Secured PDF - options & issues when creating secured PDF file

There are many options to consider when creating a secured PDF. This paper covers the protection methods and security features available for secured PDF files.

When creating a secured pdf file there are many issues for you to consider, including:

1. the pdf protection approach – pdf passwords or public key technology?
2. preventing sharing;
3. preventing forwarding;
4. preventing simple copy and paste;
5. preventing editing;
6. preventing screen grabbing;
7. preventing printing, allowing printing, or limiting print usage;
8. watermarking on view and/or on print;
9. document expiry methods;
10. tracking document opens and prints;
11. revoking document access;
12. use in thin client / virtual environments;
13. allowing offline use;
14. use of publications for simpler document assignment.

These secured pdf features are covered in depth below.

1) PDF Protection approach for a secured pdf file

The first question to consider when creating a secured pdf file is how easy is it for others to remove the security on the secured pdf file?

The most popular method of creating secured pdf files has been to use password protection, but passwords can be easily removed using freely available pdf password recovery programs – see PDF Encryption & Security. Clearly, if you are going to create secured pdf files then passwords are not the way forwards.

Adobe content server implemented full scale PKI technology, but that meant the sending party needed the receiving party's public key in order to create the secured pdf file. And each secured pdf file had to be protected independently for each individual recipient (so the same pdf file could end up being secured hundreds or even thousands of times, depending on the number of recipients). Clearly an internal protection scheme that needed heavy resources in server processing power to service even a small number of recipients.

By comparison LockLizard DRM secured pdf files are only protected once, using long and random encryption keys. Decryption keys required to open secured pdf files are transparently relayed

securely to the client computer and stored encrypted in a keystore. There are no passwords for the user to enter and they don't have to acquire and send a public key to anyone.

2) Preventing sharing of secured pdf files

If you decide to use passwords to create secured pdf files, then users can share the pdf and the password with others. With a LockLizard DRM secured pdf, if that pdf file is given to an unauthorized recipient they won't be able to open it (because it is encrypted). To open a LockLizard DRM secured pdf file, a user has be registered with the publisher of that actual secured pdf and also be authorized to view it. To stop users sharing a secured pdf file along with their keystore, keystores are locked to specific computers and if copied to another computer will no longer work.

3) Preventing forwarding of secured pdf files

You can't prevent users from forwarding secured pdf files to others. Even if an email policy system is in place, users will always find ways around the system (e.g. saving the secured pdf file to disk and sending it by webmail, usb stick, converting it to a zip file, etc.). What you can prevent, however, is someone opening a secured pdf file, since unauthorized recipients cannot open a secure pdf file without the correct decryption key (and license).

4) Preventing copy and paste

There is not much point in creating a secured pdf file if users are allowed to copy and paste content from it. LockLizard DRM software prevents copying and pasting by using our own secure viewer environment to control the functions available to users. We prevent plug-ins from being loaded so that third party plug-ins cannot be used to compromise the security by enabling such features.

5) Preventing editing of a secured pdf

If you allow editing, then you must provide features that allow the secured pdf to be saved both during editing and for later use. This opens up a fundamental weakness in any security system which can be exploited in order to allow copies of documents to be made and exported, so it must be avoided.

6) Preventing screen grabbing of secured pdf content

LockLizard DRM software employs a number of techniques to prevent the use of print screen and third party screen grabbers. Whilst DRM cannot totally prevent screen grabbing from taking place (nothing can stop taking a photograph of the screen) it can make copying much more

laborious, and thus discourage users by making them work hard to get a poor quality copy.

7) Preventing printing, allowing printing, or limiting print usage

Stopping users from printing a secured pdf file is the most effective way of preventing copies of your pdf documents from being created and circulated, since printed documents can be readily photocopied or scanned and then duplicated. If you must allow printing, then LockLizard DRM software enables you to apply secure watermarks to the printout (see Watermarking on view and/or print). With LockLizard DRM software you can also limit the number of high quality prints allowed and log any print requests made by users.

LockLizard DRM software automatically prevents printing to PDF drivers, so that secured pdf files cannot be readily converted to PDF format again. Documents that have been printed and scanned back in and then converted to pdf will only ever be image documents (so basically one big image in a pdf file). That process loses all the bookmarks, links, and search capabilities, which are the key main usage features of electronic documents.

