用 Open ID 建立 SSO

國網中心 莊子民

tmchuang@nchc.org.tw

2011/3/8

Outline

- 什麼是 OpenID？
- 為什麼我們要用 OpenID？
- OpenID 怎麼運作的？
  - OpenID 的三個角色
  - OpenID 帳號提供者
  - Delegating Authentication 說明與介紹
  - 個人資料交換
- 你要想要 OpenID 為你做什麼
- OpenID 技術探討

什麼是 OpenID

- 你還在用 excel 表格來管理自己的帳號密碼嗎?
- OpenID 是實現了 Single Sign-On（單一簽入）技術的其中一種作法。
- 2006 年由數個網路服務公司，整合既有的想法與技術，共同提出的規範。
- 一套『**開放標準**』的規範，目前 OpenID 規範由 OpenID.net 開發中。
- 目前規範 OpenID 2.0

為什麼我們要用 OpenID？

- OpenID 是一個以**使用者為中心**所推出的網路身份認證服務。
- 以**網站為基礎**的認證協定，適用於網路的服務，結合了認證、識別、信賴、授權等服務。

圖片截取自 http://myid.tw
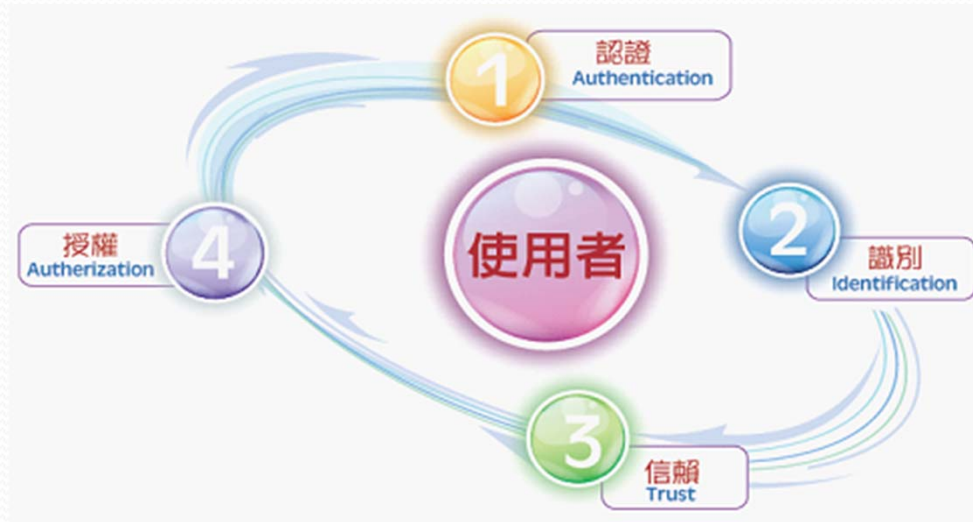
OpenID 特性

- **方便性**
  - 只要向 OpenID 帳號發行者註冊,就可以登入。
  - 認證流程由 OpenID 帳號發行者負責
  - 身份資料交換機制
- **突破性**
  - OpenID 是 Identity 2.0 的實踐
  - Identity 2.0
    - 源自 Web 2.0 理論,也被稱為 digital identity,網際網路身份認證。
    - 使用以使用者為中心的技術,強調的是一個簡單並且開放的身份辨識方法。
  - 2008年 Google, Microsoft, Yahoo! 與 MySpace 等宣布支援
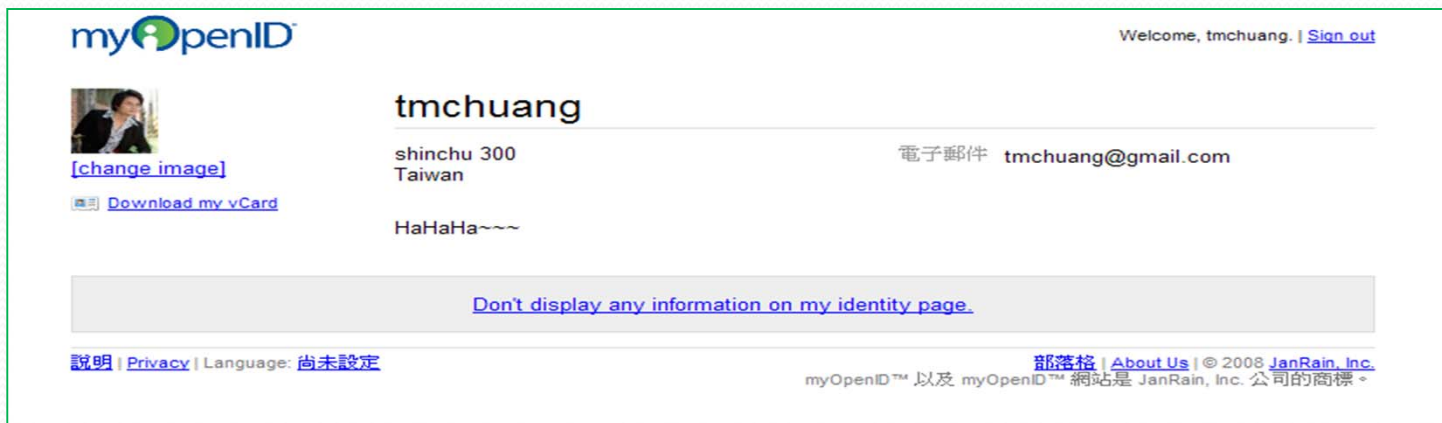 - 2009年5月 Facebook 宣布加入

OpenID 特性(續)

- **獨特性**
  - 使用者為中心(User-Centric)的身份認證機制
  - 就擁有專屬於自己的個人認證識別（OpenID URI）
  - 此 URI 可轉為 URL 做為該 OpenID 擁有者的個人資料頁面
