



Open these sticky notes to read the speaker narrative.

Reducing Risk with Document Security

Bryant Bell

Marketing Manager
Adobe Systems Incorporated
mmiddlet@adobe.com

Rick Borstein

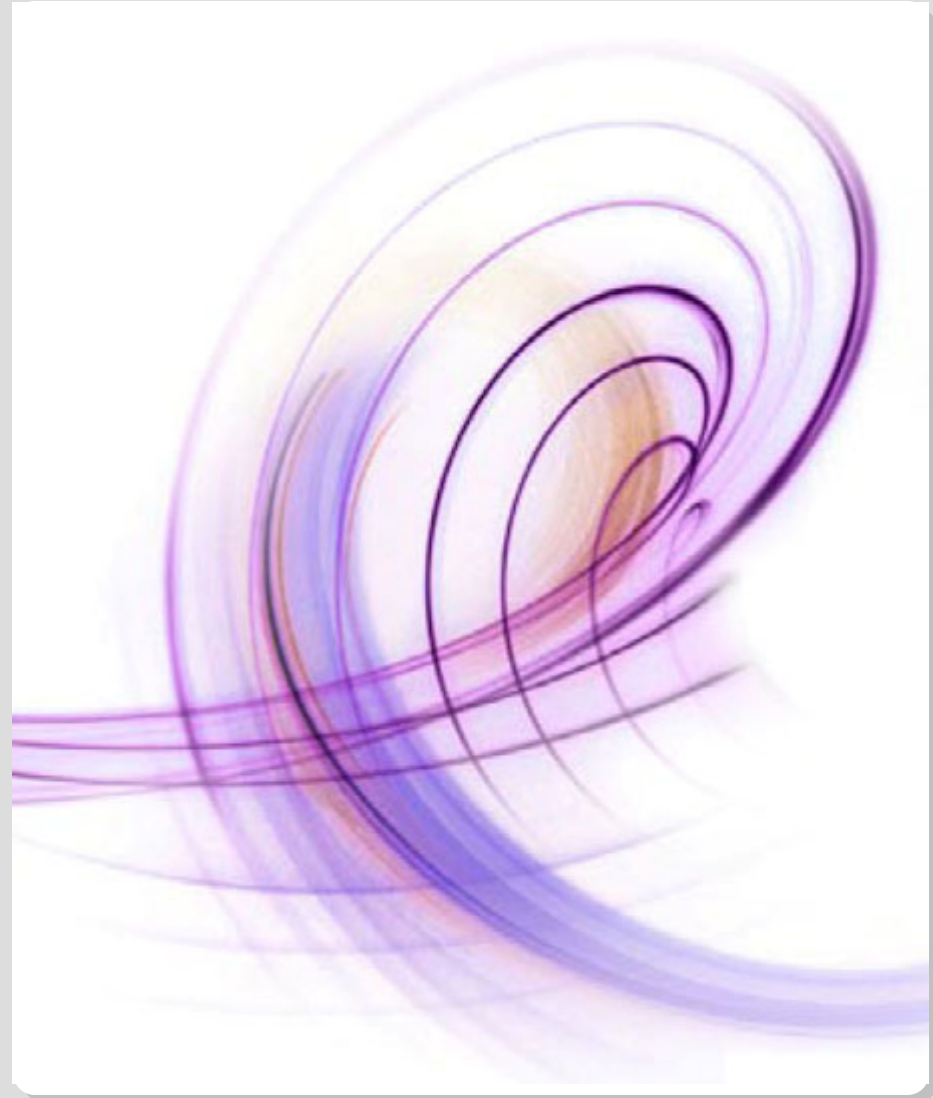
Business Development Manager
Adobe Systems Incorporated
borstein@adobe.com





What we'll cover . . .

- Background Slides
- Acrobat Security Methods
 - Passwords (demo)
 - Policies (demo)
- Removing Sensitive Information
 - Redaction (demo)





Document Sharing Risks

... involves **exchanging** sensitive information both internally and externally

Failure to follow proper **document security processes** can lead to ...

Theft of work product

Contracts, agreements ...

Accidental disclosure of information

Metadata, Improper Redaction, Hidden Info

Unauthorized disclosure of confidential information

Your document opened by the wrong party

Qualities of a Secure Document Solution

- Confidentiality
 - Who can access it?
- Authorization
 - What can they do with it?
- Accountability
 - What have they done with it?

