



澳門特別行政區政府
財政局

國際稅務信息交換系統
(金融帳戶信息自動交換)

登入及操作手册

版本 1.0

版本記錄

版本號	版本描述	版本日期
1.0	初版	12/2025

目錄

第一章 簡介.....	1
第二章 介面佈局.....	2
第三章 登入系統.....	2
3.1. 商社通用戶首次登入.....	3
3.2. 商社通用戶登入.....	6
第四章 用 戶 管 理.....	7
4.1. 新增用 戶.....	9
4.2. 修改用 戶.....	10
4.3. 移除用 戶.....	11
第五章 金 融 機 構 資 訊.....	12
5.1. 基本資訊.....	12
5.2. 管理的投資實體.....	12
第六章 資 訊 管 球.....	14
6.1. 修改資訊.....	14
6.2. 管理投資實體.....	17
6.3. 管理電子證書.....	18
6.3.1. 添加電子證書.....	19
6.3.2. 上載電子證書.....	20
6.3.3. 刪除電子證書.....	20
第七章 金 融 帳 戶 信 息 報 送.....	21
7.1. 金融機構檔案.....	21
7.2. 報送檔案.....	22
7.2.1. 期限內報送.....	24
7.2.2. 期限內資料的更正.....	24
7.2.3. 分拆上載 XML 檔案.....	25
7.2.4. 期限後報送.....	28
7.2.5. 零申報.....	28
7.3. 統計報送信息.....	30
7.3.1. 金融機構報送統計.....	30
7.3.2. 投資實體報送統計.....	31
第八章 財政局資源下載.....	32
8.1. 下載財政局電子證書.....	32
8.2. 下載加密輔助軟件.....	33
附錄一 取得金融機構的公開密鑰(Public-Key)說明.....	34
附錄二 簽署及加密說明.....	40
附錄三 簽署及加密代碼示例.....	45
附錄四 加密輔助軟件說明.....	47

第一章 簡介

“國際稅務信息交換系統”(以下簡稱系統)主要提供平台讓各報送信息的金融機構報送金融帳戶信息到財政局，本手冊主要對系統的各業務功能作詳細說明，同時載有與信息報送相關的注意事項供金融機構作參閱。

為保障良好的系統使用體驗，建議使用 Chrome 或 Edge 瀏覽器登入系統。系統(版本 1.0)主要包含下列 5 個業務功能：

1. 金融機構資訊

載有金融機構的基本資訊、倘有管理的投資實體資訊。

2. 用戶管理

具有系統用戶管理權限的用戶可進行開戶申請、修改用戶資訊及移除用戶操作(詳情請參閱“第四章 用戶管理”)。

3. 資訊管理

供金融機構修改機構資訊、管理投資實體及管理電子證書。

4. 金融帳戶信息報送

供金融機構報送金融帳戶信息及查看報送統計數據。

5. 財政局資源下載

供金融機構下載財政局電子證書、加密輔助軟件。

系統會按照用戶職務權限來對功能進行分配，即用戶登入系統後可以使用的功能會因職務不同而異。

第二章 介面佈局



(圖 2-A)

1. 菜單區：當前用戶所擁有的權限菜單，可跳轉到不同的頁面。
2. 資料查詢區：輸入相應查詢條件，可快速篩選需要的資料。
3. 按鈕區：本菜單中主要功能按鈕。
4. 資料展示區：當前用戶所能查看到的資料，可根據查詢條件進行過濾。
5. 行操作按鈕：可對列表中同一行相應的資料進行額外的操作，如「修改」、「移除」等。

第三章 登入系統

新登記的金融機構，需先聯絡本局（電話：85990799 或電郵 aeho_info@dsf.gov.mo），本局會向每一金融機構提供專屬的系統識別號(AEOI ID)。

系統分別設有生產環境及測試環境。生產環境為正式報送資料的環境，而測試環境僅用於檔案報送及系統運作的測試用途。建議金融機構以模擬數據進行測試。測試環境內的所有資料均不會用作稅務信息交換，亦不會影響生產環境資料。金融機構可透過以下網址登入系統：

生產環境網址：<https://eoi.fi.dsf.gov.mo>

測試環境網址：<https://test-eoi.fi.dsf.gov.mo>

3.1. 商社通用戶首次登入

生產環境

必須由商社通管理員進行首次登入，完成開戶程序後系統預設有“用戶管理”權限，可新增其他用戶。

測試環境

為方便金融機構進行測試，商社通用戶(管理員及工作人員)均可進行首次登入，完成開戶程序後系統亦預設有“用戶管理”權限。

(有關用戶權限詳情請參閱“第四章 用 戶 管 理”)

點擊【實體】，進入登錄頁面。



(圖 3.1-A)

進入登錄頁面後，商社通用戶可選擇編號類型。



(圖 3.1-B)

選擇登入編號類型後輸入對應編號、帳戶名稱、密碼，點擊【登入】。

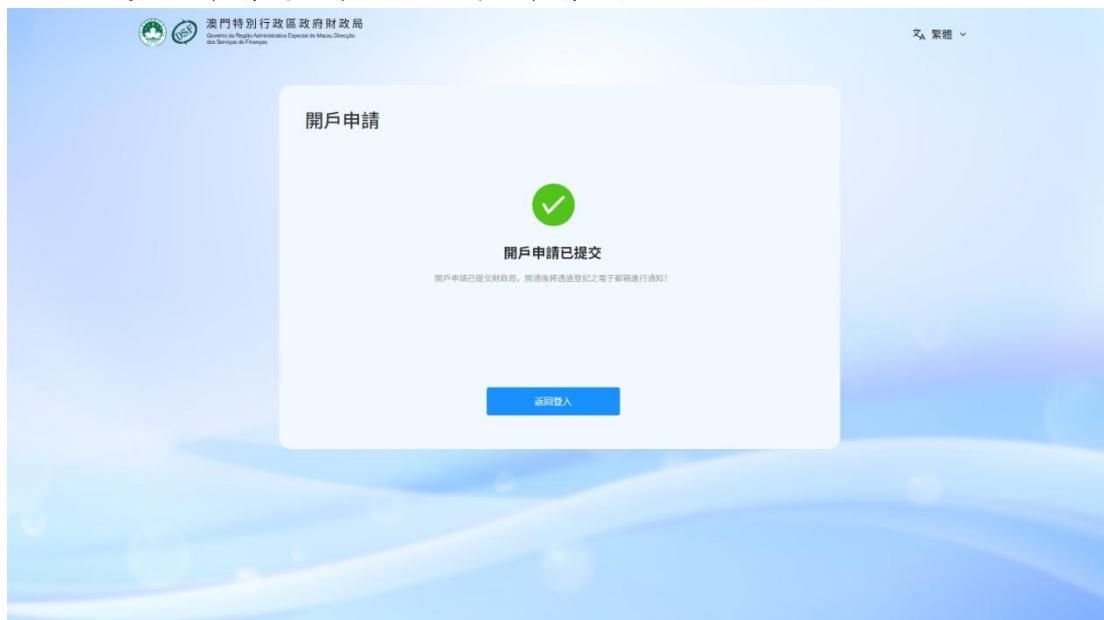


(圖 3.1-C)

首次登入時，用戶須於開戶申請頁面輸入姓名(將顯示於系統中作識別用途，亦會於部份電郵提示內顯示)、電子郵箱(用於登入時接收驗證碼)、驗證碼，最後點擊「提交申請」按鈕以提交申請，有關用戶待財政局開通後即可使用。

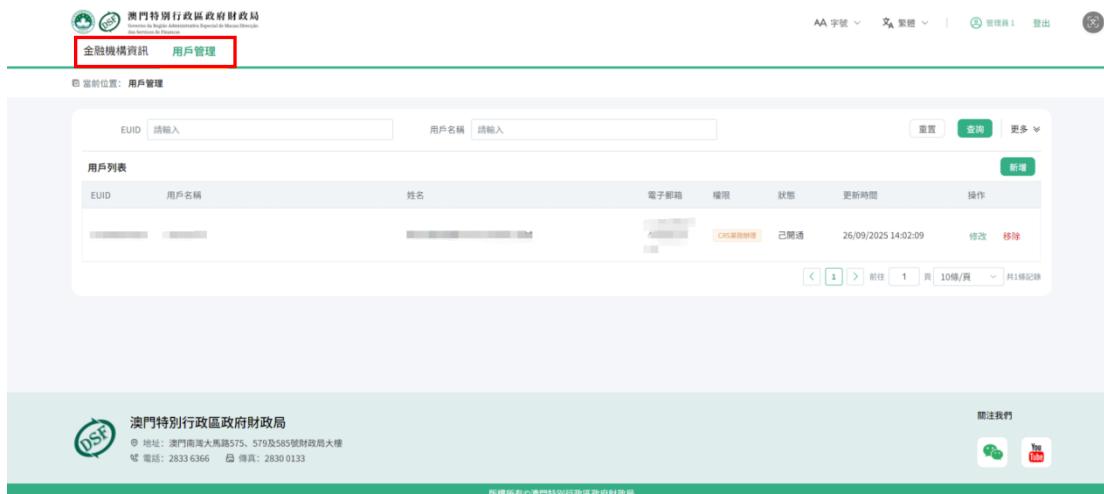
(圖 3.1-D)

完成提交申請後，系統顯示開戶申請已提交。



(圖 3.1-E)

管理員再次登入系統時，介面菜單的業務功能有【金融機構資訊】及【用戶管理】。



(圖 3.1-F)

3.2. 商社通用戶登入

進入網址後，點擊【實體】，進入登錄頁面。



(圖 3.2-A)

進入登錄頁面後，商社通用戶可選擇編號類型。



(圖 3.2-B)

選擇登入編號類型後輸入對應編號、帳戶名稱、密碼，點擊【登入】。



(圖 3.2-C)

每次登入均須輸入通過電郵接收之驗證碼，才可成功登錄。



(圖 3.2-D)

第四章 用戶管理

金融機構可於用戶管理頁面進行系統用戶管理。系統設有“用戶管理”及“CRS 業務辦理”兩種用戶權限，同一用戶可擁有一種或兩種權限，相關功能如下：

“用戶管理”權限

用戶可查看金融機構資訊、亦可於用戶管理頁面申請新增用戶、修改用戶資訊及移除用戶，首次登入時系統已預設商社通管理員擁有“用戶管理”權限。

“CRS 業務辦理”權限

用戶可查看金融機構資訊、進行資訊管理、報送金融帳戶信息及下載財政局資源。

用戶管理和 CRS 業務辦理兩類角色的權限劃分如下表：

功能	用戶管理	CRS 業務辦理
金融機構資訊	O	O
用戶管理	O	X
資訊管理	X	O
金融帳戶信息報送	X	O
財政局資源下載	X	O

具有“用戶管理”權限的用戶登入後，點擊【用戶管理】，可進入用戶管理頁面。

The screenshot shows the 'User Management' section of a web application. At the top, there are search fields for 'EUID' and 'User Name', and buttons for 'Reset', 'Search', and 'More'. Below this is a table titled 'User List' with columns: EUID, Name, Email, Permissions, Status, Last Update, and Actions. Two user entries are listed:

EUID	Name	Email	Permissions	Status	Last Update	Actions
[REDACTED]	[REDACTED]	[REDACTED]	CRS業務辦理 用戶管理	已開通	12/11/2025 16:22:16	修改 移除
[REDACTED]	[REDACTED]	[REDACTED]	用戶管理 CRS業務辦理	已開通	13/11/2025 08:48:31	修改 移除

At the bottom of the page, there is a footer with the logo of the Macao Government Financial Bureau, address, phone number, copyright information, and social media links.