  - 提供代理認證（Delegating Authentication）的機制
- **整合性**
  - 利用代理認證的機制，整合網路上的身份，方便其他使用者辨認又可清楚代表自己。
  - 提供管理已認證的網站、是提供已登入過的網站歷史紀錄 及追蹤不正常的登入情形 etc...

OpenID 長相

- 利用 URI (Uniform Resource Identifier) 作為專屬識別
  - URI 是在網路上呈現一串如網址般的文字及符號的字串，用來識別名字資源。
  - 格式就如同網址一般，網址所含的內容完全沒有限制
    Ex: http://tmchuang.myopenid.com
      http://openid2.colife.org.tw/user.aspx?tmchuang

OpenID 怎麼運作的

- 這個符號就是代表 OpenID，提示使用者輸入 OpenID URI 的意思。

https://sourceforge.net/account/login.php

OpenID 的三個角色

OpenID Provider (OP)
OpenID 帳號提供者
提供註冊 OpenID ，如 Yahoo、
Google、Microsoft Live
Message、MyOpenID、myid.tw

**由不同 Provider 提供的 OpenID
就會被視為不同的 ID**

Relying Party (RP)
受信任的網站
支援 OpenID 驗證的網站
如 facebook 等

使用者

OpenID Login
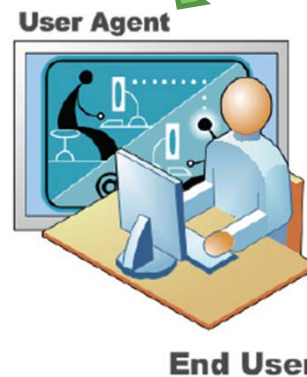
- http://bingo.handlino.com/login

Random Life 和多繽紛樂

Login

CREATE · LIST · VIEW BY TAG

OpenID Login

OpenID: http://

☐ Remember this URL

SUBMIT

Y! Sign in with a Yahoo! ID

填入已註冊的 OpenID
http://tmchuang.myopenid.com/

OpenID Login (con't)

OpenID Login (con't)

- 已認證登入，但沒有使用者記錄，填寫之。

Yahoo OpenID

Yahoo OpenID (con't)

YAHOO!

