Ministry of Finance

Republic of China (Taiwan)

A Brief Introduction in Respect of

Taiwan's International Exchange of Information Platform (IEIP)

Table of Contents

Figure

Table

1 Prologue

1.1 Scope of Service

The main function of the IEIP is to provide enrolled users with secure exchange services for data transmissions. In the first phase (beginning September 2020), transmission service provided by the IEIP will only be available to the "financial account information which being in conformity with the OECD's Common Reporting Standards" (hereinafter referred to as CRS). In the foreseeable future (the following phases), the scope of the IEIP service for transmission will be extended to the "Country-by-Country Reports which being in line with the BEPS Action 13," and other information, e.g., data in relation to a specific request or a spontaneous exchange raised or provided by a Jurisdiction for carrying out the necessary exchange of information.

1.2 Process Overview

The primary features of the IEIP are to provide services with respect to enrollment, certificate management, account management, secure data transmission, and status of data transmission. The process of enrollment and access to the IEIP are demonstrated in Figure 1 below:

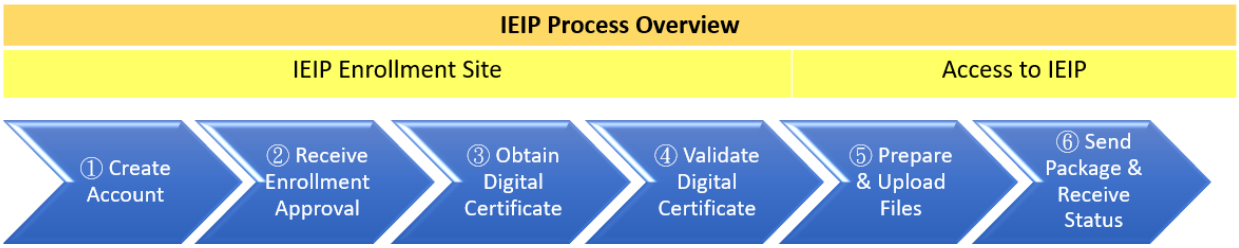

Figure 1: IEIP process overview

1.3 System Availability

IEIP will be available 24 hours a day for an enrolled user. All users who own valid IEIP accounts will be notified of planned outages, as well as unplanned outages that are expected to last more than 8 hours.

IEIP is accessible to enrolled users over the Internet via Hypertext Transfer Protocol Secure (HTTPS) or Secure File Transfer Protocol (SFTP). System Requirements for access to the IEIP via HTTPS or SFTP are summarized in Table 1.

Table 1: System requirements

Items	Technical Specifications
Browsers for HTTPS	Microsoft Internet Explorer 11 or later Mozilla Firefox 45 or later Google Chrome Apple Safari
FTP clients[1]	FileZilla Client 3.5.x
SSH clients[2]	FileZilla Client 3.5.x
JavaRuntime Environment (JRE)	JRE 1.8 or later
JavaScript	JavaScript enabled
File Size	File uploads and downloads are limited to a size of 200 MB compressed

1.4 Secure Data Transmission

IEIP requires the main file for transmission to be digitally signed and be encrypted with AES-256 key. With digital signature in place, it is ensured that the aforesaid file is not altered in transmission and the receiver can verify that the received message is identical to the sent message. With AES encryption technology in place, it is ensured that the aforesaid file is securely protected. In addition, when a supported web browser connects to IEIP via HTTPS, the Transport Layer Security (TLS) cryptographic protocol provides communication security over the Internet and the session is encrypted for data confidentiality.

1.5 Data Retention

IEIP prohibits long-term data storage. Data packets that contain errors, such as with an unencrypted payload or virus, will be automatically deleted. After the IEIP informs an enrolled user to download a file, the IEIP will start counting; the file must be downloaded within 10 days. In the case that the file is not downloaded within the time limit, the file will be deleted automatically. The file will also be deleted automatically within 48 hours, counting from the time the downloading process is performed by an enrolled user.

[1] Technical specification of the FTP clients will be expended depending on the IEIP's development.
[2] Technical specification of the SSH clients will be expended depending on the IEIP's development.

2 Digital Certificate

2.1 Approved Certificate Authorities

IEIP only accepts certificates issued by approved Certificate Authorities (CA), as listed in Table 2.