(圖 4-A)

頁面下方的「用戶列表」將顯示所有用戶的基本資訊及相關狀態，包括：

待開通—等待財政局通過該申請。

已開通—申請已通過，該用戶有權限進行 CRS 業務辦理或用戶管理。

4.1. 新增用戶

點擊用戶管理頁面的「新增」按鈕，進入新增用戶頁面。



(圖 4.1-A)

於新增用戶頁面輸入商社通 EUID、姓名、電子郵箱(用於登入帳戶時接收驗證碼)及選取權限後，點擊「提交」按鈕以提交申請(有關申請將顯示於「用戶列表」，狀態為待開通)，有關用戶待財政局開通後即可使用。如點擊「取消」按鈕則可取消此次申請。

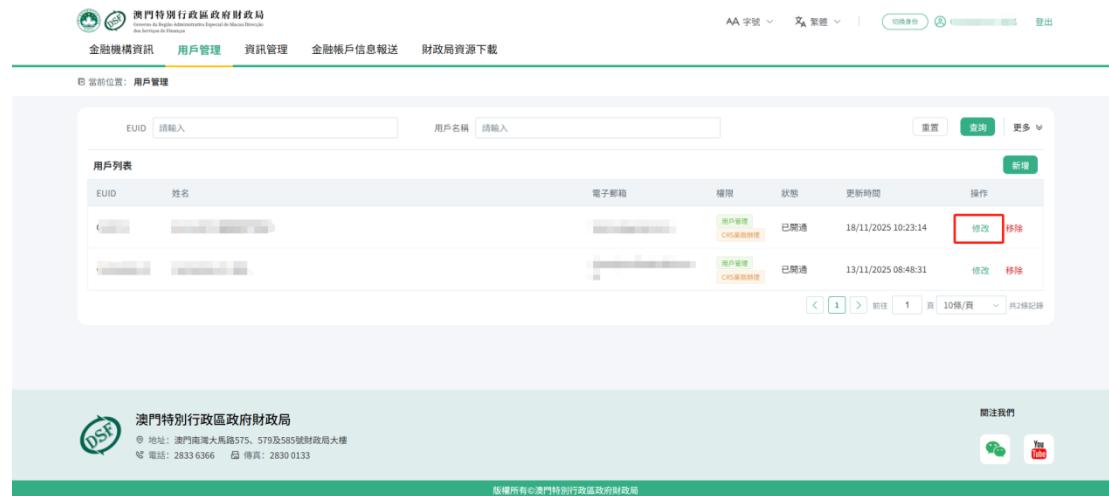
A screenshot of the '新增用戶' (Add User) form. The form has several input fields: '機構名稱' (Institution Name), '系統識別號' (System Identifier), '納稅人編號' (Taxpayer Number), '商社通EUID' (please enter), '姓名' (Name) with a red asterisk indicating it's required, and '電子郵件' (Email) with a red asterisk. Below these fields is a section for '權限' (Permissions) with checkboxes for 'CRS業務辦理' and '用戶管理'. A large red box surrounds the entire group of required fields. At the bottom right are '取消' (Cancel) and '提交' (Submit) buttons.

(圖 4.1-B)

頁面中帶“*”的為必填欄位

4.2. 修改用戶

點擊用戶管理頁面的「修改」，進入修改用戶頁面。



The screenshot shows the 'User Management' section of the Macao Government website. At the top, there are search fields for 'EUID' and 'User Name', and a 'Search' button. Below is a table titled 'User List' with columns: EUID, Name, Email, Permission, Status, Update Time, and Operation. Two rows of user data are listed. In the 'Operation' column for the second row, there is a green 'Modify' button with a red border, which is highlighted with a red box. Other buttons in the same row include 'Delete' and 'Details'. At the bottom of the table, there are navigation buttons for pages 1-10, 10 items per page, and a total of 22 records.

(圖 4.2-A)

於修改用戶頁面修改電子郵件、權限後，點擊「提交」按鈕即可保存修改。
如點擊「取消」按鈕則不會保存修改。



The screenshot shows the 'Modify User' form. It includes fields for 'Organization Name', 'System Identifier', 'Taxpayer ID', 'EUID', 'Name', and 'Email'. The 'Email' field is highlighted with a red box. Below the email field are three checkboxes: 'Permission' (marked with an asterisk), 'CRS business handling' (checked), and 'User Management' (checked). At the bottom right are 'Cancel' and 'Submit' buttons.

(圖 4.2-B)

頁面中帶“*”的為必填欄位

4.3. 移除用戶

點擊用戶管理頁面的「移除」按鈕，再於彈出視窗點擊「確認」，便可移除該用戶。如點擊「取消」按鈕則該用戶仍然保留。

The screenshot shows the 'User Management' section of the Macao Government Financial Bureau's website. At the top, there are navigation links: 'Financial Institution Information', 'User Management' (which is highlighted in green), 'Information Management', 'Financial Account Information Report', and 'Financial Bureau Resource Download'. On the right side, there are settings for 'Text Size' (AA), 'Font Style' (繁體), and a search bar with a magnifying glass icon. Below the header, a breadcrumb trail indicates the current location: 'User Management'. The main content area is titled 'User List' and contains a table with columns: EUID, Name, Email, Permissions, Status, Last Update Time, and Operations. Two rows of data are shown. In the first row, the 'Operations' column contains two buttons: 'Modify' and 'Delete'. The 'Delete' button is highlighted with a red border. In the second row, similar buttons are present. At the bottom of the table, there are pagination controls (previous/next, page number 1, total pages 10, and a dropdown for items per page) and a note indicating 2 records found.

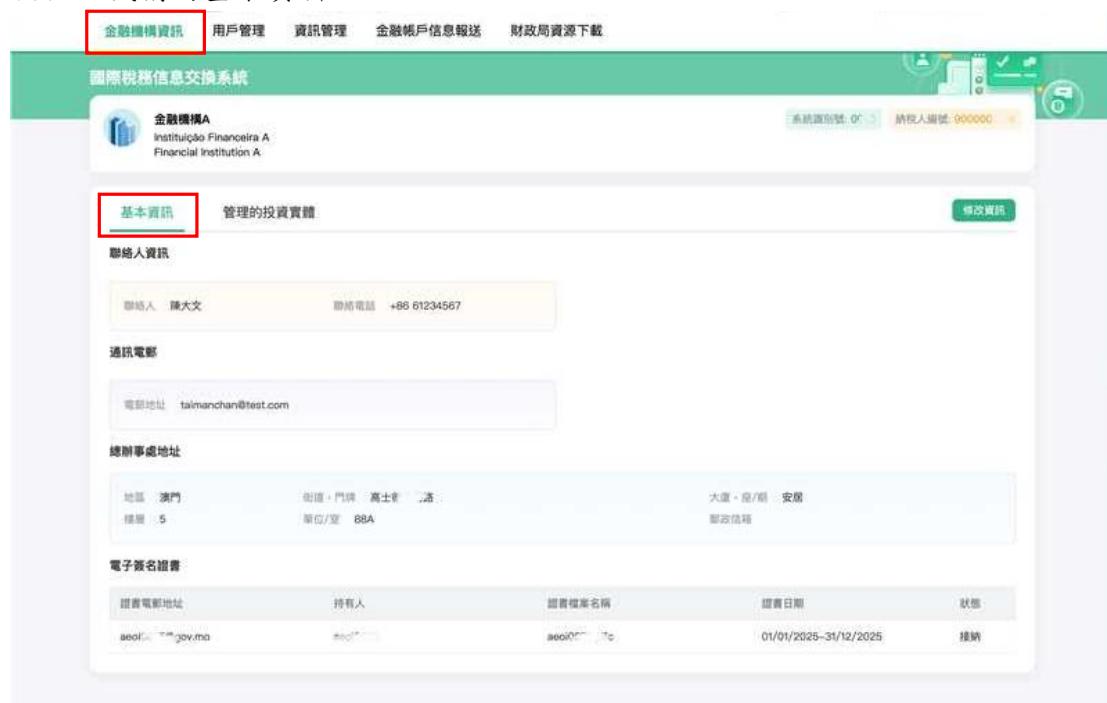
(圖 4.3-A)

第五章 金融機構資訊

5.1. 基本資訊

於基本資訊頁面可檢視當前金融機構的基本資料，包括聯絡人資訊、通訊電郵、總辦事處地址及電子簽名證書。

點擊【金融機構資訊】，進入金融機構資訊頁面後，點擊「基本資訊」以檢視金融機構的基本資料。



The screenshot displays the 'Basic Information' page of the 'Financial Institution Information System'. At the top, there are tabs for 'Basic Information', 'User Management', 'Information Management', 'Financial Account Information Report', and 'Financial Bureau Resource Download'. The 'Basic Information' tab is highlighted with a red box. Below the tabs, the page header reads 'International Tax Information Exchange System' and 'Financial Institution A'. The main content area includes sections for 'Contact Person Information', 'Communication Details', 'Office Address', and 'Electronic Signature Certificate'. A green 'Edit Information' button is located in the top right corner of the main content area.