Yahoo! - 常見問題

我們現在需要你的許可，允許 bingo.handlino.com 辨認你的 Yahoo! 用戶身份

按下面的「同意」按鈕後，意味著你同意 Yahoo! 可將你重新定向到 http://bingo.handlino.com，並允許 http://bingo.handlino.com 辨認你的 Yahoo! 用戶身份。但 http://bingo.handlino.com 不能知道你的 Yahoo! ID 和你的 Yahoo! 帳戶中的任何其他資料。

請記住：

- http://bingo.handlino.com 不能存取你在 Yahoo! 網站上保存的任何資料。
- Yahoo! 的私隱政策不適用於 http://bingo.handlino.com，故請仔細閱讀其私隱政策，了解他們如何使用你的個人資料。
- Yahoo! 與 http://bingo.handlino.com 沒有任何聯盟關係，對於你提供給 http://bingo.handlino.com 的任何用戶資料，雅虎不能保證其安全性。

▶ 登入許可

請檢視以下條款，並在下面表示你同意與否。   全部檢視並列印 🖨

自動登入服務條款－請仔細閱讀

您於第三人網站使用自動登入機制者，您必需自行承擔相關風險。Yahoo!奇摩雖然已採取相關措施保護隱私權及使用者資料之完整，且Yahoo!奇摩對於其他公司並已實施安全
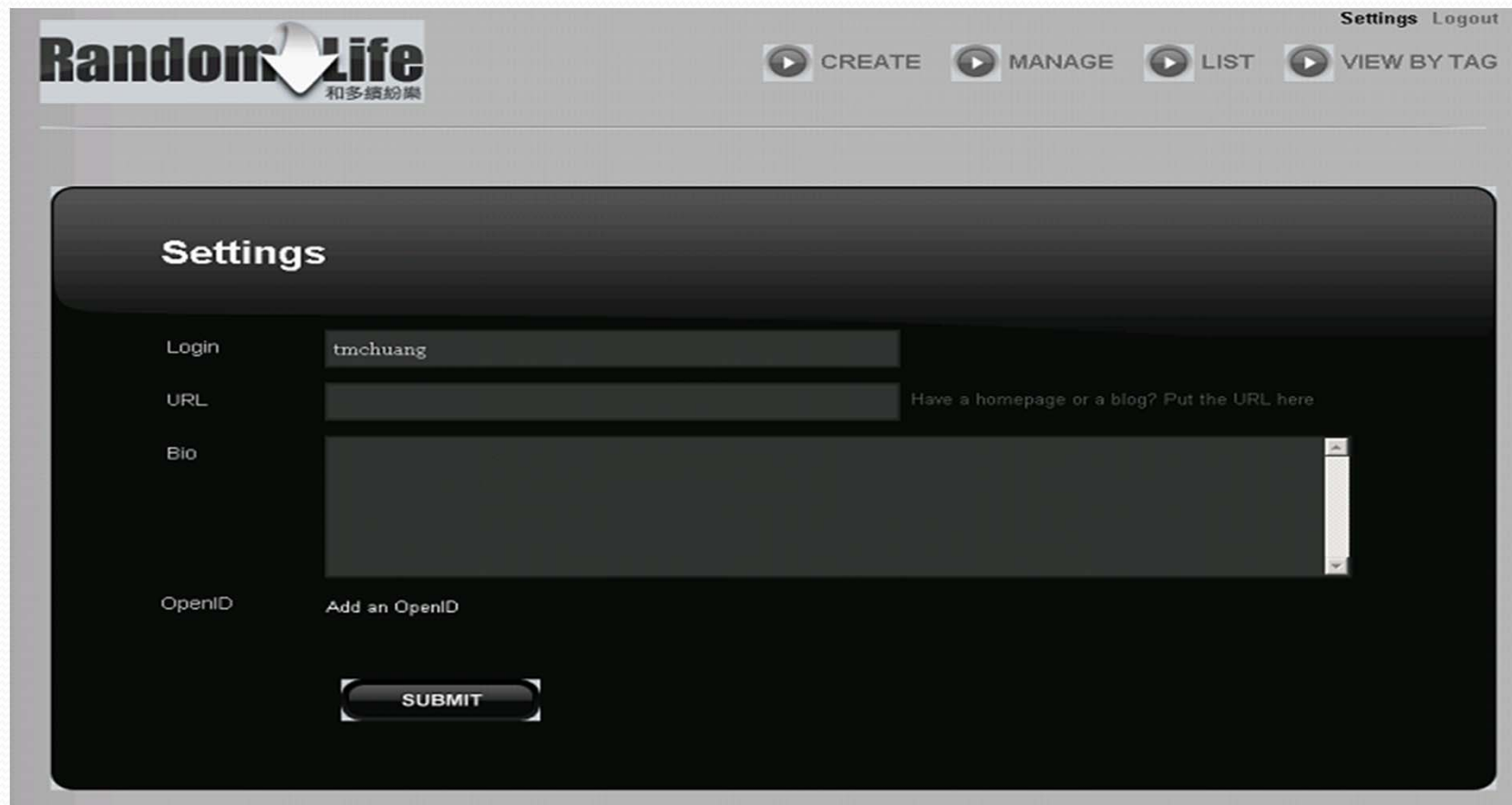
按「同意」按鈕表示你已閱讀並理解這些條款。

