IRS

FATCA | Foreign Account Tax Compliance Act

International Data Exchange Services (IDES)

User Guide

Publication 5190 (12-2014) Catalog Number 67386F Department of the Treasury Internal Revenue Service IRS.gov

Table of Contents

Introduction

About FATCA

The Foreign Account Tax Compliance Act (FATCA) was enacted as part of the Hiring Incentives to Restore Employment (HIRE) Act in March 2010. FATCA was created to improve transparency and address tax non-compliance by US taxpayers. Generally, FATCA requires foreign financial institutions (FFIs) and passive non-financial foreign entities (NFFEs) to report to the IRS certain information about financial accounts held by U.S. taxpayers, or by foreign entities in which U.S. taxpayers hold a substantial ownership interest. In addition, an FFI commits to the reporting requirement by registering and signing an agreement with the IRS. In most cases, FFIs that do not register with the IRS will be subject to 30 percent withholding on all US-source payments.

Financial Institutions (FIs) that register with the IRS under FATCA are issued a Global Intermediary Identification Number (GIIN) and appear on the FFI List published by the IRS. The FFI List is used to determine whether an FI is registered with FATCA and therefore whether payments to the FI must be withheld upon. The FFI List Search and Download tool allows users to search entities by GIIN, financial institution name, or country. For more information on FATCA, visit the FATCA Home Page.

To facilitate FATCA implementation for FFIs operating in jurisdictions with laws that prevent the FFIs from complying with the terms of the FFI agreement, the Treasury Department developed two alternative model intergovernmental agreements (IGAs) (Model 1 IGA and Model 2 IGA) that allow FFIs operating in such jurisdictions to perform due diligence and reporting on their account holders to achieve the objectives of FATCA.

Purpose of Guide

This guide is intended to serve as a tool for FIs and Host Country Tax Authorities (HCTAs) who enroll in the International Data Exchange Service (IDES) to transmit data. The document assumes that the reader is familiar with the FATCA regulations and is experienced with extensible markup language (XML) and schema technology.

Table 1 - FATCA Related Documents List provides a list of related FATCA publications.

Document	Description
FATCA Online Registration User Guide (Publication 5118)	Provides instructions for the online system to complete an electronic Form 8957, FATCA Registration
FFI List Search and Download Tool User Guide (Publication 5147)	Provides instructions on how to use the FFI List Search and Download Tool to search for an approved GIIN
FATCA XML Schema v1.1 User Guide (Publication 5124)	Explains the schema and elements of Form 8966
FATCA Sender Metadata Schema v1.0 User Guide (Publication 5188)	Explains the schema and elements of a FATCA metadata file (Link to 5188 will be added once guide is published)

Comments

We appreciate your feedback on the quality and usefulness of this publication. Please send comments, with a reference to chapter, section, and page number(s), to lbi.fatca.ides@irs.gov.

Technical Support

Technical assistance is available 24/7/365 through the IDES Customer Service Help Desk.

International Data Exchange Service (IDES)

About IDES

The IDES web application is a secure managed file transfer service that is available to both FIs and HCTAs to facilitate FATCA reporting. This reporting is provided for under Tax Information Exchange Agreements (TIEAs), Intergovernmental Agreements (IGAs), and other guidelines that outline how financial institutions will implement FATCA. The data collected through IDES will be incorporated into IRS compliance operations.

IDES is accessible to registered users over the Internet via Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP). The system only accepts encrypted electronic submissions, and will allow for the transmission of FATCA reporting in the approved Intergovernmental FATCA XML

Schema v1.1 (FATCA XML). IDES provides for an end-to-end controlled file transfer with enhanced monitoring and security features. For more information on FATCA regulations, Form 8966 and instructions, FATCA XML, and other related topics, visit the FATCA Home Page.

The main function of IDES is to provide authorized users with secure exchange services for FATCA data transmissions, with the additional protection of a Public Key Infrastructure (PKI). The primary features of IDES are:

- Enrollment
- Certificate Management
- Account Management
- Secure Data Transmission
- Status of Data Transmission (Alerts and Notifications)

Figure 1 - IDES Process Overview describes the enrollment process to access IDES.