(圖 5.1-A)

金融機構可點擊「修改資訊」按鈕以更改基本資訊(詳情請參閱“6.1 修改資訊”)。



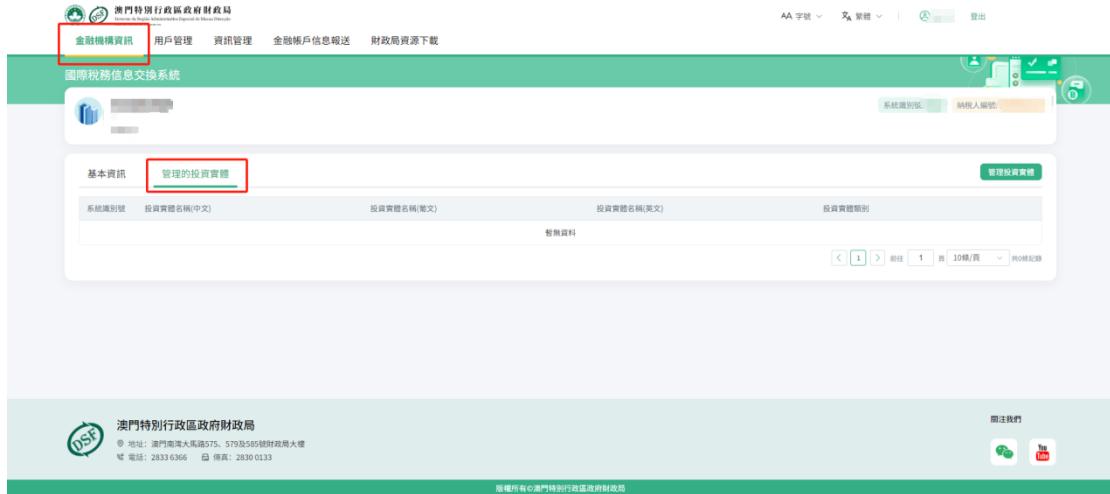
This screenshot shows the same 'Basic Information' page as above, but the 'Modify Information' button in the top right corner of the main content area is highlighted with a red box.

(圖 5.1-B)

5.2. 管理的投資實體

於管理的投資實體頁面可檢視由金融機構所管理的投資實體列表，當中載有投資實體的基本資訊。

點擊【金融機構資訊】，進入金融機構資訊頁面後，點擊「管理的投資實體」以檢視投資實體的資訊。



(圖 5.2-A)

點擊頁面內「管理投資實體」按鈕，金融機構可於管理投資實體頁面申請新增、更改或取消投資實體資料（詳情請參閱“6.2 管理投資實體”）。



(圖 5.2-B)

第六章 資訊管理

6.1. 修改資訊

金融機構可於修改資訊頁面檢視所有曾提出的修改申請及其處理狀態，亦可申請修改基本資訊。

依次點擊【資訊管理】-【修改資訊】，進入修改資訊頁面。



The screenshot shows the 'Information Management' section of the system. At the top, there are tabs: 'Financial Institution Information', 'User Management', 'Information Management' (which is highlighted with a red box), 'Financial Account Information Report', and 'Cabinet Resource Download'. Below the tabs, it says 'Current Position: Information Management > Modify Information'. A green button labeled 'Modify Information' with a checkmark is also highlighted with a red box. There are dropdown menus for 'Application Type' (选择) and 'Status' (选择). Below these, there is a table titled 'Information Modification Application List' with columns for 'Application Type' and 'Status'.

(圖 6.1-A)

修改資訊頁面下方的「資訊修改申請列表」將顯示所有修改資訊申請記錄及其處理狀態，狀態包括：

- 待處理—剛提交一份新申請時，狀態為待處理。須待財政局完成處理，金融機構才可再提交新增申請。在待處理的狀態下，如金融機構須對已提交的申請作出修改，則須先撤銷已提交的申請，再作新增申請。
- 接納—申請已被接納。
- 拒絕—申請已被拒絕。
- 撤銷—申請已由金融機構撤銷。

點擊「新增申請」按鈕，進入新增申請頁面。



The screenshot shows the 'New Application' page. At the top, there are tabs: 'Financial Institution Information', 'User Management', 'Information Management' (which is highlighted with a red box), 'Financial Account Information Report', and 'Cabinet Resource Download'. Below the tabs, it says 'Current Position: Information Management > New Application'. There are dropdown menus for 'Application Type' (选择) and 'Status' (选择). A green button labeled 'New Application' is highlighted with a red box. Below these, there is a table titled 'Information Modification Application List' with columns for 'Application Type', 'Status', 'Processing Time', and 'Action'. The table currently shows 'No Data'.

(圖 6.1-B)

金融機構可於新增申請頁面更改機構名稱、聯絡人、電郵地址及總辦事處地址資料(須至少提供一個聯絡人資訊及一個有效通訊電郵地址)。金融機構須先點選需修改的內容才可更改、添加或移除相應資料。

金融機構資訊 用戶管理 資訊管理 金融帳戶信息報送 財政局資源下載

當前位置：資訊管理 > 新增申請

機構名稱

機構名稱(中文) 機構名稱(英文) 機構名稱(英文) #

聯絡人

聯絡人 聯絡電話

電郵地址

聯絡電郵

總辦事處地址#

地區 澳門 澳門 澳門 澳門
街道，門牌
大廈，座/期
樓層 單位/室
郵政信箱

提示：“#”標識的欄位將用作報送用途

(圖 6.1-C)

頁面中帶“*”的為必填欄位

例如：金融機構需更改聯絡人資料，則須先點選「更改聯絡人/電話」，然後更改、添加或移除聯絡人資料。

點選「更改聯絡人/電話」，可直接更改現有聯絡人及聯絡電話。

點擊「+添加」按鈕，並於新增的欄位內輸入資料以新增聯絡人及聯絡電話。

點擊「移除」按鈕，再於彈出視窗點擊「確認」後，可移除該條數據；如點擊「取消」則可取消移除操作。

联络人	联络电话	操作
[Red box]	+853(中国澳门)	<button>删除</button>

+ 添加

(圖 6.1-D)

联络人	联络电话	操作
[Red box]	+853(中国澳门)	<button>删除</button>

(圖 6.1-E)

倘需更改機構名稱、電郵地址及總辦事處地址，則進行對應修改操作。

輸入資料後，點擊「提交申請」按鈕以提交申請(有關申請將顯示於「資訊修改申請列表」)。如點擊「取消」按鈕則可取消此次申請。

取消 提交申请

(圖 6.1-F)

6.2. 管理投資實體

於管理投資實體頁面可檢視所有關於管理的投資實體曾提出的申請及其狀態，金融機構可為所管理的投資實體提出新增、更改及取消申請。

依次點擊【資訊管理】-【管理投資實體】，進入管理投資實體頁面。



The screenshot shows the 'Information Management' section of the system. The 'Management of Investment Entities' sub-tab is active and highlighted with a red box. Other tabs like 'Financial Institution Information', 'User Management', 'Information Reporting', and 'Cabinet Resource Download' are visible but not selected.

(圖 6.2-A)

進入管理投資實體頁面後，下方的「管理的投資實體申請列表」將顯示所有投資實體申請記錄及其處理狀態，包括：

- 待處理—剛提交一份新申請時，狀態為待處理，如金融機構須對提出的申請作出修改，則須先撤銷已提交的申請，再作新增申請。
- 接納—申請已被接納。
- 拒絕—申請已被拒絕。
- 撤銷—申請已由金融機構撤銷。

點擊「申請」按鈕，會彈出新增申請視窗。



This screenshot shows a modal window for submitting a new application. The 'Submit' button at the bottom right is highlighted with a red box. The window contains fields for 'System Identification Number' and 'Investment Entity Name', along with search and filter options.

(圖 6.2-B)

於新增申請視窗，金融機構可按需點選申請類型(新增、更改或取消)及輸入相應資料。

The screenshot shows the '新增申請' (New Application) page. It has a sidebar with '資訊管理' (Information Management) and '管理投資實體' (Manage Investment Entity). The main area has a title '新增申請'. Fields include: '申請類型' (Application Type) with radio buttons for '新增' (Selected), '更改', and '取消'; '系統識別號' (System Identifier) with a dropdown set to '系統自動分配' (Automatically assigned); '投資實體名稱(中文)' (Investment Entity Name (Chinese)) with placeholder '請輸入'; '投資實體名稱(葡文)' (Investment Entity Name (Portuguese)) with placeholder '請輸入'; '投資實體名稱(英文)' (Investment Entity Name (English)) with placeholder '請輸入'; '投資實體類別' (Investment Entity Category) with radio buttons for '退休基金', '投資基金', '信託', and '其他'; '申請日期' (Application Date) showing '08/10/2025 15:28:31'; and '狀態' (Status) with '接納' (Accepted) selected. Buttons at the bottom are '取消' (Cancel) and '提交' (Submit).

(圖 6.2-C)

頁面中帶“*”的為必填欄位

輸入資料後，點擊「提交」按鈕以提交申請(有關申請將顯示於「管理的投資實體申請列表」)。如點擊「取消」按鈕則可取消此次申請。

6.3. 管理電子證書

於管理電子證書頁面可檢視當前登記的電子證書及其處理狀態，金融機構可於此頁添加、上載、下載或刪除電子證書。

依次點擊【資訊管理】-【管理電子證書】，進入管理電子證書頁面。

The screenshot shows the '管理電子證書' (Management of Electronic Certificates) page. At the top, there's a navigation bar with '資訊管理' (Information Management) and '管理電子證書' (Management of Electronic Certificates) both highlighted with red boxes. Below the navigation is a table with three columns: '電子簽名證書' (Electronic Signature Certificate), '證書電郵地址' (Certificate Email Address), and '證書檔案名稱' (Certificate File Name). A red box highlights the '管理電子證書' button.

(圖 6.3-A)

管理電子證書頁面將顯示所有已登記的電子簽名證書及其處理狀態，包括：

- 待上載—等待金融機構上載電子證書檔案。
- 待處理—等待財政局驗證電子證書。
- 接納—證書已被接納，可用作核對電子簽署。
- 拒絕—證書已被拒絕。
- 停用—證書已被財政局停用。
- 過期—證書已過期。

The screenshot shows a table titled '電子簽名證書' (Electronic Signature Certificate). The columns are: 證書電郵地址 (Certificate Email Address), 持有人 (Holder), 證書檔案名稱 (Certificate File Name), 證書日期 (Certificate Date), 狀態 (Status), and 操作 (Operation). There is a '新增' (Add) button at the bottom left of the table.