[同意]   [不同意]

Yahoo OpenID (con't)

- 用不同的方式登入，視為不同一個人

OpenID Providers

Other Well Known & Simple Providers

In addition, there are several dedicated OpenID providers that are generally recommended by various members of the community. While not a comprehensive list, each of these providers offers a free and secure OpenID to use across the web.

Chi.mp allows you to create your own social hub on an OpenID domain you own and control.

ClaimID is an easy way to manage your online identity with OpenID.

myID.net is an OpenID provider with support for groups and the Korean language.

myOpenID is the first standalone provider for both individuals and businesses, with secure multi-factor authentication.

VeriSign's Personal Identity Provider is an OpenID provider with support for multi-factor authentication.

Your Internet ID lets you build a social identity to use on the web.

OpenID Providers (con't)

中央研究院資訊科技創新研究中心
http://myid.tw

國網中心 Co-Life 團隊
http://oepnid2.colife.org.tw

http://openid.org.cn

http://87id.com/zh_CN

OpenID Providers (con't)

Surprise! You may already have an OpenID.

If you use any of the following services, you already have your own OpenID. Below are instructions on how to sign in with each of the following providers on an OpenID enabled website. (When you see bold text, you should replace it with your own username or screenname on that service.)

Google

Look for the "Sign in with a Google Account" button or use your Google Profile URL.

YAHOO!

Look for the "Sign in with Yahoo" button.

YAHOO! JAPAN

Look for the "Yahoo! JAPAN IDでログイン" button.

LIVEJOURNAL

Enter "**username**.livejournal.com"

Hyves

Click the "Sign in with Hyves" button.

Blogger

Enter your blog URL: "**blogname**.blogspot.com"

flickr

Look for the "Sign in with Yahoo" button or use your photostream URL

orange

Click the "Sign in with Orange" button or enter "orange.fr"

mixi

mixi is a web service that allows users to communicate with their friends and acquaintances.

myspace

Look for the "Login with MySpaceID" button or enter "www.myspace.com/**username**"

WORDPRESS.COM

Enter your WordPress.com URL, for example: "**username**.wordpress.com"

AOL

Look for a "Sign in with AOL" button or enter "openid.aol.com/**screenname**"

OpenID 代理認證機制

- MyOpenID URI
  - http://tmchuang.myopenid.com
- Google OpenID URI
  - https://www.google.com/accounts/o8/id?id=AItO awlWm3dFpddNJ0TWllz0h9J7-ImdMh_MPsI
- Yahoo Openid URI
  - https://me.yahoo.com/a/ZsXnzPUlmcDMIJ6oMN 422pIP6GXxOrDXQw--#bf1b4

用你的熟悉的 URL 來取代上述的 OpenID URI

OpenID 代理認證機制(con't)

在自己擁有的網站首頁(http://new.colife.org.tw) 的 HTML 內加入
第一行是OpenID 認證伺服器的位址，第二行即為委任 OpenID URI 地址

```
<html>
<head>
    <title>tmchuang openid.delegate test</title>
    <link rel="openid.server" href="http://openid2.colife.org.tw">
    <link rel="openid.delegate" href="http://openid2.colife.org.tw/user.aspx?tmchuang">
    <link rel="openid2.provider" href="http://openid2.colife.org.tw">
    <link rel="openid2.local_id" href=http://openid2.colife.org.tw/user.aspx?tmchuang">
    <meta http-equiv="X-XRDS-Location" Content="http://openid2.colife.org.tw/op_xrds.aspx" />
</head>
<body>

this is a testing...

</body>
</html>
```

