

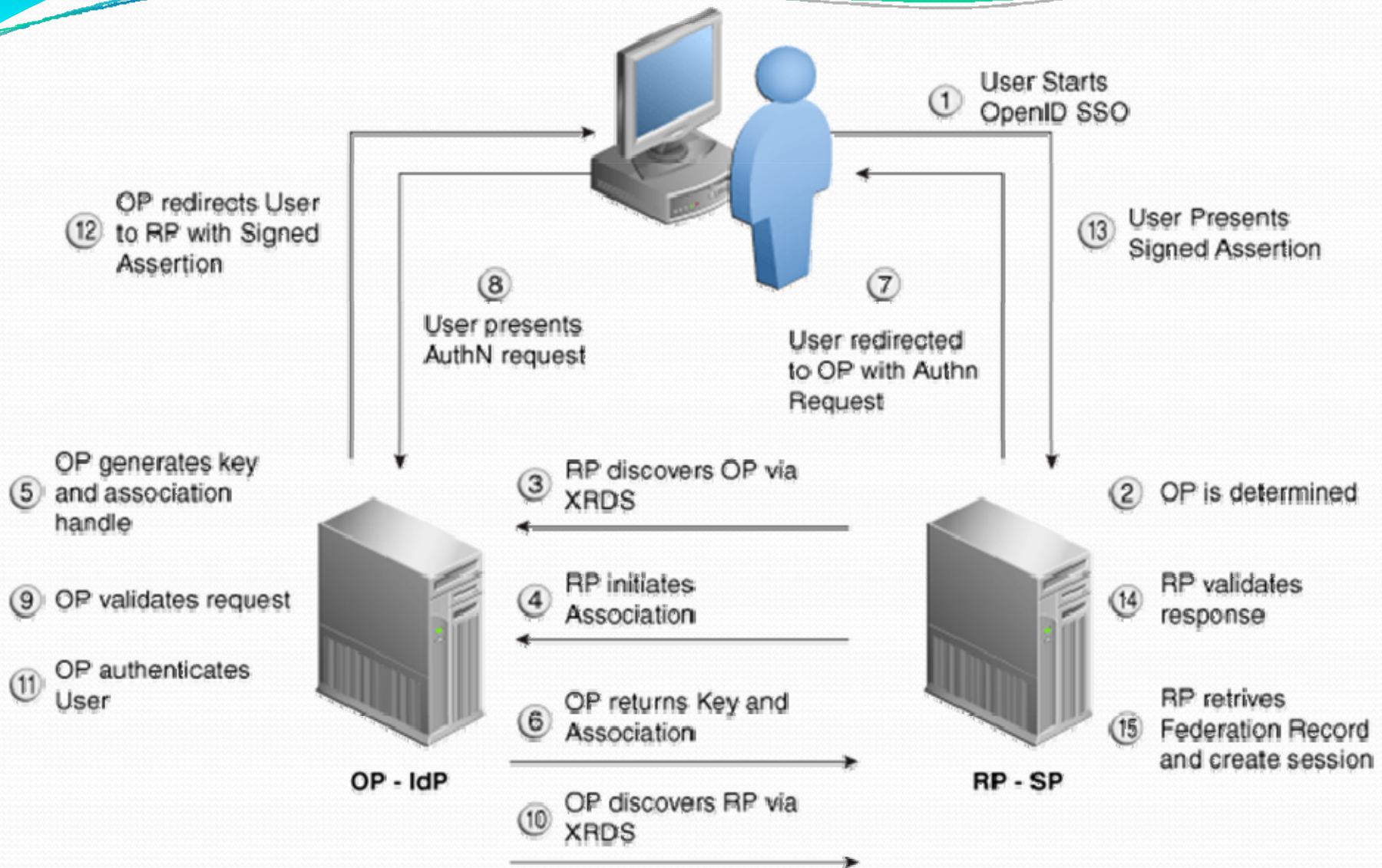
臺中市政府教育局 OpenID Provider建置經驗分享

蕭聖哲 (front713@gmail.com)