(圖 6.3-B)

6.3.1. 添加電子證書

添加電子證書前，金融機構(“由另一實體管理的投資實體”¹除外)須先行取得郵電局 eSignTrust 發出的「高級電子簽名」證書(申請詳情請參閱郵電局之相關網頁：<http://www.esigntrust.com>)，用於簽署向財政局報送的資料檔案，同一機構於系統最多可登記 5 張電子證書。

點擊管理電子證書頁面的「+添加」按鈕，於新增的欄位內輸入證書電郵地址及持有人姓名後，再點擊「確認」按鈕即可新增一張證書。如點擊「取消」按鈕則不會添加該證書。

添加證書後，金融機構須上載對應電子證書檔案到系統(詳情請參閱“6.3.2 上載電子證書”及附錄一)。

The screenshot shows a form for adding a new certificate. It has fields for '證書電郵地址' (Certificate Email Address) and '持有人' (Holder), both of which are highlighted with red boxes. Below the form is a green '+添加' (Add) button. To the right of the form, there are buttons for '待上載' (Pending Upload), '確認' (Confirm), and '取消' (Cancel).

(圖 6.3.1-A)

¹ “由另一實體管理的投資實體”是指《金融帳戶信息的通用報送標準及盡職調查程序》(“指引”)第八條第一款(七)項(2)分項的投資實體。亦即由“指引”第八條第一款內所指的存款機構、託管機構、特定保險公司或同款(七)項(1)分項所指的另一投資實體所管理的實體。

6.3.2. 上載電子證書

新添加、電子證書續期或更新電子證書後，金融機構須上載對應電子證書檔案到系統。點擊管理電子證書頁面的「上載」按鈕，從本地設備上載對應持有人的電子簽名證書檔案(副檔名必須為 p7c)。上載成功後，電子簽名證書的狀態將轉為“待處理”，須待財政局接納後方可使用，另狀態為接納的證書檔案可供下載。

電子簽名證書					
證書電郵地址	持有人	證書檔案名稱	證書日期	狀態	操作
chantaiman@abcbank.com	Chan Tai Man			待上載	上載 刪除

(圖 6.3.2-A)

6.3.3. 刪除電子證書

倘已登記的電子證書不再被用作簽署資料檔案，可於系統中刪除該電子證書。另外，如須更改已登記電子證書的電郵地址或持有人，須先刪除該電子證書後再重新添加。

點擊管理電子證書頁面的「刪除」按鈕，再於彈出視窗點擊「確認」，便可刪除該電子簽名證書。如點擊「取消」按鈕則該電子簽名證書仍然保留。

電子簽名證書					
證書電郵地址	持有人	證書檔案名稱	證書日期	狀態	操作
chantaiman@abcbank.com	Chan Tai Man			待上載	上載 刪除

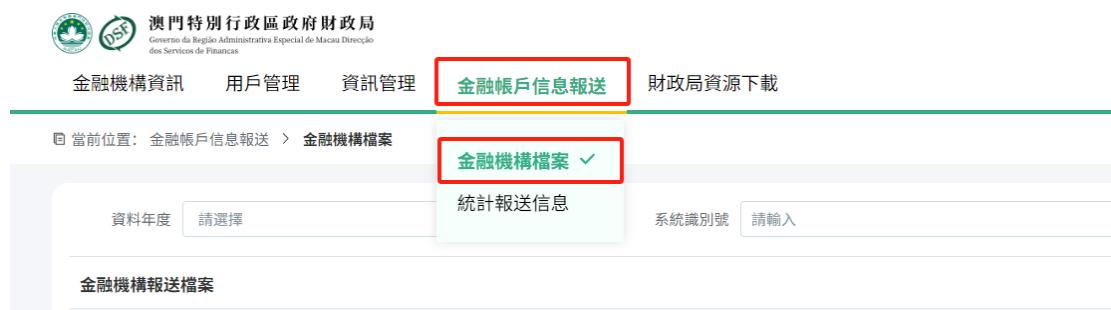
(圖 6.3.3-A)

第七章 金融帳戶信息報送

7.1. 金融機構檔案

於金融機構檔案頁面可進行金融帳戶檔案報送及零申報，亦可檢視所有曾報送的檔案資料及其狀態，以及可對檔案進行篩選查詢及檢視結果。進行檔案報送時，金融機構將須報送金融帳戶信息生成 XML 格式的數據檔案(詳情請參閱 AEOI XML Schema User Guide)，並完成簽署及加密後(詳見附錄二及附錄三)，可透過系統的金融機構檔案頁面進行檔案報送。

依次點擊【金融帳戶信息報送】-【金融機構檔案】，進入金融機構檔案頁面。



(圖 7.1-A)

頁面中的「金融機構報送檔案」列表載有曾報送的檔案基本資料及其處理狀態，包括：

待處理—上載金融帳戶檔案後，等待系統處理中。

接納—系統已接納有關檔案。

拒絕—系統已拒絕有關檔案。

被取代—於期限內，曾報送檔案且被接納，如之後再報送的另一檔案又被接納，則舊資料會被刪除，且狀態會由接納轉為被取代(詳情請參閱“7.2.2. 期限內資料的更正”。

當前位置：金融帳戶信息報送 > 金融機構檔案

資料年度	系統識別號	機構名稱(英文)	檔案名稱	報送日期	上載類型	狀態	操作
2024	Test F1.A	0.zip	16/12/2025	期限後(增量)	接納	查看 檢視結果
2024	Test F1.A	0.zip	12/12/2025	期限後(增量)	拒絕	查看 檢視結果
2024	Test F1.A			12/12/2025	零申報	被取代	查看
2024	Test F1.A	0.zip	12/12/2025	期限後(增量)	拒絕	查看 檢視結果
2024	Test F1.A	0.zip	12/12/2025	期限後(增量)	拒絕	查看 檢視結果
2024	Test F1.A	0.zip	09/12/2025	期限後(增量)	拒絕	查看 檢視結果
2024	Test F1.A			09/12/2025	零申報	被取代	查看
2024	Test F1.A			09/12/2025	零申報	被取代	查看

(圖 7.1-B)

7.2. 報送檔案

於金融機構檔案頁面，點擊「新增檔案」按鈕，跳轉至新增金融帳戶信息報送頁面。

當前位置：金融帳戶信息報送 > 金融機構檔案

(圖 7.2-A)

於該頁面上載金融帳戶檔案(檔案名稱及格式必須符合系統要求，詳情請參閱 AEOI XML Schema User Guide)。

The screenshot shows the 'New Financial Account Submission' form with several fields marked with a red asterisk (*) indicating they are required:

- * 系統識別號 (System Identifier): A dropdown menu.
- * 機構名稱(英文) (Institution Name in English): An input field.
- * 上載類型 (Upload Type): A dropdown menu.
- * 報送日期 (Submission Date): A date picker set to 28/12/2025.
- * 檔案名稱 (File Name): An input field containing '上傳檔案' (Upload File).

(圖 7.2-B)

頁面中帶“*”的為必填欄位

報送檔案步驟如下：

1. 點擊「系統識別號」欄位選取報送檔案所屬的金融機構或投資實體。
(註：倘金融機構已為其管理的投資實體申請系統識別號，下拉式清單將一併顯示所有的投資實體供選取。)
2. 點擊「資料年度」欄位選取報送檔案所涉及的資料年度。
選取資料年度後，「上載類型」欄位將根據資料年度顯示(期限內-全量)或(期限後-增量)，詳情請參閱“7.2.1. 期限內報送”及“7.2.4. 期限後報送”。
3. 點擊「上傳檔案」按鈕，選取本地檔案資源進行上載。
4. 點擊「提交」按鈕報送檔案。

上載檔案後，系統將隨即執行檔案檢查程序，即校驗必填欄位、上載檔案格式和命名規則等，如通過檢查則返回金融機構檔案頁面，且有關檔案將顯示於「金融機構報送檔案」列表，操作欄中的「查看」按鈕及「檢視結果」按鈕可分別查看檔案基本資料及詳細檢視結果；如不通過檢查，系統會顯示對應提示。

倘取消報送可點擊「取消」按鈕返回金融機構檔案頁。

點擊「查看」按鈕後，可查看當前檔案提交後的基本信息及其狀態。

The screenshot shows a table of submitted files. The columns include 資料年度 (Data Year), 系統識別號 (System Identifier), 機構名稱(英文) (Institution Name (English)), 檔案名稱 (File Name), 報送日期 (Submission Date), 上載類型 (Upload Type), 狀態 (Status), and 操作 (Action). The first row has its 'View' and 'Review Result' buttons highlighted with a red box.

資料年度	系統識別號	機構名稱(英文)	檔案名稱	報送日期	上載類型	狀態	操作
2024	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	期限內(全量)	拒絕	查看 檢視結果
2024	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	期限後(增量)	被取代	查看 檢視結果

(圖 7.2-C)

The screenshot shows a modal window titled 'View'. It displays the following details:
資料年度: 2024
機構名稱(英文): [REDACTED]
系統識別號: [REDACTED]
檔案名稱: [REDACTED]
上載類型: 期限內(全量)
報送日期: 22/10/2025
狀態: 拒絕
At the bottom right of the modal is a green '關閉' (Close) button.

(圖 7.2-D)

點擊「檢視結果」按鈕後，可查看當前檔案檢查結果詳情。

The screenshot shows a search interface for financial institution reports. The search bar includes fields for '資料年度' (Year), '系統識別號' (System ID), and '檔案名稱' (File Name). Below the search bar is a table titled '金融機構報送檔案' (Financial Institution Report Files) with two rows of data. The columns include '資料年度' (Year), '系統識別號' (System ID), '機構名稱(英文)' (Institution Name (English)), '檔案名稱' (File Name), '報送日期' (Submission Date), '上載類型' (Upload Type), '狀態' (Status), and '操作' (Action). The first row has a status of '拒絕' (Rejected) and a '檢視結果' (View Result) button highlighted with a red box. The second row has a status of '被取代' (Replaced) and a '檢視結果' (View Result) button.

