keypoint

FATCA NEWSLETTER

Issue No. 1197/IT - July 2016

New Encryption Mode Conversion

From Monday July 11 2016, the IRS will convert the AES cipher mode from Electronic Code Book (ECB) to Cipher Block Chaining (CBC) at 12:00 AM. The CBC cipher mode for AES encryption of payload files must be applied to all transmissions. Additionally, AES key files must be a 48 bytes file containing a 32 byte AES key and a 16 byte Initialization Vector (IV).

FATCA XML Notification Schema v2.2

As mentioned above, from July 11 2016 all the payload files in data packets that are received from the IRS must be using the AES CBC cipher mode. The file will be decrypted in the reverse manner with a 48 byte key file separated into 32 byte AES key and a 16 byte IV.

A new file error notification code is created by the IRS that indicates an 'Incorrect AES key size'. The IRS will update the FATCA XML Notification Schema with the notification code "NKS". If the ECB cipher mode with a 32 byte AES key file is used by the filers, a decryption error will be received.

Common NKS errors:

- Data packet transmitted using ECB cipher mode
- Data packet does not include a 16 byte IV in the key file
- Data packet key size is not 48 bytes
- Data packet does not contain the concatenated key and IV

For more information, enquiries and events please do not hesitate to contact: *Ranjith Kumar* on ranjith.kumar@keypoint.me or *Chahira Ashcroft* on chahira.ashcroft@keypoint.me