



protectedpdf™

Powered by
Vitrium systems™

	Reader	Protectedpdf Server	Customer Database (External Identity Provider) ¹	Distribution/ Fulfillment System
Operating System	Windows 98/2000/XP/ Windows 7 Linux Solaris Mac OS AIX HP/UX	Windows 2003 Server Windows 2008 Server	Any	Any
Application/Software	Adobe Reader 6.0.1 (or newer) Adobe Acrobat Standard 6.0.1 (or newer) Adobe Acrobat Professional 6.0.1 (or newer) Foxit Reader 3.2	ISS 6.0/ISS 7.0 .Net 3.0/.Net 3.5	Any	Any
Data Store	Adobe Cookie Container ²			
Information Store		Document Published Document Settings Communication Settings Audit Logs Physical Protectedpdf Files	Customer Credentials Document Access Rights by Customer Customized Audit Logs	Physical Protectedpdf Files
Protocols (Ports)	HTTP (80)/HTTPS (443)	HTTP (80)/HTTPS (443) SOAP	HTTP (80)/HTTPS (443) SOAP	Any

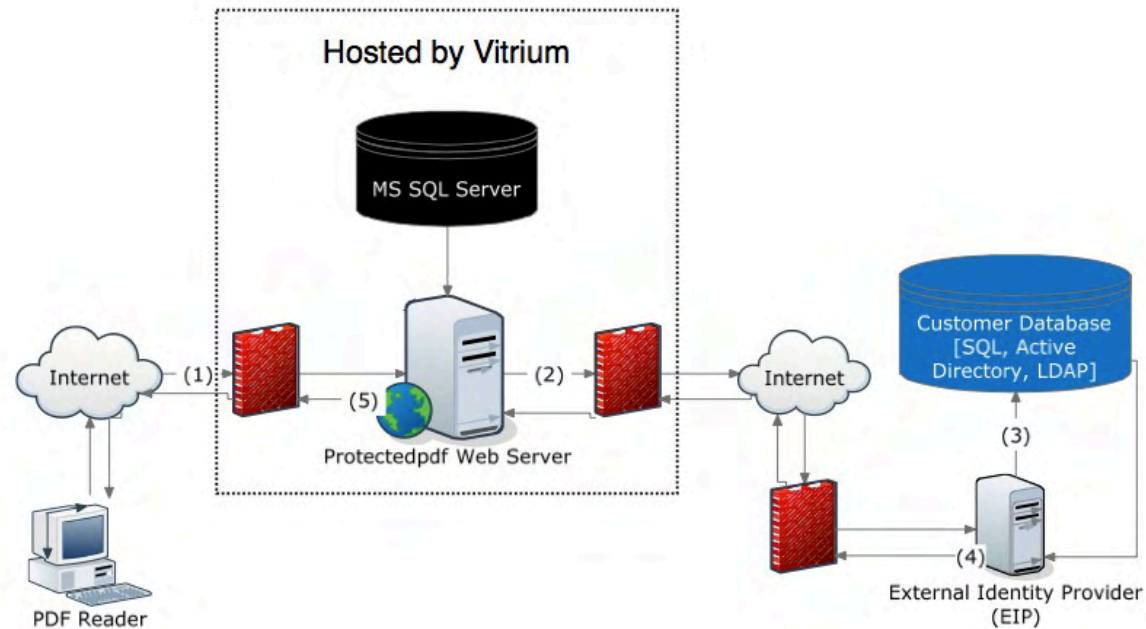
¹ Customer Database needs to implement web services specifications as described in protectedpdf External Identity Provider Kit (source code available)

² This is different from where Internet Explorer cookies are stored

Contact a Sales Representative:
866.403.1500

Protectedpdf - Powered by Vitrium
www.protectedpdf.com

Protectedpdf Deployment - Hosted By Vitrium



(1) The PDF Reader enters their login credentials into the protectedpdf in-document logfin page, including a user identifier, defined by the PDF's owner (username, email, serial number, etc.) and a password. The password is transferred using challenge response, such as a SHA1 hash. This information, along with the IP address, machine GUID (used to uniquely identify a computer) and the document ID is sent to the protectedpdf server.

(2) The protectedpdf web server determines whether the document has been retired, if so a message is relayed to the PDF reader. If it has not

been retired, the protectedpdf web server packages the information from the protectedpdf document as an Authentication context and transmits this to the PDF owner's External Identity Provider (EIP) web service. This constitutes all the information required to make the decision whether to grant access to the protected content.

