A joint knowledge initiative by ***Vizag Industrial Scan & Vizag Customs***

Digital Signature Certificate for EXIM documentation with Customs

J M Kishore

The important and prioritized issue before the Ministry of Finance is Trade facilitation through simplification of Custom Procedures. The Hon'ble Finance Minister had recently stated that creation of environment for ease of doing business is on top of the list of the Government initiatives. One such activity is introduction of electronic submission of *digitally signed* Customs documents in the process of International Trade. For the purpose of carrying out imports and exports, filing of various documents such as Bills of Entry, Shipping Bills, Export General Manifest (EGM), Import General Manifest (IGM), and Consol General Manifest (CGM) is necessary.

With the introduction of online filing and self assessment procedure in Customs clearances, integrity and non-repudiation of the documents being filed has become necessary. The facility of digitally signing the documents that are filed electronically would enhance the acceptability of such documents . The reliance on digitally signed Customs process documents shall also result in the reduction of hard copies of these documents.

With effect from **01.04.2015,** the facility to use Digital Signature Certificate for filing Customs process documents was provided to Stake holders. These include Individuals such Importers, Exporters, Customs Brokers, Airlines, Shipping Lines, Shipping Agents etc, Trade partners such as Banks, Custodians, PQIS, FSSAI etc. Further, the ACP (Accredited Clients Programme) importers, who are recognised as highly compliant and given assured facilitation in Import clearances by Customs were already required to mandatorily file their Bills of Entry with digital signature w.e.f. **01.05.2015**. This is to ensure that there is no mis-use of the online filing system by imposters (persons who assume the Accredited Client's name and identity).

Mandatory use of Digital Signature by Customs Brokers, shipping lines and air lines in filing documents to Customs w.e.f. 01-01-2016:

In order to increase coverage of digitally signed documents and subsequent phasing out of physical / manual submission of documents, on 23-10-2015, Central Board Of Excise and Customs has issued instructions vide Customs Circular No. 26/ 2015, that all importers, exporters using services of Customs Brokers for formalities under Customs Act, 1962, shipping lines and air lines shall have to file customs documents under digital signature certificates mandatorily with effect from 01.01.2016. Further, wherever the customs process documents are digitally signed, the Customs will not insist on the user to physically sign the said documents. The importers/ exporters desirous of filing Bills of Entry or Shipping Bills individually may however have the option of filing declarations/ documents without using digital signature.

The process of obtaining the Digital Signature Certificate:

All the stake holders dealing with Customs and filing documents for clearance of import and export goods are advised to obtain Digital Signature Certificates being issued by CBEC. The utility is being provided free of cost through the ICEGATE website (https://www.icegate.gov.in) supported by M/s (n)Code. Indian Customs EDI Gateway (ICEGATE) is the gateway for the users of Indian Customs EDI system.

All the Individuals, Trade Partners and Govt. Agencies can connect ICEGATE for documents filing, data sharing or for administrative, statistical, analytical or policy making purposes. All Importers, Exporter, Customs Brokers, Shipping Lines, Airlines or their agents who are authorized to file any document through Remote EDI System at ICEGATE will have to use the Class 3 Digital Signature Certificates for digitally signing the Customs Documents (Bills of Entry, Shipping Bills, IGM, EGM, CGM) before submitting them to ICEGATE for processing.

(See box for The steps involved in obtaining DSC)

Submit the signed file to ICEGATE.

The user authorized for signing documents shall use DSC in his name and execute signing process and send the Digitally signed documents to ICEGATE. On receiving the digitally signed documents the ICEGATE server side verifier shall verify the user's credentials, validity of certificate, CAs credentials, Public Certificate Revocation List (CRL) status and the result of authentication and then integrate the data into ICES database. The data so integrated will also have a flag to indicate that the submitted document was digitally signed. The Customs officers will be able to identify on the system whether a particular electronic document has been filed after signing with Digital Signature Certificate or not.

In case of any technical difficulty in digitally signing the said documents, the users may contact

(i) icegate.helpdesk @icegate.gov.in (phone no. 1800 301 1000) and (ii) dscsupport@ncode.in from 10 a.m.to 6 p.m. on working days (phone no. 1800 233 1010).

(For complete details visit https://www.icegate.gov.in/digitalSign/digitalSign.html)

Benefits of Digital Signature implementation:

With Digital certificates it can e ascertained that the message/document has not been altered during transmission. Thus it ensures **integrity** . Digital Signatures provide **authentication** of the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user only. Another important benefit is **non repudiation.** Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it . A digitally signed document can easily be **tracked** and located in a short amount of time. Finally, the implementation is certainly **environment friendly** as lot of paper can be saved, which in turn may reduce the number of trees which are cut for making the paper.

(The writer is Assistant Commissioner of Customs, Custom House, Vizag)

Please send in your comments/thoughts to info@viscan.in and jmkishore@gmail.com

Steps for obtaining DSC

- Go to the ICEGATE website home page using https://www.icegate.gov.in
- Click on the Digital Signature button
- User will be directed to Digital signature page
- Click on 'Common Signer Utility to digitally sign Customs Document' link
- User will be directed to Common Signer web page
- Click on Text or XML file signing link
- User will be directed to the file signing page. Wait for initialization to complete.
- Click on Sign file button
- A pop up will be displayed from where user can select file to be signed. Select the file and click on Open.
- Another pop up will be displayed. User can select the certificate (which he has already installed) from the list and click OK.
- Validation status of the certificate will be displayed and file will be signed.
- Signed file will be saved at same location.

You may like to know.....

➢ **What is a Digital Signature Certificate?**

Digital Signature Certificate (DSC) is the digital equivalent (that is electronic format) of physical or paper certificates. A Digital Certificate can be presented electronically to prove identity on the Internet or to sign certain documents digitally. Just as physical documents are signed manually, electronic documents are required to be signed digitally using a Digital Signature Certificate.

➢ **Who issues the Digital Signature Certificate?**

A licensed Certifying Authority (CA) issues the digital signature. A Certifying Authority (CA) is one who has been granted a license to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. The list of CA's is available at http://www.cca.gov.in .

➢ **What is the validity period of a Digital Signature Certificate?**

The Certifying Authorities are authorized to issue a Digital Signature Certificate with a validity of one or two years.

➢ **How much time do CAs take to issue a Digital Signature Certificate?**

The time taken by CAs to issue a DSC may vary from three to seven days.

➢ **What is the legal status of a Digital Signature?**

Digital Signatures are legally admissible in a Court of Law, as provided under the provisions of IT.

➢ **What are the Contents of a Digital Certificate**

- Serial Number: Used to uniquely identify the certificate.
- Subject: The person, or entity identified.
- Signature Algorithm: The algorithm used to create the signature.
- Signature: The actual signature to verify that it came from the issuer.
- Issuer: The entity that verified the information and issued the certificate.
- Valid-From: The date the certificate is first valid from.
- Valid-To: The expiration date.
- Key-Usage: Purpose of the public key (e.g. decipherment, signature, certificate signing...).
- Public Key: The public key.
- Thumbprint Algorithm: The algorithm used to hash the public key certificate.
- Thumbprint (also known as fingerprint): The hash itself, used as an abbreviated form of the public key certificate.

➢ **What are the Classes / varieties in a Digital Certificate?**

- Class 1 -for individuals, intended for email.
- Class 2- for organizations, for which proof of identity is required.
- Class 3- for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.
- Class 4 -for online business transactions between companies.
- Class 5 -for private organizations or governmental security.