(圖 7.2-E)

倘有關檔案被系統拒絕，檢視結果頁面的列表將顯示涉及的「錯誤編碼」及「錯誤描述」(錯誤編碼詳情請參閱 AEOI Status Message User Guide)，部份涉及帳戶報告的錯誤對應的 DocRefId 及其於檔案中的路徑將分別顯示於「記錄編號」及「錯誤位置」欄位內。

點擊「下載 StatusMessage」按鈕，可下載包含完整檢查結果的 Status Message 檔案。

The screenshot shows a detailed view of a rejected document. At the top, it displays basic information: '機構名稱(英文)' (Institution Name (English)) - Financial Institution A1, '資料年度' (Year) - 2024, '報送日期' (Submission Date) - 17/12/2025 09:27:41, and '狀態' (Status) - 拒絕 (Rejected). To the right, it shows '系統識別號' (System ID) - 0, '上載類型' (Upload Type) - 期限後(增量) (Exceeded Deadline (Incremental)), '檔案名稱' (File Name) - 20241217_00.zip, and '處理日期' (Processing Date) - 17/12/2025 09:30:08. Below this, a table lists '錯誤編碼' (Error Code), '記錄編號' (Record ID), '錯誤位置' (Error Location), and '錯誤描述' (Error Description). The first entry is 50004 and the error description is 'Failed signature check.' At the bottom right, there are navigation buttons and a green '返回' (Back) button, with a red box highlighting the '下載 StatusMessage' (Download StatusMessage) button.

(圖 7.2-F)

7.2.1. 期限內報送

金融機構須最遲於每曆年的 6 月 30 日，以電子加密方式向財政局提供屬上一曆年的信息，以 2025 年度之資料為例，對應之期限內報送期間為 2026 年 1 月 1 日至 2026 年 6 月 30 日。在該法定期限內報送，金融機構上載的檔案須包含全量資料(即所有須報送的金融帳戶信息)。

7.2.2. 期限內資料的更正

在期限內報送的檔案，倘發現已接納的金融帳戶信息有誤或遺漏，金融機構可重新上載包含全量資料檔案(即包含所有金融帳戶信息的檔案)。新上載之檔案

如符合以下三個條件，相應資料年度曾被接納的資料將被刪除(無論新上載檔案有否其他錯誤)，有關檔案的狀態將由“接納”轉為“被取代”。如未能符合相關條件，先前已接納的資料將不受影響。

刪除相應資料年度曾被接納資料之條件：

1. 屬報送期限內的資料；
2. 檔案名稱最後 2 位數字的序號為 00 (如：202001992021041011203000.zip)；
3. 檔案通過電子證書簽署及之前的一系列檢查。

資料年度	系統識別號	機構名稱(英文)	檔案名稱	報送日期	上載類型	狀態	操作
2024	31/10/2025	期限後(增量)	拒絕	查看 檢視結果
2024	30/10/2025	期限內(全量)	拒絕	查看 檢視結果
2024	30/10/2025	期限內(全量)	拒絕	查看 檢視結果
2024	30/10/2025	期限內(全量)	拒絕	查看 檢視結果
2023	29/10/2025	期限後(增量)	接納	查看 檢視結果
2024	29/10/2025	期限內(全量)	被取代	查看 檢視結果
2024	29/10/2025	期限內(全量)	拒絕	查看 檢視結果

(圖 7.2.2-A)

7.2.3. 分拆上載 XML 檔案

在報送期限內，如金融機構須要報送的帳戶資料數量多於 60 萬筆，或因業務需要而不能一次性上載資料，請將資料分拆上載至系統。

分拆上載 XML 檔案的規則/要求如下：

1. 分拆上載 XML 檔案僅適用於報送期限內資料；
2. 分拆後每個檔案大小須小於 800MB；
3. 同批次的 XML 檔案名稱除最後 2 位數字外須完全一致。而每個檔案名稱最後 2 位數字的序號須按順序命名(序號由 00 開始增加至 99)，以報送 2025 年度的資料為例(同批次檔案被分拆為 3 個檔案)，檔案名稱分別如下：

202501992026041011203000.xml (0199 為金融機構之 AEOI ID)

202501992026041011203001.xml

202501992026041011203002.xml

4. 每個 XML 檔案須以新增記錄(OECD1 - New Data)類型編制，且須符合 AEOI XML Schema 規範；
5. 每個檔案須獨立進行電子簽署及加密等處理，從而得到對應的.zip 檔案 (即每個 zip 檔案內均含 xml 資料檔案及其 Key 檔案)；
6. 同批次首個上載之檔案序號必須為 00
(如：202501992026041011203000.zip)；

7. 同一批次檔案必須按順序逐一上載，金融機構無須等待檔案處理結果即可上傳下一個檔案，系統將按上載的順序逐一對檔案進行處理；
8. 同一批次的首個檔案(如：202501992026041011203000.zip)如符合條件，相應資料年度報送的資料將被刪除(請參閱“7.2.2 期限內資料的更正”)，如要清除上一批次已被接納的資料，金融機構只須上載另一批次的首個檔案，即檔案名稱中的日期或時間部份與已提交的不同(如：202501992026041112200000.zip)；
9. 除同批次首個上載的檔案外，其後上載的檔案倘被系統拒絕，系統並不會刪除先前已接納的資料，金融機構只須以同一檔案名稱重新上載正確的資料即可。

以分拆檔案報送期限內資料例子：



(圖 7.2.3-A)

7.2.4. 期限後報送

法定報送期後，倘發現已報送的金融帳戶信息有誤或遺漏，金融機構祇須上載相應的增量資料，即僅需要包含新增/更正的帳戶資料。金融機構可上載多個新增、更正或刪除帳戶資料的檔案。系統將按檔案上載的順序逐一處理。倘上載的多個檔案中有檔案未能通過檢查時，系統將按順序處理其餘檔案。

如金融機構須要新增、更正或刪除的帳戶報告多於 60 萬筆，金融機構可上載多個不多於 60 萬筆資料的檔案，以完成有關操作。

7.2.5. 零申報

倘報送信息的金融機構在執行盡職調查程序後，確認上一曆年沒有須報送帳戶，則可透過此頁面通知財政局，聲明該年度沒有須報送帳戶信息及說明相關理由。往後年度即使上述情況維持不變，金融機構仍須每年作出申報。

於金融機構檔案頁面，點擊「零申報」按鈕，可新增零申報。



The screenshot shows a web-based application interface for financial institutions. At the top, there is a navigation bar with links: '金融機構資訊' (Financial Institution Information), '用戶管理' (User Management), '資訊管理' (Information Management), '金融帳戶信息報送' (Financial Account Information Reporting) which is highlighted in green, and '財政局資源下載' (Ministry of Finance Resource Download). Below the navigation bar, there is a search bar with dropdown menus for '資料年度' (Data Year) and '系統識別號' (System Identifier), and buttons for '重置' (Reset), '查詢' (Search), and '更多' (More). A breadcrumb trail indicates the current location: '當前位置: 金融帳戶信息報送 > 金融機構檔案'. On the right side of the search bar, there are two buttons: '零申報' (Zero Declaration) and '新增檔案' (Add New File). The '零申報' button is highlighted with a red rectangular box.

(圖 7.2.5-A)

點擊「零申報」按鈕後，彈窗打開零申報頁，可新增零申報。

零申報

* 系統識別號 請選擇

機構名稱(英文) 請輸入

* 資料年度 請選擇

本機構主要管理基金/信託/其他投資實體，故並沒有維持任何金融帳戶。

本機構雖開始營運，但於該資料年度並沒有維持任何金融帳戶。

* 兹聲明 本機構經執行盡職調查後，確認所擁有的金融帳戶中並沒有須報送帳戶。

其他情況/補充說明：

請輸入

申請日期 01/11/2025

取消 確認

(圖 7.2.5-B)

頁面中帶“*”的為必填欄位

零申報步驟如下：

1. 點擊「系統識別號」欄位選取申報的金融機構或投資實體。
2. 點擊「資料年度」欄位選取報送檔案所涉及的資料年度。
3. 選取零申報的原因(可多選)，或選取「其他情況/補充說明」並手動輸入必填的補充信息。
4. 點擊「確認」按鈕提交申請，系統會校驗必填欄位及保存信息，並返回金融機構檔案頁。

倘取消申請，點擊「取消」按鈕返回金融機構檔案頁。

7.3. 統計報送信息

統計報送信息頁面顯示金融機構各資料年度所報送金融帳戶的統計數據。

依次點擊【金融帳戶信息報送】-【統計報送信息】，進入統計報送信息頁面。



(圖 7.3-A)

7.3.1. 金融機構報送統計

於統計報送信息頁面點擊「金融機構報送統計」，該頁面內的金融機構報送統計列表會顯示金融機構各資料年度的報送狀況及相關的統計數據。

列表中的「有效帳戶報告總數」欄位載有金融機構於該資料年度的有效帳戶報告總數，即不包括已被刪除的帳戶報告；「有效檔案總數」欄位載有金融機構於該資料年度的有效檔案總數，即不包括曾被接納但之後被取代的檔案。

金融機構資訊	用戶管理	資訊管理	金融帳戶信息報送	財政局資源下載
當前位置：金融帳戶信息報送 > 統計報送信息				
金融機構報送統計				投資實體報送統計
資料年度 請選擇				重置 查詢
金融機構報送統計				
資料年度	上載類型	有效帳戶報告總數	有效檔案總數	
2024	已申報	23,491	1	
< 1 > 前往 <input type="text" value="1"/> 頁 10條/頁 共1條記錄				

(圖 7.3.1-A)

7.3.2. 投資實體報送統計

於統計報送信息頁面點擊「投資實體報送統計」，該頁面內的投資實體報送統計列表顯示由該金融機構管理的所有投資實體於各資料年度的報送狀況及相關的統計資料。

列表中的「有效帳戶報告總數」欄位載有投資實體於該資料年度的有效帳戶報告總數，即不包括已被刪除的帳戶報告；「有效檔案總數」欄位載有投資實體於該資料年度的有效檔案總數，即不包括曾被接納但之後被取代的檔案。

金融機構資訊 用戶管理 資訊管理 **金融帳戶信息報送** 財政局資源下載

當前位置：金融帳戶信息報送 > 統計報送信息

金融機構報送統計 **投資實體報送統計** (選項)

系統識別號 請輸入 投資實體名稱 請輸入 **重置** **查詢**

資料年度 請選擇

投資實體報送統計

資料年度	系統識別號	投資實體名稱	投資實體類型	報送狀態	有效帳戶報告總數	有效檔案總數
暫無資料						

< **1** > 前往 頁 10條/頁 共0條記錄

(圖 7.3.2-A)

