



आयकर निदेशालय (पद्धति)  
**DIRECTORATE OF INCOME TAX (SYSTEMS)**  
ए आर ए सेन्टर, भूमि-तल, ई-2, झण्डेवालान एक्सटेंशन,  
ARA Centre, Ground Floor, E-2, Jhandewalan Extension,  
नई दिल्ली / New Delhi-110055

F. No. System/ITBA/Digital Signature/16-17/181

Dated: 16-02-2018

To

**The Principal Chief Commissioners of Income-tax/CCsIT (By Name)**

Ahmedabad/ Allahabad/ Amritsar/ Bangalore/ Baroda/ Bhopal/ Bhubaneshwar/  
Bareilly/ Chandigarh/ Chennai/ Cochin/ Coimbatore/ Dehradun/ Delhi/ Durgapur/  
Guwahati/ Hubli/ Hyderabad/ Indore/ Jaipur/ Jalpaiguri/ Jodhpur/ Kanpur/ Kolkata/  
Lucknow/ Ludhiana/ Madurai/ Meerut/ Mumbai/ Nagpur/ Nashik/ Panaji/  
Panchkula/ Patna/ Pune/ Raipur/ Rajkot/ Ranchi/ Shimla/ Shillong/ Surat/ Thane/  
Trichy/ Trivandrum/ Udaipur/ Vishakhapatnam; and

**The Principal Commissioner of Income-tax/CsIT/CsIT(CO)(By Name)**

Agra/ Bikaner/ Calicut/ Dhanbad/ Gandhinagar/ Gwalior/ Jabalpur/ Jalandhar/  
Kolhapur/ Muzaffarpur/ Mysore/ Patiala/ Rohtak/ Sambalpur/ Varanasi/  
Vijaywada/ Delhi(CO)/ Mumbai(CO)/ Chennai(CO)/ Ahmedabad(CO)/ Bangalore(CO)/  
Bhopal(CO)/ Bhubaneshwar(CO)/ Kolkata(CO)/ Cochin(CO)/ Chandigarh(CO)/  
Hyderabad(CO)/ Jaipur(CO)/ Kanpur(CO)/ Patna(CO)/ Pune(CO)/ Guwahati(CO)/  
Nagpur(CO)/ Lucknow(CO).

Sir/Madam,

**Sub: Digital Signature Certificate(DSC) Policy-2018 –reg.**

Kindly refer to the above subject.

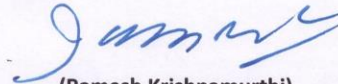
2. As a part of the day to day functioning of the Department, officers are/will be required to issue letters, notices, orders to Income Tax assesseees or other addressees within the Department or outside by using digital signature. CBDT has already mandated filing of APAR online through ITBA-HRMS system. All this can only be achieved through Digital Signature. IPR is/will be filled online and digitally signed by the officer through DSC. Department has already started issuance of DSC, since April 2017.

3. Accordingly, Digital Signature Certificate (DSC) Policy-2018 has been designed and is issued with the approval of Competent Authority. This policy will be used for issue of DSC Token to the officers concerned.

4. The above may kindly be brought to the notice of all relevant users working under your charge.

5. This issues with the approval of Pr. DGIT(S)

Yours faithfully



(Ramesh Krishnamurthi)  
ADG(S)-3, New Delhi

Copy to:-

1. The P.P.S. to Chairperson, Member(L&C), Member(Inv.), Member(IT), Member(Rev.), Member(A&J) & Member(P&V), CBDT for information.
2. The P.S. to Pr. DGIT(S) for information.
3. The Web Manager to Database cell, CBDT with a request to upload in [irsofficersonline.gov.in](http://irsofficersonline.gov.in) website.
4. The ITBA Publisher with a request to upload in ITBA Portal.



