



OpenOffice.org & StarOffice DRM

Open Media Commons Workshop
March 15-16, 2006

Malte Timmermann
Technical Architect
Sun Microsystems GmbH

About the Speaker

- Technical Architect in StarOffice/OpenOffice.org Development
- Working on StarOffice since 1991
- Main focus: Core Development
 - > Accessibility
 - > Security (Digital Signatures. DRM soon)
 - > Performance
 - > Past: EditEngine, VCL, Help System, BasicIDE, ...

About this presentation

- Some general information about document protection
 - > Based on my best current knowledge, no DReaM specific things included
 - > Hope to learn here what Office Suite customers really need ;)
- Evaluation of potentialities, no concrete plans for StarOffice or OpenOffice.org right now!

Agenda

- What is StarOffice / OpenOffice.org?
- Why Document Protection?
- Permissions and Restrictions
- StarOffice / OpenOffice.org Solutions?
- Conclusion
- Q&A

What is StarOffice / OpenOffice.org?

- Integrated productivity suite with word processor, spreadsheet, presentation, drawing, database, ...
- Open Source
 - > StarOffice code base is available as OpenOffice.org under the LGPL license
- Multi Platform
 - > Sun supports StarOffice on Windows, Linux, Solaris
 - > OpenOffice.org available for more platforms
- Support for different languages
 - > CJK and CTL
 - > Right to Left and Vertical Writing

What is StarOffice / OpenOffice.org?

- Interoperable with MS Office documents
 - > Can read and write MS Office files
 - > Comparable feature set
- Native format is OASIS OpenDocument Format
 - > Open XML standard for documents
 - > ISO standardization is in progress
- Create (accessible) PDF files
 - > Tagged PDF, TOC, Hyperlinks, Controls
- Digital Signatures
 - > W3C DSIG, open standard

Why Document Protection?

- Content producers want to sell content and want to make sure that it's only used by customers who paid for it
 - > Ebooks (as well as Music, Movies, ...)
 - > Avoid free distribution / piracy
- Companies want to protect their documents so that they can only be read by authorized people
 - > Confidential information
 - > Avoid unauthorized usage

Different Scenarios

- Content sellers often don't know much about their customers
 - > User authentication is quite difficult
 - > *No trust in user (customer)*
 - > They trust more in certain applications
 - > They lock the content to these applications
 - > Even to certain devices!
 - > Customers don't like this strong restrictions for paid content!
 - > What happens if I buy new devices?
 - > What happens if the content provider / licensee goes away?
 - DRM == Digital *Restrictions* Managements ;)

Different Scenarios

- Companies know their employees
 - > User authentication is quite easy
 - > Companies (should) trust their employees
 - > User authentication is enough, no locking into certain software necessary
 - > Use any device or software!

Document Protection Basics

- Encryption
 - > Content is encrypted
 - > Key distribution necessary
 - > Encrypted within the data file
 - > Encrypted within separate license file
 - > Licensing Server (Authentication and key exchange)
- Security can be enhanced with using a “Trusted Platform”
 - > This need TPM and the full stack of hard/software, signed applications
 - > Hard to achieve, but without that people with permission to open the file have a good chance to remove protections

Document Protection Key Distribution

- Public Key Infrastructure (PKI)
 - > Deploy document decryption key within the media file or an external license file
 - > Decryption key itself is encrypted with the users public key, only this user can decrypt it with his private key
 - > Can be provided for multiple users
 - > Advantage:
 - > No complex server infrastructure needed, use existing PKI
 - > Disadvantages
 - > Needs modification of media file on each distribution, or distribution of separate license files
 - > No rights revocation possible after file is deployed
 - > No document time-out possible

Document Protection Key Distribution

- Rights Management or Licensing Server
 - > Keys and rights are managed on server
 - > User is authenticated by some server, software receives decryption key from server
 - > Advantage:
 - > Dynamic rights managements, access rights can be changed any time after document deployment
 - > Can also be done role based, roles can changed any time
 - > Time-out for documents possible
 - > Document always remains the same
 - > Disadvantages
 - > Complex server infrastructure with secure key exchange needed

Permissions and Restrictions

- Licensing Server and PKI can only guarantee the basic permission, if the user is allowed (able) to open the document
 - > Time period can be used on key request with licensing server
- Restrictions like “can't print, save as, ...” are only application logic, cannot be enforced by any server!
 - > Application can be modified to not apply restrictions
 - > **Restrictions may lock out Assistive Technology!**
- Trusted Platform is needed for full security
 - > But what is with the “Analog Gap”? User can still copy...

StarOffice/OpenOffice.org Solutions ?

- Preconditions:
 - > We have an Open Source Client, which can be modified by anyone
 - > We don't want to lock the user into certain environments
 - > (Currently) no trusted platform and signed applications, so only basic permissions possible
 - > We might offer the “Restrictions” as a convenience feature, but it must be clear that the software can quite easily be modified to ignore the restriction
 - > But even this might fit the needs of companies for 'inhouse usage', policies can do the rest

StarOffice/OpenOffice.org Solutions ?

- Key Distribution
 - > PKI based solution?
 - > This might be a convenient solution for personal usage, to protect private documents or to pass encrypted documents to certain people without the need of key distribution
 - > Server based solution?
 - > This is what companies need for their internal documents
 - > No special protection against software modifications should be needed for internal documents
 - > Do we really need DRM then?
 - It might help for managing document life cycle and for protecting stolen or leaked documents
 - > Wouldn't a Document Management System be the better solution here?

StarOffice/OpenOffice.org Solutions ?

- Platforms for server based solution
 - > Open Rights Management solution?
 - > Not existent right now, but this is the preferred way to go
 - > Adobe Lifecycle Server?
 - > Server support for multiple platforms, including Solaris
 - > Microsoft Rights Management Server?
 - > Only Windows
 - > But might be needed for migration projects or heterogeneous environments

StarOffice/OpenOffice.org Solutions ?

- Should OpenOffice.org & StarOffice be able to load DRM protected MS Office documents?
 - > Only possible if user authentication is enough
 - > Be aware – that makes it much easier for people to remove MS document restrictions!

Conclusion

- For private use, the PKI solution just for document encryption could be nice
 - > But that is not DRM
- StarOffice might support different DRM systems
 - > But it doesn't help much to protect only StarOffice files, DRM for all used file formats would be needed in a company
 - > We must make sure to not lock out Assistive Technology!
 - > People can still use the “Analog Gap” for copying the content
- What about using Document Management Systems instead?
 - > StarOffice and OpenOffice.org should have good support for and integration with Document Management Systems

Q/A



OpenOffice.org & StarOffice DRM

Malte Timmermann

Malte.Timmermann@sun.com