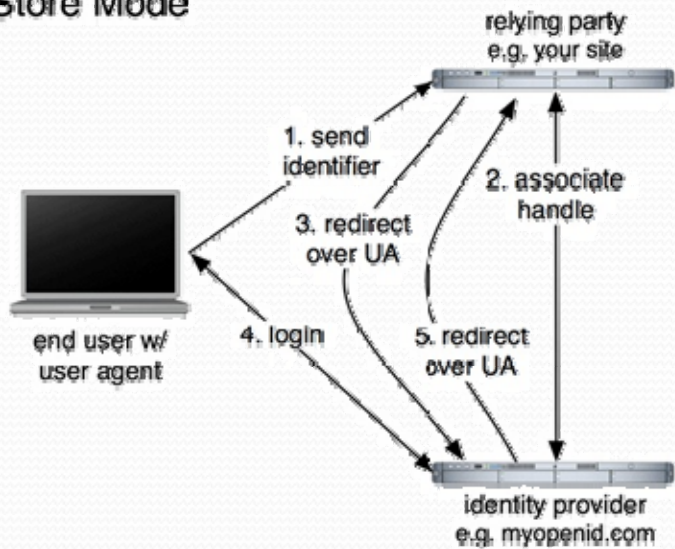
劉育彰 (brucelyc@tc.edu.tw)

Outline

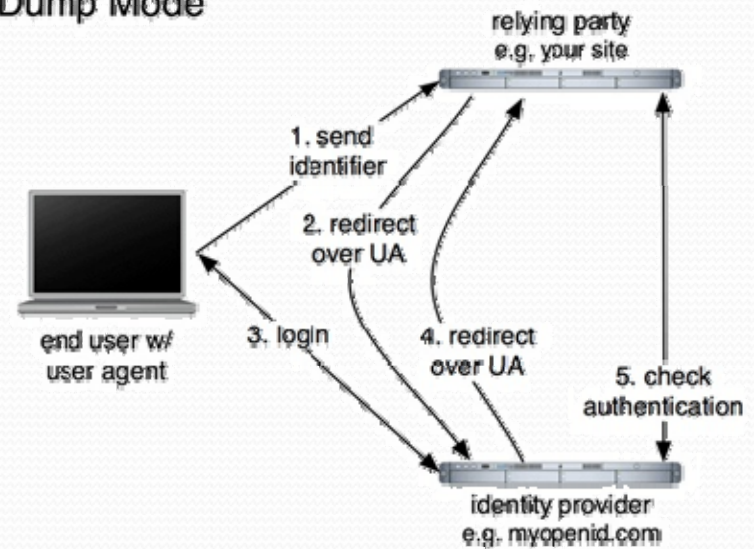
- OpenID Authenciation Flow
- Software requirements
- Implementation expreiences
- Security issues



