CENTRAL VIGILANCE COMMISSION

Technical note from National Informatics Center

Solution for Hosting of Signed Documents

1. Integrity of Document:

   The documents should be digitally signed by the person submitting them. The web server to which the documents are submitted for hosting, should verify the signature before hosting each.

2. Secure Hosting:

   'HTTPS' should be used for both uploading and downloading of documents to avoid alteration of documents over the network.

3. Digital Signing and submission:

   The documents submitted for hosting may be in PDF or MS-WORD format

   The document is digitally signed at the document submission end by a digital signing tool and by using a private key stored in a smart card. The detached (PKCS#7) signature file is generated.

   The document and the signature are uploaded to the server. The uploading procedure may be automated through a program. This involves development effort.

   The web server can verify the digital signatures programmatically when the files are uploaded.

   The files and their verified signatures are hosted for downloading by end users.

This procedure will ensure that the signer is confident of what he/she is signing. The person involved in web hosting is sure that the documents are properly signed. The end users benefit that the document they are downloading is authentic and that the integrity of the document is maintained.

4. Download procedure:

   a. The user verifies the digital signature of the document on the web site.
   b. User downloads both the documents and the signature.
   c. User can verify the signature of the documents by using any standards Compliant Document Signing Tool which can verify a PKCS#7 detached signature.

5. Certificate for Digital Signature:

   a. The signature should be generated using a certificate issued by a Certification Authority(CA) trusted under Controller of Certifying Authorities (CCA). This is mandatory for legal validity of the digital signature.
   b. The end user should ensure that the certificate used for signing the document is issued by a trusted CA.