Principal Chief Materials Managers
All Zonal Railways, PUs, CORE, COFMOW, WPO, RWP
ED/Stores, RDSO
SPMM/NAIR

Sub. : Guidelines for Procurement, Use and Management of Encryption Certificate for E-Tendering and E-Auction
Ref. : i) CRIS’s letter No. CRIS/GM-PS/EPS/16-D/2019 dated 15.11.2019
      ii) CRIS’s letter No. CRIS/GM-PS/EPS/10 dated 28.01.2015

Vide letter under reference (ii) CRIS had issued guidelines for procurement, use and management of Encryption Certificate for e-tendering and e-auction and the same was also discussed during the review meeting of sale of scrap held on 13.11.2019 at NR Hq., New Delhi.

CRIS’s letters under reference are enclosed herewith for reiteration of the instructions. The same may please be strictly followed.

DA: As above

(Vinod Kumar)
Director RS(M)
No. CRIS/GM-PS/EPS/16-D/2019

Dated: 15-11-2019

Director, Railway Stores (M)
Ministry of Railway
Railway Board
Rail Bhawan, New Delhi - 110001


Use and Management of Encryption Certificate for E-Tendering and E-Auction was discussed in the review meeting of sale of scrap held on 13/11/2019 at Northern Railway, Baroda House, New Delhi. In the meeting it was directed that that guidelines on the subject matter available on IREPS website will be reiterated by Railway Board to all concerned. A copy of the guidelines dated 28-01-2015 issued by CRIS and available on IREPS website is enclosed herewith for necessary action.

Enclosed: As above

(S.A.M. NAQVI)
GM (EPS)
Sub: Guidelines for Procurement, Use and Management of Encryption Certificate for E-Tendering and E-Auction

I. In order to ensure confidentiality of bid data and reserve price, a system of encryption called asymmetric cryptography has been employed in the Indian Railways E-Procurement System (IREPS) and Integrated Materials Management Information System (IMMIS). The asymmetric encryption is achieved through a Digital Encryption Certificate (hereinafter referred to as DEC).

The encryption certificate is to be procured from a Certifying Authority (CA). The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities and also to ensure that none of the provisions of the Act are violated. Thus, the encryption certificates are to be procured only from CA's licensed by CCA of India. List of CA's licensed by CCA of India is available on the website of CCA i.e. http://www.cca.gov.in.

II. Each individual tendering unit or auction conducting unit shall require one Digital Encryption Certificate. Separate tendering authorities and/or auction conducting authorities require separate Encryption Certificates. Stores depots where the activity of purchasing as well as auction of scrap is taking place would require two different Digital Encryption Certificates. The requirement of DEC's is summarized as under:

1. One DEC for each Stores Headquarters' Office (This will be common for all the purchase sections of Stores Hqrs. office)

2. A separate DEC for Headquarters' Office of each department like Engineering, Medical, etc. who are involved in E-Tendering through IREPS/IMMIS (common for all the purchase sections of the concerned department)

3. One DEC for Divisional Stores Officer (Sr.DMM or DMM or AMM, as applicable) of all Divisions using IREPS/IMMIS (Only one DEC is to be procured in the name of In-charge of the division even if more than one Stores Officer is posted in the division)

3.1. An additional DEC would be required for Divisional Stores Officer of those divisions which are conducting e-Auction through IREPS

4. One DEC for Stores Depot In-charge (Dy.CMM or SMM or AMM, as applicable) of all Stores Depots using IREPS/IMMIS for purchase activity
4.1. An additional DEC would be required for Dy.CMM/Depot of those depots which are conducting e-Auction through IREPS.

5. One DEC for Dy.CMM/Construction for all construction units using IREPS/IMMIS for purchase activity. In case Dy.CMM/Construction is not posted in the construction unit, the DEC may be procured in the name of SMM/Construction or AMM/Construction, as the case may be.

III. TECHNICAL REQUIREMENTS

1. Railways shall procure Encryption certificate class III SHA-256 Hash Algorithm and 2048 bit RSA Key. The certificate should have its roots up to RCAI and should be IT Act 2000 compliant. The digital certificates may be procured from CA's with two years validity.