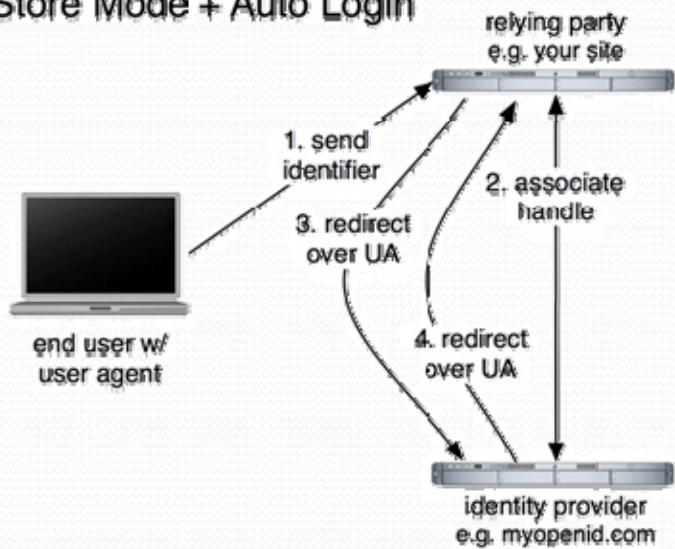
Store Mode



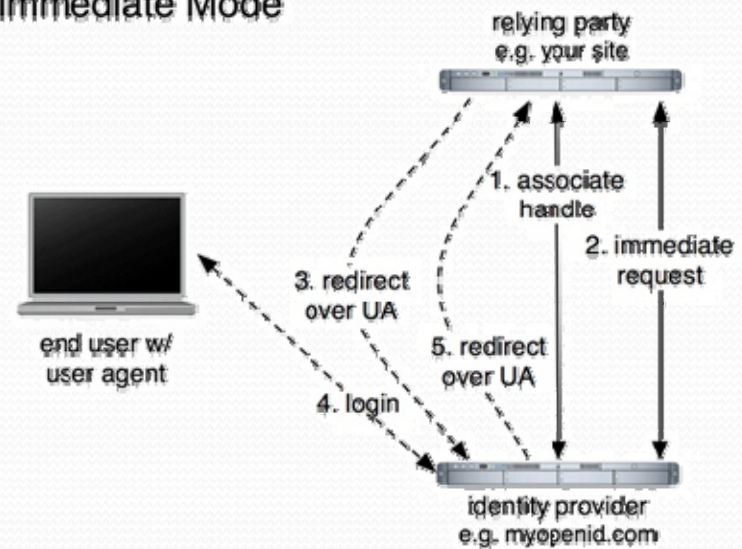
Dump Mode



Store Mode + Auto Login



Immediate Mode



Openid 2.0 Libs

- <http://janrain.com/openid-enabled/>
 - PHP
 - Ruby
 - Python
- <http://dotnetopenauth.net/>
 - Dot Net Framework 3.5
- <http://code.google.com/p/openid4java/>
 - Java

OpenID Simple Registration Extension (SREG)

- OpenID Simple Registration is an extension to the OpenID Authentication protocol that allows for **very light-weight profile** exchange.
- It is designed to pass eight commonly requested pieces of information **when an End User goes to register a new account with a web service.**
- A single field **MUST NOT be repeated** in the response.
- Ref: http://openid.net/specs/openid-simple-registration-extension-1_0.html

SREG fields

欄位參數	欄位名稱	格式說明
openid.sreg.nickname	使用者暱稱/ID	使用者設定的任意文字
openid.sreg.email	E-mail	符合格式的E-mail位址
openid.sreg.fullname	全名	使用者設定的任意文字
openid.sreg.dob	出生日期	格式為YYYY-MM-DD
openid.sreg.gender	性別	「F」代表女性、「M」代表男性
openid.sreg.postcode	郵政代碼	使用者國家的郵政代碼
openid.sreg.country	國家/地區	用ISO3166代號表示，臺灣為TW
openid.sreg.language	語言	用ISO639代表號示，中文為ZH
openid.sreg.timezone	時區	使用Timezone database的代號來表示，臺灣所在時區為「Asia/Taipei」

OpenID Attribute Exchange (AX)

- OpenID Attribute Exchange is a service for OpenID that enables **transport of personal identity information**.
- 相較於SREG規格，Attribute Exchange擁有的優勢為：
 - 不再限制僅能交換 9 個限定的欄位資料，賦與RP與OP自定所需欄位與其資料類型的能力。
 - 一個資料欄位可交換多筆資料。
 - 除單純的從OP端載入資料，更可在使用者於RP端更新資料時將資料送回OP，或是未來RP可以在後端接收OP送出的資料更新。
- Ref: http://openid.net/specs/openid-attribute-exchange-1_0.html

AX example

臺中市雲端閱讀認證服務平臺規格書(read.tc.edu.tw)

Subject	Subject Identifier	Value
姓名	openid.sreg.fullname	說明一
主要學校代碼	http://axschema.edu.tw/school/id	說明二
識別碼	http://axschema.edu.tw/person/guid	說明三
職稱別	http://axschema.edu.tw/person/roles	說明四
級任班級	http://axschema.edu.tw/school/masterclass	說明五
班級人數	http://axschema.edu.tw/school/classstunum	說明六
年級代碼	http://axschema.edu.tw/school/yearno	說明六
班級代碼	http://axschema.edu.tw/school/classno	說明六
座號代碼	http://axschema.edu.tw/school/siteno	說明六

AX example(cont'd)

