INLAND REVENUE BOARD OF MALAYSIA

USER GUIDE FOR THE PREPARATION AND ENCRYPTION OF FILES FOR TRANSMISSION THROUGH THE HASIL INTERNATIONAL DATA EXCHANGE FACILITY (HiDEF)

(Revised Version – April 2018)

Contents

1. DATA PREPARATION FOR CRS XML REPORT

1.1 Overview

This section describes how to prepare a CRS data file. Before you begin, you must have a valid certificate from an IRBM approved certificate authority.

1.2 Prepare the CRS XML File

These instructions may change with maintenance updates to the system. HiDEF will only accept files in .zip format. Each archive will contain three files and it will consists of the following files:

- MyCRSID_CRS_Metadata.xml
- MyCRSID_CRS_Payload
- MyCRSID_CRS_Key

Steps	Process	File Naming Convention
---	Obtain a digital certificate from an approved Certificate Authority (CA)	MyCRSID_CRS_Cert.cer
1	Prepare and validate the CRS XML file Digitally sign the file	MyCRSID_CRS_Payload.xml
2	Compress the CRS XML file with compatible zip utility	MyCRSID_CRS_Payload.zip
3	Encrypt the CRS XML file with AES-256 key	MyCRSID_CRS_Payload
4	Encrypt AES key with IRBM public key	MyCRSID_CRS_Key
5	Create sender metadata	MyCRSID_CRS_Metadata.xml
6	Create the transmission file.	MyCRSID_RPTYR_CRS_UTC.zip
7	Transmit the data packet to HiDEF and receive delivery confirmation	N/A

1.3 MyCRSID

A MyCRSID is created after registration. The ID is a unique 8 character-length number that identifies the transmission. This ID will be included in both HiDEF system alerts and notifications generated by the IRBM.

1.3.1 RPTYR

RPTYR represents the reporting tax year. It is a 4 character-length number in YYYY format.

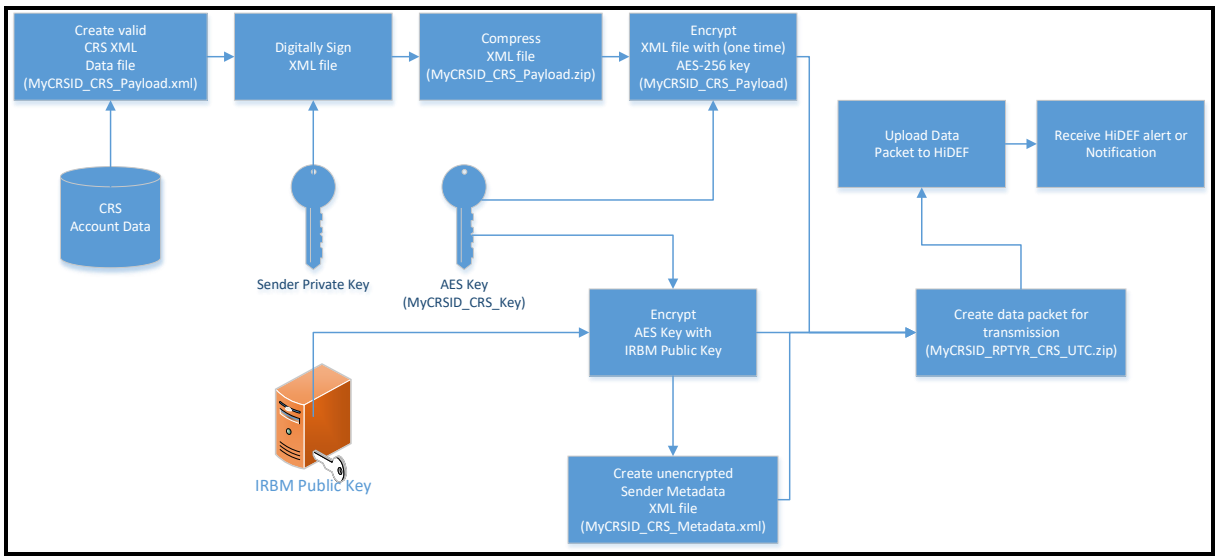
1.3.2 UTC

UTC represents a timestamp including milliseconds. 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, the timestamp for January 25, 2016 at 16:30:45.321 is represents by 20160125T163045321Z.

2. PROCESS TO PREPARE AND TRANSMIT XML FILE



STEP 1 - CREATE AND VALIDATE THE CRS XML FILE

Step 1 explains on how to create a sender payload file. Each CRS XML file contains information about the accounts required to be reported under CRS. Ensure that all XML elements have prefixes, do not use default namespaces. For information on the CRS XML and in relation to CRS Report, see CRS XML Schema, CRS User Guide (XML Schema) Ver 2.0 and sample for CRS Payload XML file, please click here.