第八章 財政局資源下載

8.1. 下載財政局電子證書

此連結可下載財政局電子證書用作對金融帳戶檔案進行加密(下載的證書可直接使用，無需轉換格式)，且可配合由本局提供的加密輔助軟件一併使用。

依次點擊【財政局資源下載】-【下載財政局電子證書】，下載證書檔案。



(圖 8.1-A)

點擊「下載」按鈕後，將財政局電子證書下載至本地設備。



(圖 8.1-B)

點擊「取消」按鈕可取消下載。

8.2. 下載加密輔助軟件

此連結可下載加密輔助軟件以對金融帳戶檔案進行電子簽署、加密及壓縮處理(詳情請參閱“附錄四 加密輔助軟件說明”)。

依次點擊【財政局資源下載】-【下載加密輔助軟件】，下載軟件。



(圖 8.2-A)

點擊「下載」按鈕後，將加密輔助軟件下載至本地設備。



(圖 8.2-B)

點擊「取消」按鈕可取消下載。

附錄一 取得金融機構的公開密鑰(Public-Key)說明

步驟一、

前往澳門 eSigntrust 網頁，網址：<http://www.esigntrust.com/cn/index.php>



步驟二、

1. 點擊“資料庫”；
2. 點擊“搜尋和檢查 eSignTrust 電子證書的狀態”。

The screenshot shows a web browser window for the eSignTrust Certification Services website. The URL in the address bar is www.esigntrust.com/cn/repository.html. The page title is "eSignTrust Certification Services". The top navigation bar includes links for "有關eSignTrust" and "聯絡我們", and language options "繁體 | PORT | ENG". A search bar is also present.

The main menu at the top has several items: "電子證書", "服務", "資料庫" (highlighted with a red box), "支援及下載", and "網上服務". Below this, a secondary navigation bar shows "資料庫" (highlighted with a blue box) and "主頁 > 資料庫 > 資料庫".

The main content area is titled "eSignTrust的作業" and lists several links:

- eSignTrust的證書政策
- eSignTrust的認證作業準則
- 信賴方協議
- 登記人協議
- 保護私隱聲明

Below this, there are two sections: "根證書/簽發認證實體證書" and "證書狀態及資料".

In the "證書狀態及資料" section, item 2. "搜尋和檢查 eSignTrust 電子證書的狀態" is highlighted with a red box.

步驟三、

1. 於“搜尋電子證書的狀態及資料（第三代 G03 證書）”項目下；
2. 點擊“搜尋機構標準證書”。

The screenshot shows the eSignTrust website interface. The top navigation bar includes links for '有關eSignTrust' (About eSignTrust), '聯絡我們' (Contact Us), '繁體' (Traditional Chinese), 'PORT' (Portuguese), and 'ENG' (English). A search bar is also present. The main content area features the eSignTrust logo and navigation links for '電子證書' (Digital Certificate), '服務' (Services), '資料庫' (Database), '支援及下載' (Support and Downloads), and '網上服務' (Online Services). A sidebar on the left is titled '資料庫' (Database) and lists options: '搜尋eSignTrust證書狀態' (Search eSignTrust certificate status), '撤銷eSignTrust證書' (Revoke eSignTrust certificate), and '尋找證書撤銷清單' (Find certificate revocation list). The main content area displays the title '搜尋eSignTrust電子證書的狀態' (Search eSignTrust digital certificate status) and a note about OCSP and LDAP services. Below this, a section titled '以LDAP搜尋電子證書的狀態及資料' (Search digital certificate status and data via LDAP) includes links for '以LDAP搜尋政府機關或個人電子證書' (Search government agency or individual digital certificate via LDAP) and '以LDAP搜尋機構或安全電郵之電子證書' (Search organization or secure email digital certificate via LDAP). A numbered list on the right indicates steps: 1. 搜尋電子證書的狀態及資料 (第三代G03證書) (Search digital certificate status and data (Third Generation G03 certificate)) and 2. 搜尋機構標準證書 (Search organization standard certificate).

步驟四、

1. 於 E-mail Address 欄位輸入電子簽名證書的電郵地址；
2. 點擊“Search”；

The screenshot shows the Digital ID Services search interface. The top navigation bar includes links for 'Home', 'Digital ID Center', and 'Help with this Page'. The main content area features the eSignTrust logo and the title 'Digital ID Services'. Below this is a search form titled 'Search For Digital IDs'. It includes instructions: 'To search the online database for anyone's Digital ID, enter the name or e-mail address, and click the SEARCH button. You cannot use wildcard characters.' and 'Please read the Relying Party Agreement below before starting your search. When you click the SEARCH button, you accept the terms of the Relying Party Agreement.' The search form has fields for 'Enter the E-mail Address:' (example: john_doe@esigntrust.com) and 'Search for IDs that are:' with options for 'Valid', 'Expired', 'All', 'Revoked', 'Pending', and 'Approved'. A red box highlights the 'Enter the E-mail Address:' field and the 'Search' button.

3. 點擊電子證書持有人有效的證書“XXX XXX XXX (Valid)”；

The screenshot shows a web browser window titled "Results" with the URL <https://onsite.corp.esigntrust.com/services/MacaoPostandTelecommunicationsBureauCorporateDigitalCertifi...>. The main content area is titled "Digital ID Services" and "Search Results". It displays a list of matching Digital IDs. A note explains that the icon next to a listing indicates the owner's preferred ID for encrypting secure e-mail messages. A row for "XXX XXX XXX (Valid)" is highlighted with a red box, and the number "3." is written next to it. Below this row, it says "Digital ID Class 2 - OnSite Subscriber" and "Validity period from Oct-10-2023(GMT) to Oct-09-2026(GMT)". At the bottom, there are links for "New Search" and "Copyright © 2013, Symantec Corporation. All rights reserved." followed by the Symantec logo.

4. 核對及記下電子證書持有人名稱 (可用於財政局系統登記證書持有人)

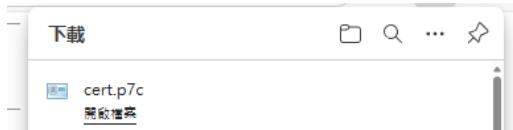
5. 點擊“Download”；

The screenshot shows a web browser window titled "Digital ID Information" with the URL <https://onsite.corp.esigntrust.com/services/MacaoPostandTelecommunicationsBureauCorporateDigitalCertific...>. The main content area is titled "Digital ID Services" and "Digital ID Information". It shows a table of digital ID details. The "Name" field, containing "XXX XXX XXX", is highlighted with a red box, and the number "4." is written next to it. The table includes fields for Status (Valid), Validity (Oct.10.2023 - Oct.09.2026), Class (Digital ID Class 2 - OnSite Subscriber), Address (not available), Subject (Country = MO, Organization = Macao Post and Telecommunications Bureau, etc.), and Serial Number. Below the table, a note states: "If this is the correct ID, you can download or revoke the Digital ID." A "Relying Party Agreement" section contains a scrollable text box with the title "Macao Post and Telecommunications eSignTrust Certification Services Relying Party Agreement" and the instruction "YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING AN ELECTRONIC CERTIFICATE ("CERTIFICATE") OF MACAO POST". At the bottom, the number "5." is written next to a red box around the "Download" button, and the "Download" button itself is highlighted with a red box.

6. ID Format 選擇“S/MIME Format (Binary PKCS#7)”；
7. 點擊“Submit”下載檔案。

The screenshot shows a web browser window titled "Download Digital ID" at the URL <https://onsite.corp.esigntrust.com/services/MacaoPostandTelecommunicationsBureauCor>. The page header includes the "eSignTrust" logo and "Digital ID Services". A "Help with this Page" link is visible. The main content area is titled "Select Format to Download Digital ID". Step 6 is indicated by a red box around the "ID Format" dropdown menu, which is currently set to "S/MIME Format (Binary PKCS#7)". Step 7 is indicated by a red box around the green "Submit" button. Below the dropdown, there is a "Relying Party Agreement" section containing a text box with terms and conditions, a "Click the Submit button to download the Digital ID." instruction, and a "Copyright © 2013, Symantec Corporation. All rights reserved." notice.

8. 取得副檔名為 p7c 的電子證書檔案。



附錄二 簽署及加密說明

Step 1 – Sign the XML File

File Naming Convention : YYYYXXXXYYYYMMDDHHMMSS00.xml

Step description :

- Prepare the 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" />
- It is required that the XML file be signed by first creating a SHA2–256² hash. The sending Financial Institution will then create an RSA digital signature using the 2048-bit private key from eSignTrust.
- After validating the schema, digitally sign the XML file using W3C Recommendation XML Signature Syntax and Processing (Second Edition)³ “enveloping” signature. s
- Use the digital signature “enveloping” type. The “enveloped and detached” types will cause the transmission to fail. The file name is “YYYYXXXXYYYYMMDDHHMMSS00.xml”. The file name and extension are case sensitive and any variation in file name or format will cause the transmission to fail.

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

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

3. XML Signature Syntax and Processing (Second Edition), June 2008, <http://www.w3.org/TR/xmldsig-core/>

Step 2 – Compress the XML File

File Naming Convention : YYYYXXXXYYYYMMDDHHMMSS00.zip

Step description :

- Ensure “zip” is the file extension used by the compression tool or library.
- Ensure the file is compressed using the deflate compression algorithm.

Summary :

- The file name is “YYYYXXXXYYYYMMDDHHMMSS00.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.