說明一：`^\u3400-\u9fa5]{2,6}$`

說明二：`^[0-9]{6}$`

說明三：`Hex(SHA256(^[A-Z]{1}[1-2A-D]{1}[0-9]{8}$))`

說明四：多重值

1. `{"sid":014637,"title":["系統管理者","學校管理者","教師","學生"]}`

2. `{"sid":014638,"title":["教師"]}`

說明五：`^[0-9]{4}$`

說明六：`^[0-9]{2}$`

Our Choice (1) – Java Platform

- CentOS 6
- JDK 7u 45
- Apache Wicket 6.11.0 → Java MVC Framework
- Glassfish Community Server 4.0
- MySQL Database
- GCA SSL Certificate
- Openid4java Lib 0.9.8
- Personal URL
 - <http://openid.tc.edu.tw>
 - <http://username.openid.tc.edu.tw>



臺中市政府教育局
Education Bureau, Taichung City Government



臺中市政府教育局OpenID服務

臺中市教師登入

臺中市學生登入

臺中市政府教育局版權所有 Copyright © 2013. All Rights Reserved.

最佳瀏覽解析度 1024x768px. 建議使用瀏覽器 Firefox5.0以上或IE8.0以上或google chrome版本瀏覽本站.

臺中市政府教育局地址：42007 臺中市豐原區陽明街36號 [【位置圖】](#)

市話總機代表號：04-22289111 [《各科室電話分機》](#)

辦公時間：8:00-17:00，中午休息時間：12:00-13:00 彈性上下班時間：8:00-8:30、13:00-13:30、17:00-17:30

[【網路安全宣言】](#) [【隱私權政策】](#)

最後更新時間:10/24/2013 11:18:37



臺中市政府教育局OpenID服務

您好，您使用的網站要求手動輸入帳號與密碼來請求認證，請求認證網站是：

<http://mail.edu.tw/>

請輸入您的公務帳號： .openid.tc.edu.tw

You had selected 3 animals.



請輸入您的密碼：

登入

臺中市政府教育局OpenID服務

請確認要回傳的資訊（若已預先勾選表示介接網站要求回傳此資訊）

姓 名 : 蕭聖哲

電 子 郵 件 : front713@gmail.com

教育雲－個人代碼 : b62897db4f09d77448148e9e43bacd980535d9383f3db14aeb1ed61d9d89fcfd

雲端電子郵件職稱 : [{"id":"064725","title":["教師","縣市管理者"]}]

教育部－學校代碼 : 064725

一次認證

臺中市政府教育局OpenID服務

您好，您使用的網站要求手動輸入帳號與密碼來請求認證，請求認證網站是：

<http://mail.edu.tw/>

請選擇行政區：

請選擇學校：

請輸入您的班級座號（例如：60101）：

Select all three kittens below



請輸入您的密碼：

Our Choice (2) – PHP Solution

- CentOS 6 above
- PHP 5.2 above
- Apache 2 above
- Optional (LDAP, MySQL, Radius, etc ... extension)
- Include Oauth, SAML, etc
- Portal URL
 - <http://sso.tc.edu.tw>
- Personal URL
 - <http://username.sso.tc.edu.tw>

PHP Solution



The screenshot shows a web browser window with the address bar containing `http://brucelyc.sso.tc.edu.tw/`. The page title is "請輸入您的帳號及密碼". The main content area has a blue header with the text "中市教育雲" (Taichung Educational Cloud Service) and "認證雲服務" (Authentication Cloud Service). Below the header, there is a login form with the following fields and elements:

- Language selection: [English](#) | [繁體中文](#)
- Form title: 請輸入您的帳號及密碼
- Account field: 帳號
- Password field: 密碼
- Verification code field: 驗證碼
- Login button: 登入

