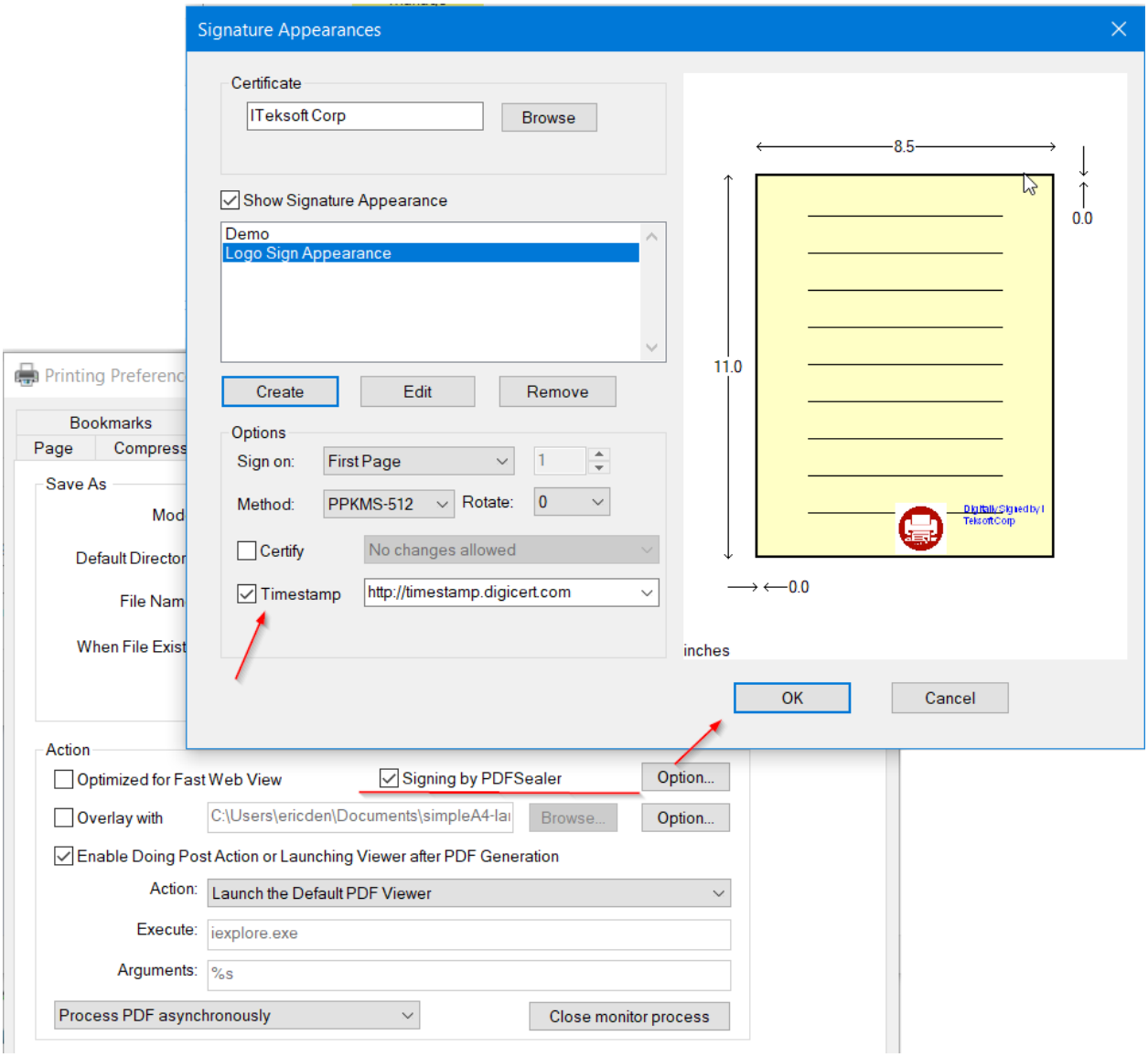
When digital signing PDFs, users need a certificate with private key, which can be a self-signed created by PDFSealer directly too. For document interchanging, users may need certificates issued from trusted CA (Certificate Authority).

