tracker SOFTWARE PRODUCTS
Tips&Tricks

January, 2011

This Month's Tips & Tricks Topic:

PDF Digital Signatures - Part 1: The Basics

All PDF-XChange Products allow you to digitally sign your PDF as you create PDF files from any windows based application using the PDF-XChange Standard virtual print driver or after the fact using PDF-Tools or PDF-XChange Viewer (licensed). But a lot of users do not understand the relevance or concepts behind digital signatures and how they can be applied to use with PDF documents. This will be the first in a two part series priming users with the basics of Digital Signatures and Part 2 will outline how to use the various PDF-XChange products Digital Signature capabilities.

There is a lot of information and specifics to this topic and this newsletter's goal is to introduce the basics of the subject. If there are aspects of Digital Signatures that do not get covered in this article that you would like covered in future articles please email us at sales@tracker-software.com.

In today's electronic commercial, legal and academic environments the issue of an electronic document's authenticity and integrity is of the utmost importance. And as modern workflow in many sectors has evolved, using electronic documents rather than paper, the need for documents to pass through various hands requiring approval, editing and signing off on, need a secure way to verify the authenticity of any individual involved through this process. This is where Digital Signatures come in.

PDF supports two kinds of digital signatures: *approval signatures* and *certification signatures*. Any number of approval signatures may be applied to a PDF document but only one certifying signature may be applied and it must be the first digital signature. Approval signatures are used in the same manner as the ink on paper signatures we are all familiar with. Certification signatures are considered a part of creating the PDF file so only occur once at the beginning.

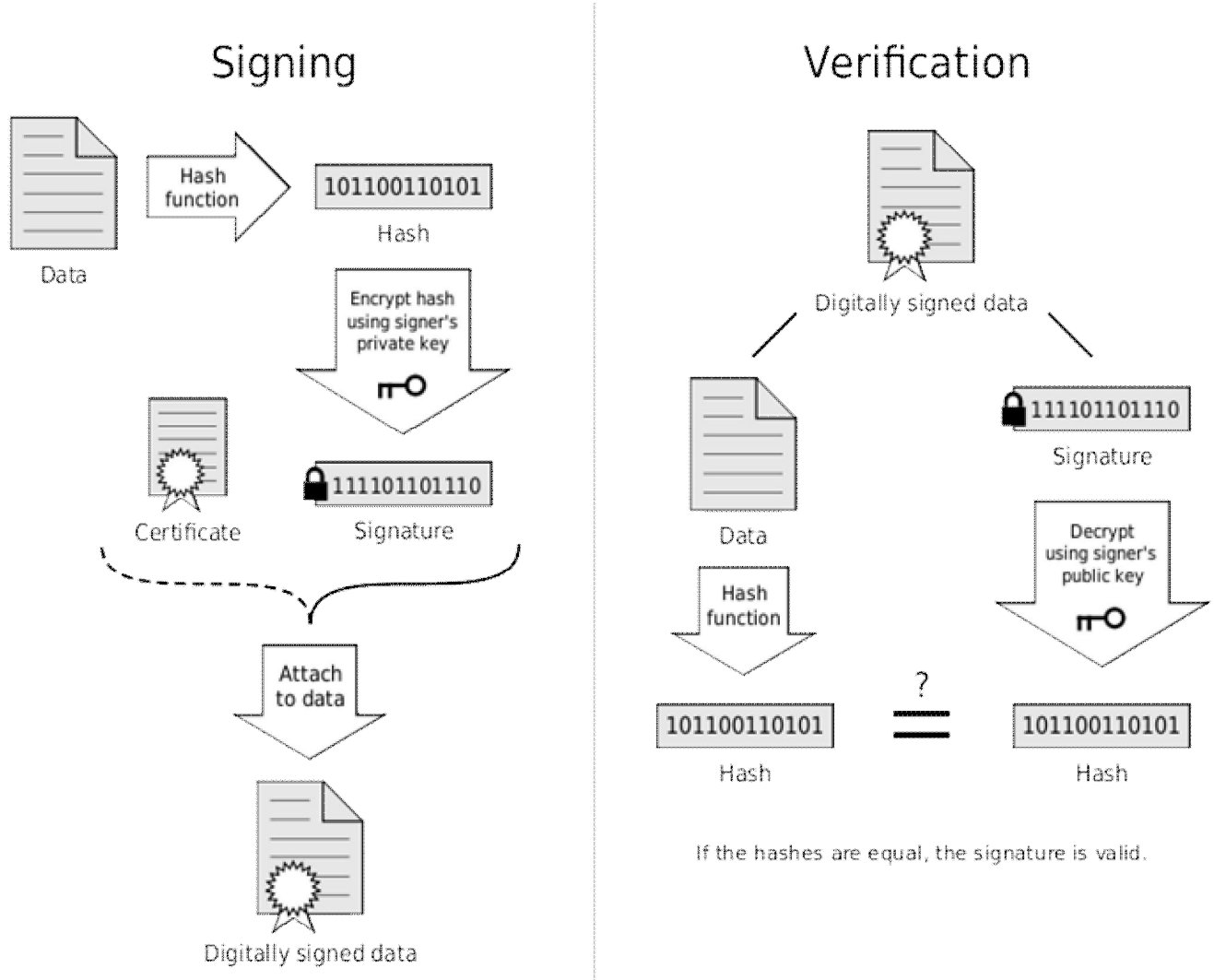
Today we are only going to discuss certification digital signatures. The idea of a certification signature is to make sure that the document is authentic and has been unaltered since it was signed by the authenticating party. Each time a signature is applied to a document, a new message digest is created. This digest stores an encrypted 'hash' version of the document (taken at the time of signing) and then embeds it along with the signature inside the document. When a recipient receives the file and validates the signature, another digest is generated and then compared with the original digest to confirm they have remained the same.