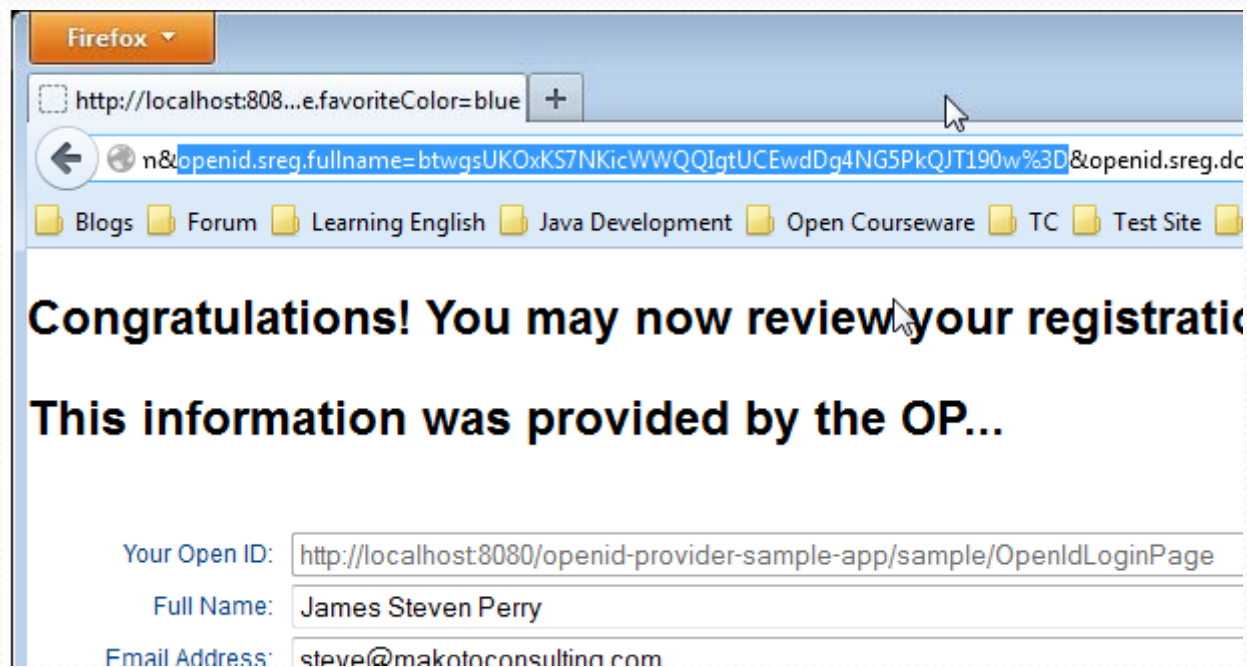
At the bottom of the page, there is a copyright notice: Copyright © 2013 Bruce Liu.

Implementation experiences

- Test for compatibility
 - <http://openid.net/>
 - <http://stackoverflow.com/>
 - <https://isp.moe.edu.tw/>
- Data Source
 - LDAP
 - Database
 - Mail
 - Web Service
 - 校務系統

Security Issues -- Http Get Parameter

- Association → DH Key → Encrypt return value (OP) → Decrypt received value (RP)