Table 2: Certificate Authorities accepted by the IEIP

Certificate Authority	Type of Certificate	RSA key length
Sectigo (formerly Comodo)	Extended Validation SSL Certificates (EV SSL)	4096-bit RSA key
DigiCert	EV SSL	4096-bit RSA key
Entrust	EV SSL	4096-bit RSA key
GoDaddy	EV SSL	4096-bit RSA key
GlobalSign	EV SSL	4096-bit RSA key
IdenTrust	EV SSL	4096-bit RSA key

2.2 Certificate File Format

Before a user begins the IEIP registration process, he/she is required to obtain one valid digital certificate issued by an approved CA (please refer to Table 2). Certificates in other formats, such as self-sign, will be rejected by the IEIP. IEIP will ONLY accept supported formats for the digital certificates issued by an approved CA. These supported formats are:

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

IEIP will convert digital certificates received in DER format to Base64 for storage and retrieval.

3 Services of the IEIP

3.1 Enrollment

A web-based system allows users to register, set, and maintain the associated accounts (please refer to Figure 2). When a new user registers, it is required for him/her to have a valid digital certificate. After that user is properly enrolled, he/she will become a Jurisdiction Administrator and acquire a username and associated password for the access to the IEIP environment.

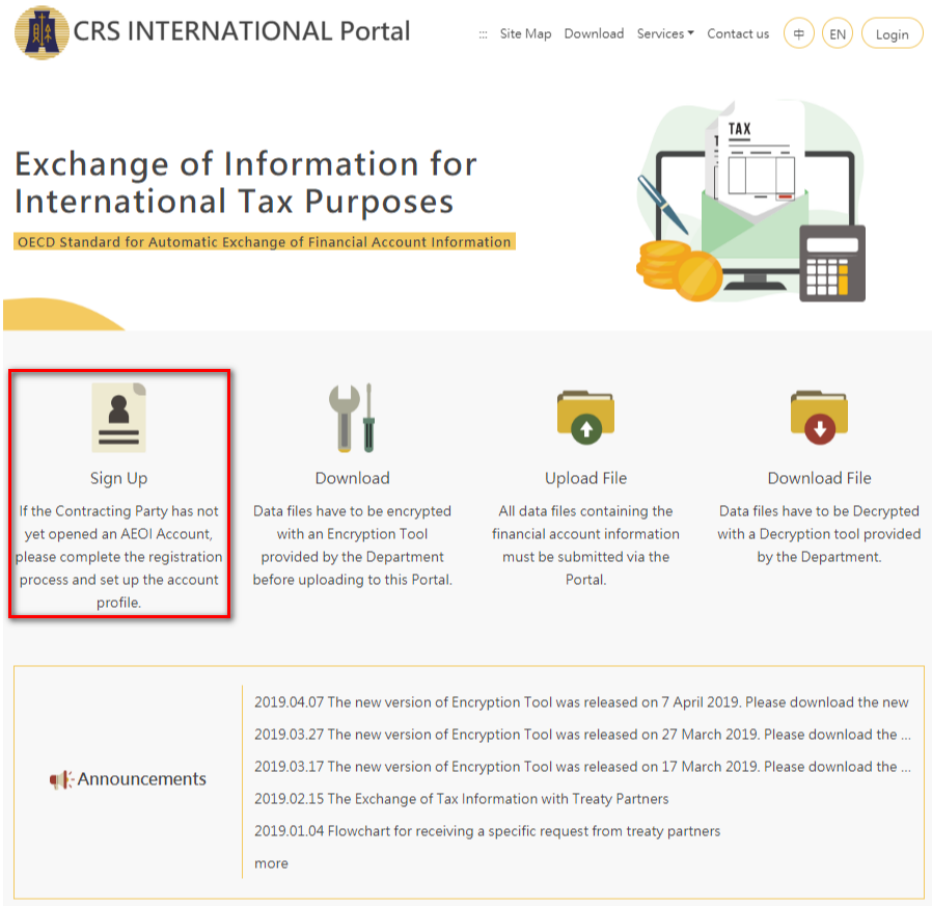

Figure 2: Enrollment[3]

3.2 Account Management

A Jurisdiction Administrator will have the power to add general user, disable and enable general users, and maintain other settings in association with his/her Jurisdiction. The general user of a Jurisdiction acquires only limited accessibility enough for his/her operations.

