a system for managing which files may be accessed by specific individuals or groups, a content management system (CMS) may be needed. There are many providers of CMS technology, and some PDF security solutions offer CMS-like functionality. Products like Adobe Acrobat Pro and Drumlin's PDF Publisher offer multi-file selection and publishing plus automated batch publishing of secure PDFs. Some systems, such as those from FileOpen and LockLizard, offer CMS-like facilities, but most offerings do not, leaving these facilities to be provided via established intra-corporate CMS implementations or in-network systems and services.

Cross document text searching is a requirement in some situations, and currently this is only supported in the Adobe Acrobat suite, with indexes pre-built to support this form of search. Note that cross-document text search of encrypted files is not possible without a special external index file of text strings, because the secured documents cannot be searched directly by generic tools.

Question 9: Do you require a tailored PDF reader and or service?

If the answer is "yes", you need to work with a third party supplier that permits tailoring and branding of their offerings. This is often referred to as "white labelling". Suppliers, such as Drumlin Security, FileOpen, Bluefire and LockLizard are often happy to support in-house or third party development teams to implement tailored solutions that include components from their proprietary suites, and/or to offer managed services and client software that is branded and tailored. There are also a number of providers of PDF library software, i.e. toolkits (generally separate toolkits for each technology platform). These may be used to create branded PDF readers, or PDF reader facilities within other applications or services. Note that the licensing models for most such providers are often based on the number of end-user licenses issued that are based on these libraries and/or are restricted to use within a single app or application. In the latter case a separate license is required for each app and each platform.

Question 10: Should I publish using PDF or ePUB?

If your books are highly formatted and contain a lot of images, tables and similar formatted items, and you wish to retain these you will need to stick with the PDF format and/or create images from the pages which you can then publish online. This may restrict the range of devices to which you can 'effectively' publish, owing to the limited size of such devices.

On the other hand, the use of the ePUB format, which is XML based, provides for greater flexibility if you are looking for wide cross-device support and are not concerned about formatting, tables, images etc. The reason is that ePUB allows for re-formatting of the file on the fly, for example changing the size of text in order to make it more readable, and automatically *re-flowing* the text (so it is re-arranged on the page) to fit the display window offered by the device in question. Adobe Content Server digitally protects PDF and reflowable ePUB content for Adobe Digital Editions and supported mobile devices such as Sony's ebook reader.

Question 11: Should I publish PDFs offline or online, or both?

Let's start with the Online options

There are any number of online services that will display PDFs converted to an alternative format (to flash or html5 nowadays, not to ePUB as PDF to ePUB rarely works!). Widely used for Magazines in "page flip" format, do they have a broader role?

Examples: issuu (mainly for Magazines and brochures), PDF2HTML5 (our secure online equivalent of our offline Javelin PDF readers), Scribd (a PDF book publishing platform - for mobile devices they now use an app instead), and Zyyne (a French-based service, similar to issuu). Google Play books display PDFs in some instances, but does so strictly as images (most Google Play books are in ePUB format and displayed online or offline using ePUB reader software).

There are three main technology options for online PDF display (many services provide all 3, with an "adaptive" interface that selects the best option based on the device):

1. Convert the PDF to Adobe Flash. This is what many of the Magazine and brochure display services provide for desktops and laptops, often using a Flipbook-type display.

Advantages: Excellent display quality, good navigation, good printing functionality (if required, but not secure), fast and simple if implemented correctly

Disadvantages: iPADs and Android devices do not support Flash, so strictly for PCs and Macs, which must have a recent version of flash installed (most do). Long term support for Flash by Adobe is no longer available. Not especially secure, but may be "good enough" for many applications. Note that many web browsers now prevent Adobe Flash from being displayed unless pre-authorized by the end user.

2. Convert the PDF to HTML5. There has been an enormous amount of interest in HTML5 and how it could replace PDFs as the preferred display format. Files can be converted statically or dynamically - dynamic conversion is the norm. See examples on our PDF2HTML5 website here.

Advantages: Widespread support for HTML5 in all modern web browsers and the latest mobile devices; no requirement for software distribution or document distribution; fair to very good quality display and navigation; options for augmenting with multimedia (e.g. embedded video).