Your digital signatures can be easily customized to make just the information you want to share visible and used to display your physical signature, a corporate logo, or whatever other graphic you'd like to appear alongside your signature. You can edit the appearance of your signature at the time of signing a document.

A digital signature scheme typically consists of three algorithms:

- A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm that, given a message and a private key, produces a signature.
- A *signature verifying* algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, a signature generated from a fixed file and fixed private key should verify the authenticity of that file by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.



A public key certificate, usually just called a certificate, is a digitally-signed statement that binds the value of a public key to the identity of the person, device, or service that holds the corresponding private key. One of the main benefits of certificates is that hosts no longer have to maintain a set of passwords for individual subjects who need to be authenticated as a prerequisite to access. Instead, the host merely establishes trust in a certificate issuer.
Most certificates in common use are based on the X.509v3 certificate standard.

Typically, certificates contain the following information:

- The subject's public key value.
- The subject's identifier information, such as the name and e-mail address.
- The validity period (the length of time that the certificate is considered valid).
- Issuer identifier information.
- The digital signature of the issuer, which attests to the validity of the binding between the subject's public key and the subject's identifier information.

A certificate is valid only for the period of time specified within it; every certificate contains Valid From and Valid To dates, which set the boundaries of the validity period. Once a certificate's validity period has passed, a new certificate must be requested by the subject of the now-expired certificate.

What needs to be understood about these certificates is that you can create a digital certificate, (self-signed), on your computer that will verify that a document has not been changed since the certificate was applied but it will not provide verification of the signer's digital identity. Digital Identity verification can only be established by being issued a digital certificate through a Certificate Authority. Commercial CAs such as, Verisign, Entrust , and GeoTrust charge to issue certificates that will automatically be trusted by most PDF related programs. Aside from commercial CAs, some providers issue digital certificates to the public at no cost. Large institutions or government entities may have their own CAs.

So either a self-signed or a CA issued certificate can be used to verify the documents state, but only a CA issued certificate can verify a user's digital identity. Both can be stored on your computer as a physical file or imported into the Windows System Store.

