

## Clarification on Security features of PDF.

I also wanted to clarify something I heard it on the call with regards to password encryption, digital signatures, and certification. These are three different things that serve very different purposes, and password encryption is not our only encryption option. Let me give the quick rundown. I've cc'ed Ed so he can correct me if I got any of this wrong.

Encryption - this prevents unauthorized users from accessing the PDF file. This can be done 2 ways - password, or Public Key/Private Key certificate (not to be confused with certification)

- password - you need a password to encrypt and decrypt the file.
- Public key/private key - The PDF file is encrypted using the public key, and only the user who has the private key can decrypt the file. (see my note above about having a Medical Emergency certificate - the private key that emergency providers can use to decrypt these files). The public key can be freely distributed, but the private key should be kept under guard.

Digital signatures - this is not encryption. This basically 'saves' the signed version of the document and does a hash so that it can detect if the part of the document that has been signed has been modified. The user can usually continue to modify the document after it signed, but Acrobat will always allow you to go back and view the document as it was when it was signed. If someone tampers with the bits that are signed, Acrobat will detect this and invalidate the signature. Note again, this is not encryption, the signed document can be viewed freely.

Certification - this again is not encryption. This serves the purpose of certifying that the document came from a certain trusted source, and that it made it to the user without being tampered with. It can also be used to add certain restrictions to the document. So for example, the bank may send you a form asking for personal information. Well it's very important that the form be certified and that you know it comes from the bank, otherwise the form could contain malicious constructs. This is accomplished in a similar fashion to Digital signatures in that a hash will be generated over a portion of the file, and that Acrobat will check that hash to ensure the document hasn't been tampered with. However there are also additional heuristics in the case of certification since certification can impose certain restrictions such as preventing modification of field values or making the entire form read only etc.

In any case, the first step is likely to figure out what to do with encryption. Signatures and Certificates will also be important, but maybe a bit later in the workflow.

Here are also a few links of interest should you want official Adobe Documents describing security within Adobe's Products and PDF:

<http://www.adobe.com/uk/security/doccontrol.html>  
<http://www.adobe.com/uk/security/digsig.html>  
<http://www.adobe.com/uk/products/server/securityserver/>  
<http://www.adobe.com/ap/security/>

Ed's reply:

Hi Anatole,

You've covered the PDF security overview very well – I don't have much to add there. Just one more comment on certification – an important facet certification is how it provides a level of rights management to a document *without* encryption. This is important because in many workflows there will be some documents that are public facing but that you may not want to

burden or risk the use of encryption in situations where the point of rights management is not obstruction but authenticity.

Take a vaccination report for example – it's a somewhat public document that may need to be provided in advance of a trip or school registration. It also may be helpful to allow it to be updated in electronic form to reflect more current vaccinations, while maintaining the existing signed records in the file. Certification at the source in this case – perhaps allowing changes to some form fields – is a nice middle ground. It doesn't restrict the file from being viewed or updated, but protects the existing information from being modified. If someone attempts to modify the document in a way that is not permitted by the certifying signature, then the tamper-evidence kicks in and invalidates the signature.

Contrast this with the alternative – using a simple signature and document level encryption – which is much more cumbersome in this situation – its not realistic (or safe in some cases) to provide passwords each time the document needs an update, also, you can't sign an unlocked document and then re-lock it without breaking a signature.

Certification has very practical use cases - it's definitely worth separating out from both regular signatures and rights management in any guidance.

Ed