**Digital Rights
Management**

- Authenticity
 - Where did this data come from?
- Integrity
 - Has it been tampered with?

**Digital
Signatures**



Adobe offers a variety of information security solutions



Password Best Practices

Good Password Practices

- No proper names or place names
 - Rick
 - Chicago
- No representative numbers
 - e.g. 062079 (June 20, 1979)
- Good passwords are . . .
 - Combinations of letters, numbers and other characters
 - At least eight characters
 - e.g. nMX8Yti6#
- Compromise for recall
 - e.g. play73maple

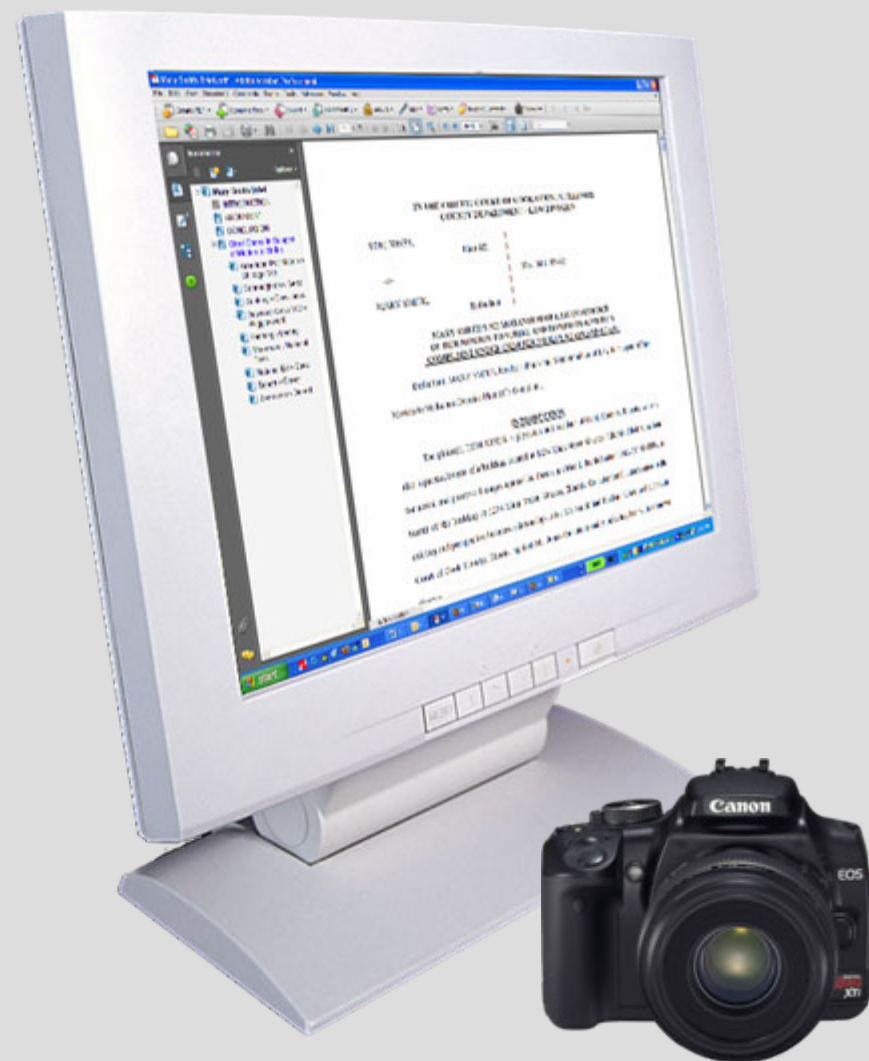
Communicating Passwords

- Never email a password to a client
- Communicate the password over the telephone
 - Instruct your client to memorize the password.
 - If the client forgets the password, they can always contact you via telephone.
- Never write down passwords



Security Issues

- Absolute Security is a Myth
 - Goals
 - Keep honest people honest
 - Make it hard for bad guys
- Once the document is open ...
 - Screen or image captures are possible
 - Time-consuming to reconstruct documents
 - Alternative?
Don't give out the document