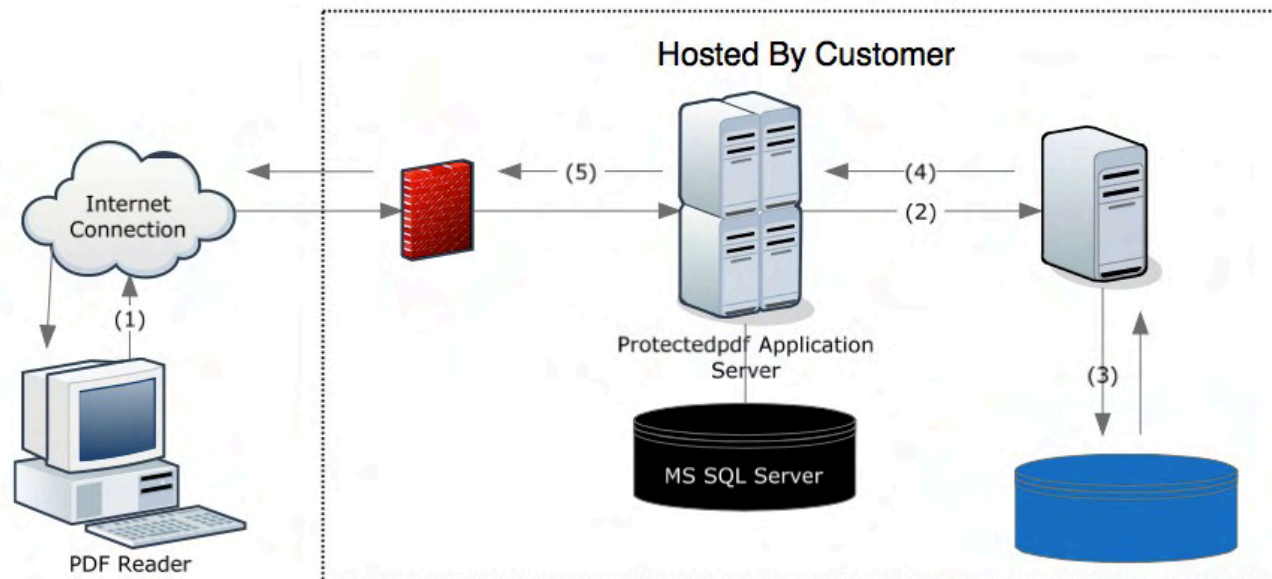
(3) The EIP analyzes the authentication context. It may need to communicate with the Customer Database to validate the credentials. When a password is entered by the PDF Reader, the hash is reproduced to verify PDF Reader identity. The PDF

Owner is free to define any business rules based on the Authentication Context in order to grant access to the document.

(4) The EIP delivers the final access rights to the protectedpdf web server. This can include a range of controls, such as offline access and watermarking. Custom alert messages can be relayed to the PDF Reader also.

(5) The protectedpdf web server processes the decision delivered by the EIP and instructs the protectedpdf document to perform the required actions.

Protectedpdf Deployment - Hosted By Customer



(1) The PDF Reader enters their login credentials into the protectedpdf in-document logfin page, including a user identifier, defined by the PDF's owner (username, email, serial number, etc.) and a password. The password is transferred using challenge response, such as a SHA1 hash. This information, along with the IP address, machine GUID (used to uniquely identify a computer) and the document ID is sent to the protectedpdf server.

(2) The protectedpdf web server determines whether the document has been retired, if so a message is relayed to the PDF reader. If it has not been retired, the protectedpdf web server packages the informa-

tion from the protectedpdf document as an Authentication context and transmits this to the PDF owner's External Identity Provider (EIP) web service. This constitutes all the information required to make the decision whether to grant access to the protected content.

(3) The EIP analyzes the authentication context. It may need to communicate with the Customer Database to validate the credentials. When a password is entered by the PDF Reader, the hash is reproduced to verify PDF Reader identity. The PDF Owner is free to define any business rules based on the

Authentication Context in order to grant access to the document.

(4) The EIP delivers the final access rights to the protectedpdf web server. This can include a range of controls, such as offline access and watermarking. Custom alert messages can be relayed to the PDF Reader also.

(5) The protectedpdf web server processes the decision delivered by the EIP and instructs the protectedpdf document to perform the required actions.

**Thank-you for contacting
Vitrium Systems.**

**A Sales Representative will be in contact to
answer any questions and provide you with
more information about protectedpdf.**

For immediate assistance, please call:

1-866-403-1500

1-604-677-1500

Vitriumsystems™