



**GOVERNMENT OF JAMMU AND KASHMIR,
GENERAL ADMINISTRATION DEPARTMENT,
CIVIL SECRETARIAT, J&K**

Subject: Issuance of Certificates for Online Services using Digital Signature-reg.

**Government Order No.1041-JK(GAD) of 2023
Dated:28-08-2023**

In accordance with Section 3 and 3A of Chapter II of the Information Technology Act, 2000, read with its Section 5 of Chapter III, dealing with promoting use of digital technologies in government operations and with a view to streamline the process of issuing digital certificates, documents and other electronic record by various departments, it is hereby ordered that the following e-authentication techniques shall be put to use in the process:

1. **Digital Signature Certificates (DSC):-** Digital Signature Certificates (DSC) are a secure and legally valid method for single/ bulk signing and issuing digitally signed certificates for online services.
2. **eSign:-** eSign service is an online electronic signature service that can facilitate an Aadhaar holder to digitally sign a document. An Aadhaar holder can sign a document after Biometric/One Time Password authentication thus requiring no paper-based application form or documents.
3. **Document Signer Mode:-** Document Signer Certificates are issued to organizational software applications for operating automatically to authenticate documents/information attributed to the organization by using Digital Signature applied on the document, documents/ Information.

All Administrative Departments/Heads of Departments/Deputy Commissioners/Managing Directors of various PSUs/Boards/Corporations are accordingly advised to adopt any of the above mentioned modes for digital signing of certificates/documents w.e.f 1st September, 2023 alongwith ensuring necessary training and awareness of employees in this regard. Details of the aforesaid authentication techniques are annexed as Annexure-A to this order for reference.

Further, the departments may contact Mr. Raman Gupta, Technical Officer, Information Technology Department (+91 94191-88330) for any technical guidance/hand holding.

By Order of the Lieutenant Governor.

Sd/-

(Sanjeev Verma)IAS,

Commissioner/Secretary to the Government

Dated:-28.08.2023

No.GAD-ADM0II/275/2023-09-GAD

Copy to:

1. All Financial Commissioners (Additional Chief Secretaries)

2. Director General of Police, J&K.
3. All Principal Secretaries to the Government.
4. Director General, J&K Institute of Management, Public Administration and Rural Development.
5. Principal Secretary to the Lieutenant Governor, J&K.
6. Principal Resident Commissioner, J&K Government, New Delhi.
7. Joint Secretary (J&K), Ministry of Home Affairs, Government of India.
8. All Commissioners/Secretaries to the Government.
9. Chief Electoral Officer, J&K
10. Divisional Commissioner, Kashmir/Jammu
11. Director, Information, J&K.
12. All Deputy Commissioners.
13. Chairperson, Special Tribunal, J&K.
14. Director, Archives, Archaeology and Museums, J&K.
15. All Heads of Departments/Managing Directors.
16. Secretary, J&K Public Service Commission
17. Director, Estates, Kashmir/Jammu
18. Secretary, J&K Service Selection Board
19. Secretary, J&K Legislative Assembly
20. General Manager, Government Press, Srinagar/Jammu.
21. Private Secretary to the Chief Secretary, J&K.
22. Private Secretary to Commissioner/Secretary to the Government, GAD.
23. Government Order/Stock file/Website, GAD. **Hindi & Urdu Versions shall follow.**