(Ramesh Krishnamurthi)  
ADG(S)-3, New Delhi



### Digital Signature Certificate (DSC) Policy (2018)



#### 1) What is Public Key Infrastructure – PKI?

A cryptographic system that uses two keys, a public key known to everyone and a private key, the private key has full control to the key owner, and has to keep in secured environment. A unique element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

#### 2) What is DSC?

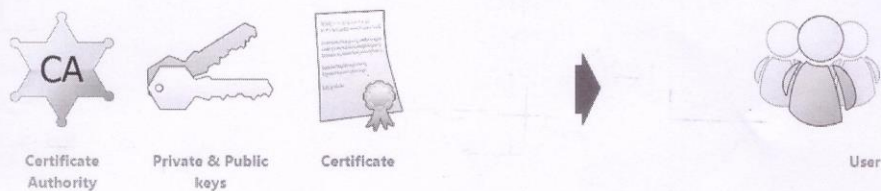
Digital signatures are a standard element of cryptographic suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering. A **digital signature** is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).

#### 3) How Digital Signatures work?

Digital Signatures Process: -

Generating a Private and Public Key

For digitally sign documents, user needs to obtain a Private and Public Key – a one-time process, it's done by Secured Signing Service while user registered. The Private Key isn't shared and is used only by user sign documents. The Public Key is available for all, used for validate the signatory's digital signature.



## Digitally Signing Document

### Create a digital signature

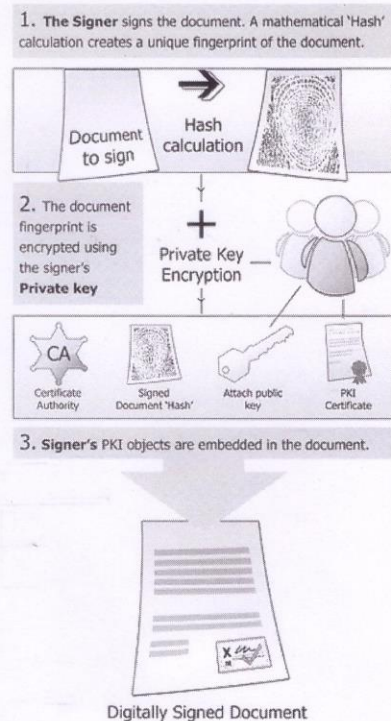
A unique document's hash that represent the document is created using a math scheme (Cryptographic) (like as SHA-2).

### Added the signature to the document

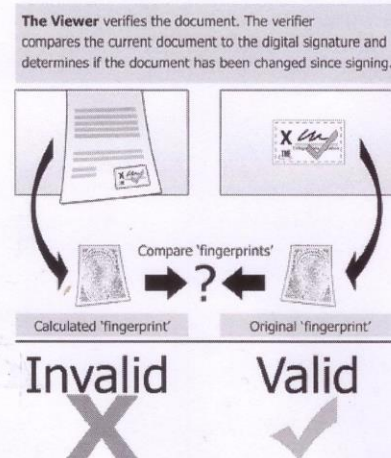
The hash result and the user's digital certificate that includes user's Public Key are mixed into a digital signature; it's done by using the user's Private Key to encrypt the document hash. The resulting signature is unique to both the document and the user. Finally, the digital signature is embedded to the document.

User-1 sends the signed document to User-2. User-2 uses User-1's public key (which is included in the signature within the Digital Certificate) to authenticate User-1's signature and to ensure the document didn't alter after it was signed.

### Signing the document:



### Verify signed document:





#### Certificate Authority (CA)

CA issued certificates to ensure the authenticity of the signatories. Certificates are similar to ID Document. When you want to identify a user in the system you check his certificate. This certificate issued in registration process once all require information filled in. In PKI world the CA uses the CA's certificate for authenticating user's identity.

#### 4) Why the DSC is required?

Signing documents with Secured Signing complies with [e-signature laws](#) worldwide, and is valid and legally enforceable as an equivalent to a signed paper contract. DSC to help organization and individuals secure online transactions with legal validity as per the Indian IT Act, 2000.

