

Configuration of Adobe Acrobat 9 According to ETSI TS 102778 (PAdES)

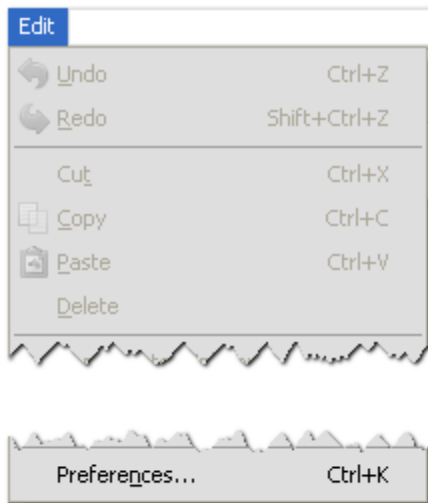
Background

The European Telecommunication Standards Institute (ETSI) recently published Technical Standard (TS) 102778 – Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signatures (PAdES). It is a five part standard that proscribes various technical considerations for both PDF files as well as conforming readers and writers of these files, such as Adobe’s Acrobat and Reader products. Part 2 of the TS specifically addresses how existing products that support ISO 32000-1, such as Adobe Acrobat 9, should sign and verify PDFs.

This document sets out to describe how preferences should be set in Acrobat or Reader 9 to ensure compliance with the standard. While screen shots and descriptions in this document are from Adobe Acrobat 9 Professional on Windows, all of the material presented also applies to other versions of Acrobat 9 as well as Adobe Reader 9 on the various OS platforms on which they are available.

Setting Preferences

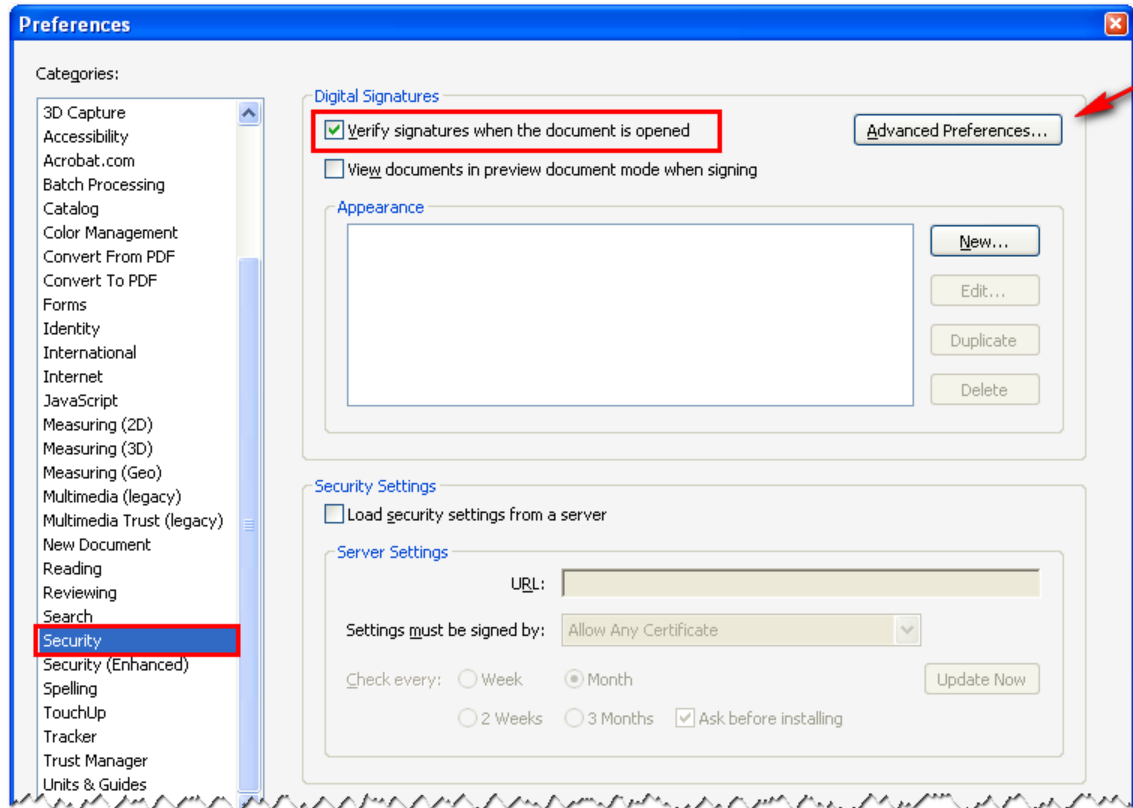
To access the preferences dialog in Acrobat, choose **Preferences** from the **Edit** menu or type Ctrl-K (cmd-K on the Macintosh).



Preference Dialog

When the preferences dialog appears, select **Security** from the scrolling list on the left hand side of the dialog (see screenshot below).

Although it should already be checked, make sure that the “*Verify signatures when the document is opened*” checkbox is checked. This will ensure that when a document is opened, the signature panel and signature status bar will correctly display the status of any signatures in the document.