Additional Secretary to the Government

(Rohit Sharma) JKAS

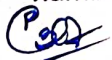
28/08

28.8.2023

Annexure-A to Government Order No.1041-JK(GAD) of 2023

Dated:28.08.2023

1. **Digital Signature Certificates (DSCs)**: DSCs ensure secure and legally valid online service certificates, offering robust authentication through electronic signatures in accordance with legal provisions. Here's a general outline of the process:
 - a. **Choose a Certifying Authority (CA)**: Select a trusted Certifying Authority (CA) accredited by the Controller of Certifying Authorities (CCA) in your country. CAs are authorized entities to issue digital signature certificates.
 - b. **Application Form**: Obtain the DSC application form from the chosen CA's website or physical location. Fill out the required details accurately and completely.
 - c. **Identity Verification**: You will need to provide valid identity and address proof documents as per the CA's requirements. Commonly accepted documents include Aadhaar card, passport, PAN card, voter ID, and utility bills.
 - d. **Verification Process**: The CA will verify your submitted documents. This may involve in-person verification or submission of documents through an authorized person. Some CAs offer online verification processes as well.
 - e. **Payment**: Pay the prescribed fee for the DSC as specified by the CA. Fees can vary based on the type and validity period of the DSC.
 - f. **Generate Key Pair**: Once your documents are verified and payment is confirmed, the CA will generate a key pair - a private key (kept confidential) and a corresponding public key. The private key will be securely stored on a hardware token or software, while the public key will be part of your DSC.
 - g. **Issue of DSC**: After verification and key pair generation, the CA will issue your DSC. This may involve providing you with a physical token (USB dongle) containing your DSC or sending you the DSC file along with instructions for installation.
 - h. **Installation**: Install the DSC on your computer system or hardware token as per the CA's guidelines. The installation process may include setting a PIN for accessing the private key.
 - i. **Testing**: Test the DSC by signing and verifying sample documents to ensure it's functioning correctly.
 - j. **Use**: Your DSC is now ready to use. You can sign documents, authenticate transactions, and access various online services securely.
2. **eSign**: eSign provides a streamlined method for subscribers to electronically sign online service certificates, upholding authenticity and compliance with electronic authentication standards. The process is as follows:
 - a. **Choose an eSign Service Provider**: Select a recognized eSign service provider that is compliant with legal regulations in your country. These service providers are authorized to offer eSign services.
 - b. **Provide Identity Information**: You'll need to provide your identity information to the eSign service provider. This might include details such as your name, Aadhaar number (or other identification number), and contact information.
 - c. **Aadhaar Verification**: In many cases, eSign is closely linked to Aadhaar authentication. You might be required to authenticate your identity using your Aadhaar number and a One-Time Password (OTP) sent to your registered mobile number.



- d. **Select the Document:** Choose the document you want to electronically sign. This could be a contract, agreement, form, or any other type of document that requires your signature.
 - e. **Sign the Document:** Use the eSign platform provided by the service provider to affix your electronic signature to the document. This could involve clicking a "Sign" button, entering a password or PIN, or other authentication methods.
 - f. **Generate eSigned Document:** Once you've signed the document, the eSign service will generate a digitally signed version of the document. This signed document will include your electronic signature and a timestamp.
 - g. **Download or Share:** You can usually download the eSigned document from the eSign platform. You can then store, share, or submit the digitally signed document as required.
 - h. **Verification:** The recipient of the eSigned document can verify its authenticity and integrity by using the appropriate verification tools provided by the eSign service provider or other authorized entities.
3. **Document Signer:** Document Signer mode, adhering to established guidelines, ensures the legitimacy and integrity of online service certificates, enhancing trust in digital transactions. The process is as follows:
- a. **Choose a Document Signing Tool:** Select a reputable and secure electronic document signing tool or software. There are various options available, both online and offline, that allow you to sign documents electronically.
 - b. **Create an Account (if applicable):** If the chosen tool is an online service, you might need to create an account on their platform.
 - c. **Upload Your Document:** Use the tool's interface to upload the document that you need to sign. This could be a contract, agreement, form, or any other type of document.
 - d. **Position Your Signature:** Once the document is uploaded, the tool will typically allow you to place your signature on the document. You might be able to draw your signature using a mouse or stylus, or upload a scanned image of your physical signature.
 - e. **Add Additional Information (if needed):** Depending on the tool and the document's requirements, you might also be able to add additional information like dates, text fields, checkboxes, or initials.
 - f. **Review and Confirm:** Double-check the document to ensure that your signature is correctly positioned and any additional information is accurately added.
 - g. **Apply Your Signature:** Click the "Sign" or equivalent button on the tool's interface to apply your electronic signature to the document.
 - h. **Save or Download:** After signing, you will likely have the option to save or download the signed document. Some tools might also provide options for sending the signed document to others directly from the platform.
 - i. **Verify Signature (if needed):** Depending on the context, you or the recipient of the document may need to verify the electronic signature's authenticity using appropriate verification tools.
 - j. **Store and Share:** Store the signed document in a secure location. You can share it electronically with other parties involved in the transaction.

(Rohit Sharma) JKAS
Additional Secretary to the Government

Ped
28/08

28-8-2023