OpenID 代理認證機制(con't)

OpenID 的個人資料交換

- 在 OpenID Simple Registration Extension 1.0 規格書中
有定義九個交換屬性：

全名（FullName）
暱稱（Nickname）
E-mail（Email）
生日（BirthDate）
性別（Gender）
國家（Country）
郵遞區號（PostalCode）
語言（Language）
時區（TimeZone）

OpenID 的個人資料交換(con't)

- **OpenID Attribute Exchange 1.0 – Final**

  5. Fetch Message

     5.1. Fetch Request Format
     5.2. Fetch Response Format

     - openid.ax.mode
     - **openid.ax.type.<alias>**
     - openid.ax.required
     - openid.ax.if_available
     - openid.ax.count.<alias>
     - openid.ax.update_url
     - ....

回顧 OpenID 的功能

- OpenID 的三個角色
  - OpenID Provider (OP)
  - Relying Party (RP)
  - User
- 單一簽入(SSO) (OP) 及登入認證(RP)
- 代理認證機制
- 個人資料交換機制

你要想要 OpenID 為你做什麼(OP)

- 整合帳號，Single Sign-On（單一簽入）
- 協助入口網、網教中心及加盟單位進行統一會員登入

會員 1000 人

會員 1000 人

會員 1000 人

總註冊人數 5000人

會員 1000 人

會員 1000 人
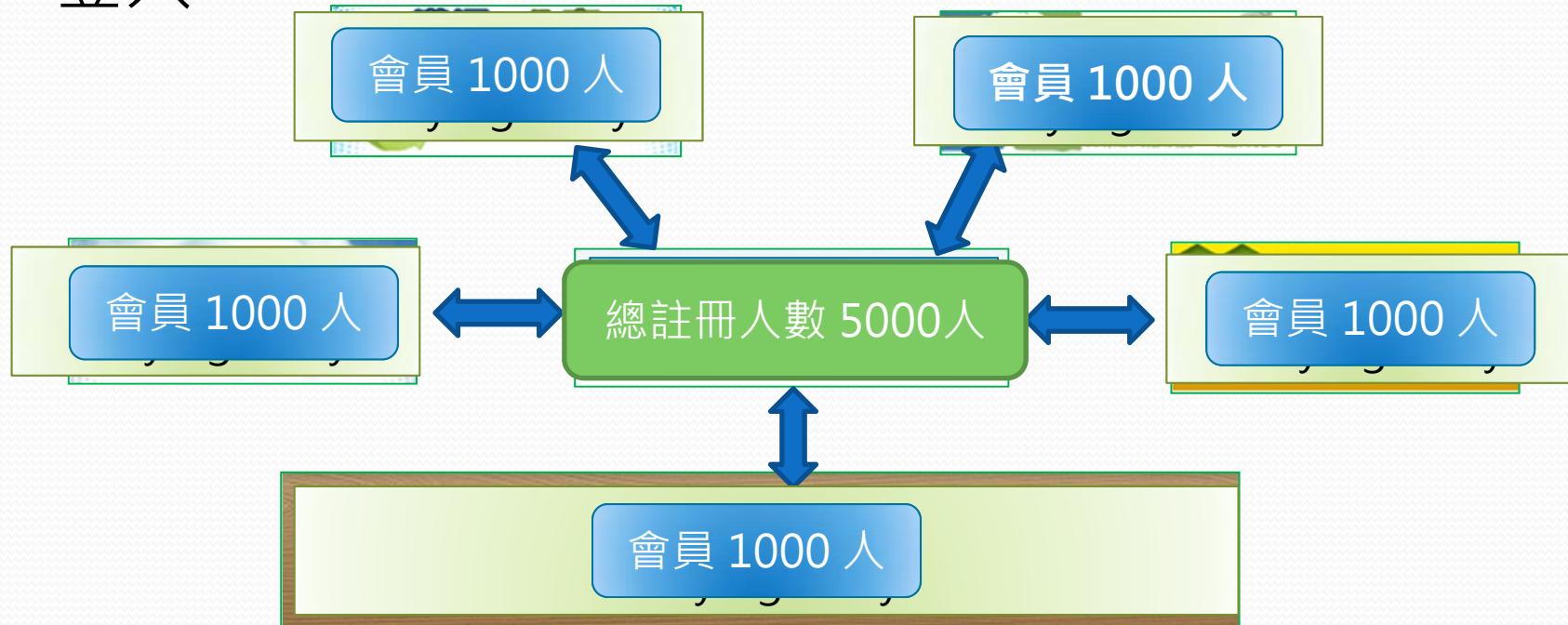
你要想要 OpenID 為你做什麼(RP)