Before You Begin

This material is intended to supplement the contents of IDES online help and is not intended to replace technical documentation to establish and test SFTP connections. Examples shown are based on a Windows environment and may differ if using other operating systems.

Table 2 - **Conventions** describe the graphics used throughout this guide.

Icon	Description
Bold	Bold text is used in steps to denote buttons or menu options intended to be clicked or selected
Emphasis	References to sections within this document
ISO Country Codes	Review the list of ISO country codes, 3-digit number
Printing	Use internet browser print option to print directly from IDES

Authorized Users

Authorized IDES users are either FIs or HCTAs. Each authorized user has limited access to the system based on the data flow model described in their agreement with the United States (for example, an IGA or an FFI agreement.) Note that for most FATCA users, the IRS is the only valid recipient for files. The table below provides additional information regarding user access based on the type of agreement.

Figure 2 – Valid User Types and Features summarizes IDES access, data flow and functionality based on valid user type and model. Some entities are eligible to enroll on behalf of themselves and their branches.

Type of Agreement	User Type	Access Description
Model 1 (Non-Reciprocal) FI transmits data directly to their HCTA then the HCTA transmits data to the IRS	FI	No Access
	HCTA	On behalf of FI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS ▪ Download alerts generated by IDES ▪ Download notifications, and Competent Authority Requests (CARs) submitted by IRS
Model 1 (Reciprocal)* FI transmits data directly to their HCTA then the HCTA transmits data to the IRS. This is a reciprocal model with	FI	No Access
	HCTA	On behalf of FI under the HCTA jurisdiction: ▪ Upload FATCA reporting for direct transfer to IRS

two-way transmission between the HCTA and the IRS		▪ Download alerts generated by IDES ▪ Download notifications and CARs submitted by IRS Reciprocal data will be exchanged with HCTA
Model 2 FI transmits data regarding: ▪ Consenting accountholders directly to IRS and ▪ Non-consenting accountholders and non-consenting non-participating FFIs directly to HCTA. HCTA may deliver data to US after a treaty request	FI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS (subject to the terms of the country's IGA)
	HCTA	Upload FATCA reporting regarding non-consenting accountholders and non-consenting non-participating FFIs for direct transfer to IRS (after treaty request) Download alerts generated by IDES Download notifications and CARs submitted by IRS
Non-IGA FFI transmits data directly to the US	FFI	Upload FATCA reporting for direct transfer to IRS Download alerts generated by IDES Download notifications submitted by IRS
	HCTA	No Access

* **Note:** For Model 1 Jurisdictions that have elected to do so, FIs may upload FATCA Reporting to IDES for HCTA's approval.

System Availability and Requirements

The IDES system requires a user name and password. The system will be available to authorized users 24/7/365, with the exception of regularly scheduled system maintenance periods. All users will be notified of planned and unplanned outages that could affect data transfers.

IDES works with all major browsers and can be accessed using different FTP clients for Secure File Transfer Protocol (SFTP).

Table 3 - System Requirements provide an overview of browsers and connections that have been successfully tested with IDES. Other similar technologies may work with IDES but have not been tested and therefore are not officially supported.

Items	Supported software versions or description
Browsers for HTTPS	▪ Apple Safari 5.0 on OS X only ▪ Google Chrome 33.x or later ▪ Microsoft Internet Explorer 9, 10, 11 (IE 8 and Compatibility View are not currently supported) ▪ Mozilla Firefox 29 or later
FTP clients for SFTP	▪ Axway Secure Client 5.8, 6.0, 6.1 ▪ cURL 7.19 to 7.22 ▪ FileZilla Client 3.5.x ▪ PSCP 0.60 ▪ PSFTP 0.60 ▪ Tectia Client 6.1, 6.2 ▪ VanDyke SecureFX 6.6.1 to 6.7 ▪ WinSCP 4.2.9 to 4.3.5
JavaRuntime Environment	▪ JRE 1.6 or later
JavaScript	▪ Enabled ▪ Cookies enabled
File Size	▪ File uploads and downloads are limited to a size of 200 MB compressed.
File Naming Conventions	▪ See Section *Preparing the FATCA XML* for file naming conventions. ▪ Only file extension .zip are authorized for file uploads to IDES in the user Outbox folders ▪ File names are case insensitive ▪ Do not use illegal characters in the name of files, such as colon, backslash, question mark or space

Note: Axway Secure Transport Web Access Plus (508-compliant WebUI) requires JRE 1.6 or later.

