International Data Exchange Service (IDES)
Data Preparation User Tips

Introduction

Due to the implementation of highly secured data transmissions, sometimes it can be challenging to trace the source of a data transmission problem. In response to user questions and common user errors demonstrated during the 2015 IDES testing windows, the IRS has compiled a list of tips to assist users with the data preparation and transmission processes.

If you identify any issues that are not covered here, please forward comments to lbi.fatca.ides@irs.gov. Due to the volume of questions received, responses to these issues will be addressed through future updates to this document or in IDES FAQs rather than via personalized responses. The suggestions below represent the most common solutions. The solutions are grouped into four categories:

Data Package
Payload file
Key file
Metadata file

All validation checks apply to the production and test environments. Certain critical errors will cause the immediate rejection of a transmission, and additional error checks will not be performed. Be aware that even if you correct the initial error, your transmission package may be rejected again if additional errors are found.

Overall Package

1. The transmission packet is in an incorrect format (not ZIP).

   The file extension must be .ZIP.

2. The file was compressed with an incorrect compression algorithm.

   All files must be compressed using the standard Deflate algorithm and common ZIP tools such as WinZip, 7Zip, etc. More information can be found at http://www.irs.gov/Businesses/Corporations/Compression-tools.

3. The data packet has an incorrect file name.

   The data packet filename must be in the format UTC_FATCAEntitySenderId.zip, where UTC represents a timestamp including milliseconds.

   For example, the filename 20150115163045322_000000.00000.TA.124.zip represents a file submitted by the Host Country Tax Authority (HCTA) for Canada created at 2015 January 15 16:30:45.32 Z.

4. The transmission packet contains subfolders.

   The transmitted ZIP file may not contain subfolders and data packets should only contain archived files at the root level.

5. The transmission packet contains additional files.

   There are too many files archived in a folder. The ZIP file should only contain one payload file, one metadata file, and either one or two keys. No other files can be included. Ensure you have the proper naming UTC_FATCAEntitySenderId.zip.

Type of File	Model 1, Option 2 (Only) - Attach 4 Files	Models 1 & 2 - Attach 3 Files
Metadata	FATCAEntitySenderId_Metadata.xml	FATCAEntitySenderId_Metadata.xml
Key File(s):	FATCAEntityReceiverId_Key	FATCAEntityReceiverId_Key
	HCTAFATCAEntityId_Key	N/A
Payload	FATCAEntitySenderId_Payload	FATCAEntitySenderId_Payload

6. The transmission packet failed virus scan.

   The transmission packets are scanned for viruses during the upload process and will be rejected and/or deleted if a virus or other threats are detected.

Payload file

7. The payload was not attached to the file.

   A valid XML payload is required with each transmission packet. The requirement also applies to test packages. If the payload file is not present, the transmission is rejected even if the other parts of the data packet are created properly.

8. The payload file was not in the proper XML format.

   The payload file must be in XML format document and created according to the published XML schema. If the data is presented in a non-XML format, your transmission will be rejected.

9. The payload file has an incorrect filename.

   The payload file name must be in the proper naming convention or format FATCAEntitySenderID_Payload.

   For example, if the sender is an HCTA, the file name should be 000000.00000.TA.NNN_Payload, where NNN is the three digit ISO code for the HCTA's country. Note that there is no extension on the file. Also check for correct capitalization.

10. The payload file is not encrypted or fails entropy check.

    It is not possible to determine whether a file is properly encrypted. IDES applies an entropy check to determine if a file was likely to be encrypted. If the file does not pass the entropy check, it will not be accepted. Encrypt the payload using a randomly generated AES-256 key with the following settings:

    - Cipher Mode: CBC
    - Salt: No Salt
    - Initialization Vector: 16 byte IV
    - Key size: 256 bits/32 bytes
    - Encoding: None
    - Padding: PKCS#5 or PKCS#7

11. The payload file is not signed.

The payload file must be digitally signed by the sender using the standard RSA digital signature method. More information can be found at http://www.irs.gov/Businesses/Corporations/Digital-Signatures-for-Data-Preparation.

12. The digital signature is not valid.

IDES requires an enveloping signature and the SHA2-256 algorithm. If an incorrect digital signature type or algorithm is used, the digital signature will fail validation. Any changes to the XML after the digital signature has been performed will cause the validation to fail. There are digital signature validation tools available that can be used to verify the signature is valid before submission.

13. The digital signature used the wrong signature type, such as enveloped or detached.

The XML must be signed with an enveloping digital signature. If the wrong digital signature type is applied the data packet will fail validation. If you create a different kind of signature but move the signature block within the XML file so that it appears to be an enveloping signature, the file will still fail validation.

14. The key used for signature does not match the certificate store.

The private key used to perform the digital signature must correspond with the certificate that was uploaded during IDES enrollment. IRS sample keys and certificates should not be included as part of the data packet.

15. The file contained incorrect encryption settings. The file may contain one or more incorrect settings, such as:

- Wrong cipher mode
- Salt settings
- Wrong key size
- Encoding applied
- Wrong padding

More information can be found at http://www.irs.gov/Businesses/Corporations/IDES-Data-Transmission-and-File-Preparation or review Item 10 above.