- 提升網站登入人數及人次

```
          註冊人數 1000人
註冊人數 1000人          註冊人數 1000人

註冊人數 1000人                          註冊人數 1000人
              總會員 9000 人
註冊人數 1000人                          註冊人數 1000人

      註冊人數 1000人    註冊人數 1000人
```
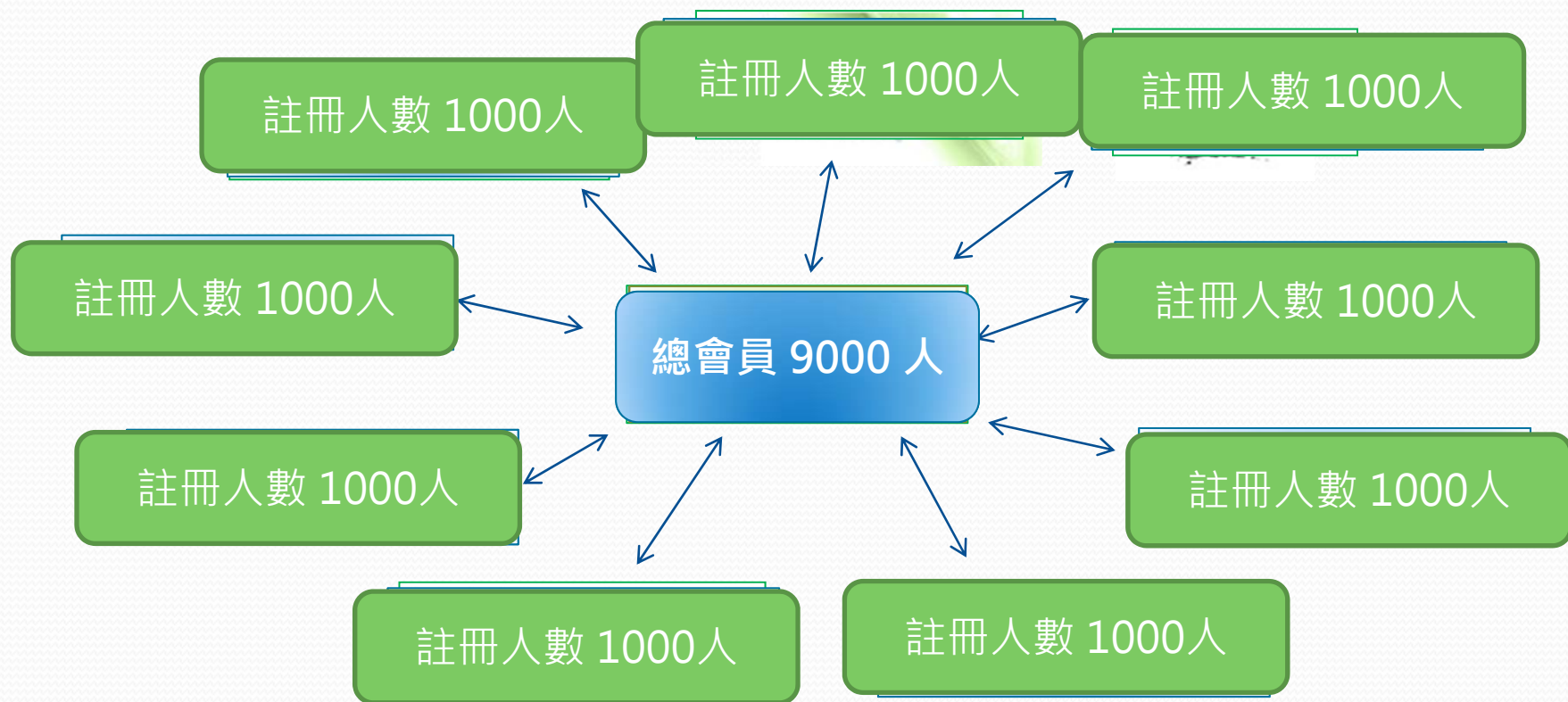
OpenID 技術探討