Data Security

IDES provides secure file data transfers by using symmetric and asymmetric encryption schemes to encode data. IDES uses the Advanced Encryption Standard (AES), a specification for encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).

When a supported web browser connects to IDES via HTTPS, the Transport Layer Security (TLS) cryptographic protocol provides communication security over the Internet and the session is encrypted for data confidentiality. When a supported FTP client connects to IDES via SFTP, the Secure Shell (SSH) network protocol provides secure file transfer functionality over a reliable data stream. The IDES Enrollment website requires account authentication through the use of strong passwords. Files cannot be opened, read, or decrypted at any point during data transmission.

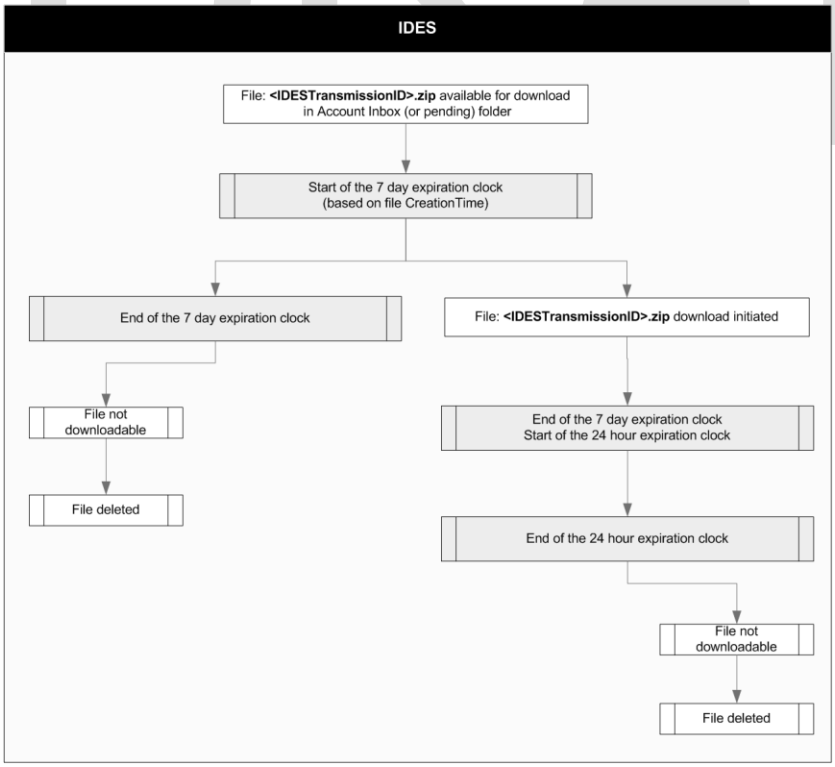
File Retention

IDES provides secured temporary file storage for data transmissions; however, IDES is not a data storage service. IDES file retention policy states that each file transmitted remains available for download in the recipient's account inbox folder for a period of 7 days. If the recipient does not download the file within 7 days, it expires and will be deleted. For this reason, expired files cannot be downloaded.

If the recipient initiates the download of a file within 7 days, that file will remain available for download for 24 hours only from the time the download is initiated. After 24 hours the file expires and will be deleted. Note that an inbox folder may contain several different transmitted files at the same time, each with a different payload.

Any files in error, such as files with an unencrypted payload or infected with a virus, will be deleted immediately.

Figure 3 - File Retention Flow shows the process to delete files from IDES.



