Chapter VI
Bid Opening and Evaluation

Chapter VI

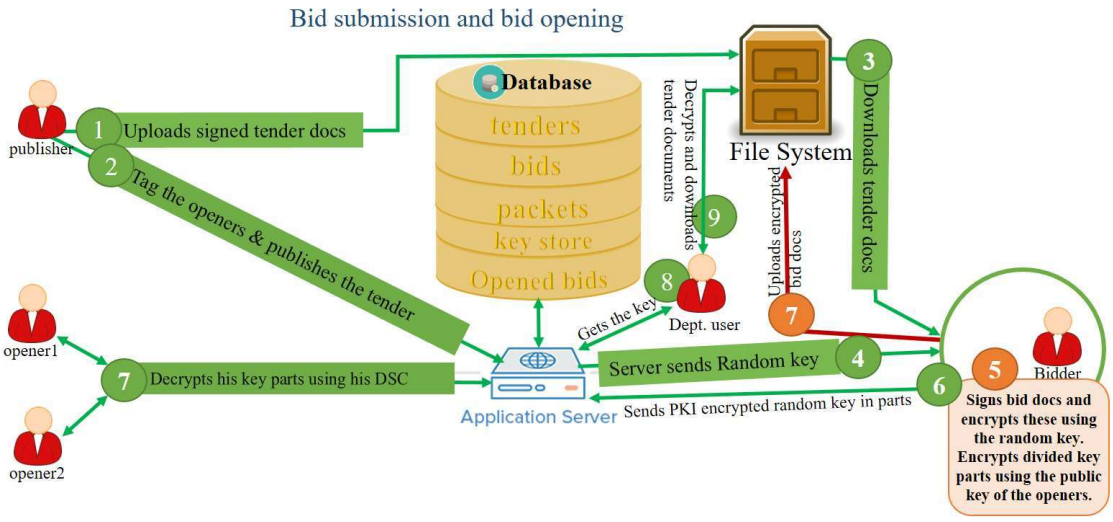
Bid Opening and Evaluation

6.1 Packet opening and bid decryption

As per SRS, the system shall support encryption of bids submitted by the bidder, using the Public Key of the Bid Opening Authority. Encryption shall be done at the client side, and the encrypted bid shall be time locked by the system, till the time of bid opening. Only the Bid Opening Authority shall be able to decrypt the submitted bids only at the bid opening time, using the Private Key of the Bid Opening Authority. There were two types of processes for bid opening- single cover and two-cover.

In case of two-cover process, stage wise bid opening and decryption is to be followed, with the financial bid cover remaining encrypted till the completion of technical evaluation. Financial bid cover would be decrypted only for those bidders who have qualified in the technical evaluation.

Figure 6: Flowchart showing processes of bid submission and bid opening



In the bid opening process, the designated bid openers first opens the cover packet (**Step 7** in above picture). The date of opening is recorded in the database. After that, each bid of the tender is decrypted by the authorised departmental user one by one (**Steps 8 and 9)** and the date of bid decryption is recorded in the database.

The e-Procurement system was implemented in Odisha in July 2008. A total of 3,22,897 tenders were published up to 31 March 2022 against which 17,42,000 bids were received. Audit analysed the database tables with data related to opening and decryption of bid packets, and found the following inconsistencies.

6.1.1 Risk of change in bid openers through manual intervention at the back end of the system

System Security

As per system design, at the time of creation of tender, the tender creator selects the bid openers. The system allows configuring any four bid openers out of which any two or three can open the bid at the actual bid opening time. The details of bid openers is recorded in the database. At the time of submission of bid documents by bidders, the documents are digitally signed by the bidder and encrypted using the bid openers' public key. The details of bids, bid openers, and the random encryption key data are stored in the key store table of the system in parts, thereby ensuring that nobody can open or decrypt the bid.

At the time of tender opening, the tender is opened online by the authorized bid openers who have been configured at the time tender creation. Any two, three or four officials as configured can open the bids once the bid opening date and time is reached. The decryption key is updated in the key store at the time opening of tender. Then the encrypted bid documents are decrypted and opened one by one by the bid opener. As the decryption key is updated at the time of opening of tender, the bid opener should be same as defined at the time of creation of tender.