Disadvantages: Not as secure as offline; not supported by some older web browsers (depends on when they were last updated); conversion may not always be perfect, depending on how the original PDF was created (formatting, fonts etc).

Almost all flipbook systems use page image records as a fallback solution. A big advantage of these systems is that they are simple to set up and manage, with all the data (documents, user-related data, tracking etc) kept centrally, and the building blocks are readily available at relatively low cost.

Overall conclusion: excellent for applications such as magazines, some brochures/catalogs, and documents with large fonts and lots of graphics. Variable quality as a reading experience

(particularly on mobile devices) depending on implementation and type of document. Some services offer pure PDF downloads as an option, so provide online and offline display, but generally without security.

Now the Offline option

There are several advantages to offline working, e.g. using a system like the Drumlin DRM service with Javelin PDF readers for the main technology platforms: PC, Mac, iPAD/iPhone and Android. Adobe and their DRM partners provide similar products and services. These include:

- instant access to the documents at all times, when continuous online connectivity is not possible or desired. This is particularly useful when travelling, in offsite locations, in training rooms, workshops, on board ships and aircraft etc
- the quality of the screen presentation is almost always better, as is the local functionality that can be provided (e.g. integration with catalogs, markup etc)
- speed of display and moving around the document is faster, and very large documents can be handled with ease (e.g. 1000+ pages – our largest client document is 35,000 pages)
- security can be far stronger than for online systems
- strict print control is possible (PC/Mac solutions), which is not practical for online systems

The main disadvantage of an offline system is that it can require a bit more work from both the publisher and the end user. And there are occasionally situations where offline operation is not an option (e.g. where downloading and use of third party apps and/or secured documents is not permitted, e.g. due to corporate policy and security systems). These can often be worked around, either via onsite measures (approval of the app, enabling of proxy server support) or offsite measures (authorizing a file offsite/via open WiFi connectivity, or using license-based authorization), or by using an online service as described above.

Online or Offline?

From the very brief summary above it is clear that there is a strong demand and widespread use of online PDF display, mainly in the "media" sector at present, with offline being the preferred route for documents that are designed to be read in detail and/or printed. There is also merit in combining the two, e.g.: enabling simple previews and promotions to be provided; allowing ancillary documents (e.g. promotional materials, videos etc) to be displayed; providing a subscription-based access service; and in addressing the security constraints that may apply for some sites.

Question 12: What is the difference between permissioning-based systems and authorization-based systems?

There are three main approaches that can be taken to provide digital rights management (DRM) for documents:

1. User-independent authorization systems: these are systems where files are downloaded and are authorised for offline usage by either: device identification, which requires prior registration of the device; or by entry of an authorisation code that is checked on a central

DRM system (does not require prior registration). Note that with this second approach there is little or no requirement for central service management as the process is very largely automated.

These are “automated authorization based systems". Examples of device-based systems are Amazon Kindle, iPADs with iBooks, and devices like Kobo and Nook. An example of a non-device based authorization system (with no prior user registration) is the standard Drumlin service, with Javelin as the end-user reader.

2. User and/or device-dependent systems: these are systems where each person downloading a document must be pre-registered on a centrally managed service, and then each publication they are permitted to view is centrally enabled for them. These are “permissioning based systems".

3. Online-based systems: approaches 1 and 2 assume the files are to be downloaded and read offline - no host connectivity is required after the initial stage of downloading and enabling. In many ways a simpler alternative is a hosted service, where the files are kept centrally and displayed via a browser. A pure HTML5 based solution (with username/password login and other protective measures) would be an example of such a facility. Note that this option is very simple to manage because the files are held centrally, and access can be managed at the school or class level (with usage tracking) rather than at the individual student level (although the latter is entirely possible - just a bit more work administratively). The compromises here are: (i) the files can only be viewed online; (ii) access is controlled via permissioning, so requires manual management; (iii) the quality of display is typically not as good as offline PDF readers; (iv) the security is not as strong; (v) if printing is required, offline or in-network printing are the only safe options.

READ MORE ABOUT ONLINE AND OFFLINE PRODUCTS AND SERVICES FROM US