Requirements

Certain requirements are needed to create a new account on the IDES Enrollment site. Requirements differ for HCTA and FI users.

Table 4 - IDES Enrollment Requirements provides an overview of information needed to use the enrollment portal.

Valid User Type		
Requirements	**HCTA**	**FFI**
Registered GIIN[1] See *IRS FFI List* for more information	N/A	X
HCTA GIIN **Pre-assigned user name**	The IRS provided user names to your local Competent Authority. Contact the IRS for more information	N/A
Valid certificate issued by an IRS approved certificate authority (CA) See Section, *Obtaining a Certificate*	X	X
Public and Private Key	X	X
Email address of additional users	X	X

Note: For FIs that do not have a requirement to obtain a GIIN, a separate web link will direct user to a modified Enrollment page.

HCTA User Name and Password

All countries under Model 1 IGAs have a pre-assigned username and HCTA GIIN. Each HCTA GIIN is in the format: **000000.00000.TA.<ISO>**. ISO is the ISO 3166-1 numeric standard country code. The first time a user logs on to IDES, the user is required to change its assigned username and create a password. A letter containing information on the username and enrollment instructions will be sent to an appropriate contact from each country based on their agreement with the United States. For additional information, contact FATCA IDES at lbi.fatca.ides@irs.gov .

[1] For information on how to obtain a GIIN, refer to the FATCA Online Registration System User Guide, Publication 5118

Obtaining a Digital Certificate

Purpose of Digital Certificates

Certificates and their related private keys are used to sign and decrypt messages between the sending party and the IRS. A digital certificate binds an identity to a public key. Certificate Authorities (CA) issue certificates after an identity proofing process to verify the certificate owner. The individual identified in the certificate has possession and control over the private key associated with the public key found in the certificate.

Approved Certificate Authorities

The IRS only accepts certificates issued by approved CAs. A published list of certificate authorities and acceptable digital certificate products are available on IRS.gov.

Table 5 - Certificate Authorities summarizes a list of IRS-approved CAs.

Certificate Authority	Type of Certificate	External Website Links
DigiCert	SSL Plus (Single Name)	https://www.digicert.com/welcome/ssl-plus.htm
Entrust	Standard SSL	http://www.entrust.net/ssl-certificates/standard.htm
GlobalSign	Organization SSL	https://www.globalsign.com/ssl/organization-ssl/
IdenTrust	TrustID Server (SSL)	https://www.identrust.com/certificates/buy_trustid_server.html
StartCom	StartSSL EV	https://www.startssl.com/?app=30
Symantec/Verisign	Secure Site SSL	http://www.symantec.com/ssl-certificates/secure-site/?inid=vrsn_symc_ssl_SS
Thawte	SSL Web Server	http://www.thawte.com/ssl/web-server-ssl-certificates/index.html

Uploading a Digital Certificate to IDES

After a registered user obtains a digital certificate, the user will provide the certificate to IDES during the enrollment process. The certificate is validated once upon upload by checking with the Certificate Authority (CA) that issued the certificate. IDES stores the certificate and makes it available to other IDES users who will use it to verify digital signatures and encrypt symmetric key files. It is the responsibility of IDES users to verify that the certificate is still at the time they attempt to use it.

Public Key Certificate

A public key certificate is an electronic document used to prove ownership of a public key, also known as a digital certificate. The IRS Public Key certificates can be downloaded during IDES enrollment. The administrative user will upload the digital certificate for the FI or HCTA during enrollment. All public keys or certificates are made available for all IDES users.

Maintaining Certificates

IDES uses a Public Key Infrastructure (PKI) to manage and revoke digital certificates. The Certificate Authority sets the lifetime of each digital certificate, typically up to one year. IDES requires one digital certificate per user.

A Certificate Revocation List (CRL) is a list of digital certificates that have been revoked, meaning that they are not trustworthy, and should not be used. CRLs are always issued by the trusted CA and are publicly available. IDES validates all digital certificates against the most current CRL published from each trusted CA to identify any revoked digital certificates. A revoked digital certificate will be deleted from IDES, along with the associated public key contained in the digital certificate. IDES will immediately deactivate the user account associated with a revoked digital certificate.