[3] Design of the web page and its detailed functions may be subject to change depending on the IEIP's development.

Jurisdiction Administrator may perform account management via IEIP (please refer to Figure 3). For instance, when Jurisdiction Administrator would like to add a general user for its Jurisdiction, he/she can create a user name and enter that general user's email and press "Invite" to initiate the invitation process. IEIP will email a one-time password (OTP) to that general user, inviting him/her to log in to complete the general user's account creation.

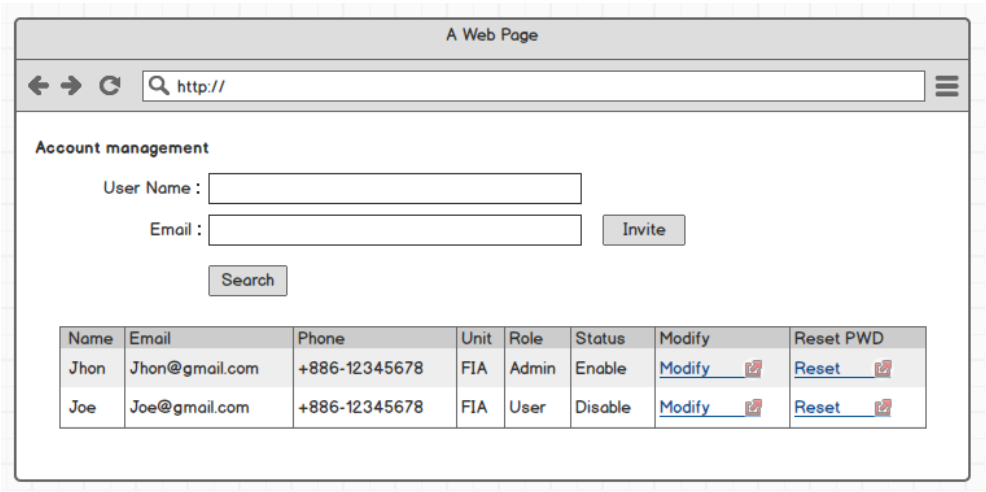

Figure 3: Account management for a Jurisdiction Administrator[4]

3.3 Certificate Management

3.3.1 Upload a digital certificate

After a Jurisdiction Administrator completes the enrollment process and logs into the IEIP for the first time, IEIP will guide him/her (as shown in Figure 4) to insert its AgreementID[5] and select a digital certificate (a public key) to be uploaded for its Jurisdiction. In addition, a Jurisdiction Administrator is responsible for maintaining the validity of the certificate at all times in order for its Jurisdiction to perform the necessary verification and encryption operations.

[4] Design of the web page and its detailed functions may be subject to change depending on the IEIP's development.

[5] AgreementID is a serial number that is issued by the IEIP after enrollment for uploading a digital certificate, data transmission, etc.

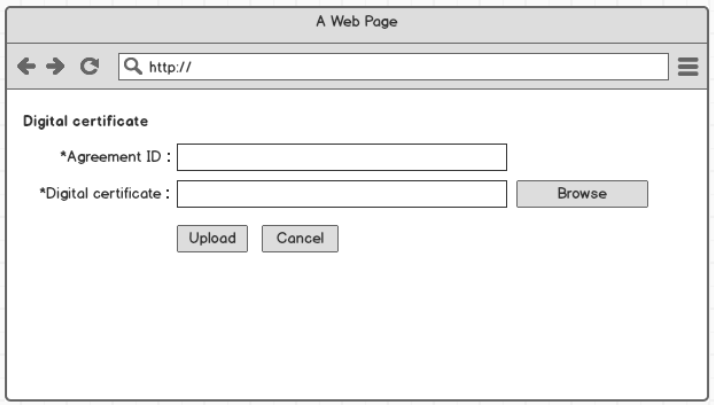

Figure 4: Upload a digital certificate[6]

3.3.2 Download a digital certificate

Jurisdiction Administrator can also download Taiwan's digital certificate (a public key) for its transmission via the IEIP (please refer to Figure 5).