Step 3 – Encrypt the XML File with AES 256 Key

File Naming Convention : YYYYXXXXYYYYMMDDHHMMSS00

Step description :

- After compression, encrypt the file “YYYYXXXXYYYYMMDDHHMMSS00.zip” using the AES–256 cipher with a randomly generated “one–time use” AES key.
- There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility :
 - Cipher Mode : CBC (Cipher Block Chaining)
 - Salt : No salt value
 - Initialization Vector (IV) : 16 byte IV. The IV must, for the FI performing the encryption, be random and unique for every encryption.
 - Key Size : 256 bits / 32 bytes – the key size should be verified. Moving the key across operating systems can affect the key size.
 - Encoding : None. There can be no special encoding. The file will contain only the raw encrypted bytes.
 - Padding : PKCS#7 version 1.5
- The AES encrypted file name is “YYYYXXXXYYYYMMDDHHMMSS00”. The file is case sensitive and any variation in file name or format will cause the transmission to fail.
- 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)

- Advanced Encryption Standard (FIPS 197), November 2001

Process : Validate Certificate

Step 4a – Encrypt the AES Key and IV with Public Key of Recipient

File Naming Convention : N/A

Step description :

- 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 Certificate Authority designated responder

Process : Encrypt the AES Key

Step 4b – Encrypt the AES Key and IV with Public Key of FSB

File Naming Convention : YYYYXXXXYYYYMMDDHHMMSS00_Key

Step description :

- After validating the certificate, use the public key from FSB's certificate to encrypt the 32 byte AES 256 key concatenated with the 16 byte IV. The encrypted value must be 48 bytes in length.
- The public key encryption uses the standard RSA algorithm. There are several steps necessary to perform AES encryption. The following agreed settings should be used to maintain compatibility :
 - Padding : PKCS#1 version 1.5
 - Key Size : 2048 bits
- The encrypted file name is “YYYYXXXXYYYYMMDDHHMMSS00_Key”.

Summary :

- There will be 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 XML file name is “YYYYXXXXYYYYMMDDHHMMSS00”
2. Asymmetric encryption – the public key encrypted AES 256 key file name is “YYYYXXXXYYYYMMDDHHMMSS00_Key”

Step 5 – Create the transmission file (data packet)

The two files to be contained in a data packet are :

File Name	Description
YYYYXXXXYYYYMMDDHHMMSS00	Encrypted XML using a randomly generated one-time use key
YYYYXXXXYYYYMMDDHHMMSS00_Key	Key encrypted using FSB's public key

The data packet will be named :

File Name	Description
YYYYXXXXYYYYMMDDHHMMSS00.zip	Transmission file to be sent

For example : 201701992018031512302000.zip

附錄三 簽署及加密代碼示例

- XML Signature Syntax and Processing (Second Edition)
<https://www.w3.org/TR/xmlsig-core/>
- C# XML Signature
[https://msdn.microsoft.com/en-us/library/system.security.cryptography.xml.signedxml\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.security.cryptography.xml.signedxml(v=vs.110).aspx)
- Java XML Signature
<http://docs.oracle.com/javase/8/docs/technotes/guides/security/xmlsig/XMLEDigitalSignature.html>
- C# AES Encryption
[https://msdn.microsoft.com/en-us/library/system.security.cryptography.aes\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.security.cryptography.aes(v=vs.110).aspx)
- C# RSA(Certificate) Encryption
[https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsacryptoserviceprovider\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/system.security.cryptography.rsacryptoserviceprovider(v=vs.110).aspx)
- Java Encryption
<http://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html#SimpleEncrEx>

附錄四 加密輔助軟件說明

1. 簡介

本局提供的加密輔助軟件功能為對 XML 資料檔案進行電子簽署、加密資料及壓縮資料。

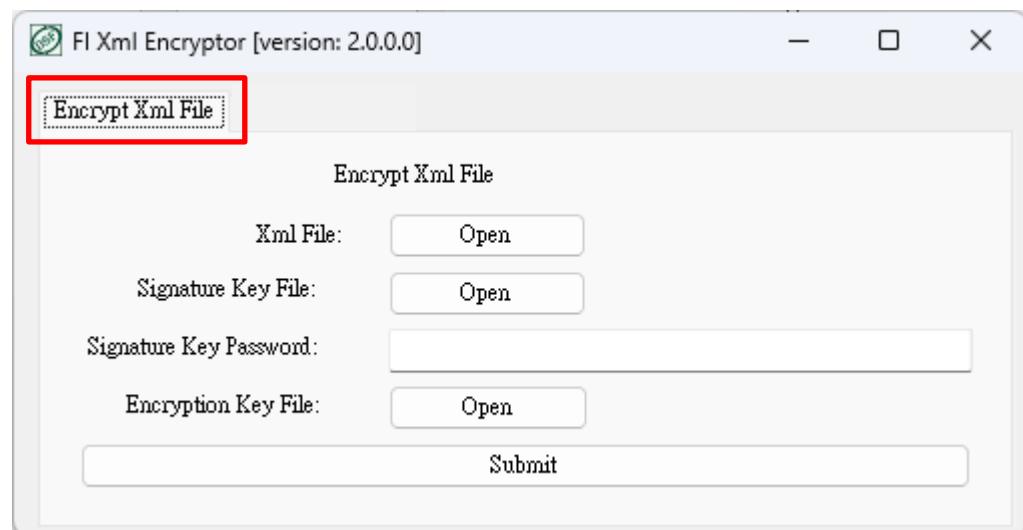
1.1 建議運行環境：

Windows 7 (64 bit)或以上

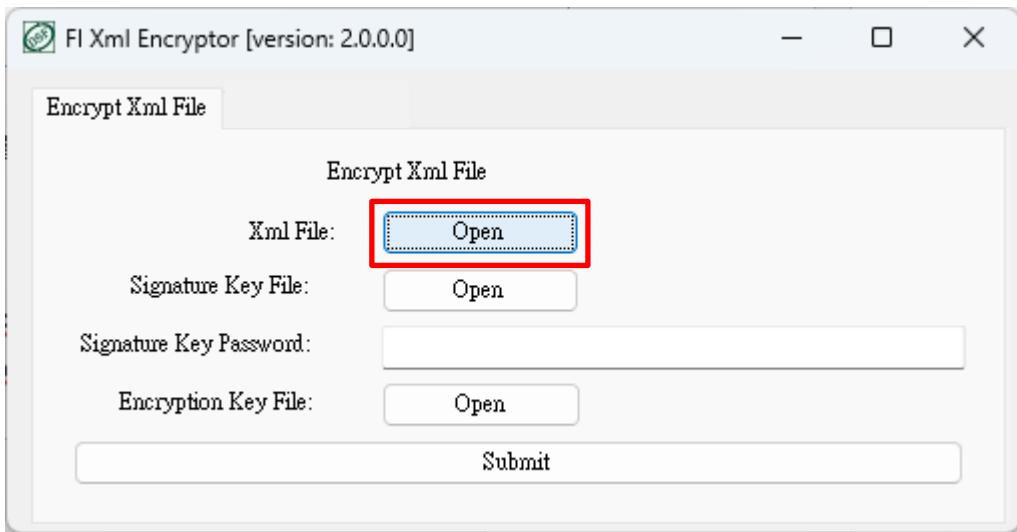
Net Framework 4.5.2

2. 簽署及加密 XML 資料檔案的操作方法

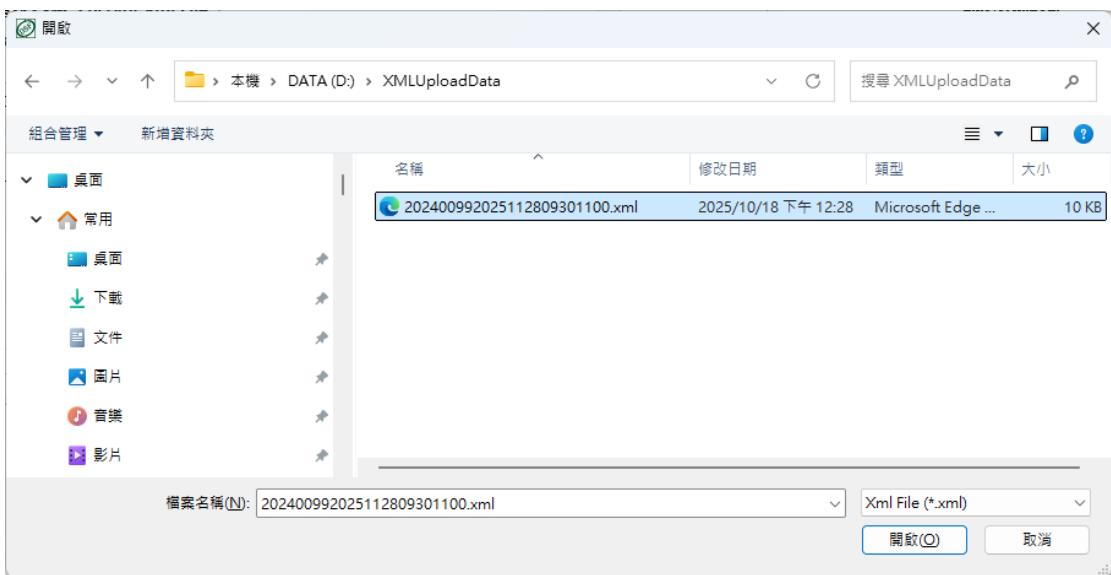
步驟一： 打開輔助軟件，選擇標籤“Encrypt Xml File”