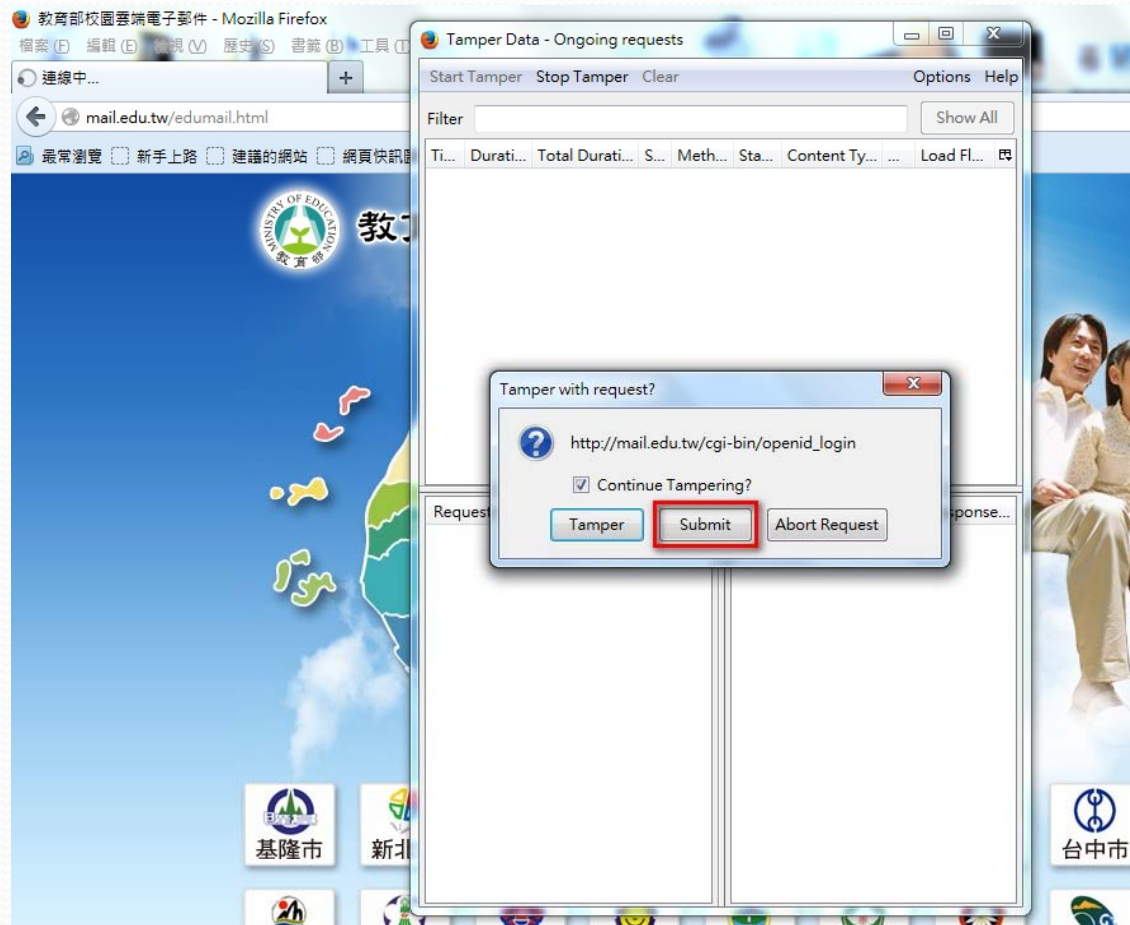


Security Issues -- Http Get Parameter

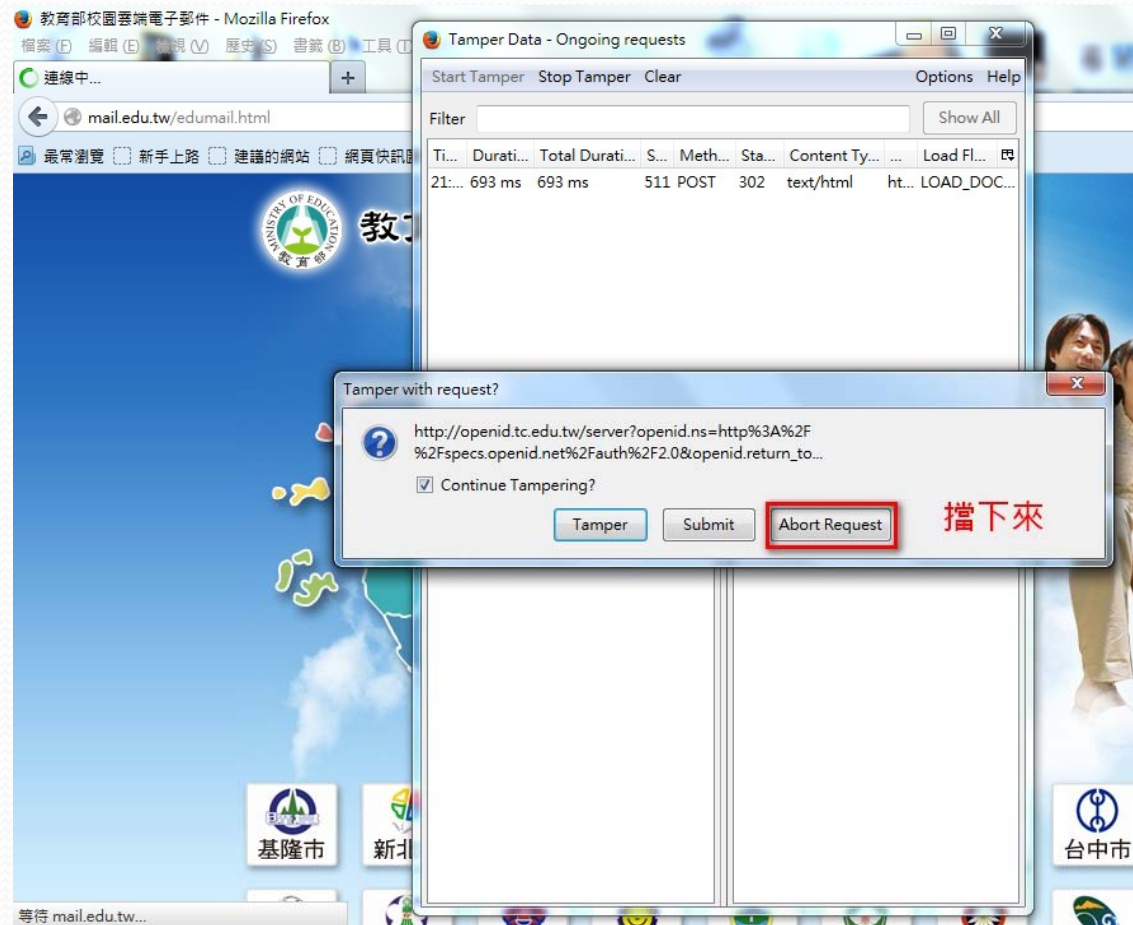
```
SecretKeySpec spec = new SecretKeySpec(Base64.decode(mac), "AES");  
Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");  
cipher.init(Cipher.ENCRYPT_MODE, spec);  
String result = new String(Base64.encode(cipher.doFinal("James Steven Perry".getBytes())));
```

```
//decryption  
SecretKeySpec spec = new SecretKeySpec(Base64.decodeBase64(mackey), "AES");  
Cipher cipher;  
try {  
    cipher = Cipher.getInstance("AES/ECB/PKCS5Padding");  
    cipher.init(Cipher.DECRYPT_MODE, spec);  
    value = new String(Cipher.doFinal(Base64.decodeBase64(value)));  
    log.info("Decrypt AES : " + value);  
} catch (Exception e) {  
}
```


Security Issues -- Redirect(1)



Security Issues -- Redirect(2)



Security Issues -- Redirect(3)

The screenshot displays two windows from the Tamper Data tool. The 'Tamper Details' window on the left shows a table with one entry: 'URL' with the value 'http://openid.tc.edu.tw/'. A