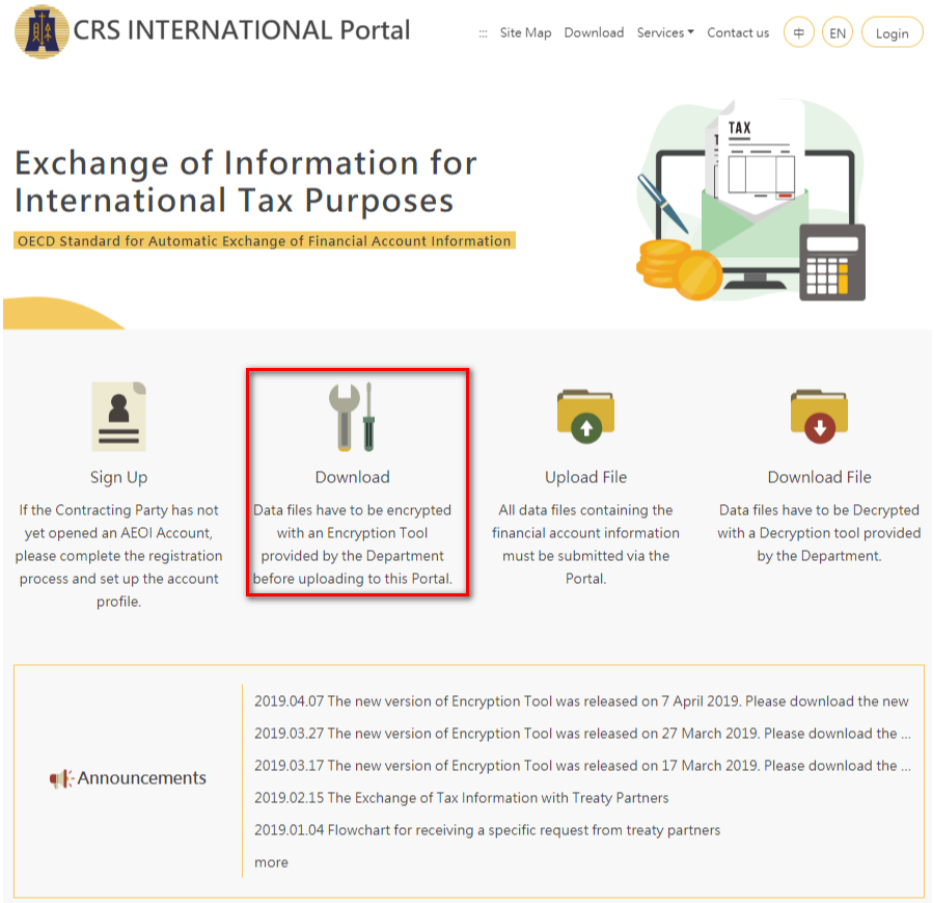

Figure 5: Download Taiwan's digital certificate for transmission[7]

[6] Design of the web page and its detailed functions may be subject to change depending on the IEIP's development.

[7] Design of the web page and its detailed functions may be subject to change depending on the IEIP's development.

4 Data Preparation for Transmission

4.1 Data for CRS Transmission

IEIP will only accept files in .ZIP format for CRS transmission. An archive (data package) is required to be created for the purpose of CRS transmission. Each archive contains three files which consist of the following:

- SenderAgreementId_CRS_Metadata.xml
- SenderAgreementId_CRS_Payload
- SenderAgreementId_CRS_Key

4.2 Process to Prepare and Transmit an Archive for the Purpose of CRS

Overview process to prepare and transmit a file for the purpose of CRS is demonstrated in Table 3, and its flowchart is illustrated in Figure 6.

