NeST-GDL -GEN.02
Version 1.0
July, 2017
Status: Released

# Encryption-decryption mechanism

# for

# open bids in GeM

Government of India
Ministry of Electronics & Information Technology
New Delhi – 110 003

# Application process for obtaining the key pair

Class 3 certificate is required for encryption/ decryption of Bids. The requirement for obtaining class certificate is as under

1. An Electronic Application Form (e-form) decided by the Certifying Authority (CA) has to be filled online. Verification of the credentials will be as per Identity Verification Guidelines (available on *cca.gov.in*).

2. For verification of the credentials, currently physical presence is required for obtaining class 3 certificate. In place of this, Aadhaar with biometric verification can serve the purpose after dynamic authentication with OTP.

**Key generation:**

A key pair will be generated on a High Security Module (HSM) applying Asymmetric algorithm based on one of the cryptography algorithms as notified under the Rules and Regulations of the IT Act.

**Key Storage:**

The public-private key pair will be generated applying PKI standards, i.e. using one of the cryptography algorithms RSA, Diffie-Hellman or Elliptic Curve Discrete Logarithm as notified under the Rules and Regulations of the IT Act. The bidder will use public key of the buyer to encrypt the bid.

- The buyer will use his/her Private Key to decrypt the bid.
- The private key of the bid owner (buyer) will be stored on an HSM complying FIPS 140-2 Level 2. HSM is temper proof storage device that keeps the keys in scrambled form and does not allow making copies.
- The public key with the key owner's attributes such as name, organisation, key identifier, and validity period etc. would be made available through the Buyer's Class 3 Encryption Certificate.

**Key Splitting:**

- Provision to split Private Key into configurable number of key parts will be built so that when all key parts are combined together only then decryption takes place.
- At the buyer end, private key will be split into more than one key component and these components will be stored on HSM in groups with assigned PIN to each key holder. Generally, it is seen that all the key holders are not present as some of them may be on leave at bid opening time.

  For example, the private key is split into three components C1, C2 and C3 for three key holders (H1, H2, H3) and it is decided that only two holders will be present at bid opening time. Then H1 will have PIN for (C2, C3), H2 will have PIN for (C1, C3) and H3 will have PIN for (C1, C2). In this arrangement presence of any two out of the three key holders would be sufficient to open the bid.

**Key Usage:**

Valid Public Key will be embedded into GeM application Bid submission form, allowing Bidders (Suppliers/Service Providers) to encrypt their bids for submission.

- The buyers (Bid Owners) will open the bid at designated time by giving their PIN after being dynamically authenticated through OTP.
- Current practice as per guidelines for compliance to Quality Requirement of e-Procurement Systems is that Private Key used for decryption remains available with the buyer (i.e. officer of buying department)
- The provision of storing private key on HSM and PIN before applying Private Key by buyer(s) to open Financial Bid in GeM has been used to ensure that Private Key is applied by its owner.

**Audit Logs:**

The details of each event, its time of occurrence and executor would all be recorded on HSM, so that these logs cannot be truncated, modified, deleted or added.

It is suggested to get this proposed process certified by STQC as in the current process, Buyer held Dongle ensures that authentication is handled locally, whereas in the proposed process, the authentication is carried out remotely since keys will be stored on HSM.

The comparison of current process and proposed process is given below to show that both have the same security strength, i.e. one with dongle and other with HSM storage having process certified by STQC.

| | Current Process | Proposed Process |
|---|---|---|
| Key Storage | Encryption –Decryption Keys are stored on external Dongle to ensure meeting FIPS 140-2 level 2 standard. | Encryption –Decryption Keys are stored on HSM that also ensure compliance to FIPS 140-2 level 2 standard. |

.