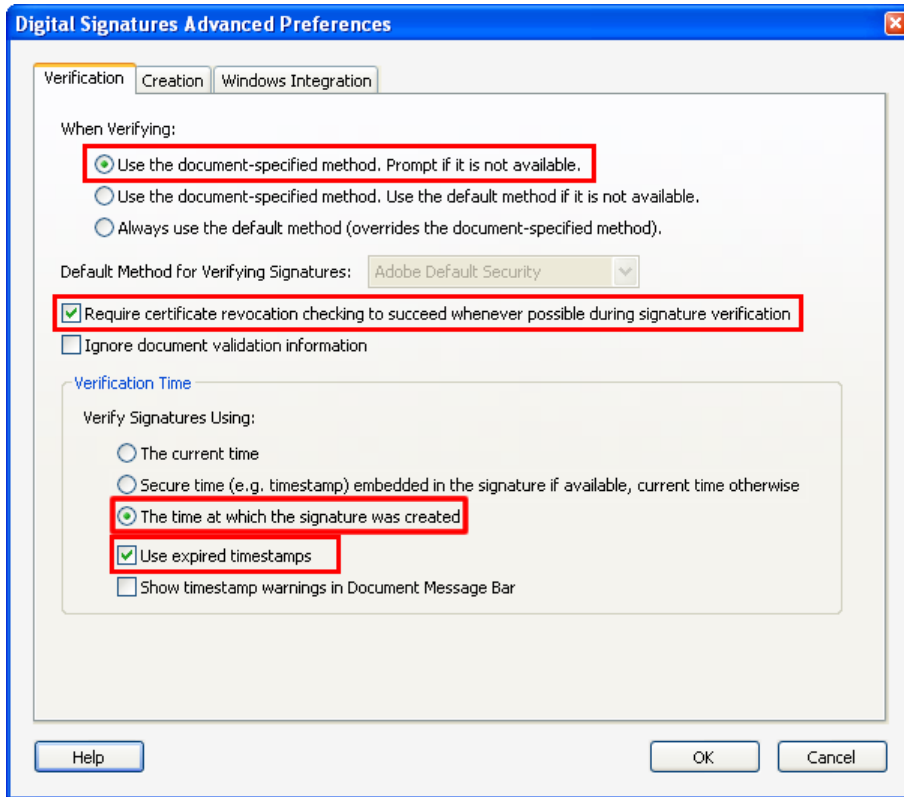


Advanced Preferences

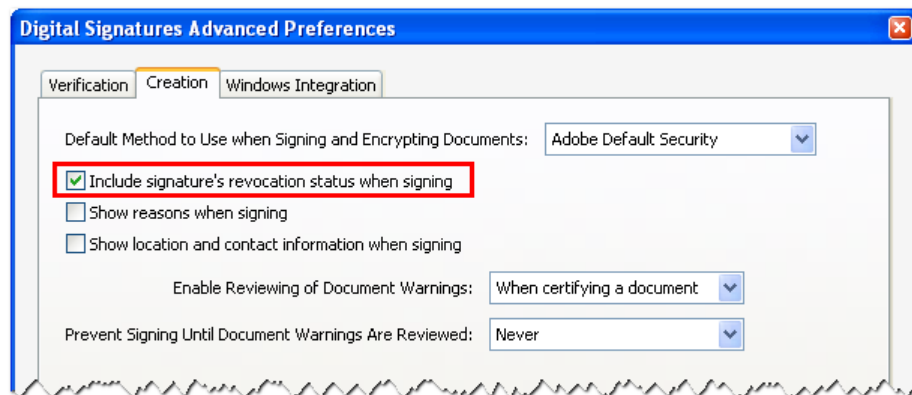
Click the **Advanced Preferences** button to bring up some additional preferences that need to be specifically configured to match the requirements of PAdES.

Configure the settings on this screen to match what is shown in the screenshot below. The first stipulates that if the document pre-specifies a specific method for signing (via a “seed value”), it should be used. When it cannot be used, a warning should appear so that a conscious decision can be made how to address the missing signature method.

When verifying any signature that contains revocation information (as recommended in PAdES), it is important to make sure that it is used and its validity considered. Checking the box highlighted in the picture will set things accordingly. In addition, should a signature contain a valid timestamp (again, as recommended by PAdES) it is necessary to use the time specified there as the signing time. The third highlighted preference, when set, makes sure that that happens. Of course, when a timestamp is not present, the current time is used. Allowing expired timestamps (the fourth highlighted area) enables the proper time of checking for other objects even if the stamp itself has expired.

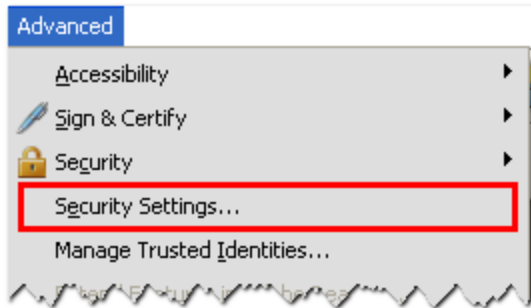


Clicking on the **Creation** tab at the top of the dialog will bring up some additional options that control what happens when a signature is created. The most important one is highlighted in the picture below – *“Include signature’s revocation status when signing”*. Checking this will cause Acrobat to follow the recommendation from PAdES to include any available revocation information (either as CRLs or OCSP) with the signature so that it can be used for future verification.



TimeStamps

As mentioned earlier, PAdES recommends the use of a secure server to provide a timestamp when signing a document. If one is available, then it is possible to add it to Acrobat using **Security Settings** in the **Advanced** menu.



After selecting **Time Stamp Servers** in the list on the left, clicking the **New** button will present a dialog where all of the details of the server can be added. If there is only a single server in the list, it will be considered the default. To change the default to something else, when there are multiple servers, use the **Set Default** button.

