

PDF/H and Security in Adobe Reader

Reader acts to enforce and obey the security settings on a file. It doesn't allow for addition of permissions or modification of permissions. This table provides a matrix of functionality and whether it's available in Acrobat and Reader.

	Acrobat	Reader
Secure Docs	Y	N
Open Secure Docs	Y	Y
Sign/Certify Docs	Y	N*
Verify Signatures & View Integrity Info	Y	Y

* *UR/RE Only*

Reader won't allow modifications of security settings to either secured or unsecured PDF files. Reader will enforce all encryption-based permissions or policies for viewing, printing and modification* (*for modification see Usage Rights below).

Encryption and Document Permissions

- Password - when opening one of these files Reader will request a password
- Public/Key/private key - If you have the private key that unlocks the particular document, Reader will allow you to see the document. Public/Private Key distribution is currently outside the scope of most public-facing applications in the US. These types of applications currently have much more applicability in Europe, where key infrastructure and certificate deployment programs are tied to national ID initiatives. Users of Reader may, however, generate their own certificates and keys ad-hoc to allow parties that send them information confidentially. You can create a digital ID in Reader, and distribute the public key. You can do so by going to the Document menu and clicking on "Security Settings". So, hypothetically someone using Adobe Reader could create a certificate and send the public key to their doctor. The doctor would have to have Acrobat or another writer application in order to secure the document. This scenario is unlikely since most users know little about certificates. It's potentially more likely between Medical Professionals than it is between doctors and patients.

Certificates and Digital Identities

Reader will allow users to create or import digital identities for use in PDF signatures. Self-signed credentials (see Encryption and Document Permissions above) can also be used to sign documents. Reader can import digital IDs from the Windows Certificate Store (on Windows) or via standards based interfaces like PKCS#11 & PKCS#12 for smartcards and tokens, or software certificate files. Reader enforces authentication to these credentials as appropriate.

Digital Signatures

- Reader will allow you to verify the integrity of a digital signature but will not let you sign documents. (Except in the case of Reader Extended files, see below). Signature creation (with Usage Rights only) and verification in Reader is full-featured and includes performing of full certificate path building and validation, verification of certificate revocation information, verification of secure time-stamps, document integrity checking – and the ability to detect modifications between signatures and display this information to the user. Reader accepts and enforces the use of signature field-based parameters for signing in PDF documents (seed values).

Certification

- Reader will allow you to verify the integrity of a certifying signature, but will not let you certify documents. Reader will also obey any restrictions placed upon the document by the certifying signature. Reader will detect and display any available information about the nature of the content

to be signed – dynamic content, form fields, annotations – and inform the user of potential implications of signing dynamic content.

Usage Rights

PDF Usage Rights (PDF Ref v1.6; section 8.7 “UR” - commonly referred to by the Adobe “Reader Extensions” product name) allows a viewing application (such as Adobe Reader) to enable or permit additional functionality on a per-document basis. Some features, like the saving of changes to secured files, can be enabled in viewing applications through the use of UR functionality. With regards to security, UR enabled documents will allow users to apply digital signatures in Reader. They will not however allow for Certification or encryption within Reader.