



## The Role of Encryption in Document DRM

Author: Dr Stephen Hitchen

Dr Hitchen has designed award winning access control, encryption and DRM devices over the past 20 years

Document DRM (dDRM) involves controlling both access to and use of (through digital rights restrictions) the content of documents.

In terms of a security solution, this is completely different from protecting documents using encryption, where the aim is solely to prevent an unauthorised user from accessing the content; in dDRM the authorised user must also be considered an adversary, who will attempt to circumvent the digital rights restrictions.

Any security solution is only as strong as the weakest part. In dDRM encryption of the content (using an established algorithm such as AES) would easily be the strongest part of the solution, and therefore of relatively minor importance.

Far more important in determining the quality and security of a dDRM solution are factors such as:

- How the encryption key is secured from the **authorised** user.

In dDRM, although the user must have the key to decrypt the document, it must at the same time be secured from the user. Otherwise they could simply separately decrypt the content, circumventing the digital rights controls.

Protection of the key may take the form of additional encryption of the key, using an obfuscated algorithm<sup>⊕</sup> (e.g. 'White Box' encryption)

---

<sup>⊕</sup> Contrary to the belief of some, code obfuscation is now a well established area of computer science. There are many academic papers, and a significant amount of research, in this area. A number of commercial companies specialise in this.

- How the dDRM software is protected against reverse engineering, modification, disabling *etc.* Techniques such as encryption of binary files, code signing, anti-debugging and anti-disassembling measures, code obfuscation, etc, must be used to prevent users from attacking the software. This must be incorporated into the design from the start – it's not something that can be tacked on later – the design itself must be resistant to attack.
- Protection against unauthorised copying (including screen capture) of the protected content.
- Prevention of access to the memory holding the content while it is open by an application.
- Encryption of the temporary files, produced during the course of using the content.
- Encryption of the system paging file (sometimes called the 'swap' file).
- Transparency of use, the more transparent a dDRM system is to the user, the less chance there will be of user errors. Ideally a dDRM system should have a mechanism to automatically and invisibly enforce document security from a central location.

All of these are areas of potential weakness in a dDRM solution. Most commercial dDRM solutions either ignore many of these aspects or implement them poorly.

 [info@avocosecure.com](mailto:info@avocosecure.com)

US: +1 415 839 9433

International: +44 207 851 6070

 [www.avocosecure.com](http://www.avocosecure.com)