介接 IR 系統之各校 Single Sign On API 設計說明

一、認證模組運作機制

1. 連線規則：請盡量使用 SSL 也就是 https 連線，以避免資料外洩。
2. 認證程序

(1) IR 系統中需要認證才能使用的網頁，若使用者 session 不存在，將會自動導至您所提供的認證網頁網址（**請在 sso.redirect_url 設定登入頁面 URL**）。

導至認證網頁時，請記得連線的 servlet。IR 系統會自帶 linkFrom 參數至 sso.redirect_url 設定之認證登入頁面，記載來源之連結 url，若有需要可以用 request.getParameter(“linkFrom”)等方式取用。

(2) 各校認證系統進行認證，回傳該使用者是否有權限使用 IR。若無權限，則請自行提供登入失敗或權限畫面告知使用者。

(3) 若可使用 IR 系統，請導回原始連結的 Servlet 網頁(步驟 2 中所記之來源連網網頁)，並回傳 SessionID(參數名稱為 sess，參數內容請自行訂定一“唯一”的一串英數字號碼)。

例如: http://ir.xxx.edu.tw/sso-login?sess=abd32432hiofds

(4) IR 系統收到回傳之 session 後，將會以 web service 型式，根據上一步驟取得的 SessionID 向各校索取使用者資料。（**請在 sso.requestdata_url 設定 API URL**）

(5) IR 系統收到使用者資料後，處理後續登入系統事宜。

I. 以使用者 email 檢查是否存在系統，若不存在則自動建立。

II. 比對 UnitName 與 IR 類別名稱，給予基本的上傳權限。

(6) 登入完畢後，IR 系統會導回之前欲連線的網頁。

(7) 登出：IR 系統登出時，會一併呼叫各校所提供之登出 API 以處理登入之善後事宜(非必要)。

二、使用 SSO 程序

(1) 更改[IR]/config/dspace.config 中之相關設定

```
plugin.sequence.org.dspace.eperson.AuthenticationMethod = \
        org.dspace.eperson.SSOAuthentication,org.dspace.eperson.PasswordAuthentication
webui.sso.autoregister = true                    #使用 sso 時請先將其設為 true
sso.enable = true                                #使用 sso 時請先將其設為 true
sso.redirect_url = https://xxxxxxx/xxxx          #認證網頁 URL
sso.requestdata_url = http://xxxxxxx/xxxx        #提供取得使用者資料的 API 程式 URL
sso.logout_url = https://xxxxxxxxx/logout.jsp    #若登出時需要執行某些程式才能完整清除
                                                   session 及使用者資訊，請提供網址，否則不用
```

註：sso.redirect_url、sso.requestdata_url 及 sso.logout_url 之程式，均請自行撰寫相關程式

(2) 請提供 web service 型式的 API，可讓外部以 sessionID 取得使用者資料。

Web service 呼叫範例：（IR 系統將會以此格式呼叫在 sso.requestdata_url 所設定的 API）

```
<?xml version=”1.0” encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <checkSession xmlns="http://tempuri.org/">
      <SessionID>sess </SessionID>
    </checkSession>
  </soap:Body>
</soap:Envelope>
```

webService 回傳之使用者資料範例：各校需自行開發 API（如 sso.requestdata_url 所設定），可以接受上述格式的 webservice 呼叫，並回傳以下格式的 xml 資料。（資料欄位需完全相同）

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <checkSessionResponse xmlns="http://tempuri.org/">
      <checkSessionResult>
<SEQ>73380</SEQ>
#使用者於校內的 ID,如學號,身分證字號或員工編號
```

```
<FromIP>140.112.xxx.xx</FromIP>
#使用者連線來源
<Email>xxx@XXX.XXX.XXX</Email>
#NTUR 系統將以此作為 IR 系統之識別 unique ID
<FirstName>Tony</FirstName>
#若是中文名稱可自行選擇決定三個字都放 FirstName 欄位,或是姓名分開
<LastName>Chen</LastName>
<AccountStatusCode>0</AccountStatusCode>
#若是 AccountStatusCode 欄位目前 IR 系統尚不使用，請先填 0
<UnitCode>A902000</UnitCode>
#單位代碼,將會暫存於 IR 系統中以備日後使用
<UnitName>中文系</UnitName>
#單位名稱,使用者登入系統時將以此單位名稱比對系統類別名稱,給予基本的上傳權限。單位之層級請以「:」符號分隔 ，例如-文學院:中文系:中文組。
            </checkSessionResult>
        </checkSessionResponse>
    </soap:Body>
</soap:Envelope>
```

(3) 登出:IR 系統登出時,若需要提供 API 來處理遠端認證伺服器的 session 控制,請在 config 檔裡註明 url，登出時會一併呼叫該網頁(傳遞參數 sess)。