keypoint

FATCA NEWSLETTER

Issue No. 1192/IT - March 2016

Issue Number: 2016-2

Encryption Mode

The Internal Revenue Service (IRS) cipher mode is used for encryption from Electronic Code Book (ECB). IRS have decided to update their encryption from Electronic Code Book (ECB) to Cipher Block Chaining (CBC).

The reason for the change is that CBC cipher is a stronger algorithm for encrypting data that can be implemented in code or by any other software.

Due to the switch from ECB to CBC, IDES will no longer accept data packets encrypted with EBC cipher mode starting July 9 2016 which forces all users to transmit data packets with the CBC cipher mode.

Improved AES-256 Key Encryption

Current ECB Encryption Mode	Update to CBC Encryption Mode
Step 1: Create payload file- Encrypt XML file with AES-256 key • Cipher mode: ECB • Initialization Vector (IV): no IV • Key size: 256 bits/32 bytes	Encrypt XML file with AES-256 key • Cipher mode: CBC • Initialization Vector (IV): 16 byte IV Key size: 256 bits/32 bytes
Step 2: Encrypt AES key and IV key file - Encrypt AES key and IV key with public key of each recipient	Encrypt AES key and IV with public key of each recipient. The resulting 48 byte key includes the 32 byte AES key, plus the 16 byte IV.

Encryption Testing

IRS have opened a test period starting from 16 June up to 30 June 2016 to test the security update using the new CBC cipher mode. All data packets recived by 9 July 2016 and onwards with ECB cipher mode will be reject by the IRS. Applying the reversed process of encrypting will allow you to decrypt the data packets along with the 48 byte key file segrigated into a 32 byte AES key and a 16 byte IV.

Decryption Notification Code

Incorrect AES Key Size (NKS) formed a new decryption notification code which notifies you with data packets errors. If an NKS notification is recivied, the date packet must be reviewed for the following common errors:

- Data packet transmitted with ECB cipher mode
- Data packet does not include IV in Key File
- Data packet key size is not 48 bytes
- Data packet does not contain the concatenated key and IVr

For further information on FATCA services offered at Keypoint, please do not hesitate to contact:
Ranjith Kumar on ranjith.kumar@keypoint.me or *Chahira Ashcroft* on chahira.ashcroft@keypoint.me