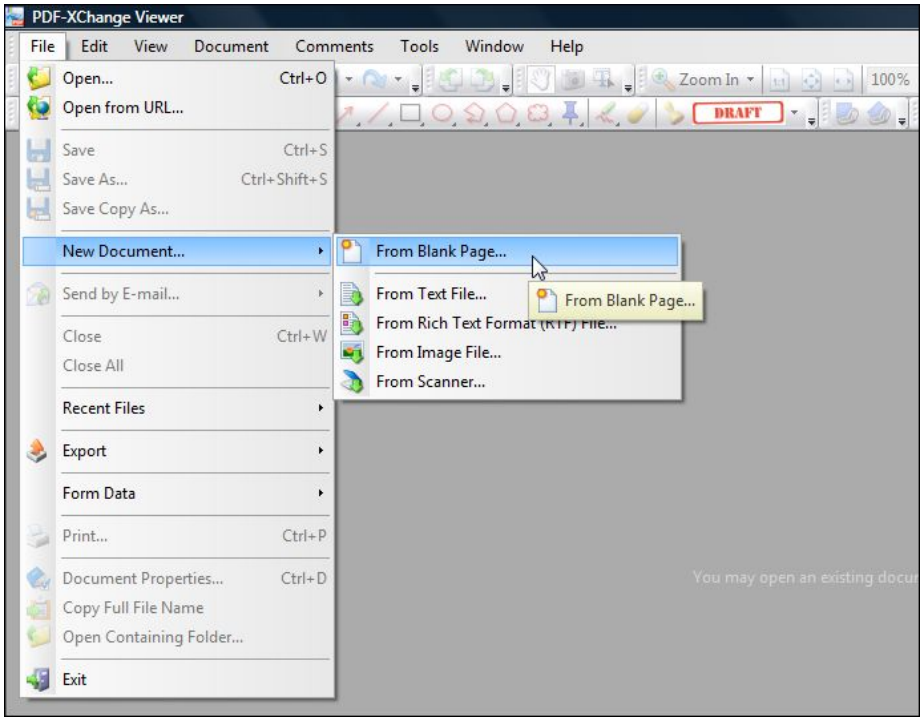
So let's look at how to create a Self-Signed Certificate using the PDF-XChange Viewer.

STEP 1
Create a New Blank PDF

Run the PDF-XChange Viewer and create a new blank document using :

File->New Document->From Blank Page

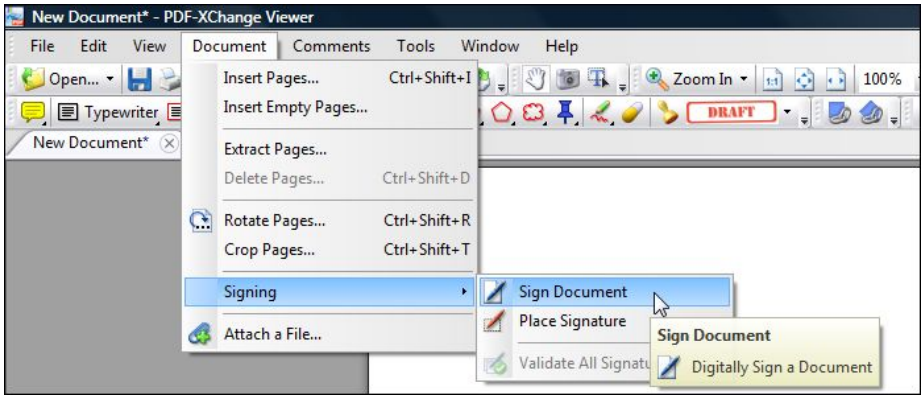
This will open a new empty PDF file.