The Online Certificate Status Protocol (OCSP) is an Internet protocol designed for real-time verification of digital certificates against a database of revoked digital certificates. IDES tests all digital certificates using the OCSP to verify whether the digital certificates are valid. For example, when a transmission uses an expired digital certificate, IDES tests the certificate using the OCSP, confirms the certificate is revoked, and deletes the transmitted file. Users are not able to transmit the file, until a valid digital certificate is resubmitted.

IDES Enrollment

Overview

IDES Enrollment is required for FI and HCTA access to the IDES environment. Users must enter a valid GIIN and certificate to enroll. FFIs or HCTAs with invalid or expired certificates cannot enroll.

IDES Enrollment Options:

- Add, Update and Delete a User
- Update Certificate
- Disable/Enable a User
- Select Alert Preferences
- Create Metadata File

Accessing IDES

The IDES system will be available 24 hours per day, 7 days per week, with the exception of regularly scheduled system maintenance periods. Users will be notified of any unplanned outages that are expected to last more than 8 hours. IDES can be accessed through:

- IDES Enrollment Web User Interface
- Secure File Transfer Protocol (SFTP)

Preparing the FATCA XML

Overview

This section describes how to prepare and transmit a FATCA data file to IDES. Before you begin, you must have a valid certificate from an IRS approved Certificate Authority.

Preparing the FATCA XML File

These instructions are preliminary and may change with maintenance updates to the system. IDES will only accept files in .zip format. A file submitted in IDES is called a *transmission archive or transmission file.* Each archive will contain either three or four files depending on the IGA Model or type of agreement.

Table 6 - Prepare and Transmit an XML File describes the process to prepare and send a file.

Steps	Process	File Naming Convention
---	Obtain a digital certificate from an approved Certificate Authority (CA). See *Section, Obtaining a Certificate*	Not applicable
1	Prepare and validate the FATCA XML file Digitally sign the file	[SenderGIIN]_Payload.xml
2	Compress the FATCA XML file with compatible zip utility	[SenderGIIN]_Payload.zip
3	Encrypt the FATCA XML file with AES-256 Key	[SenderGIIN]_Payload
4	Encrypt AES key with public key of each recipient and For Model 1, Option 2 (only). Encrypt AES key with public key of HCTA	[ReceiverGIIN]_Key [HCTAGIIN]_Key

5	Create sender metadata	[SenderGIIN]_Metadata.xml
6	Create the transmission file	[UTC]_[SenderGIIN].zip
7	Transmit the package to IDES and receive delivery confirmation	N/A

Step 1. Prepare and Validate the FATCA XML File

Step 1 explains how to create a sender payload file. Each FATCA XML file contains information about all account holders that are US taxpayers associated with the financial institution, and includes data elements from Form 8. For information on the FATCA XML and related Form 8966, FATCA Reports, see FATCA XML Schemas and Business Rules for Form 8966.

Step 1a – Sign the XML File

Digital signatures provide the advantage of nonrepudiation and data integrity. Integrity ensures that the messages are not altered in transit. The receiver can verify that the received message is identical to the sent message. Nonrepudiation allows the sender of a message to be uniquely identified. A sender uses its own private key to digitally sign the message. Senders and recipients of FATCA files will be able to ensure that (1) the file was sent by a FATCA partner and (2) the file was not corrupted during compression, encryption, and decryption or altered during transmission to or from IDES.

Sign XML File:

Process	Descriptions	File Naming Convention
Sign XML File	▪ After validating the schema, digitally sign the FATCA XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition) "*Enveloping*" signature. ▪ To generate the digital signature[2], the XML file is processed by a "one-way hashing" algorithm to generate a fixed length message digest.	N/A

[2] Digital Signature Standard (DSS) (FIPS 186-4), July 2013, nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

	▪ IRS requires SHA2-256[3] hash with a 2048-bit RSA key as the standard for digitally signing FATCA files.	
Summary	▪ The "*Enveloping*" digital signature is contained inside the "[SenderGIIN] _Payload.xml" file.	▪ [SenderGIIN]_Payload.xml

Step 2 - Compress the XML File

The XML file "[SenderGIIN]_Payload.xml" should be compressed using a compatible compression utility and the standard Deflate compression method.