- 技術資料來源 http://openid.net/
- 目前規範 OpenID 2.0
- Support Language
  - http://openid.net/developers/libraries/
  - Asp.Net(C#)、PHP、Coldfusion、Java、Perl、Python、Ruby、Squeak/Smalltalk、Apache 2

導入規劃 --- OP or RP

- 規範 OpenID 1.0 或 2.0 ?
- To be an OpenID Provier or Relying Party ?
  - RP
    - 登入流程設計、相容原本的使用者系統、結合多個 OpenID 帳號
    - 需要什麼個人資料，OpenID Provider 是否有提供？
    - 帳號記錄的變更
  - OP
    - OP & RP
    - What is your OpenID URI format ?
      ex: http://tmchuang.myopenid.com
          http://openid2.colife.org.tw/user.aspx?tmchuang
    - 註冊欄位資料 (Simple Registration & Fetch Message)
    - 隱私權政策
- 使用何種開發語言

OpenID 登入流程

OpenID Server(OP)

Consumer (RP)

User

OpenID Provider

Relying Party

1. 進行登入程序

2. 選擇登入 OpenID

3. 檢查 OpenID URI 是否有效

4. 回應 XRDS 文件

5. 要求登入認證及個人資料回傳

6. 導向登入頁面

7. 填寫登入資料

8. 回傳使用者資料、登入狀況及驗證 RP 登入頁面的合法性

9. 登入成功,開放權限
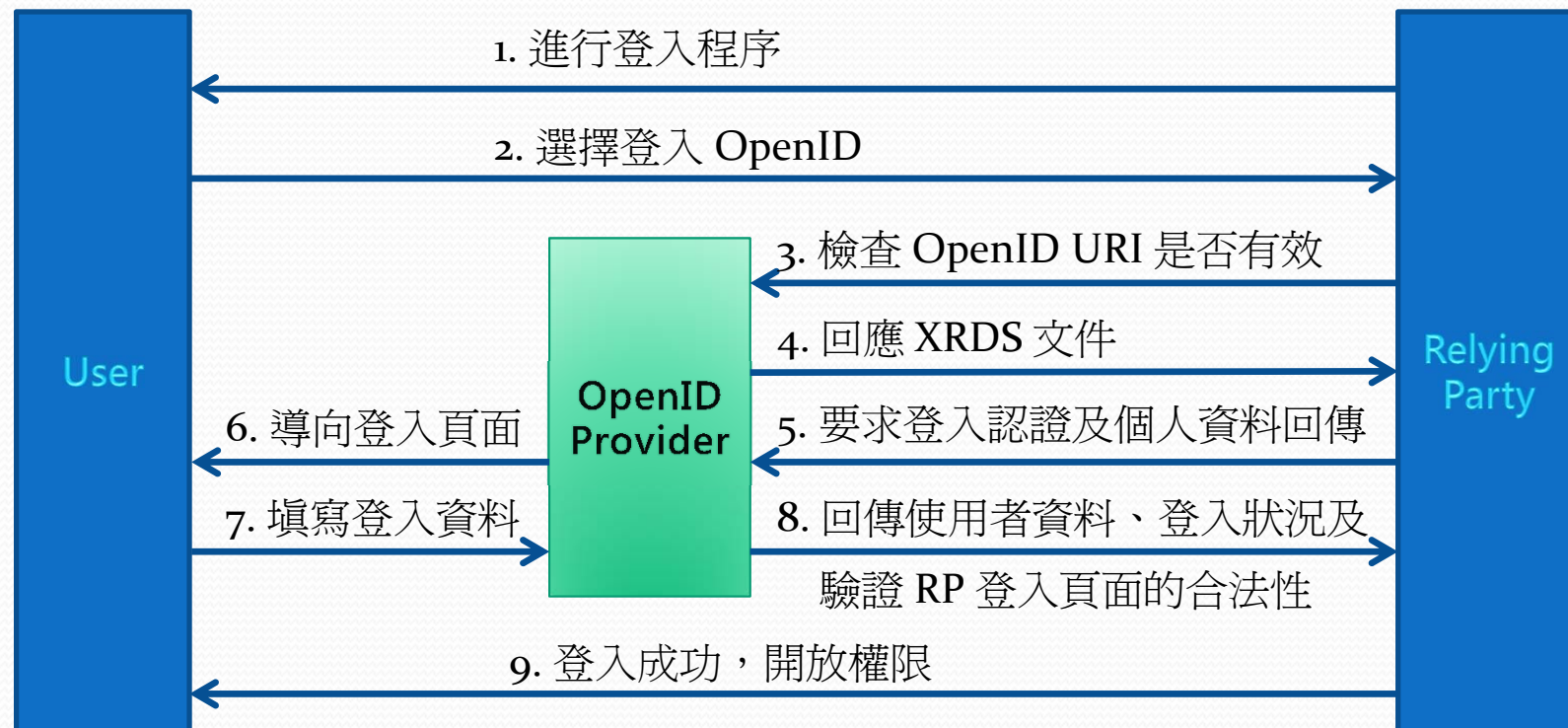
To be a RP --登入流程設計

- 重點：填帳號密碼的地方，是在 OpenID Provider 。

http://vcenter.iis.sinica.edu.tw
/lab/login/index.php

http://www.myopenid.com

To be a RP -- 登入流程設計

- 獨立頁面處理

變更直接輸入帳號/密碼

已進入 Co-Life OpenID 認證程序

To be a RP -- 登入流程設計

- 不建議使用的版型

已進入 OpenID
認證程式

To be a RP -- 登入流程設計

- 較好的做法一

To be a RP -- 登入流程設計

- 較好的做法二

To be a RP – 個人資料交換處理

- OpenID **Simple Registration** Extension 1.0

  全名（**FullName**）、暱稱（**Nickname**）、**E-mail**（**Email**）

  生日（**BirthDate**）、性別（**Gender**）、國家（**Country**）

  郵遞區號（**PostalCode**）、語言（**Language**）、時區（**TimeZone**）

  - Require（需要,可選擇）
  - Request（必需,一定要）

- OpenID **Attribute Exchange** 1.0 – Final

  5. Fetch Message

    5.1. Fetch Request Format
    5.2. Fetch Response Format

OpenID Attribute Exchange