STEP 2 - DIGITALLY SIGN CRS XML FILE

Digital signatures are used to assure data integrity, which means that the messages are not altered in transmission. HiDEF can verify that the received message is identical to the sent message. FI uses its private key to digitally sign the message. Senders (FI's) and recipient (IRBM) of CRS files will ensure that the file was not corrupted during compression, encryption, and decryption, or altered during transmission to or from HiDEF.

Sign XML File:

Process	Description	File Naming Convention
Sign XML File	• Prepare the CRS reporting data using XML element prefixes. Do not use the default namespaces. • To generate the digital signature1, the XML file is processed by a "one-way hashing" algorithm to generate a fixed length message digest. • Depending on the tool used to perform the digital signature, a different type of canonicalization method may be required. The following methods are acceptable: ○ <Canonicalization Method Algorithm="http://www.w3.org/2001/10/xmlexc-c14n#"/> ○ <Canonicalization Method Algorithm="http://www.w3.org/TR/2001/RECxml-c14n-20010315"/> • IRBM requires that the payload file be signed by first creating a SHA2-256 hash. The Sender will then create an RSA digital signature using the 2048-bit private key that corresponds to the public key found in the Sender's digital certificate on HiDEF. • After validating the schema, digitally sign the CRS XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition)3 "enveloping" signature. • Use the digital signature "enveloping" type. The "enveloped and detached" types will cause the transmission to fail. • The file name is "MyCRSID_CRS_Payload.xml". The file is case sensitive and any variation in file name or format will cause the transmission to fail.	MyCRSID_CRS_Payload.xml

STEP 3 - COMPRESS THE XML FILE

The XML file "MyCRSID_CRS_Payload.xml" should be compressed using a compatible compression utility and the standard Deflate compression method.
Recommended compression tools.

Tool	Version	Operating 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

Compress XML File

Process	Description	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.	MyCRSID_CRS_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 transmission failure and how to modify and resubmit the file. • The file name "MyCRSID_CRS_Payload.zip". The file is case sensitive and any variation in file name or format will cause the transmission to fail. • Note: The current supported compression is ZIP compression using the standard Deflate compression method.	N/A

STEP 4 - ENCRYPT THE XML FILE WITH AES 256 KEY

AES is one of the most secure encryption algorithms and the preferred encryption standard for HiDEF. The file is encrypted to protect FI and taxpayer sensitive information.

Process	Description	File Naming Convention
Encrypt XML File	• After compression, encrypt the file "MyCRSID_CRS_Payload.zip" using the AES-256 cipher with a randomly generated "one-time use" AES key. • While performing AES encryption, there are several settings and options depending on the tool used to perform encryption. IRBM recommended settings should be used to maintain compatibility: ○ Cipher Mode: CBC (Cipher Block Chaining).	MyCRSID_CRS_Payload

	○ Salt: No salt value ○ Initialization Vector: 16 byte IV ○ Key Size: 256 bits / 32 bytes – Key size should be verified and moving the key across operating systems can affect the key size. ○ Encoding: There can be no special encoding. The file will contain only the raw encrypted bytes. ○ Padding: PKCS#7 or PKCS#5 • The AES encrypted file name is "MyCRSID_CRS_Payload". The file is case sensitive and any variation in file name or format will cause the transmission to fail.	

STEP 5 - ENCRYPT THE AES KEY WITH IRBM PUBLIC KEY

The next step is to encrypt the AES key with the IRBM public key. The file is encrypted to protect the AES key. All CRS partners must validate the IRBM X.509 Digital Certificate to an approved CA. An X.509 Digital Certificate contains the public key for IRBM, and it can be retrieve from the IRBM website.

