eOffice
A DIGITAL WORKPLACE SOLUTION

DIGITAL SIGNING TOOL FOR SECURE DOCUMENTS

Automation has become an integral part any organization through information digitalization leaving away the manual process using physical paper documents. Instead of routing the paper documents manually, the electronic channels have been used extensively for transitioning the documents in digital form. But the major challenges of maintaining identity, authenticity and security of the document for further acknowledgement and approval in the whole transition process.

NAVNEET KAUR
Scientific Officer/Engineer –SB
navneet.kaur@nic.in

The physical paper document with ink signatures or authenticity stamps can raise the questions of trust due to the lack of uniqueness, privacy and durability, where an electronic document with digital signature can provide added assurances of the evidence to provenance of identity, authority, and status of the document as well as acknowledging informed consent and approval by a signatory.

DIGITAL SIGNATURES VS. INK ON PAPER SIGNATURES

An ink signature can be applied in a paper document only and can be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult. Also in a physical paper document there is always a concern about its durability.

Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink all pages of the contract.

Also the signing process of a physical document requires physical routing to the signatory which increases organizational costs, requires additional time, and prohibits an organization from realizing the true benefits of information digitalization. In contrast, a digital signature can be applied on an electronic document eliminating physical routing thereby saves the cost, time and adds the efficiency to the entire process.

DIGITAL SIGNATURE CERTIFICATE

A digital certificate is the credentials and identity of any person or authority or an organization in electronic form and issued by a Root CA (Certification Authority).

It is used for encrypting and decrypting information with the help of private and public key pair maintained by a sophisticated and mathematically proven technology known as Public Key Infrastructure (PKI). Information can be decrypted only when both a private key and a public key match each other.

eOFFICE-DIGITAL SIGNING TOOL

eOffice-Digital Signing Tool is a desktop tool used for digitally signing the electronic documents using X.509 certificates, thereby integrity, authenticity and non- repudiation of the document is maintained. Digitally signed documents provide required

Trust level, Authenticity and Non-Repudiation between the sender and receiver of the document and ensuring its legal validity as per IT Act 2000.

The first version of Digital Signing Tool (1.0) works on Microsoft Windows, SUSE Linux (V 10.1/11.0/12.4), Red Hat (V 5.6/6.0) and similar clients with Java support. It provides single or multiple signature process on a single document by reading digital certificates from USB token provided by the CA.

The advantages of putting the digital signature in a document are:

- Ensures that the content of the document has not been altered (Integrity) during transition over electronic channels.
- Guaranties that the document is coming from the actual person who had sent it (Authenticity).
- The person who has signed the document can not deny the signature (Non- repudiation).

FEATURES

The Digital Signing Tool provides the following features:

- Digitally signing PDF files using certificates available in the USB device.
- Verification of signatures for checking authenticity of the signer.
- Multiple signing facilities on a single PDF.
- Easy to use through an intuitive Signer interface.
- Preview of document on a single click.
- Enabling the signature visibility in the PDF based on signer's choice.

TECHNOLOGY

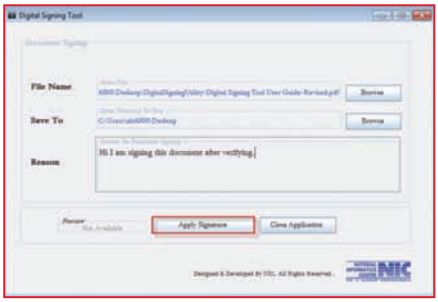
DST is open source product build upon java platform and swing to give GUI. Open source signing API are used.

We have used Java, Swing, and JCA.It supports to windows, SUSE Linux (V 10.1/11.0/12.4), Red Hat (V 5.6/6.0) and similar clients with. Java support.

HOW IT WORKS

Single and Multiple Signing

The Signer requires providing the PDF file for signing and the folder location where the signed document to be stored with some optional parameters.



More than one signer can put their signature on an already signed paper as required. The figure-2 shows the signatures of single and multiples signers in a single document.

Multiple Signatures

Single Signature

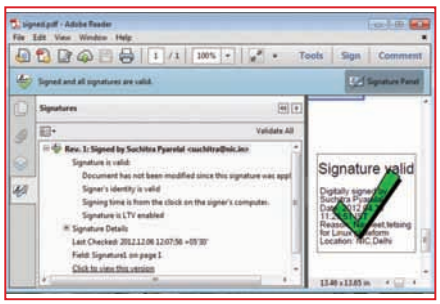
SIGNATURE VALIDATION

Some of the Root CA's are included by default in Windows Certificate Store (Trusted Root Certification Authorities) and only a few are included in Adobe Certificate Store. Microsoft and Adobe use different Certificate Stores different certificate validation procedures.

In the Adobe Certification validation procedure if the signing certificate (or the Root CA that issued the signing certificate) is not included in Adobe Store, the digital signature is considered "Not trusted" when a Signer opens a document with Adobe Reader, it will show "Validity Unknown". However this has no impact on the signing engine. To trust a signature the Signer must add the signing certificate on the Adobe certificate store because only a few Root CA's are considered trusted by default by Adobe certificate validation engine.

In order to make a signature trusted for the PDF, the steps specified in the following link be followed. *http://www.signfiles.com/manuals/ValidatingDigitalSignaturesInAdobe.pdf*

After verification the document will



appear as shown below:

HOW TO OBTAIN

DST can be downloaded from "intranic" under "eoffice Services" tab in "Downloads" Section with respect to user's Operating System.

LET'S MAKE A SECURE WORLD !