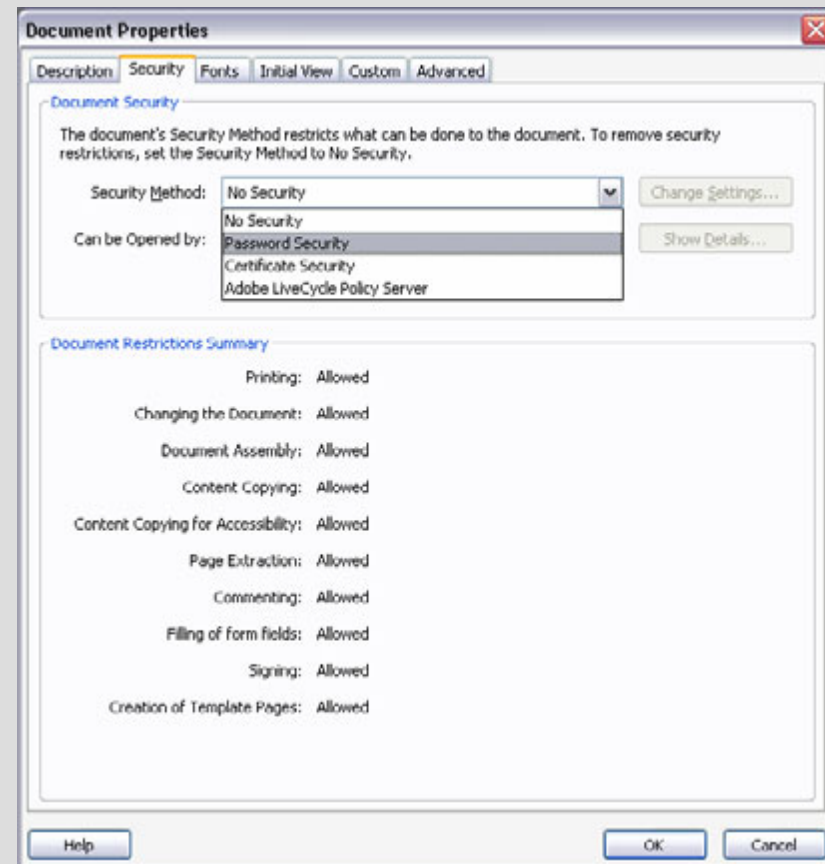


Original monitor image © 1997-2007 Hemera Technologies Inc., a wholly owned subsidiary of Jupiter Images Corporation. All Rights Reserved



Acrobat Security Methods

- Password Security
- Adobe LiveCycle Policy Server (Adobe Document Center)
- Certificate Security





Acrobat 8 Password Security

How can I make sure only someone with the right password can open the document?

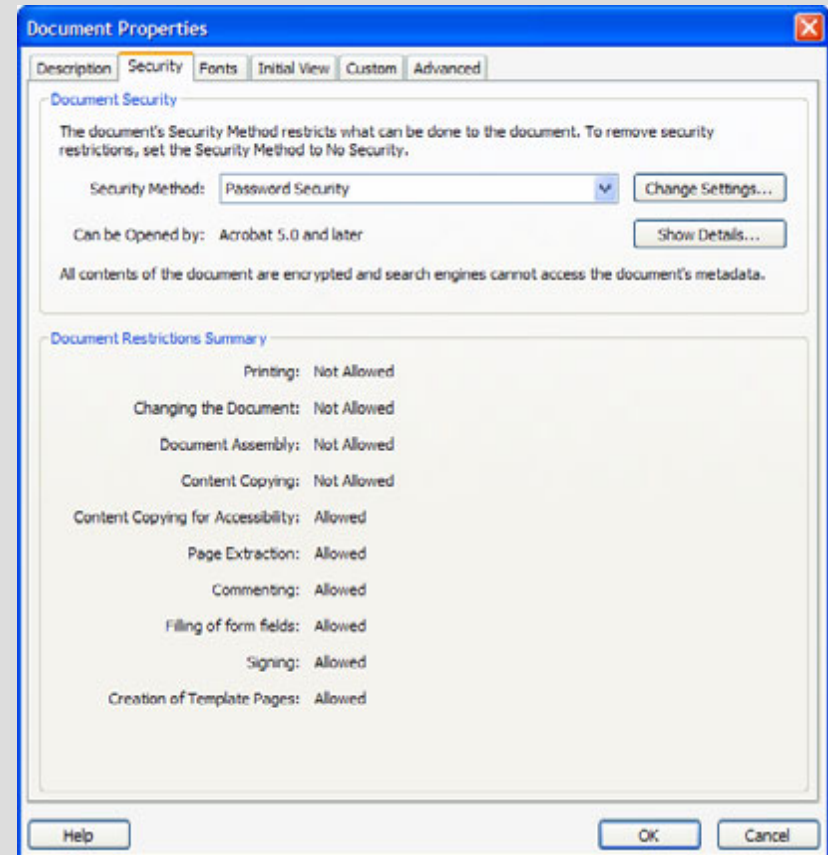
How do I prevent someone from printing a document? If they do, how can I include a watermark on the printout?