Table 7 - Recommended Compression Tools based on compression testing and supported algorithms.

Tools	Version	Host System
WinZip	17.5	Windows
7-Zip	9.2	Windows or Linux
Windows built-in zip utility	N/A	Windows
Linux/Unix standard zip utility	N/A	Linux/Unix
Apple built-in archive utility	MAC OS X 10.3 and later	MAC

[3] Secure Hash Standard (SHS) (FIPS 180-4), March 2012, csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

Compress XML File:

Process	Descriptions	File Naming Convention
Compress XML File	▪ The compressed file "zip" is the file extension used by the compression tool or library ▪ Other tools may be used but the compression method must be recognized by one of the five tools or libraries for the file to be successfully processed	▪ [SenderGIIN]_Payload.zip
Summary	▪ If the file is not recognized or processing fails, the file will be rejected. The sending partner will receive a notification that explains the reason for the failure and how to modify and resubmit the file ▪ Note: The current supported compression is ZIP compression using the standard Deflate compression method	N/A

Step 3 - Encrypt the XML File with AES 256 Key

AES is one of the most secure encryption algorithms and the preferred encryption standard for IDES. The file is encrypted to protect the AES Key.

Encrypt XML File with AES Key:

Process	Descriptions	File Naming Convention
Encrypt XML File	▪ After compression, encrypt the file "[SenderGIIN]_ Payload.zip" using the AES-256 cipher with a randomly generated "one-time use" AES key. ▪ The AES encrypted file is called SenderGIIN]_Payload"	▪ [SenderGIIN]_Payload

Additional information regarding the AES-256 encryption algorithm and keys can be found in:

- NIST Special Publication 800-57:
  Recommendation for Key Management – Part 1: General (Revision 3)
  csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- Advanced Encryption Standard (FIPS 197), November 2001,
  csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Step 4 - Encrypt the AES Key with Public Key of Recipient

The next step is to encrypt the AES key with the public key of each recipient. All FATCA partners must validate the recipient's X.509 Digital Certificate to an approved CA. An X.509 Digital Certificate contains the public key for each FATCA partner, including the IRS, and is retrieved from the IDES Enrollment site.

Encrypt AES Key with Public Key:

Process	Descriptions	File Naming Convention
Validate Certificate	▪ To validate certificate: 1. Verify the certificate chain; 2. Check the revocation status of the certificate chain. There are two methods: ▪ Retrieve a Certificate Revocation List (CRL) or ▪ Send an Online Certificate Status Protocol (OCSP) query to a CA designated responder	N/A
Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key and specify "*PKCS7 with Padding*" ▪ The encrypted file is called "[ReceiverGIIN]_Key" "ReceiverGIIN" is the GIIN of the recipient of this AES Key	▪ [ReceiverGIIN]_Key
Summary	▪ FATCA reporting with one recipient will have two encrypted files: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file called "[SenderGIIN]_Payload" 2. Asymmetric encryption - the Public Key encrypted AES 256 Key file called "[ReceiverGIIN]_Key"	N/A

Note: For most FATCA partners (e.g., Model 1 (Non-Reciprocal), Model 2 and non-IGA) the IRS is the only recipient.

Step 5 - Encrypt the AES Key – Model 1, Option 2

Under IGA, Model 1, Option 2, an FI submits a FATCA XML file to IDES. The HCTA reviews and releases or denies the file to the IRS. The HCTA and the IRS will decrypt the same FATCA XML file. The FI creates a duplicate of the original AES 256 Key. The duplicate AES 256 Key is encrypted with the HCTA Public Key.