16. The FATCA XML Schema v1.1 contains invalid elements.

Only elements described in the published XML schema may be used. Certain elements are required in the transmitted payload XML. Review the FATCA XML Schema v1.1 User Guide at http://www.irs.gov/pub/irs-utl/Pub5124UserGuide.pdf for details.

17. The FATCA XML Schema v1.1 contains illegal characters.

Certain characters cannot be used in the FATCA data packet or must be replaced with entity references. Review the information at http://www.irs.gov/Businesses/Corporations/FATCA-XML-Schemas-and-Business-Rules-for-Form-8966 for details.

Note that some signature tools may insert illegal characters in the KeyInfo element when generating a signature. The KeyInfo element should be removed before submitting the data packet.

Key files

18. There is no key file in the transmission data packet.

    A key file representing each receiver for the package must be present in the data packet.

19. The key file has an incorrect file name.

    The key file name must be in the correct format FATCAEntityReceiverId_Key. Files received by the IRS should have a file named 000000.00000.TA.840_Key.

20. The data packet has the incorrect key size.

    The unencrypted key file should have a length of 48 bytes, 32 bytes for the AES key and 16 bytes for the IV. Encrypt the key file and place it in the archived data packet. The key size should be 256 bytes. Verify the key size before and after encryption. If you move the key file between operating systems, it may add extra characters that cause an incorrect key size or transmission failure.

21. The key file is not encrypted or fails entropy check.

    It is not possible to determine whether a file is properly encrypted. IDES applies an entropy check to determine if a file was likely to be encrypted. If the file does not pass the entropy check, it will not be accepted. Encrypt the payload using a randomly generated AES-256 key with the following settings:

    - Cipher Mode: CBC
    - Salt: No Salt
    - Initialization Vector: 16 byte IV
    - Key size: 256 bits/32 bytes
    - Encoding: None
    - Padding: PKCS#5 or PKCS#7

22. The key file is encrypted with an incorrect key.
    The 48 byte key and IV must be encrypted with the AES public key of the recipient. For files received by the IRS, use the public key available at www.ides-support.com.

23. The wrong padding was used during the encryption process.

    The padding used during the key encryption must be PKCS#1 v1.5. Ensure the tool used to perform the encryption has the correct padding settings.

24. The data packet is missing the second key file (Model 1 Option 2 Only).

    If you submit under Model 1 Option 2, there should always be two keys present in the archived data packet. One key for the IRS and the second key will be used by the HCTA. More information on keys required for the Model 1 Option 2 can be found in Step 5, Section 9.2 of the IDES User Guide.

25. The data packet contains a second key file and you are not under a Model 1 Option 2 (M1O2) IGA.

    Only submitters under a Model 1 Option 2 agreement should submit a data packet with two key files. All other submitters should submit an archived data packet that contains only one key file.

Type of File	Model 1, Option 2 (Only) - Attach 4 Files	Models 1 & 2 - Attach 3 Files
Metadata	FATCAEntitySenderId_Metadata.xml	FATCAEntitySenderId_Metadata.xml
Key File(s):	FATCAEntityReceiverId_Key	FATCAEntityReceiverId_Key
	HCTAFATCAEntityId_Key	N/A
Payload	FATCAEntitySenderId_Payload	FATCAEntitySenderId_Payload

Metadata file

26. The metadata file has an incorrect file name.

    The metadata file name must be in the recommended format FATCAEntitySenderId_Metadata.xml. For example, if the sender is an HCTA, the file name should be 000000.00000.TA.NNN_Metadata.xml, where NNN is the three digit ISO code for the HCTA's country

27. The metadata file is encrypted.

    The metadata file must NOT be encrypted. IDES reads the metadata file and uses the elements to identify and route the transmission.

28. There are invalid elements in the metadata schema.

    Please review the Metadata user guide at www.irs.gov/pub/irs-pdf/p5188.pdf for information on the fields to use in the Metadata file.

29. There are missing required elements in the metadata schema.

    IDES validates the following mandatory elements in the metadata Schema:
    - FATCAEntitySenderID (see #31 below)
    - FATCAEntityReceiverID
    - FATCAEntCommunicationTypeCd
    - SenderFileID
    - FileCreateTS
    - TaxYear (see #33 below)
    - FileRevisionInd

30. There is an incorrect type code (NTF or RPT) in the metadata schema.

    All FATCA reporting files submitted to the IRS should have the transmission type code RPT. RPT is the only allowable entry. The NTF code is used for Notifications that are sent in response by IRS. If the incorrect code (NTF) is used on a report, the file cannot be processed and will fail validation.

31. The metadata SenderID element does not match the IDES account used.

    The SenderID in the metadata file must represent the GIIN associated with the user who is logged in to IDES and transmitting the data packet.

32. The metadata ReceiverID element is not the IRS GIIN.

    The ReceiverID in the metadata file must be the IRS GIIN: 000000.00000.TA.840.

33. The metadata TaxYear element is invalid or missing.

    A valid TaxYear must be specified.

34. The metadata file contains illegal or restricted characters.

    Certain characters are prohibited and must be encoded or replaced with entity references. Review the information at http://www.irs.gov/Businesses/Corporations/FATCA-XML-Schemas-and-Business-Rules-for-Form-8966 for details.