**Security aspects of eKuber**

Reserve Bank of India in coordination with various State Governments, C&AG, CGA, had devised a standardized e-Payment (e-Kuber) which is completely compatible with the needs of each State Government, notwithstanding their unique internal processes, ISO 20022 messaging standards for information flow, complete capability to integrate with State Government systems with focus on security and integrity of messages.

e-Kuber is the Centralized processing unit of Reserve Bank of India. Govt of Assam has adopted e-Kuber from the year 2016 with all treasuries being directly integrated with the e-Kuber system. All payments as being submitted by the DDO’s to respective Treasuries across Assam and after being approved by Treasury Officer are being routed to beneficiaries through e-Kuber.

The communication between eKuber and the Treasury systems happens through SFTP servers located at RBI and Treasury system hosted at the Data center located at Kar Bhawan, Guwahati, Assam. The public IP addresses at both ends are being white listed so that communications happens only between the specified IP address and no third party interference happens. Also the files (payments, acknowledgements, scrolls etc) which were being shared by both the systems are digitally signed by server level certificates and follows ISO 20022 standardized Payment Message definitions which are globally accepted definitions and Universal financial industry message scheme.

The following messages are exchanged in the e-Payment process flow:

* Pain.001.001.08 --> e-Payment files from Government to e-Kuber
* Pain.002.001.08 -->e-Payment Acknowledgement/Negative Acknowledgement from e-Kuber to Government
* Pain.007.001.07--> Recall of scheduled e-Payments
* Camt.054.001.06--> Debit/Return Notification for e-Payments from e-Kuber to Government
* Camt.053.001.06 --> Account Statement from e-Kuber to Government
* Admi.004.001.02 --> Acknowledgement/Negative Acknowledgement of Debit Notification /Return Notification and Account Statement

The files are digitally signed using Class 2 certificates (DSC) as per recommendations by RBI and the following points are being taken into consideration while generating a signature for the ePayments file.

* The Government's application should generate an xml file (with extension .xml in lower case) which contains the Payments.
* The entire content of the XML file from the **<RequestPayload>** tag to **</RequestPayload>** tag (inclusive of the tags and prolog) should be considered as one message for digital signing purposes.
* The digital signature should be generated as a part of PKCS12 envelope as plain bytes. A PKCS12 envelope will contain the certificate used for signing (known as signer certificate) as well as the digital signature itself.

**Note:**ThePKCS12 envelope should not be BASE-64 encoded. It should not contain any start and end identifiers. The plain PKCS12 envelope which is a sequence of bytes should be written into the .sig file.The .sig file should have the same name as the .xml file. The only difference is in the extension.

* The digital signature should be generated using SHA-2(512 bits) algorithm for message digest and RSA-2048 algorithm for encryption.

Also the userid and passwords are well defined with standard security practices and accesses are restricted to specific folders and subfolders only, default port numbers are not followed for the SFTP access. Also ssh connections are allowed against specific internal IPs only. Data related to the transactions are well maintained in the database systems with internal IP details as to who has uploaded the data to the SFTP server. Separate user level is created at the Application level such that files can be uploaded by them only.