8) Watermarking on view and/or print

LockLizard DRM software enables publishers of pdf documents to apply dynamic watermarks to secured pdf files that automatically insert the users name, email, company name, and a date/time stamp at print time to discourage sharing of printed documents since the originator of those documents is clearly identifiable. Similarly, these dynamic variables can be inserted at view time to discourage screenshots from being taken and distributed.

Because LockLizard DRM software uses dynamic variables, the publisher of the secured pdf file only has to protect one pdf document for all users. With Acrobat pdf security you have to protect each pdf file individually for each user in order to customize it with their user details.

LockLizard DRM software also enables static watermarks (graphic images) to be applied at the same time as dynamic ones. Static watermarks may be used to prevent forgery (as they are with banknotes) or to establish ownership, and can be under the main content.

9) Secured pdf files and document expiry

LockLizard DRM software enables the publisher of a secured pdf to enforce document expiry.

There are many reasons you may want to expire pdf documents such as:

- complying with document retention policies;
- updating or replacement of old documents;
- trial usage (e.g. 1 view before purchase);

- complying with project timescales;
- Enforcing subscription periods.

LockLizard DRM software enables you to expire secured pdf files:

- After a number of views;
- After a number of days;
- On a fixed date;
- After a number of prints;
- When a subscription period has ended.

10) Tracking secured pdf files

Tracking when a secured pdf file has been opened or printed can be essential for accountability purposes where you want to ensure that the recipient has not only received the secured pdf file but has also read and/or printed it.

LockLizard DRM software enables you to record all document opens and prints and displays the number of times each document has been opened and printed. You can even filter results over a specific date range.

11) Revoking access to secured pdf files

Being able to revoke access to secure pdf files can be vital for controlling confidential documents or where chargebacks have been applied against the purchase of a document.

LockLizard DRM software enables publishers to revoke secured pdf files at any time ensuring your documents are always under your control (note: online usage must be enforced).

12) Use in thin client / virtual environments

Being able to limit and control the number of computers that a secured pdf file can be viewed on is at the heart of any DRM licensing system. However, most DRM systems don't prevent viewing secured pdf files in thin client / virtual environments. If a secured pdf file can be viewed in a thin client / virtual environment then it means that a secured pdf licensed for a single computer can be used on ALL computers in the thin client / virtual environment. It may make you question why you bothered to secure it to begin with.

LockLizard DRM software automatically prevents use of secured pdf files in thin client / virtual environments unless they have been specifically authorized by the publisher of those files.

13) Allowing offline use

Not everyone wants to be (or is able to be) connected to the Internet every time they open a secured pdf file. LockLizard for example have customers that view secured pdf files from CD whilst out at sea, where Internet facilities are either unavailable or unreliable. Some PDF DRM systems force the user to always be connected to the Internet every time they want to view and/or print a secured pdf file, or even to be online for the whole of the time it is being used.

LockLizard DRM software supports both online and offline usage. You can always require users to be connected to the Internet (so checks can always be made with the licensing server for any updates – like removal of access, etc.), or make them go online after *n* days (e.g. check with the licensing server once a month for any updates), or allow them to view and print secured pdf files permanently offline. Obviously the latter gives the publisher of the secured pdf file less control, and means they cannot instantly revoke access to secured pdf files, but it does provide greater flexibility for the user. Choosing the right DRM checking mechanism is really about risk assessment - when you have the tools that LockLizard provide so you can do that.

14) Use of publications for simpler document assignment

Unlike other PDF DRM software, LockLizard DRM software enables you to create secured pdf files that are part of a publication. Access can then be given to the publication by one command, rather than you having to allocate individual secured pdf files. From a management point of view, publications are therefore not only a convenient way of grouping secured pdf files, but a simpler way of assigning access to them. Publications are essential for magazine type subscriptions where a customer buys access to a continuing service and not just a single document. They are also useful where a bundle of documents is being administered, such as documents being disclosed for legal purposes, a training course, tests relating to drug licensing and so on.

About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection for PDF, flash, ebooks, elearning, software, and web based content. We protect information with US Government strength encryption and rights management controls to ensure complete protection against copyright piracy. Use our DRM software to control document use - stop copying, prevent printing, disable print screen, expire content, instantly revoke access to information, and track document usage (views and prints). http://www.locklizard.com