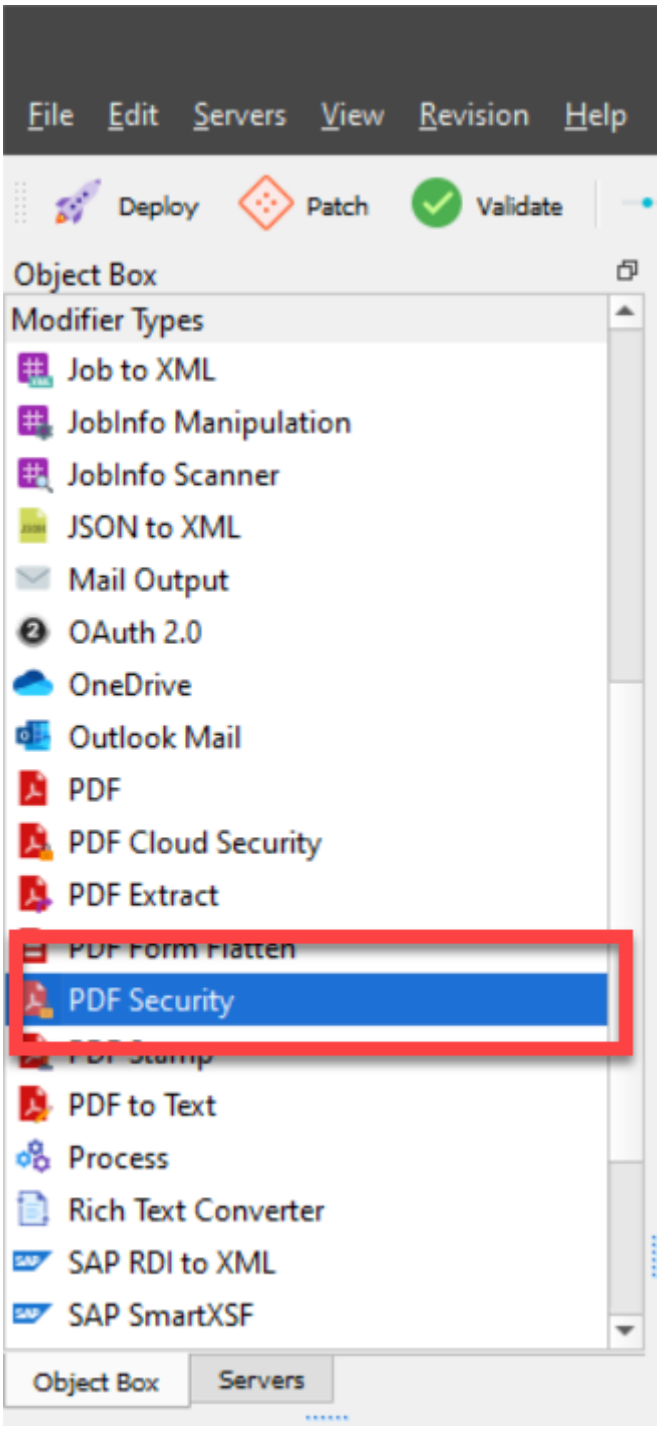
How does the Lasernet PDF Security Modifier work?

Mikael Wängelin - 2023-11-17 - Comments (0) - Lasernet FAQs

The Lasernet PDF Security Modifier is an optional add-on for Lasernet that can be used to encrypt and sign generated PDF documents.

Accessing the modifier properties

1. All modifiers can be found by opening the **Modifier** menu located at the bottom left of an open Lasernet build. This will display a list of all available modifiers and all modifiers currently used in the build in the Object box.



