

1. What is a Digital Certificate?

Digital Certificate is a unique pair of a Public key and a Private key issued to an individual (either for his own use or use as an authorized representative of an organization such as partnership firm, private limited company or a public limited company). The data encrypted by a Public Key of a Digital Certificate can be decrypted only by matching Private Key of the same Digital Certificate and vice versa.

Additionally, the Private Key of a Digital Certificate is used to sign the data to ensure non – repudiation.

2. What types of Digital Certificates are required to work on the system?

It is imperative for the bidder to have a valid SHA-2 compliant Class – II/Class – III Digital Certificate pair of Encryption and Signing certificates in the name of Authorized Representative of the Organization/Proprietor for Encryption of Bid Data and Signing of online Bids. In absence of either of these, the bidder will not be able to enter his bid.

3. Who is responsible for issuing Digital Certificates in India?

A Digital Certificate is issued by Certifying Authorities registered with Controller of Certifying Authorities of Government of India. There are several organizations registered as Certifying Authorities and issue Digital Certificates through their authorized partners. The updated list of Certifying Authorities can be viewed at www.cca.gov.in. Users should not procure certificates issued by CAs not Registered under Controller of Certifying Authorities of Government of India.

4. What is e-Token device?

e-Token is a device to store Digital Certificates securely. A Digital Certificate installed on a secure e-Token cannot be copied.

5. What is encryption and decryption?

Encryption means changing a set of data information into non – readable format. Decryption means changing a set of encrypted data information back into original format. This activity is done using the encryption certificate.

6. What is Hashing?

Hashing means generating a thumbprint of a set of data information.

Hash is well defined algorithm in the Information Technology Act, 2000.

Hash is one – way. You can generate Hash value of a set of data information but not set of data information out of a Hash value.

Hash is unique to a set of data information. Any change in the original set of data information will result in change in the Hash value.

7. Why do I have to submit the Bid in two parts?

This is required to be done in order to maintain the sanctity and confidentiality of the Bid Data from the time it is prepared until its opening, and also thereafter at any time. In case the stages are reduced to one, there are chances that the sanctity and confidentiality of the Bid Data Bid Data may be compromised. This will be a fundamental flaw in the process of Electronic Tendering.

8. Does the completion of any one of the Bid Submission stages ensure that the Bid Data will be available to the Competent Authority at time of opening of the Tender?

No. The Bidder has to ensure that both the Hash Submission as well as Re-encryption stages are duly completed within the allotted time frame to ensure that the Bid Data will be available to the Competent Authority at time of opening of the Tender.

9. Can I change my Bid Data after filling it once?

The Bid Data can be changed / modified by the Bidder as many times as required until the Last Date and time of Bid Preparation and Hash Submission.