Encrypt AES Key – Model 1, Option 1:

Process	Descriptions	File Naming Convention
Validate Certificate	▪ See Step 4 – Validate Certificate	
Encrypt the AES Key	▪ After validating the certificate, use the public key from the recipient's certificate to encrypt the AES 256 key and specify "*PKCS7 with Padding*" ▪ The encrypted file is called "[ReceiverGIIN]_Key" "ReceiverGIIN" is the GIIN of the recipient of this AES key	▪ [ReceiverGIIN]_Key
Encrypt the AES Key	▪ Encrypt the AES Key with the public key of the approving HCTA ▪ The encrypted file is called "[HCTAGIIN]_Key", where "HCTAGIIN" is the GIIN of the HCTA recipient of this AES key	▪ [HCTAGIIN]_Key
Summary	▪ FATCA reporting with two recipients should have three encrypted files: 1. Symmetric encryption - the AES 256 encrypted FATCA XML file called "[SenderGIIN]_Payload" 2. Asymmetric encryption - the Public Key encrypted AES 256 Key file called "[ReceiverGIIN]_Key" 3. Asymmetric encryption - the Public Key encrypted AES 256 Key file called "[HCTAGIIN]_Key"	N/A

Step 6 - Create Sender Metadata File

Users can create a sender metadata file to ensure that recipients accurately process FATCA XML files and notifications. Notifications are responses sent by the IRS to an FI or HCTA and state whether the file was processed correctly or contained errors.

A template metadata file is available in XML or text file format as part of the enrollment process. IDES automatically converts text metadata files into XML metadata files during file processing. FIs and HCTAs can use the template to create a metadata file to attach to the payload before uploading to IDES.

The FATCA Sender Metadata XML file is created using the IRS FATCA Metadata v1.0 Schema and the file will be called "[SenderGIIN]_Metadata.xml". All FATCA partners must provide the values for the elements in the sender metadata file. Refer to the FATCA XML Schemas page for more information.

Table 8 - Sender Metadata Schema v1.0 lists and describes metadata schema elements.

Elements	Length	Description
FATCAEntitySenderId	N/A	FATCA partner that submits data
FATCAEntityReceiverId	N/A	FATCA partner receives data
FATCAEntCommunicationTypeCd	N/A	Indicates the transmission type RPT = FATCA reporting communication NTF = FATCA Notification communication
SenderFileId	200	References the user provided transmission filename
FileCreateTs	N/A	References timestamp created by the sender transmission
TaxYear	4	Indicates the tax year (YYYY format)
FileRevisionInd	1	Indicates if this is a revised transmission
OriginalIDESTransmissionId	32	IDES Transmission ID referencing an update to an earlier transmission Optional – Use only after IRS request
Optional – Use only after RCTA request	N/A	Optional - User email address

Note: The sender metadata file is never encrypted because it is used to verify and route transmissions to the correct recipient.

Step 7 - Create a FATCA Data Packet

A file that is transmitted through IDES is known as a *FATCA data packet* or *data packet*. The data packet is an archive in .ZIP file format, and it should be created using one of the compatible data compression tools described in Table 7. IDES only supports data packets in a .ZIP file format with a .zip file extension.

Table 9 – Transmission Summary lists files contained in a transmission archiveTransmission Archive.

Model 1, Option 2	All Others
▪ [SenderGIIN]_Metadata.xml	▪ [SenderGIIN]_Metadata.xml
▪ [ReceiverGIIN]_Key	▪ [ReceiverGIIN]_Key
▪ [HCTAGIIN]_Key	▪ [SenderGIIN]_Payload
▪ [SenderGIIN]_Payload	

The file naming convention of data packet is composed of a Coordinated Universal Time (UTC) timestamp and the GIIN of the sender (SenderGIIN) as:

[UTC]_[SenderGIIN].zip

The timestamp format of the UTC is YYYYMMDDTHHMMSSmsZ where:

YYYY = 4-digit year
MM = 2-digit month
DD = 2-digit day
HH = 24-hour
MM = 2-digit minutes
SS = 2-digit seconds
ms = 3-digit milliseconds

For example, a sender of GIIN "000000.00000.TA.ISO" that transmits a data packet on January 15, 2015 at 16:30:45 can create a data packet named as:

20150115T163045123Z_000000.00000.TA.ISO.zip

Step 8 - Transmit Package to IDES

After the archive is uploaded and transmitted, IDES sends an alert to the authorized user via email. The message provides status information about the file upload. If the upload and IDES file checks are successful, IDES assigns a unique "TransmissionID" in the email. If there is an error, the alert provides an appropriate error code in the email message.