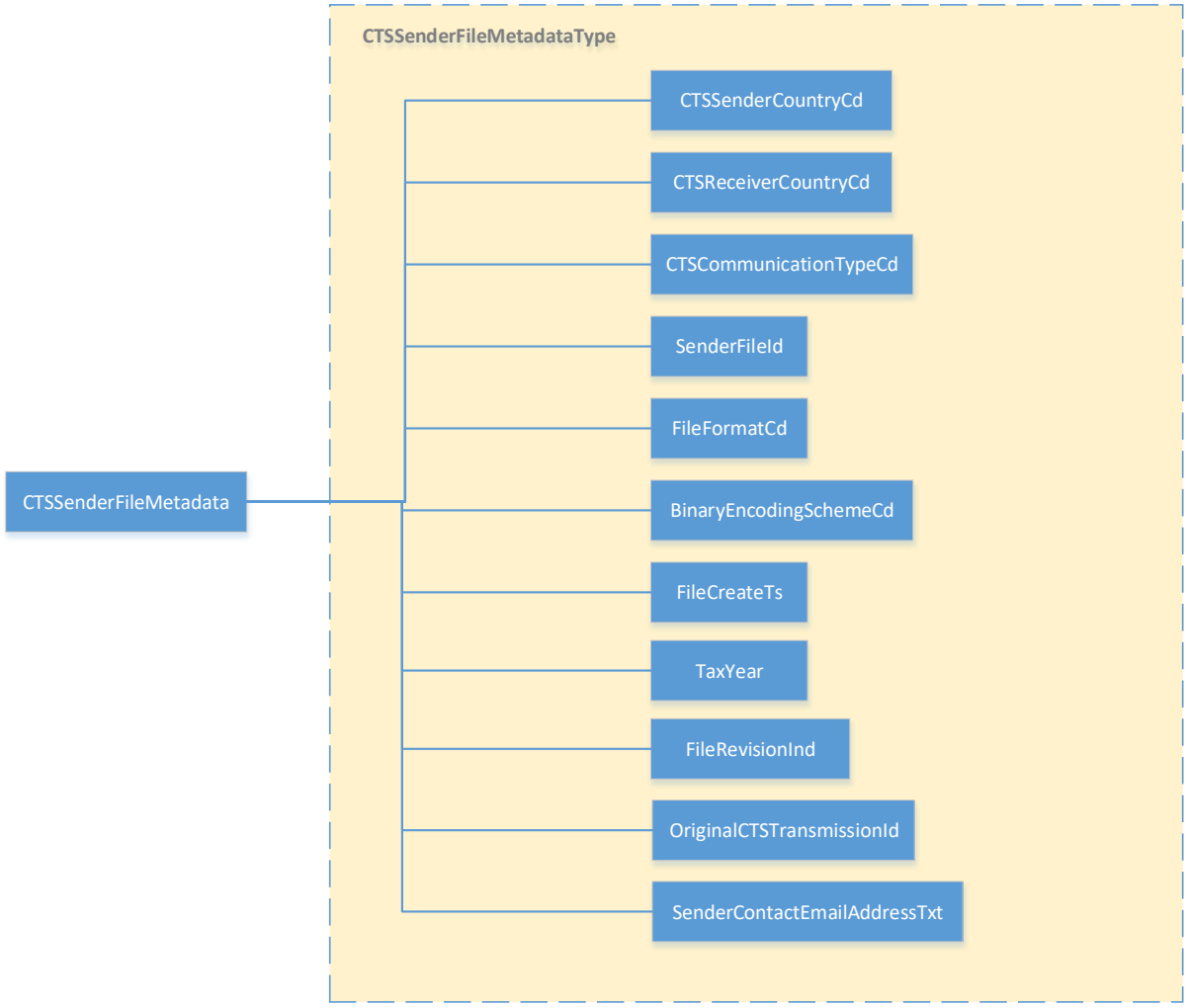
Encrypt AES Key with Public Key:

Process	Description	File Naming Convention
Validate Certificate	• To validate the 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. • The public key encryption uses the standard RSA algorithm. While performing AES encryption, there are several settings and options depending on the tool used. IRS recommended settings should be used to maintain compatibility: ○ Padding: PKCS#1 v1.5 ○ Key Size: 2048 bits • The encrypted file name is "MyCRSID_CRS_Key". "MyCRSID" is the 8-character HiDEF login id.	MyCRSID_CRS_Key
Summary	• CRS reporting with IRBM as a recipient will have two encrypted files. The files are case sensitive and any variation in file name or format will cause the transmission to fail: 1. Symmetric encryption - the AES 256 encrypted CRS XML file name is "MyCRSID_CRS_Payload" 2. Asymmetric encryption - the public key encrypted AES 256 key file name is "MyCRSID_CRS_Key"	N/A

STEP 6 - CREATE SENDER METADATA FILE

Users can create a sender metadata file to ensure that IRBM accurately process CRS XML files and notifications. Notifications are sent by the IRBM to an FI and state whether the file is processed correctly or contained errors.

FIs must create a metadata file to attach to the payload before uploading to HiDEF. The CRS Sender Metadata XML file name is “MyCRSID_CRS_Metadata.xml.” All FI’s must provide the values for the elements in the sender metadata file.



FI’s must provide the values for the required elements in the Metadata. Please note that the Metadata file is validated by the HiDEF system and if the required information is missing, the uploading process will fail.

The content to be provided in the different elements of the CRS Metadata Schema is as follows:

- The CTSSenderCountryCd element identifies the jurisdiction of the Sending Competent Authority. Only a value MY is currently allowed.
- The CTSReceiverCountryCd element indicates the jurisdiction of the Receiving Competent Authority. Only a value MY is currently allowed.
- The CTSCommunicationTypeCd element specifies the type of message transmitted. Only a value CRS is currently allowed.