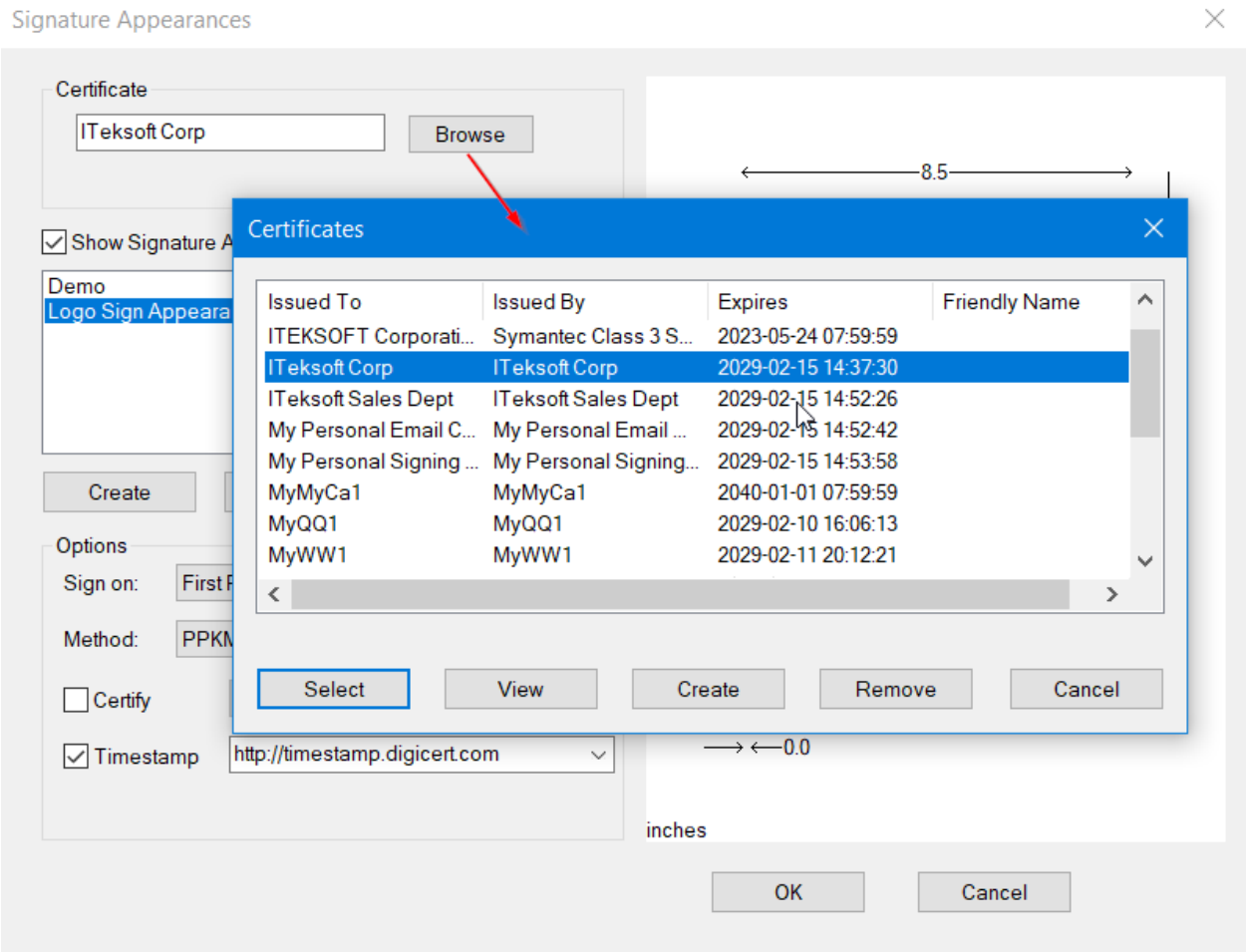


The main advantage of applying a PDF signature is that it allows a user defined signature appearance added onto the existing PDF. The reader will verify the signature and show the result on the appearance directly. This way gives an intuitive and straightforward way to authenticate and verify the digital signatures. Users can also apply invisible signatures on the PDF by disabling showing signature appearance. Such signatures can also be verified and viewed by the Acrobat Reader signature properties.

To add a trusted timestamp when digitally signing the PDF file, please turn ON the option [Timestamp] as illustrated in the Signature Appearances dialog. When enabled, it will send a request to the public Time Stamp Authority (TSA) server specified to countersign the digital signature with the time information stamp issued by the trusted server. It requires an internet connection to the public Time Stamp Authority (TSA) server when requesting the timestamp. The default timestamp server is set to http://timestamp.digicert.com. Other Time Stamp Authority (TSA) servers compliant with RFC 3161 are also supported.

The registry settings and embedded commands DestSignTimestamp and DestSignTSAServer are added for the corresponding UI options for enabling adding timestamps and the URL of the Time Stamp Authority (TSA) server.

PDFSealer uses Windows native certificate management for browsing and selecting certificates. Users can select any existing Windows certificate with private key to sign the PDF. If users do not have a proper certificate available, users can create a self-signed certificate directly by the [Create] button in the Certificates dialog. Users can view the details of the certificate by double clicking the certificate or click the "View" button. Those certificates without private key will not be shown in the list because such certificates are used for verification and authentication, not for signing.



When editing the signature appearance, users can adjust the width and height and change the relative position by the position attributes on the dialog. Users can also import an image for showing the scanned signature or other related graphics. In the reason and location, users can add the text for annotation to be shown on the PDF signature.

A signature will be invalidated if users modify or change the content of the PDF file. Users can append or apply extra signatures to the same PDF by incrementally updating. When PDF is modified by incrementally updating, existing signatures are still valid. Just the validity of those signatures implies only their corresponding versions of PDF are unchanged. Users can use the function in PDF reader to view the proper version of content signed.

Key Name	Value (String)	Purpose	Availability		
			UI	Command	Version
DestSignEnable	True/False	Enable signing the PDF created by calling PDFSealer.	V	V	
DestSignCertName		The certificate name selected to use to digitally sign.	V	V	
DestSignCertStore		The certificat store name. The default is the current user certificate store.		V	
DestSignShowAP	True/False	When True, it will stamp the appearance define when applying the digital signature.	V	V	
DestSignAPName		The signature appearance name defined in the signature appearance dialog.	V	V	
DestSignPageNum		The page number of the PDF where the signature appearance will be stamped. Page number starts from 1. –1 means the last page. –2 means all pages. –3 means odd pages. –4 means even pages.	V	V	
DestSignRotateAP	0/90/180/270		V	V	
DestSignFilterMethod	0/1/2/3/4	0: PPKLite SHA-1 (with legacy valid check symbol) 1: PPKLite SHA-1 2: PPKLite SHA-256 3: PPKLite SHA-384 4: PPKLite SHA-512	V	V	
DestSignCertifyMethod	-1/0/1/2	-1: Do not certify 0: Certify the PDF wth no changes allowed. 1: Certify the PDF wth allowing form fill. 2: Certify the PDF wth allowing annotation and form fill.	V	V	
DestSignTimestamp	True/False	Enable adding a timestamp countersigned by the TSA server specified.	V	V	Ver 9
DestSignTSAServer		The URL of the TSA server. The default is http://timestamp.digicert.com	V	V	Ver 9