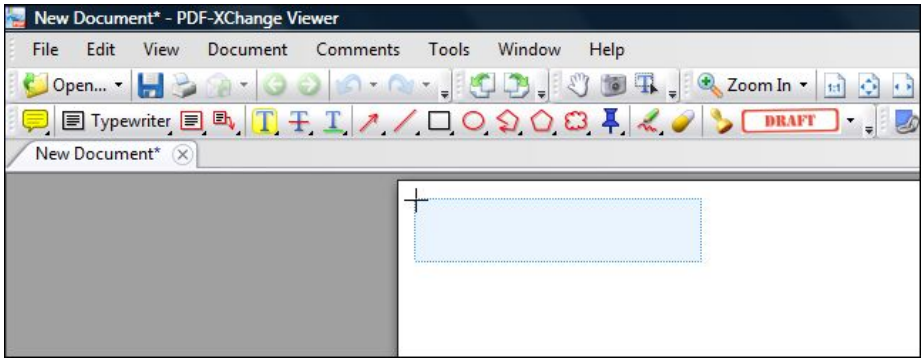
STEP 2
Open Sign Document Settings

To get to the Sign Document settings where we can create a Self-Signed Certificate, we first have to set a location for the example Digital Signature to reside. Use the menu command:

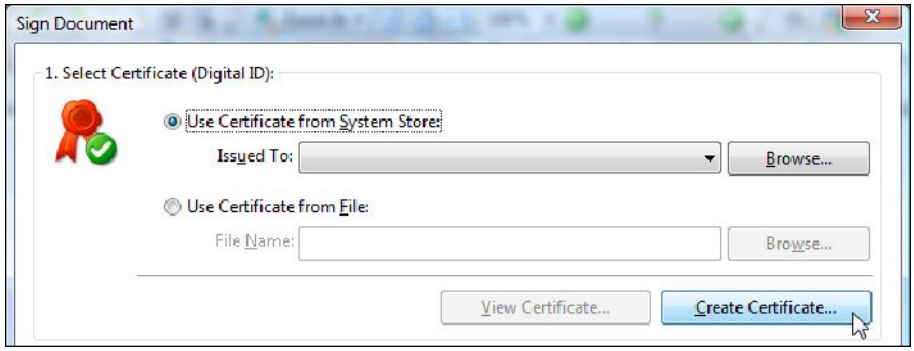
Document->Signing->Sign Document



Your cursor will turn into a crosshair with a light blue box attached to it. Select where you want your Digital Signature to placed on the document and click your left mouse button to place the signature outline rectangle.



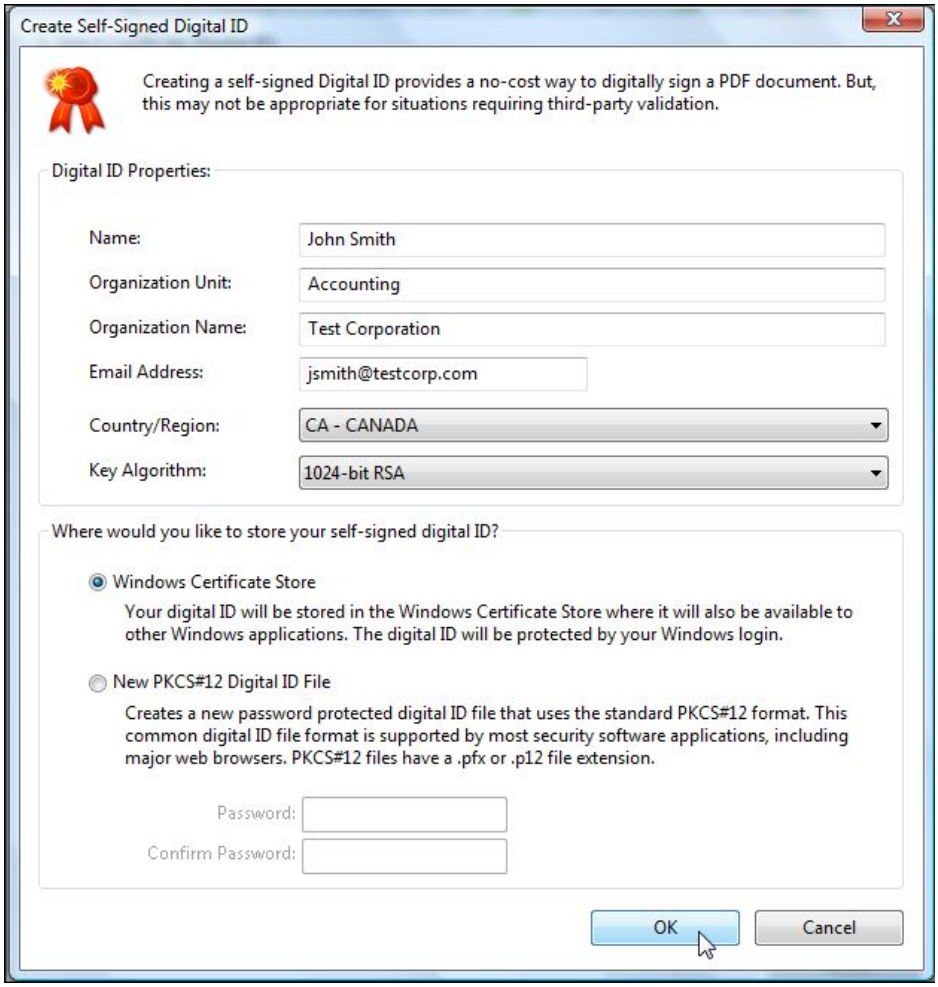
This will open up the Sign Document Dialog, where all the options for Digitally Signing a document can be set in the Viewer. Since we do not yet have a certificate, Section 1, Select Certificate, click Create Certificate.