Audit analysed the data in the bid openers master table and the key store table in the system and noticed that in three tenders, the bid openers as per the key store table were not the ones recorded in the bid openers master table, as follows:

Table No.9 : List showing undesignated tender openers

Sl. No	Tender ID	Bid opener id in key store table not matching bid openers master table
1	7687	2793
2	7691	884
3	87361	18037

(Source: e-Procurement database)

At the time of bid submission by the bidder, the symmetric key was encrypted using the public key of the bid opener as defined in the bid opener master table. However, the system recorded that decryption of the symmetric key had been carried out by another user's private key. This indicated that in these cases, the bids had been opened by users other than the designated bid openers and raised doubts on the integrity of the procurement process.

The Department stated (December 2023) that at the early stage of the application, there was a deficiency in the process of changing bid openers, which had resulted in this anomaly and had been subsequently fixed.

The response was not tenable, as Audit noticed that in one of the three tenders, there was evidence of another bid opener having been added to the bid opener master table through manual intervention at the back end of the system. As a result, Audit was unable to derive assurance that integrity of the process of

designating bid openers in the absence of a clear and verifiable trail of user actions in the system.

6.1.2 Risk of modification of decrypted bid data through manual intervention at the back end of the system

System Security

As per system flow, after opening of submitted bids against a particular tender, the bids are decrypted and stored in the 'bid decrypted' table. The 'bid decrypted' table had columns like bid identity number, packet identity number, date of decryption, the user id of the user who decrypted the bid and the tender ID. Hence, for every bid decrypted, the corresponding tender ID should have been populated in the decrypted table and there should not be any null value in the tender ID data field against any decrypted bid, otherwise the link between the tender and the decrypted bid will be lost.

Audit analysed the 'bid decrypted' table and noticed that

- A total of 15.39 lakh bids pertaining to 2.61 lakh tenders published up to 31 March 2022 had been decrypted. Out of these, 1.79 lakh decrypted bids pertaining to 50,627 tenders had tender ID recorded as 'NULL', which was highly irregular.

  As bid decryption was an automated process in the system and since every bid has to have referential integrity with respect to a particular tender, the recording of the tender ID as 'NULL' indicated the material risk that these values had arisen as a result of manual intervention at the back end of the system by the Data Base Administrator, bypassing the application controls for the decryption process.

  The Department stated (December 2023) that there had been an error in the object relational mapping in the system which had led to 'NULL' value in the tender ID field in the bid decrypted table, and this issue had been resolved.

  The response was not tenable, since it did not explain how the tender ID field could be populated as 'NULL' in case the process had been carried out through the application front end. The Government also did not furnish the details of the resolution process or patch management in this regard.

- In a total of 77,554 tenders involving 2,45,521 decrypted bids, the time of decryption of bids was recorded as before the time recorded for opening of the bids. The difference between the bid decryption time being earlier than bid opening time ranged from 55 minutes to 2,252 days, which was highly irregular. This broken chronology and logical sequencing of actions in the system indicated the risk of manual intervention at the back end of the system.

- There were 1,89,141 decrypted bids having exactly the same bid decryption start time and end time, which again indicated the risk of manual intervention at the back end of the system.

- There were 342 bids pertaining to 120 tenders in the system, which were recorded as not having been decrypted. Out of these 120 tenders, 48 tenders had either been revoked, retendered or cancelled. However, there was no explanation as to why the bids in the remaining 72 tenders were recorded as not having been decrypted. Out of these bids which were recorded as not decrypted, contracts had been awarded in the case of five bids. This discrepancy indicated the material risk that these bids pertaining to the 72 tenders had been entered into the system through manual intervention at the back end.

  The Department stated (December 2023) that the 'bid decrypted' table was implemented at a later stage and that during initial deployment, the data had been populated from other tables using deployment scripts which had resulted in the above discrepancies.

  The response was not tenable, as these discrepancies had taken place even after the implementation of the 'bid decrypted' table in 2017-18 and details of the deployment scripts previously used were not provided to Audit for verification.

Recommendation

Government may consider to

- Minimise manual interventions at the back end of the system, by adopting formal change management process to implement required functionality for users at the front end of the application;

- Ensure mandatory maintenance of application and DBA logs to record all user actions at the front and back end of the system;

- Adopt standard operating procedures for patch management, version control and documentation of scripts used in the system.