Table 3: Overview of process to prepare and transmit a file (CRS)

Steps	Process	File Naming Convention
--	Obtain a digital certificate from an approved Certificate Authority (CA)	SenderAgreementId_CRS_Cert.cer
1	Prepare and validate the CRS XML file Digitally sign the file	SenderAgreementId_CRS_Payload.xml
2	Compress the CRS XML file with compatible zip utility	SenderAgreementId_CRS_Payload.zip
3	Encrypt the CRS XML file with AES-256 key	SenderAgreementId_CRS_Payload
4	Encrypt AES key with Taiwan's public key	ReceiverAgreementId_CRS_Key
5	Create sender metadata	SenderAgreementId_CRS_Metadata.xml
6	Create the transmission file	UTC_SenderAgreementId_CRS.zip
7	Transmit the data packet to IEIP and receive delivery confirmation	N/A

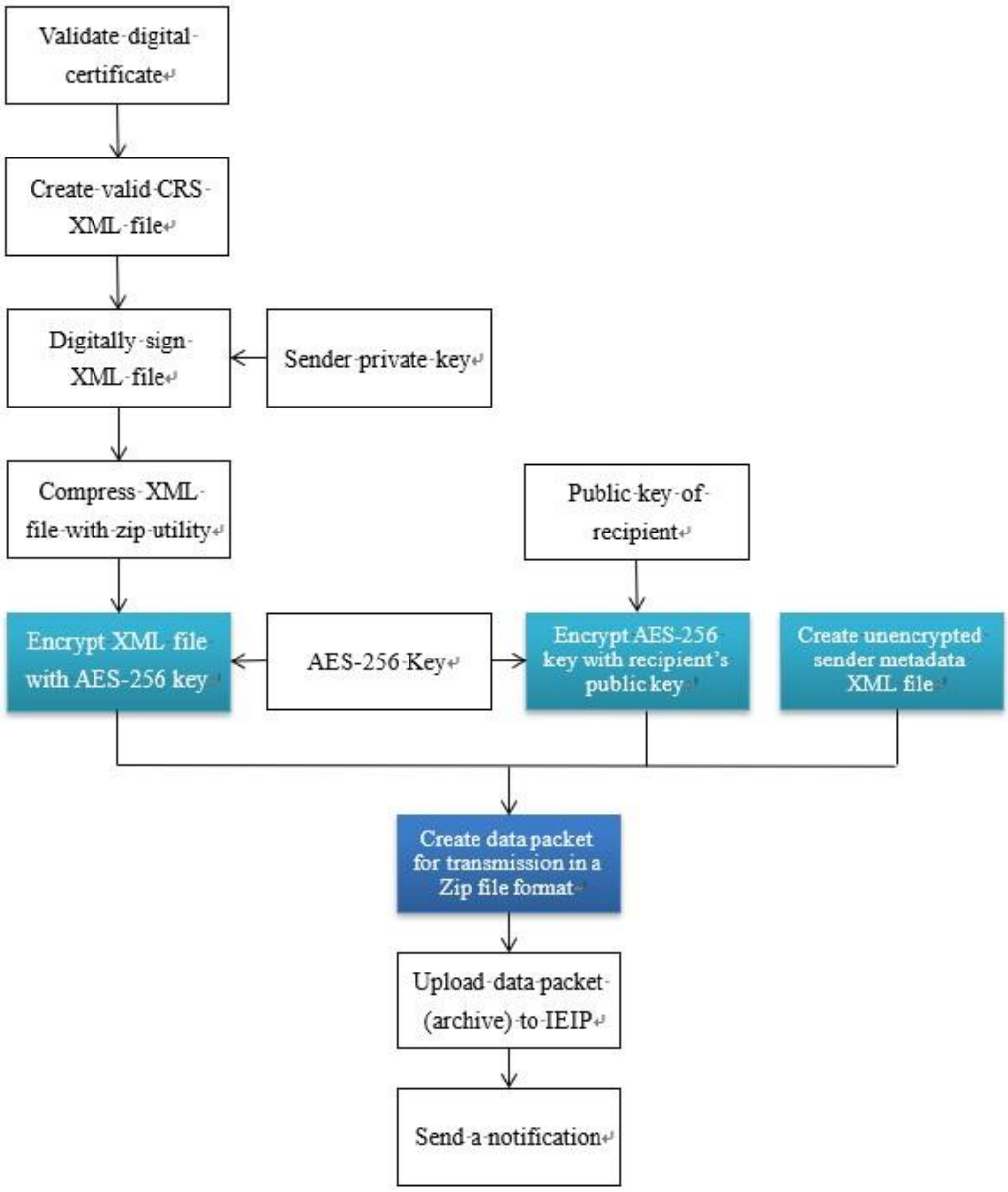

Figure 6: Flowchart with respect to preparing and transmitting a file (CRS)

4.3 Operation via HTTPS for Data Transmission

The operational environment that the IEIP provides for enrolled users to perform transmission via HTTPS is illustrated in Figure 7. An enrolled user may upload or download archives for the purpose of data transmission by clicking the associated icon shown on the web page. The IEIP will then issue instructions for guiding him/her to finish the process.