STEP 3
Creating a Certificate

In the Create Self-Signed Digital ID window, enter your information in the fields provided. The Key Algorithm field allows you to choose the strength of encryption you would like for your key. Many industry specialists feel that 1024-bit RSA is still sufficient, but it is suggested for more sensitive documents or industries that 2048-bit RSA be employed. If you wish to use 2048-bit encryption, select it from the drop down list.

Choose whether you want to store your ID in the Windows system store or a password protected physical file is your choice. I like to keep my IDs in a central repository (Windows Store) for ease of management. If you would like to use the physical file select it and provide the password for the file and click OK.



After you've created your Digital ID, you will be back on the Sign Document screen with your new certificate selected by default.

In February's Tips & Tricks Newsletter we'll look at Digitally Signing a document with the Viewer and setting up Digital Signatures to be applied to documents being converted to PDF with the PDF-XChange Standard Print Drivers, as well as formatting the look of the signature being applied to your PDF documents.

If you have any topics you would like to see covered in this newsletter please email us at sales@tracker-software.com.

Our award winning PDF-XChange Viewer is quickly becoming one of the most highly rated Free PDF Viewers around. Allowing users the advantages of many great features, the licensed Viewer can be purchased stand alone as well as bundled with these other fine products:

PDF-XChange Viewer

Those wishing to View/Modify or perform simple editing of PDF files on their Windows PC's now have an alternative!

...more details, click here

PDF-Tools

PDF-Tools is an ideal tool to compliment your existing PDF creation application or as a 'stand alone' tool in it's own right!

...more details, click here

PDF-XChange Pro

All of your PDF File Creation, Viewing, and Manipulation needs in one cool, economic package. Includes: Standard package, PDF-Tools & Viewer.

...more details, click here

Limited Time Offers

*Commercial users can get PDF-XChange 4 Lite Free with the purchase of PDF-XChange Viewer, click here for offer details

Developers will be pleased to know that in the latest Viewer ActiveX SDK, the ActiveX control no longer requires registration on the client machine. Using Microsoft “One-Click” technology, end-users do not require an administrator account to install and register the Viewer ActiveX Control. Developers now have several Software Development Kit options to harness the power of our end-user product's robust offering.

So, whether you are a software developer looking for tools to enhance your products or an end user looking for a ready made solution, we offer arguably the most comprehensive & respected solutions available anywhere in the world today, at a very affordable price.