#### 5) What are the Types of Certificate?

- **Sign**

The DSC could only be used for Signing a document. (The most popular Certificate). The most popular usage is signing the PDF file for Tax Returns, MCA and other websites.

- **Encrypt**

The DSC would be used to Encrypt a document, it can be used to encrypt and send classified information.

- **Sign & Encrypt**

Combination of both Sign & Encrypt DSC by using this category.

#### 6) What is the specification of DSC provided by Dept.?

- i. Category of Applicant: Government
- ii. Class of Certificate Required: Class II
- iii. Certificate Required: Organisation (Signing and Encryption)
- iv. Certificate Validity: 2 years from the date of activation
- v. Crypto USB token: – FIPS 140-Level 2

#### 7) Objectives of DSC usage in ITBA/HRMS application.

As a part of the day to day functioning of the Department, Officers/officials will be required to issue letters, notices, orders to Income Tax assesseees or other addressees within the Department or outside or upload documents, reports, forms or to perform several ITBA / HRMS related activities on the ITBA system. In order to enable digital authentication of such communications within and outside the Department, it is envisaged that the officers/officials shall use the Digital Signature Certificate issued to them by the Department to digitally sign such letters, notices, orders to Income Tax assesseees or other addressees within the Department or outside or upload documents, reports, forms or to perform several ITBA / HRMS related activities on the ITBA system.

**Who is admissible for the DSC?**

DSC is admissible to

- i. All officers up to the level of Income Tax Officer or equivalent in the Income Tax Department.
- ii. Selected officials such as DDOs based on need.

**8) How to apply for DSC?**

User shall raise a DSC request from the HRMS application from the ESS module. Post filing of all required details, user need to send printed and dully signed application to the local RCC admin/CCA nodal officer for DSC for approval purpose. (Please refer detailed instructions in this regard.)

**9) What is the role of local RCC Admin/CCA nodal officer wrt approval?**

On receipt of printed DSC application directly from officer/official, request needs to be approved/denied through the DSC administration interface. Further, local RCC Admin needs to forward printed copies of approved request to the respective CCA Nodal officer for DSC along with the covering letter. Local RCC Admin will keep the record of forwarded application in the below format.

RCC location: \_\_\_\_\_ RCC Admin: \_\_\_\_\_

Sr No.	Applicant's Employee ID	Applicant Name & Designation	Date of Receipt of Application	Date of forward of Application to CCA Nodal officer	Remarks (Fresh/Lost DSC Request)

**10) What is the role of CCA nodal officer wrt authorization?**

On receipt of approved DSC application(s), CCA nodal officer has to authorize the application by authorizing the page-2 of each application by dully signed & stamped along with organization seal. Further all the application needs to handover DSC vendor for further process. CCA Nodal officer will keep the record of application handed over to DSC vendor in the below format.

CCA location: \_\_\_\_\_ CCA Nodal officer: \_\_\_\_\_

Sr No.	Applicant's Employee ID	Applicant Name & Designation	Date of Receipt of Application	Date of handover of Application to DSC vendor	Signature of DSC vendor	Date of receipt of DSC with USB token	Remarks (Fresh/Lost DSC request)

All RCC Admin/Nodal officers will also maintain full record of DSCs issued to employees. So that it can be used for accounting purposes.



**11) What is the role of DSC vendor?**

DSC vendor will collect printed applications from the CCA Nodal officer for the process of issuing DSC. Further DSC vendor will organize a camp at CCA nodal officer for delivery of DSC and to educate about the DSC and its usage in ITBA/HRMS applications. DSC vendor will also facilitate in pin generation of blocked DSCs.

**12) Essentials to implement DSC (Binding of DSC with Employee code).**

On receipt of DSC USB token, individual user has change the default PIN and register DSC into the HRMS system. User also has to sign Test/Dummy letter to ensure the DSC implementation process is complete.

