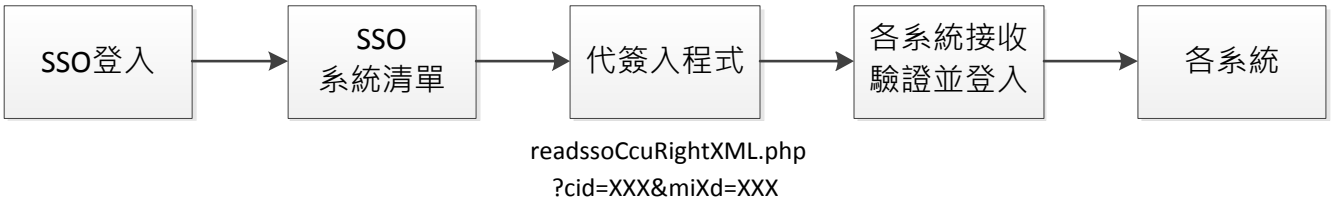
Single Sign On 代簽入程式導入相關資訊

Single Sign On(SSO)是單一入口登入機制，使用者登入 SSO 主機後，可經由 SSO 內的連結登入到其他系統。使用者可以不用記那麼多組密碼。因此其他系統需要加入一些機制與 SSO 主機配合，才能達成單一簽入的目的。

說明「代簽入」:



導入程式 readssoCcuRightXML.php + refreshSso.php

常數：

SYS_DOOR_URL	子系統端登入頁
SYS_LOGIN_URL	子系統端登入驗證判斷程式
SSO_DOOR_URL	SSO 端首頁

重要 SESSION 變數：

$_SESSION['verifySso']	SSO 登入方式辨識訊號
$_SESSION['tokenSso']	SSO 登入 token 資訊
$_SESSION['sso_enterip']	使用者端登入 IP
$_SESSION['sso_personid']	身份證字號

函式：

sso_getIP()	取得使用者 IP
chk_ssoRight($mix_info)	取得 sso 權限資訊
chk_ssoRefresh($mix_info)	延長 sso 的 session 存活時間
err_msgAlert($msg,$url)	錯誤訊息及導向頁面
ssoLogOut()	SSO 的登出導向

導入步驟

1 前置作業：把 readssoCcuRightXML.php 與 refreshSso.php 放入到網頁資料夾中，再把子系統的連結網址與 ip 給 sso 系統開發人員，以便開發人員把 ip 放入可代簽入的白名單當中。

2 設定 URL 常數

➔ refreshSso.php 的 line35, line36, line39, line40

define('SYS_DOOR_URL',"子系統端登入頁");

define('SYS_LOGIN_URL',"子系統端登入驗證判斷程式");

3 設定正式或測試平台

➔若為測試平台，請開啟 line34 的 define('_TEST_PLATFORM', true);

4 導入初期，使用雙軌並行！因此在登入驗證判斷中，須判別是從原本的方式登入，或是從 SSO 端代登入過去的。

利用 $_SESSION['verifySso'] 做為 SSO 端登入方式的辨識訊號。

因此在登入驗證判斷中除了接收身份證字號外，必需區隔判別其登入方式。

若是從 SSO 接收到登入資訊者，$_SESSION['verifySso'] 變數會存在，且被設為字串'Y'。

登入驗證判斷程式修改範例判斷如下：

```
if( empty($_POST)   AND   isset($_SESSION['verifySso'])   AND   $_SESSION['verifySso']=='Y' ) {
      //sso 代簽入的 code
      //接收 $_SESSION['sso_personid'] (身份證字號)，做登入轉換
} else {
      //原本的登入機制
}
```

5 由登入驗證判斷中，若 isset($_SESSION['verifySso'])成立，則接收 $_SESSION['sso_personid']，再做登入轉換。這部分各系統狀況不同，由各系統想辦法轉換。如果是學生，$_SESSION['sso_personid']的資料會是學號，如果是教職員工，$_SESSION['sso_personid']的資料會是身份證字號。

可用長度=9 且是否全部數字來判斷是學號或是身分證字號，php 範例如下：

```
$user_id = $_SESSION['sso_personid'];
if( strlen($user_id) == 9 && preg_match('/^\d{9}/', $user_id) ) {
      // 學生
} else {
      // 教職員工
}
```

6 在每個程式頁面 include 導入程式 refreshSso.php

目的是在判別 isset($_SESSION['verifySso']) 成立後，執行 chk_ssoRefresh($_SESSION['tokenSso'])函式，以便延長 SSO 端的 session 存活時間。(詳參閱 refreshSso.php, line 135)

7 登出機制請修改如下：

7.1 視窗關閉後自動從子系統登出，或設定 session 存活時間，時間到自動登出。

7.2 手動執行登出功能後，自動導向到子系統的首頁。

8 修改後測試下列情況，如果都正常就 ok 了

8.1 原系統登入登出方式要能正常運作

8.2 從 sso 代簽入，代簽入成功應該在子系統登入成功後的頁面

8.3 原系統已經登入的情況下，再從 sso 端代簽入，應該同樣會是跳到登入成功的畫面，不會有異常狀況發生

8.4 (這點不強制修改，考慮到有些系統沒有登出介面，這點會造成無法切換使用者)
sso 已經代簽入到子系統的情況下，另外開新分頁，直接輸入子系統網址，此時應該要直接跳轉到登入成功的頁面，而不是跳出原本子系統的登入頁面

9 測試平台：http://osa.ccu.edu.tw/~porihuang/
正式平台：http://portal.ccu.edu.tw/

更新日期：2012.06.06