



## **Adobe LiveCycle, DRM & LiveCycle Rights Management ES2**

### **Adobe LiveCycle**

Adobe LiveCycle consists of a series of products that seek to automate a number of business processes that interface with 'customers' who may be inside or outside the organization, leveraging existing Adobe PDF based technologies.

For business process aficionados, LiveCycle starts with forms (including bar code handling) and data assurance, provides a business process 'orchestration' engine (complete with a workbench), and content management with collaboration support.

But if you are looking at Adobe LiveCycle as a DRM management tool (either stand-alone or within the rather vaster architecture that Adobe LiveCycle brings with it, then you need to understand what is actually being managed by Adobe LiveCycle.

As the name suggests, AdobeLiveCycle is addressing the needs of an organization to gather and process data through the mediums of form-filling and printed/viewed results. Underpinning Adobe LiveCycle is the idea of controlled collaboration over both the forms and their attendant data, and the reporting and report distribution that are the obvious concomitant of the processing.

Whilst these functions provided by Adobe LiveCycle are important to the business processes of, say, capturing new customer information and automatically distributing it to all those areas of the corporation that might find that 'interesting' as a new sales target or opportunity, it is more difficult to see how the DRM controls match typical requirements in an information publishing environment where the recipients are not expected to be allowed to automatically process information.

So does Adobe LiveCycle provide the DRM controls that a book publisher might require, or the seller of private reports? Well, here the situation is more opaque.

### **Adobe LiveCycle Rights Management ES2**

Adobe LiveCycle Rights Management ES2 provides some controls over sharing information, but a magazine or an ebook publisher is not sharing their information with you so much as showing it to you – just like a newspaper – you buy it to read it, not to copy it into your computer and then do analysis on it or ship it on to friends and family. So the controls may not be well aligned to the requirement.

Also, whilst Adobe LiveCycle Rights Management ES2 does allow offline use of information, special provision has to be made, and a special record has to be set up with an end date, otherwise every single collection of information (the word document springs to mind, but in the brave new world it is really just a bundle of information) has to talk to an appropriate server every time it is to be used.

That is because the security policies governing use of the document are held on the server and not stored as part of the document itself. A publisher could



therefore not use Adobe LiveCycle Rights Management ES2 to protect an ebook if they wanted the user to view the ebook without having to permanently connect to a LiveCycle Rights Management ES server every time to view it.

With Adobe LiveCycle Rights Management ES2 you can control printing but that is limited to prevent or allow, but does not limit the number of copies. Controls allow for, copying content, form filling, dynamic watermarks, digital signature use, screen reader access, review and comment use, page insertion, deletion, rotation. You can control online and offline access, establish time controls for access, change usage or revoke rights after distribution and audit document usage.

You cannot, however, prevent screen grabbers from taking screen shots of sensitive documents, or prevent use in thin client/virtual environments (so once one person has authenticated, everyone in the company or external parties who have been given access to the virtual environment can view it).

### **LiveCycle Rights Management ES2 offline access**

Adobe LiveCycle Rights Management ES2 does have a feature for allowing documents to be used offline, but this must be setup as a limited 'lease' on the server for transfer to the client.

Because the document controls are held on the server and not in the document itself, letting a user view a document offline turns out not to be a very clever idea. Curiously, Adobe state in their own documentation about giving an employee offline use for 3 days, "Yet it helps ensure that if they share a protected document with an unauthorized user, it will automatically be unusable after three days of separation from the corporate network." Presumably, in other words, there is NO security during these 3 days since the only control preventing accessing the document is a username and password, which can be shared. Adobe recommend smartcard authentication as a solution... Perhaps that's why publishers are not buying into it?

Now this may not bother the corporate world, where everyone is always connected together, and everything is always on (we are assuming here that servers never fail because if they do since access is approved in real-time you will not be able to view your protected documents). So that is likely the target market for Adobe LiveCycle Rights Management, the corporate 'publishing' and corporate internal control system. And there is nothing wrong with that at all. It is a market that urgently needs to provide some very convincing answers as to how it protects PII (Personally Identifiable Information) if you are in the USA or personal data if you are in Europe (and yes, you guessed it, the rules are not identical).

Adobe LiveCycle Rights Management is something that offers some opportunities to show that access to, and sending on of data from within the organization can be restricted. And that could be a very important statement to make.

Adobe LiveCycle Rights Management however seems less useful for the corporate executive who either cannot open documents whilst on the plane or travelling (unless they have the lower control documents which are now easier to steal or give away).



But Adobe LiveCycle Rights Management does not act to bridge the gap between the internal organizational controls of the corporate, and the disparate third parties who often form the recipients of controlled information. And here the list becomes near endless. Controlling the ability of recipients to save, copy, print, screen grab, and scan without any detection is a much more difficult task than controlling internally held and processed information.

So Adobe LiveCycle Rights Management ES2 can be a very valuable architecture and toolset allowing corporations to architect the processes that interface with web based recipients and share information internally. But more specialist suppliers are needed when you need to approach DRM controls for information that is to be distributed to the wider audience.

## About LockLizard

LockLizard is a DRM (digital rights management) company that specializes in document security and copy protection for PDF, flash, ebooks, elearning, 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 stop copying, prevent printing, disable print screen, expire content, and instantly revoke access to information.

<http://www.locklizard.com>

[Safeguard PDF Security](#) and [Safeguard Enterprise PDF Security](#) provide PDF rights management, protecting PDF documents and files against unauthorized use and misuse both inside and outside the enterprise. They also provide persistent offline protection for publishers selling PDF content - PDF ebooks, reports, etc. without the use of passwords.