2. To open the *Modifier* properties, drag and drop the PDF Security modifier onto the main area.

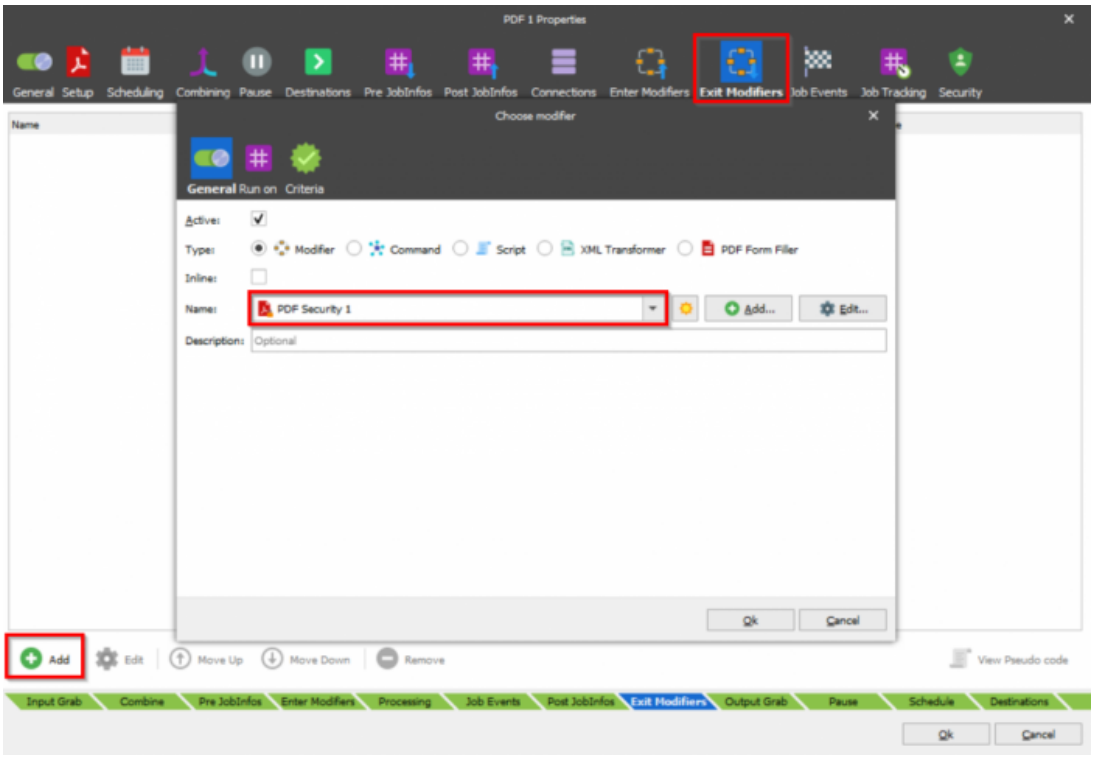
Adding the modifier to the build

After setting up the modifier properties, the modifier needs to be added to a PDF engine module. To do this, follow these steps:

1. Open the PDF engine properties and click the **Exit Modifier** tab.

2. Click **Add** to display the *Choose modifier* window, then select the **PDF Security**

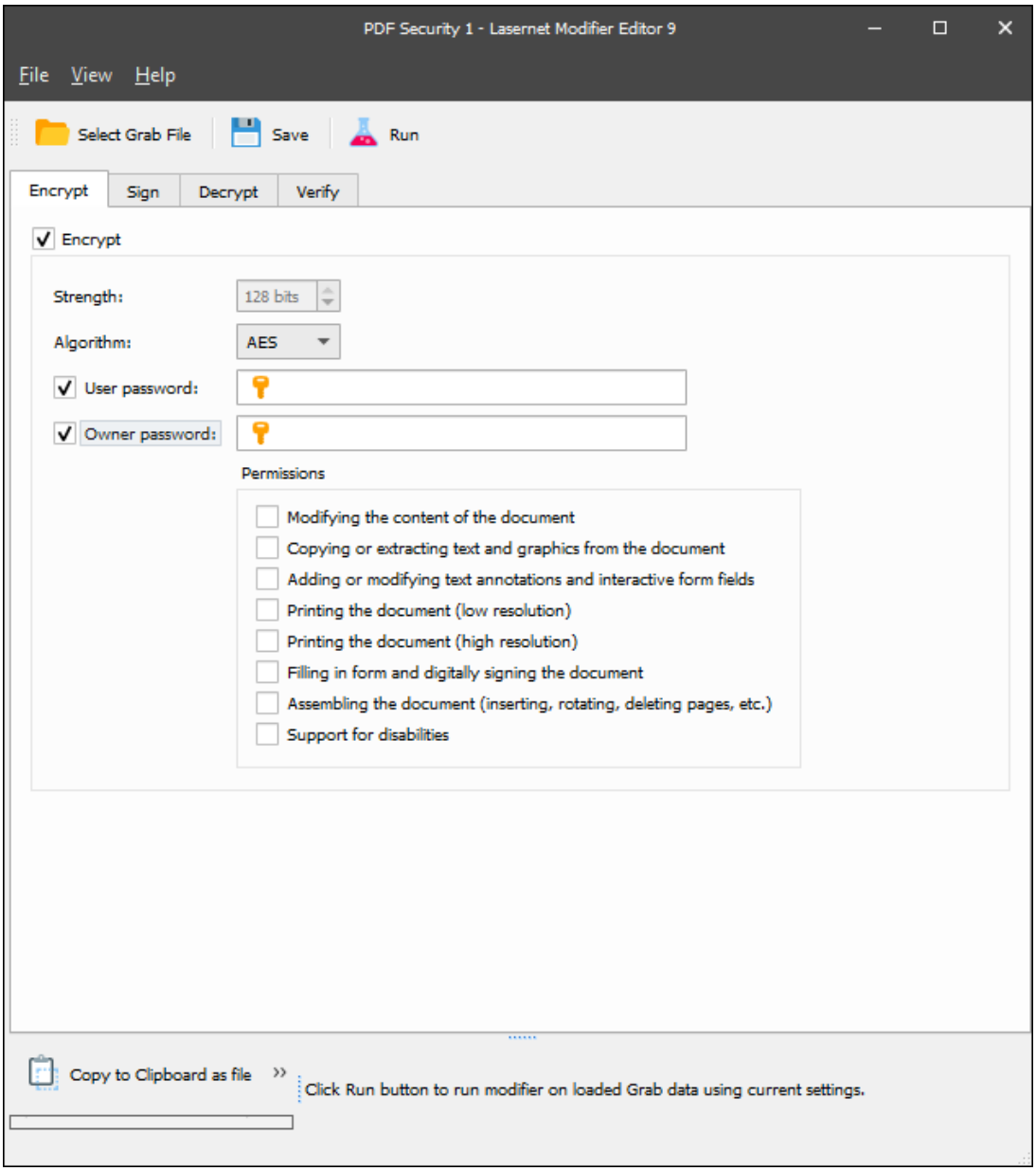
modifier created previously. This modifier needs to be added as an exit modifier, as LASERNET can only encrypt or sign the PDF after it has been created.



Encryption

Using PDF encryption allows for generated PDF documents to be secured with a designated password. The user accessing the document can also have actions disabled or enabled by setting the correct permissions.

Encryption is not allowed in conjunction with PDF/A and must not be enabled in the PDF engine, otherwise an error will appear in the Lasernet Monitor and the data will not be processed.



When encrypting there is a choice between two algorithms, *RC4* and *AES*.

RC4

- Supports key lengths from 40 to 128bits.
- Supported in PDF 1.1 and Acrobat Reader 2.0 and above.
- This algorithm has known vulnerabilities that make it less secure than AES and should only be used for backward compatibility with earlier versions of Acrobat Reader.

AES

- Supported key length of 128 bits only.

- Supported in PDF 1.6 and Acrobat Reader 7.0 and above.
- This is the recommended algorithm when backward compatibility of older versions of Acrobat Reader is not required.

Passwords

Two passwords can be defined when using encryption, a user password and an owner password. Accessing a document with a user password will allow the user to read the document and also use the actions that Lasernet Developer has allowed. Using an owner password to access the document, will give the user full rights and permissions.