2. Railways should clearly specify the Operating System XP (SP3), VISTA (SP2) and Windows 7, Windows 8 etc. and Internet Browser IE 8 to IE 11 etc.

3. The requirement of DECs shall be worked out as per details in para II. Above. The DEC should be procured in USB tokens only. Two copies of same DEC shall be procured by the tendering/auctioning units in two separate USB tokens. This requirement will have to be advised to the CAs in advance, as the CA may charge additional fee for providing two copies of the same DEC in two different tokens.

4. The device driver for the USB token shall be obtained from the CA at the time of supply. These drivers are Internet browser as well as operating system dependent, and the CA should be advised to supply suitable driver as per user requirement. Any problems related to installation or working of the DEC may be taken up with the CA only, as CRIS will not be able to provide any assistance in this regard.

5. The Digital Encryption certificate (DEC) and Digital Signing Certificate (DSC) should be procured on two different USB tokens. Under no circumstances shall the DECs and DSCs be procured on the same USB token.

6. The Complete procedure for Suspension/Revocation should also be obtained from the CA at the time of supply of DEC.

IV. MANAGEMENT AND SAFE-CUSTODY

1. Safe custody and proper handling of the USB token containing DEC is of utmost importance as bid data or the Reserve price encrypted with a particular DEC can be decrypted with the same DEC only. In case the DEC is lost, the tender which has been encrypted with the DEC cannot be opened. Similarly, it shall not be possible to decrypt the reserve price which will necessitate cancellation of e-auction lots.

2. Even after opening of the tender or completion of auction the DEC may be required for post event verification which may be mandated by the statutory/regulatory bodies like Vigilance, Police, Courts etc. Thus, the DEC is required to be preserved, even after expiry of the same, for the same period for
which the relevant encrypted records are required to be preserved as per the extant instructions.

3. One copy of the DEC shall be handed over to the user (Tender opening official or the Auction Conducting Official) under acknowledgement, and the user shall be responsible for safe custody and preservation of this DEC. The 2nd copy of the DEC shall be in the safe custody of an official authorized for this purpose by the competent authority.

4. On transfer/superannuation of the DEC holder, the DEC shall be handed over to the new incumbent. The user shall under no circumstances carry the DEC along with him even though the DEC may have been issued in his name.

5. All the expired DECs shall be kept in safe custody for the required period (refer para 2. ibid). A label shall be put on each such expired DEC indicating the name of the unit and the validity start and end date of the DEC. On transfer of an official having custody of the expired DECs, he shall handover all such DECs to the new incumbent and obtain an acknowledgement of the same.

6. The decryption of bids received against a tender can be done only with the same DEC whose public key was attached with the tender at the time of publication. Once a tender has been published the public key attached with the tender cannot be changed.

IREPS application does not permit attachment of encryption certificate to a tender whose date of opening is beyond the validity of the DEC. The postponement of tender opening date of a published tender beyond the validity date of attached DEC is also not permitted. Thus, in case the date of opening of tender is to be extended beyond the date of expiry of the attached DEC, there will be no option but to cancel the tender and re-invite the same attaching a new DEC. To avoid any inconvenience on this account, new DEC should be procured sufficiently in advance of the expiry of the existing DEC, and use of the DEC for publication of new tenders should be stopped 3-4 months before the expiry of the same. The use of existing DEC for opening of tenders will however continue till all the tenders published with the existing DEC have been opened.

7. In case of loss of DEC it shall be the responsibility of the holder of the DEC to inform the CA immediately for revocation of the DEC. The holder shall also immediately inform CRIS about loss of DEC.

Department heads are requested to circulate these guidelines to each unit/user using encryption certificate on IREPS/iMMIS.

(Rajaram Prasad)
GM/MMIS

Copy To:-
1. EDRS/G, Railway Board, New Delhi- For information and necessary action please.
2. OSD/IT (Stores) Northern Railway, Baroda House, New Delhi- For information and necessary action please.