- The SenderFileID element is a free text field to capture the file name or ID created by the Sending Financial Institution. The element helps both the Sending FI's and Receiving IRBM Authority to track and monitor a specific message. The agreed format is:

  CRS_ MY+MyCRSID +Date +SEQNO

  - MyCRSID – will be given upon registration of MYFI with HiDEF
  - Date format – YYYYMMDD
  - SEQNO – 4 digits character (0000 – 9999)

  For example, a sender with a MyCRSID of "10000001" that transmits a data packet on January 15, 2015 at 16:30:45 can create a SenderFileID as:

  CRS_MY100000012015011500001

- TheFileFormatCd element specifies the file format of message transmitted, the only allowable value being XML.

- The BinaryEncodingSchemeCd element identifies the type of encoding scheme for the transmission payload. If sending an XML file, the value should be 'NONE'.

- The FileCreateTs element identifies the timestamp for the transmission payload created by the Financial Institution. The format for use is YYYY-MM-DD'T'hh:mm:ss. Fractions of seconds may be used. Example: 2018-02-15T14:37:40.

- The Tax Year element specifying the tax year to which the file relates.

- The FileRevisionInd element is a Boolean field to indicate if the file is a revised message. The only allowable values are "true" or "false".

- The OrginialCTSTransmissionId element is a free text field to reference the unique original HiDEF transmission ID. The identifier helps both the FI's and IRBM to track and monitor messages. HiDEF Transmission ID referencing an update to an earlier transmission
  - Optional – Use only after IRBM request

- The SenderContactEmailAddressTxt element is a free text field to identify the email address of the Financial Institution.

STEP 7 - CREATE A CRS DATA PACKET

A file that is transmitted through HiDEF is known as a CRS 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 Step 3. HiDEF only supports data packets in a .ZIP file format with a .zip file extension. The files are case sensitive and any variation in the file name or format will cause the transmission to fail.

Files contained in a transmission archive or data packet :

- MyCRSID_CRS_Metadata.xml
- MyCRSID_CRS_Key
- MyCRSID_CRS_Payload

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

File Name	Description
MyCRSID_RPTYR_CRS_UTC.zip	Transmission file to be sent through the HiDEF

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 with a MyCRSID of "10000001" that transmits a data packet on January 15, 2015 at 16:30:45.123 for reporting year 2014 can create a data packet named as:

- 10000001_2014_CRS_20150115T163045123Z.zip

STEP 8 - TRANSMIT DATA PACKET USING HiDEF

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

3. HiDEF PUBLIC KEY INFRASTRUCTURE (PKI)

3.1 CURRENT LIST OF APPROVED CERTIFICATE AUTHORITIES

Certificate Authority	Type of Certificate	External Website Links
Digicert®	SSL PlusTM (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.htmlhttp://identrust.com/irs/fatca/index.html
StartCom®	StartSSLTM 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

3.2 LOCAL RESELLER

Certificate Authority	Type of Certificate	External Website Links
POS Digicert Sdn Bhd	SSL Certificates	https://www.posdigicert.com.my
TM Applied Business	SSL Certificates	http://www.tab.com.my
MSC Trustgate.com Sdn. Bhd.	SSL Certificates	https://www.msctrustgate.com

3.3 CERTIFICATE FORMAT

Before you begin the HiDEF registration process, each entity should obtain one valid digital certificate issued by an approved certificate authority (CA). Certificates in other formats, such as self-sign will be rejected. HiDEF will ONLY accept digital certificates issued by an approved CA.

Supported formats for the digital certificates are:

- Distinguished Encoding Rules (DER) binary X.509
- Privacy Enhanced eMail (PEM) ASCII (Base-64) encoded X.509

HiDEF will convert digital certificates received in DER format to Base64 for storage and retrieval. If a digital certificate is not in DER or PEM format, use Windows 7 to convert your digital certificate to DER or PEM as follows:

- Open the digital certificate with a .CRT filename extension
- Select the Details tab
- Select the “Copy to File…” button
- In the Certificate Export Wizard, select the format you want to use as either “DER encoded binary X.509 (.CER)” or “Base-64 encoded X.509 (.CER)”.

3.4 UPLOAD A DIGITAL CERTIFICATE TO HiDEF

After a Financial Institution (FI) obtains a digital certificate, the FI will provide the certificate to HiDEF. In order to do that, FI is required to login to HiDEF using myCRSID created after registration and upload the certificate. Upon upload, the certificate is validated by the Certificate Authority (CA) that issued the certificate. It is the responsibility of HiDEF users to verify that the certificate is valid before use. FI must use different digital certificate for multiple entities.

(Refer to Current list of approved Certificate Authorities for the HiDEF and Local Reseller in para 3.1 and 3.2)

3.5 PUBLIC KEY CERTIFICATE

A public key certificate, also known as a digital certificate, is an electronic document used to prove ownership of a public key. The IRBM public key certificate can be downloaded from IRBM website.