red box highlights the 'Copy' button, and the text '取得url' (Obtain URL) is written in red. The 'Encoded' radio button is selected. The 'Tamper Data - Ongoing requests' window on the right shows a table of requests and their headers.

Name	Value
URL	http://openid.tc.edu.tw/...

取得url

Filter	Show All

Ti...	Durati...	Total Durati...	S...	Meth...	Sta...	Content Ty...	...	Load Fl...
21:...	693 ms	693 ms	511	POST	302	text/html	ht...	LOAD_DOC...
21:...	n/a ms	n/a ms	u...	GET	Can...	unknown	ht...	LOAD_DOC...
21:...	0 ms	0 ms	-1	GET	Loa...	unknown	ht...	LOAD_FRO...

Request Header Name	Request ...	Response Header Name	Respons...
Host	openid.tc...	Status	Cancelled ...
User-Agent	Mozilla/5...		
Accept	text/html,...		
Accept-Language	zh-tw,zh;q...		
Accept-Encoding	gzip, defla...		
Referer	http://mai...		

Security Issues – Redirect(4)



Security Issues – Redirect(5)



Security Issues – Redirect(6)



Security Issues – Redirect(7)

Mail2000電子信箱--brucelyc - Mozilla Firefox
檔案(F) 編輯(E) 檢視(V) 歷史(S) 書籤(B) 工具(T) 說明(H)