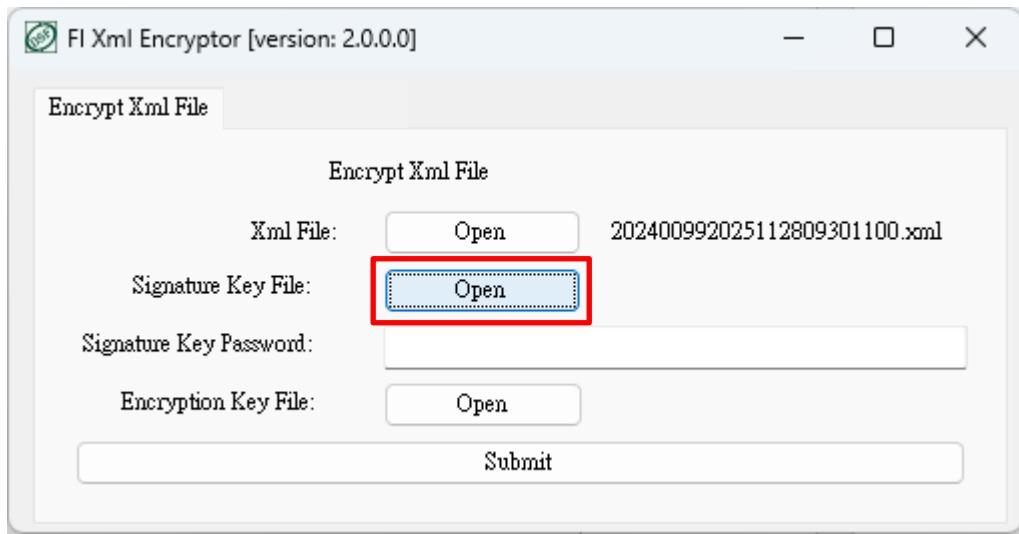
步驟二： 打開需要簽署、加密及壓縮之 XML 資料檔案



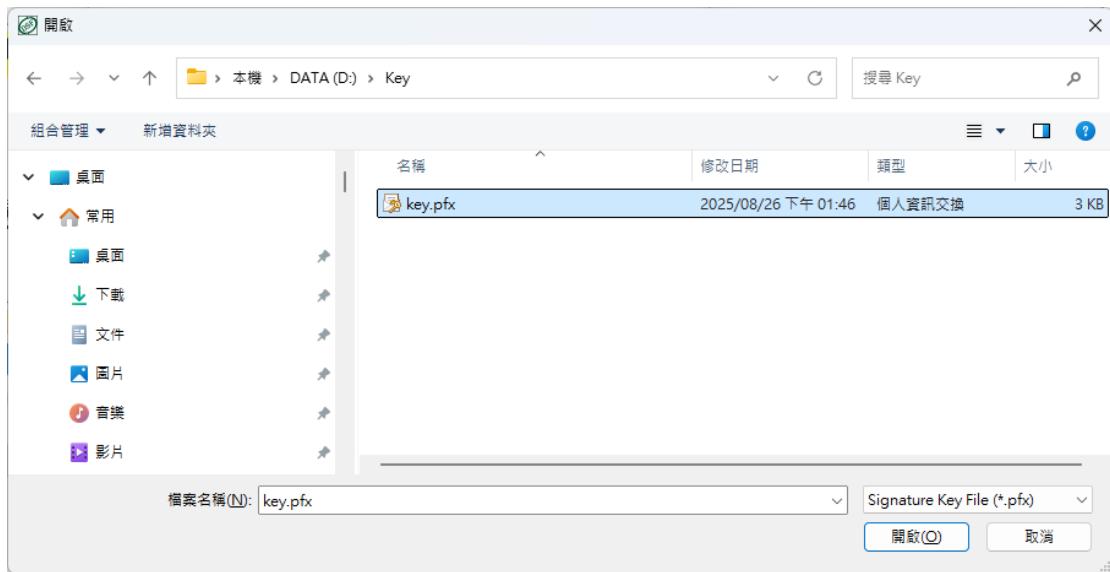
選取檔案



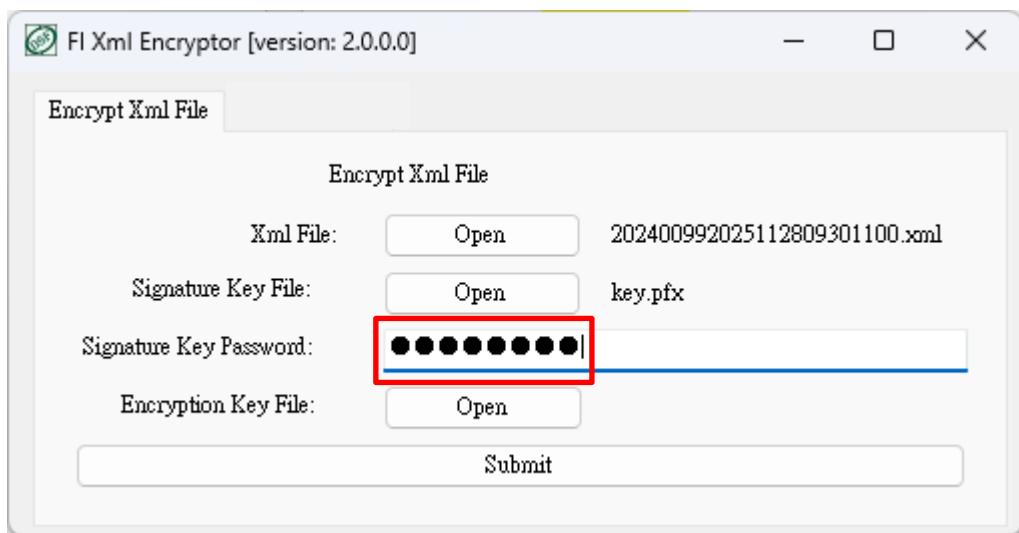
步驟三：打開 Signature Key



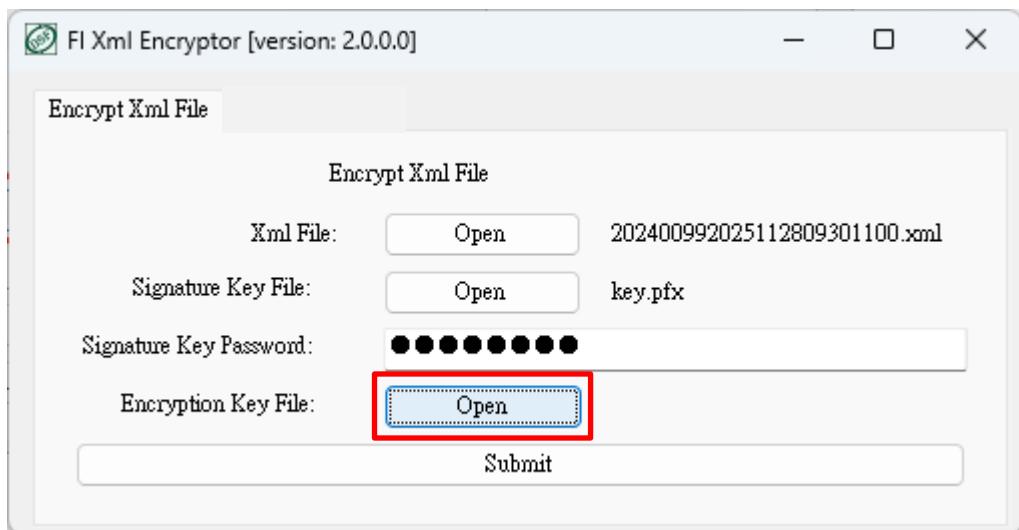
選取簽署用的 Key file(由 eSignTrust 發出的「高級電子簽名」證書 Private key)



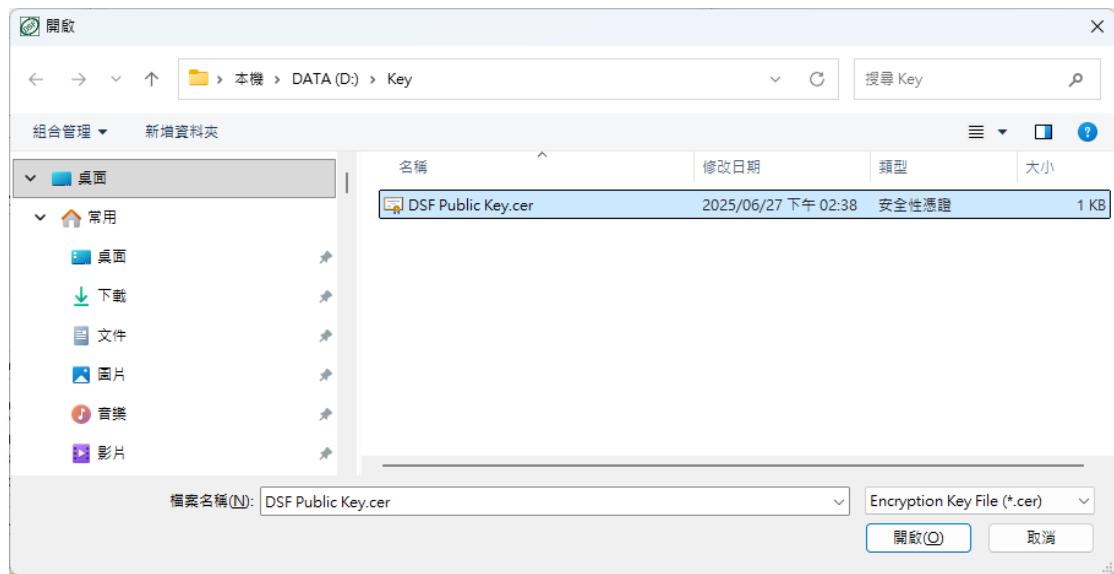
步驟四： 輸入 Signature Key 密碼(證書 Private key 密碼)



步驟五： 打開財政局之 Public Key

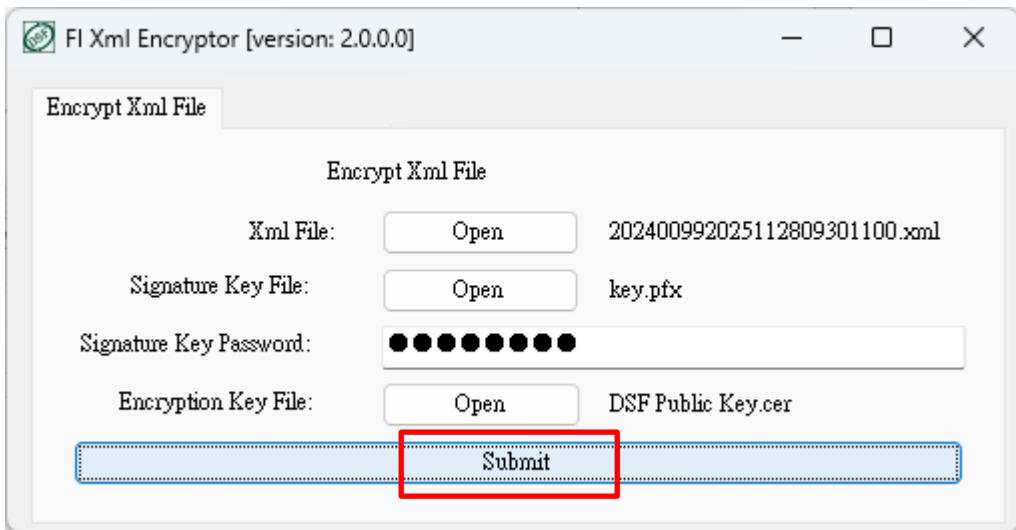


選擇 Public Key 檔案



下載財政局 Public Key 方法可參閱“8.1 下載財政局電子證書”。

步驟六： 按 Submit 儲存已完成簽署、壓縮及加密的資料檔案



需留意，上載的檔案名稱必須符合本局系統要求，詳情可參閱本局網站之資訊。