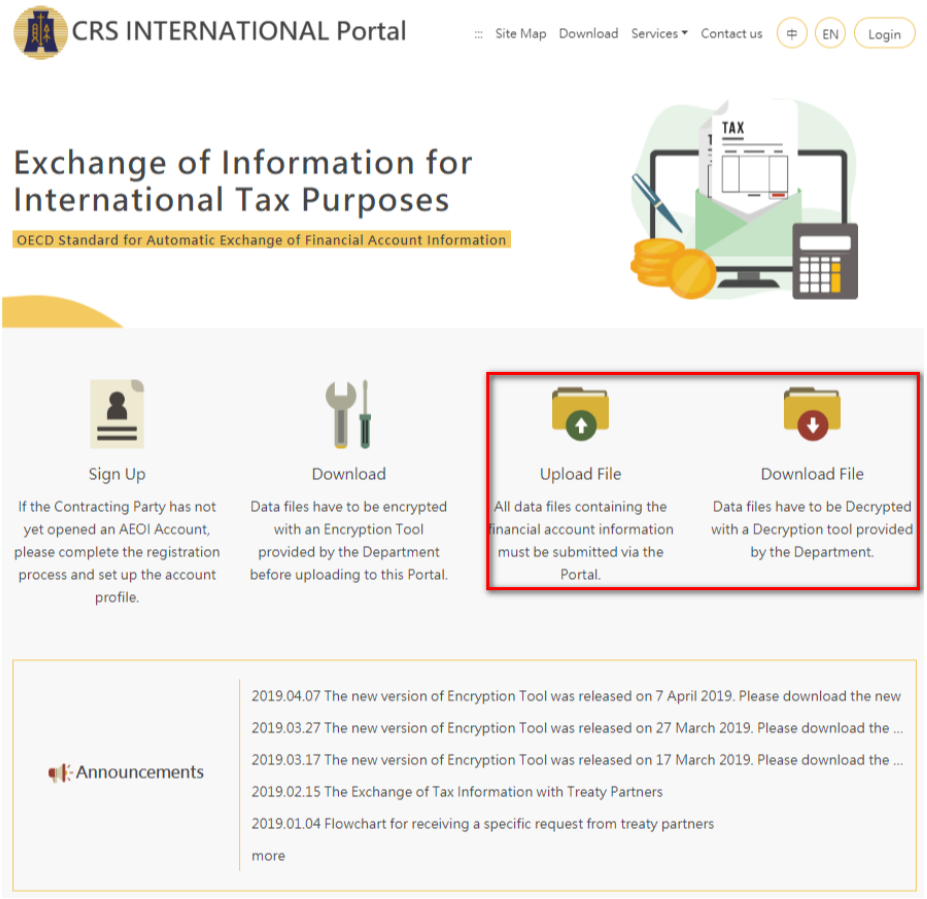

Figure 7: Operational environment for data transmission via HTTPS[8]

4.4 Operation via SFTP for Data Transmission

The IEIP SFTP Server provides users with secure access via proper application connection to manage and transfer files between hosts over a network. Preliminary information concerning connection and operation are provided below:

- Host Name: www.ieip.mof.gov.tw
- Port: 22
- IEIP SFTP Home folders:
  (1) Inbox: Download files from Taiwan
  (2) Outbox: Upload files to Taiwan

[8] Design of the web page and its detailed functions may be subject to change depending on the IEIP's development.

5 Status of Data Transmission (Notifications or Alerts)

IEIP will send notifications to enrolled users when there is an error in the archive or the files that are contained in the archive which are transmitted via the IEIP to Taiwan.

Concerning the error code for the CRS, Taiwan adopts CRS Status Message Error Codes as set out by the OECD.