How do I prevent someone from copying text from a document?



Using PASSWORD security, learn how to . . .

- Check the security of a PDF
- Remove security
- Create a password-based security policy to:
 - Set an open password
 - Limit copy, print and other document operations
 - Watermark documents when printed
- Securely send several files using a Security Envelope





Password Security



Policy-Server Security

How do I revoke access to a document even after I've sent it?

How do I find out what the recipient has done with the document?





Policy Server-Based Security

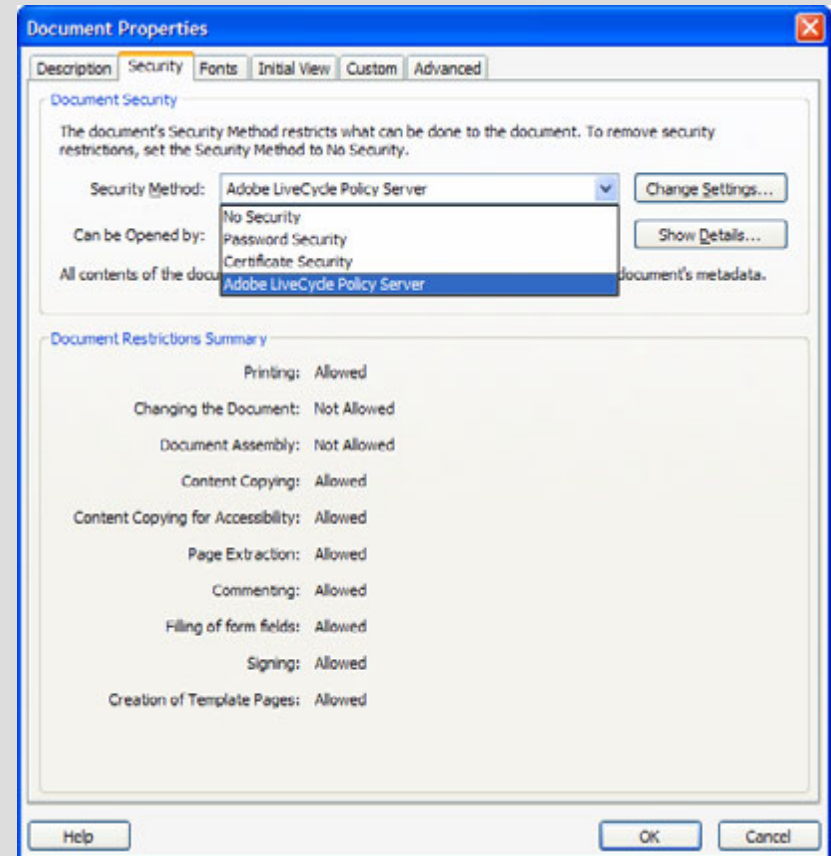
- Rights are managed on a server
 - Documents “phone home” when opened
 - Enhanced security
- Change security on a document even after you’ve sent it
- To apply security
 - Buy Adobe Policy Server — or —
 - Subscribe to the Adobe Document Center for \$19.95 per month
- Recipients do not need to pay





Using Adobe Document Center/Policy Server security, learn how to . . .

- Apply security to . . .
 - Control who can open a document
 - Control what they can do with it
 - Revoke a document
 - Expire a document
- Audit document usage
- Change policies after distribution





Policy Server Security



Removing Sensitive Information with Redaction Tools

How do I remove information from a document so I can be sure that it is safe to send?





Redaction