Mail2000電子信箱--brucelyc +

mail.edu.tw/cgi-bin/start?m=765841441&wrap=1

最常瀏覽 新手上路 建議的網站 網頁快訊圖庫

Openfind
MAIL2000

brucelyc

寫信 信件匣

- 收信匣(1/1)
- 虛擬信件匣
- 送信匣(1/1)
- 草稿匣
- 回收筒(1)
- 廣告信箱
- 信件匣管理
- 預約寄信管理
- 郵件遞送記錄

信箱資訊 **brucelyc@mail.edu.tw**

登入成功

登入資訊

2013/09/25 21:50:53	網頁登入
2013/09/25 21:41:07	網頁登入

信箱容量

雲端硬碟：	
信件使用：	2
剩餘空間：	2
總量：	3

Security Issues – Redirect(8)

教育部全國國中小學
資訊安全管理系統

市立重慶國民中學 登出

• 首頁 填報及檢視

身份：學校人員
單位：重慶國中
上次登入：首次登入

訊息公告 連絡窗口 系統說明 檔案下載 相關連結

訊息公告

- 102年學校填報期限：102/03/01 ~ 102/09/30
(請各「縣市管理員」於102/03/01前指定完成「受評核學校」)
- 102年稽核人員評量期限：102/10/01 ~ 102/12/25
(請各「縣市管理員」於102/10/01前指定完成「受評核學校」)

誤送或刻意送其他單位碼時就改變了權限

Security Issues – Advice

- OpenID Provider (OP)
 - CAPTCHA(avoid brute-force attack)
 - Force validation RP's relam
 - Force Association with dynamic parameters → DH Key Agreement
 - Enable SSL for endpoint
 - OPs SHOULD implement Javascript framebusting code to prevent their UI from being framed.
- OpenID Consumer (RP)
 - Secure key ???
- Requesting Authentication in a Popup
 - 450 px x 500 px
- Ref: http://svn.openid.net/repos/specifications/user_interface/1.0/trunk/openid-user-interface-extension-1_0.html

X-FRAME-OPTIONS

台中市OpenID



此內容無法在框架中顯示

為了協助保護您在此網站所輸入的資訊安全性，此內容的發行者不允許在框架中顯示資訊。

您可以嘗試的方式：

- 在新視窗中開啟此內容



台中市OpenID



台中市OpenID

錯誤

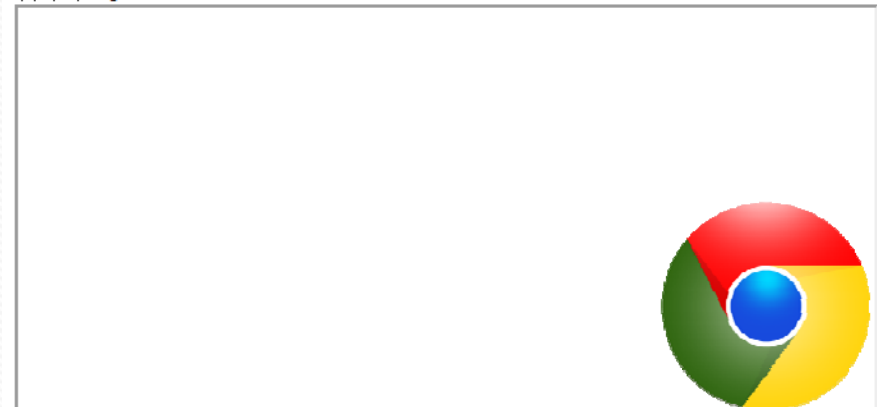
<http://openid.tc.edu.tw/>

這個網站不允許它的內容出現在頁面框架裡，它的內容需要以另外的視窗來顯示。

- 在新視窗載入文件



台中市OpenID



Privacy Issues – Advice

- Person ID Sha256 Rainbow Table
 - Char 1: A~Z(26)
 - Char 2: 1~2(2)
 - Char 3~9: 0~9(100000000)
 - Char 10: check number(1)
 - $26 \times 2 \times 100000000 \times 1 = 5.2$ 億筆
 - 建議 身分證字號 + 西元生日八碼 = 5.2 億 $\times 100000000$
- OpenID Consumer
 - 要謹慎審核，否則sha256碼會被收集，然後...

Current implementation

- 新竹縣
- 苗栗縣
- 南投縣
- 雲林縣
- 澎湖縣
- 嘉義縣
- 嘉義市
- 彰化縣
- 屏東縣