For more information on how to password protect PDF files, please see this support article, How to password protect PDF files.

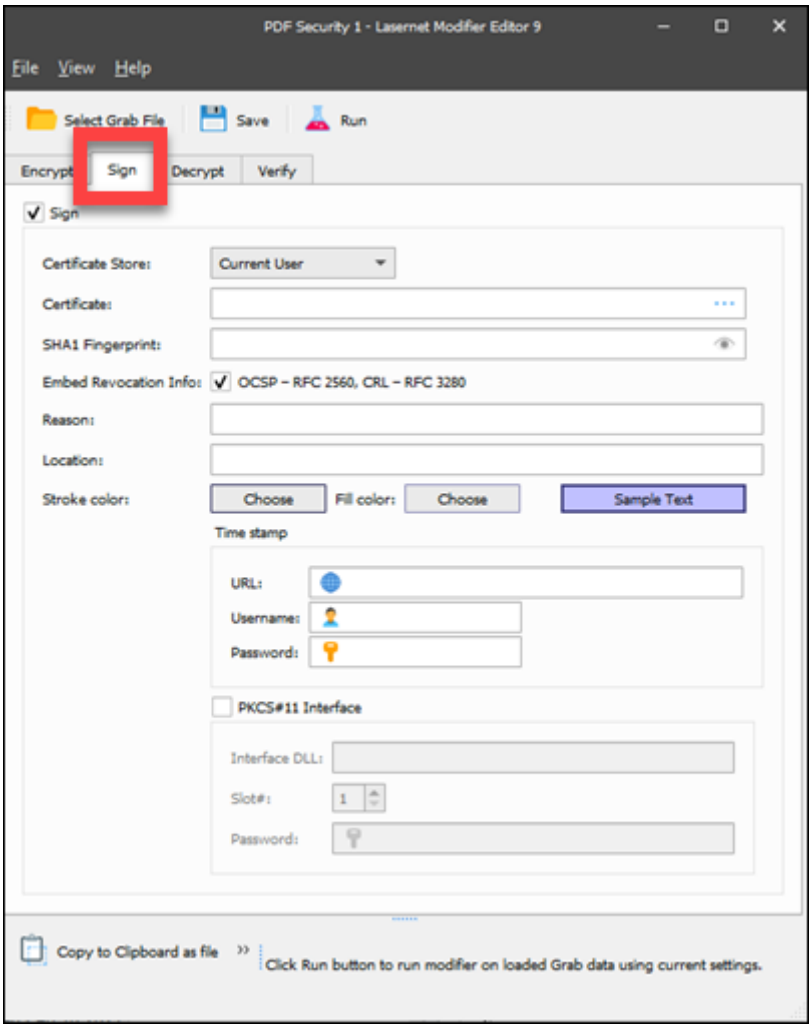
Permissions

When opening a file with a user password, the possible actions a user can take are defined here.

Sign

By signing your PDF using a digital certificate, you allow the recipient to verify both the origin and the integrity of the document. This means that the recipient is able to verify that the document came from your organization and has not been changed since it was created.

Digital signatures are supported since PDF 1.3 (Acrobat Reader 4.0) and are allowed in conjunction with PDF/A.



Certificate

Select whether the certificate is located on the Local Machine or for the Current User account. In order to sign the PDF using a digital signature, you must have a valid and appropriate certificate installed for the user account that the Lasernet service is running under.

- Lasernet 7.6 supports a maximum key length of 1024 bits. In version 7.6 you will be able to view all installed certificates, but if the certificate used is larger than 1024 bits, the data will not be processed.
- Lasernet 7.7 and above supports a maximum key length of 4096 bits.

Installed certificates must also have their key usage property set to Digital Signature and be located in the personal certificate store of the service user.

Reason

The Reason field allows you to enter a text string that will be displayed when viewing the signed PDF.

This provides a visual representation of the signature to the user, you can also select the

text and background colour for the text field.