**13) How DSC software would be installed?**

In this regard, please refer ITBA-Digital Signature Instruction. This E-loc signing utility is also available in ITBA Portal for download by the officers.

**14) How the Users would be trained & the Distribution of DSC would be executed?**

It would be the responsibility of the individual officer/official to collect the DSC from the respective CCA Nodal officer for DSC. Training of usage of DSC in ITBA/HRMS system would be the responsibility of DSC vendor by organizing camp.

**15) How the rest of Users would get training on DSC?**

Users can refer manual/training materials/videos etc. in the ITBA portal.

**16) Safe keeping of DSC**

After receiving the DSC, the User should keep a note of the DSC Sr. number as well as DSC Pin in some private/secret record to be kept in locked almirah. The DSC sr. number will be required to be quoted if DSC is lost or stolen. The User should keep the DSC safely at all times. The DSC is similar to an identity like ATM/Credit card and should be kept safely. Under no circumstances the DSC should be shared/lent to others including colleagues. Once issued, DSC will be valid upto 2 years from date of issue. **On the transfer of officer/official, DSC will be retained till the expiry of DSC and should not be surrendered.**

Events such as retirements, suspensions and death in harness would presuppose surrender of DSC to the respective RCC Admin. RCC Admin will keep record of surrendered DSC in the following format.

RCC location: \_\_\_\_\_ RCC Admin: \_\_\_\_\_

Sr No.	Applicant's Employee ID	Applicant Name & Designation	Date of Surrender of DSC	Reason of Surrender	Remark

**17) How maintenance/Management of DSC would be done on day-to-day basis?**

An employee may not be available to work on the system in five different situations: (i) employee's proceeding on leave like E.L. /H.P.L. /E.O.L. etc, (ii) employee's transfer, (iii) employee's retirement, (iv) employee's death and (v) employee's suspension.

i. When Employee proceeds on leave ( E.L./H.P.L./E.O.L. etc.)

**For officers/officials**

Where an Officer proceeds on leave (5 or more days) like E.L./H.P.L./E.O.L. etc. the DSC need not be handed over.

ii. Where Employee has been Transferred and Joined duties at new location

**In case of an officer's/official's transfer**, the DSC will remain with him/herself. (See S/16)

iii. Employee **Retirement**

**In case of an officer's/official's retirement** the DSC will be returned to the respective RCC Admin.

iv. Employee's **Death**

**In case of Officer's/Official's Death**

The procedure would remain **same** as stated in Sub Para (iii) above. The deceased officer's family will have to return the DSC to the RCC Admin

v. Employee's **Suspension**

The procedure would remain **same** as stated in Sub Para (iii) above. In any case, even if the employees DSC is not received back physically for any reason what so over, it would be the duty of the reporting officer to intimate the RCC Admin for deactivation of DSC.

**18) What happens In case of loss / misplacing of DSC token or Token is stolen?**

The employee (whether officer or official) should report loss of DSC immediately in ITBA portal. DSC will be deactivated from ITBA. A complaint may also be lodged with the police. A copy of the complaint is to be given to the RCC Admin within 24 hours of the employees reporting the loss to prevent unauthorized usage of DSC. The User, who has lost/misplaced his token will not be able to sign any document in the ITBA/HRMS application. Officer will re-apply in ITBA for new DSC. RCC-Admin. RCC Admin will send the warning letter to the Employee through his/her PCIT/CIT. Respective PCIT/CIT will ask the reason for loss/misplacement/damage of DSC from the concerned User and recommend for the issue of fresh DSC. After getting recommendation from respective PCIT/CIT, RCC Admin. will approve the DSC request. In case DSC is lost twice or more by the same employee, then the 5000/- Rs. may be asked to be paid by the user and above mentioned process will be followed. RCC Admin should revoke the lost DSC, immediately upon reporting by the officer/official.