Receiving a Notification Message from IRS

A notification is a "transmission" archive that contains encrypted documents sent from the IRS to an FI or HCTA. When the IRS sends a notification, IDES sends an email to the authorized user stating that a file is ready for download. The email correspondence includes the file name of the "TransmissionID" in the original file. Notifications are prepared using the same process and file components used to prepare the FATCA XML.

Users will need to download and unzip the notification message archive. IDES assigns each archive a unique filename [IDESTransmissionID].zip. Users can also process the elements contained in the IRS notification.

Note: In a Notification Message, the [SenderGIIN] is the IRS and [ReceiverGIIN] is either the HCTA or FFI.

Table 10 - Notification Archive Summary describes how to open the archive.

Steps	Process	File Naming Convention
1.	Validate the sender metadata file using the IRS Sender Metadata schema.	[SenderGIIN]_Metadata.xml
2.	Use your private key to decrypt the [ReceiverGIIN]_Key file	[ReceiverGIIN]_Key [HCTAGIIN]_Key
3.	Use the revealed AES key to decrypt the [SenderGIIN]_Payload.	[SenderGIIN]_Payload
4.	Decompress the [SenderGIIN]_Payload.zip	[SenderGIIN]_Payload.zip [SenderGIIN]_Payload.xml
5.	Validate “Enveloping” Digital Signature of the Notification XML file (the Payload).	N/A
6.	Validate the Notification XML file using the IRS notification schema.	N/A

Appendix A: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CRL	Certificate Revocation List
FATCA	Foreign Account Tax Compliance Act
FCPA	Federal Common Policy Root CA
FFI	Foreign Financial Institution
FI	Financial Institution
FTP	File Transfer Protocol
GIIN	Global Intermediary Identification Number
HCTA	Host Country Tax Authority
HTTPS	Hypertext Transfer Protocol Secure
IDES	International Data Exchange Service
IGA	Intergovernmental Agreement
IRS	Internal Revenue Service
NFFE	Non-Financial Foreign Entity
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PMO	Project Management Office
RSA	Rivest, Shamir and Adleman
SFTP	Secure File Transfer Protocol

SSH	Secure Shell
TIEA	Tax Information Exchange Agreement
TLS	Transport Layer Security
UTC	Coordinated Universal Time
XML	Extensible Markup Language

Appendix B: File Naming Convention

Note: N/A fields to be updated in final version

File Name	Description	Associated IGA Group
[Sender]GIIN_Payload	Encrypted payload using a randomly generated one-time use key (preference: AES-256)	All
[Receiver]GIIN_Key	Key encrypted using the receiver public key	All
[Sender]GIIN_Metadata.xml	FATCA Metadata to ensure that recipients properly process FATCA XML reports. FATCA Metadata XSD will be published on the IRS website Note: A text version of the FATCA metadata [Sender]GIIN_Metadata.txt will be accepted for partners not familiar with xml.	N/A
[HCTA]GIIN_Key	Key encrypted using HCTA public key	Model1 Option 2
UTC_[SenderGIIN].zip	N/A	N/A

Disclaimer

This document is a draft and is being provided to the public for information purposes only. Information in this document is indicative, and is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, for any purpose, without the express written of permission the IRS.

All screen shots that appear throughout the IDES User Guide (IRS Publication 5190) are used with the permission of IRS. The screen shots used in this publication—or any other screen shots from IDES or its affiliated programs—may not be extracted, copied, or distributed without written approval from the IRS SPEC Office of Products, Systems, & Analysis.