Location

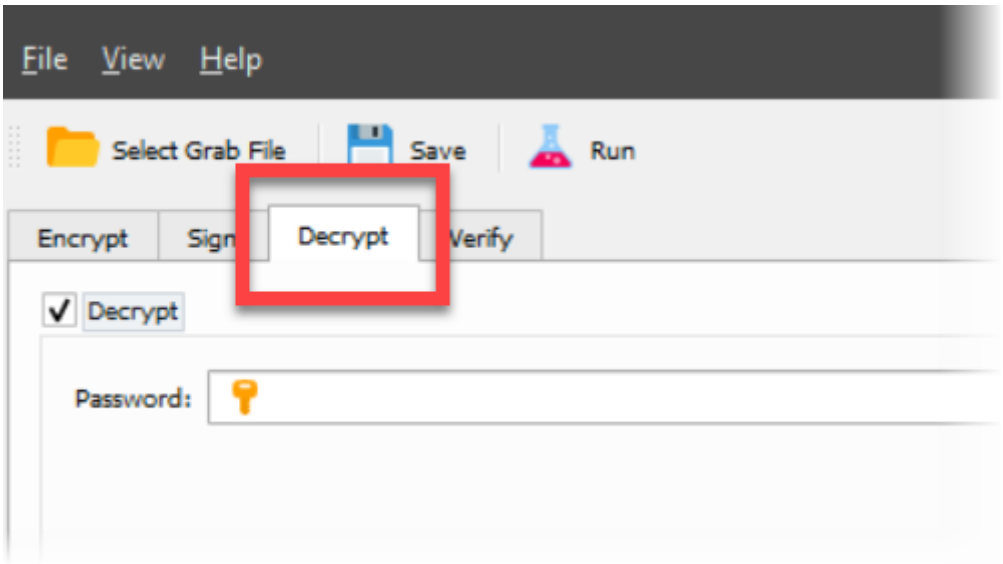
The physical location where the signature is added for example “Foxton, Cambridge”. If this property is set to an empty string no entry is created.

Timestamp

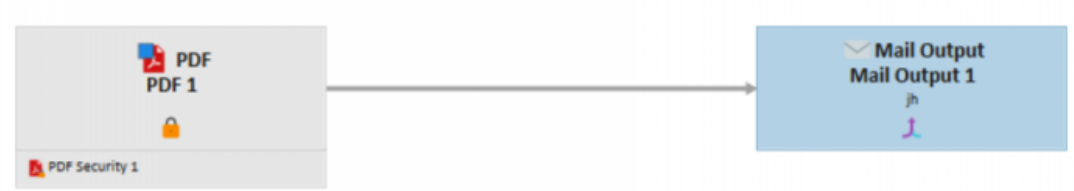
By signing your PDF with a timestamp provided by a trusted source, you can make sure that the PDF will still show a valid signature after your certificate expires. If you choose not to timestamp your PDF, the recipient will receive a warning that the certificate used to sign the PDF has expired.

Decrypt

If you need to decrypt and remove a password from an already encrypted PDF, you can use the **Decrypt** option. It’s best to create another PDF security modifier that only has decryption enabled and using either the user or owner password that has already been set, to decrypt the file.



In the example shown, an encrypted PDF is added with the owner password set to ‘efs’ and the decrypted password in the modifier set to ‘efs’ as well. When the document is processed, it will then output a decrypted PDF file.



Verify

By using a verification password, it allows you to verify the signature of an incoming PDF.

Supply the password when using a certificate to sign the document and it will validate against it to check that it has not been tampered with or altered.

The result of the validation will be stored in the PDFSignatureValid JobInfo.

This is the opposite of the Sign function. When it is given a digital signature it will check this against the signature of an incoming document. This will allow Lasernet to verify the document's source.

Testing

From version 9 of Lasernet testing can be performed within the module. This allows the user to test the output produced from a PDF.

The following steps must be performed:

1. Select the **Grab file** and choose a PDF file.
2. Click **Run** to apply the modifier.
3. Use the **Save** button to save the output PDF to another location to check.