http://www.axschema.org/types/

Attribute Types

If you would like to define a new attribute, you can follow the process outlined on the home page.

Simple Registration

If you are currently using the Simple Registration Extension with OpenID, you can use these properties to migrate to Attribute Exchange without having to store different user data.

Type URI	Label	SREG Property
http://axschema.org/namePerson/friendly	Alias/Username	openid.sreg.nickname
http://axschema.org/contact/email	Email	openid.sreg.email
http://axschema.org/namePerson	Full name	openid.sreg.fullname
http://axschema.org/birthDate	Birth date	openid.sreg.dob
http://axschema.org/person/gender	Gender	openid.sreg.gender
http://axschema.org/contact/postalCode/home	Postal code	openid.sreg.postcode
http://axschema.org/contact/country/home	Country	openid.sreg.country
http://axschema.org/pref/language	Language	openid.sreg.language
http://axschema.org/pref/timezone	Time zone	openid.sreg.timezone

http://www.axschema.org/types

Other Attribute Types

Attribute Exchange is capable of moving around many more types of data than Simple Registration. These are the types that are currently defined for use with Attribute Exchange.

Name

http://axschema.org/namePerson/friendly	Alias/Username
http://axschema.org/namePerson	Full name
http://axschema.org/namePerson/prefix	Name prefix
http://axschema.org/namePerson/first	First name
http://axschema.org/namePerson/last	Last name
http://axschema.org/namePerson/middle	Middle name
http://axschema.org/namePerson/suffix	Name suffix

Work

http://axschema.org/company/name	Company name
http://axschema.org/company/title	Job title

Date of Birth
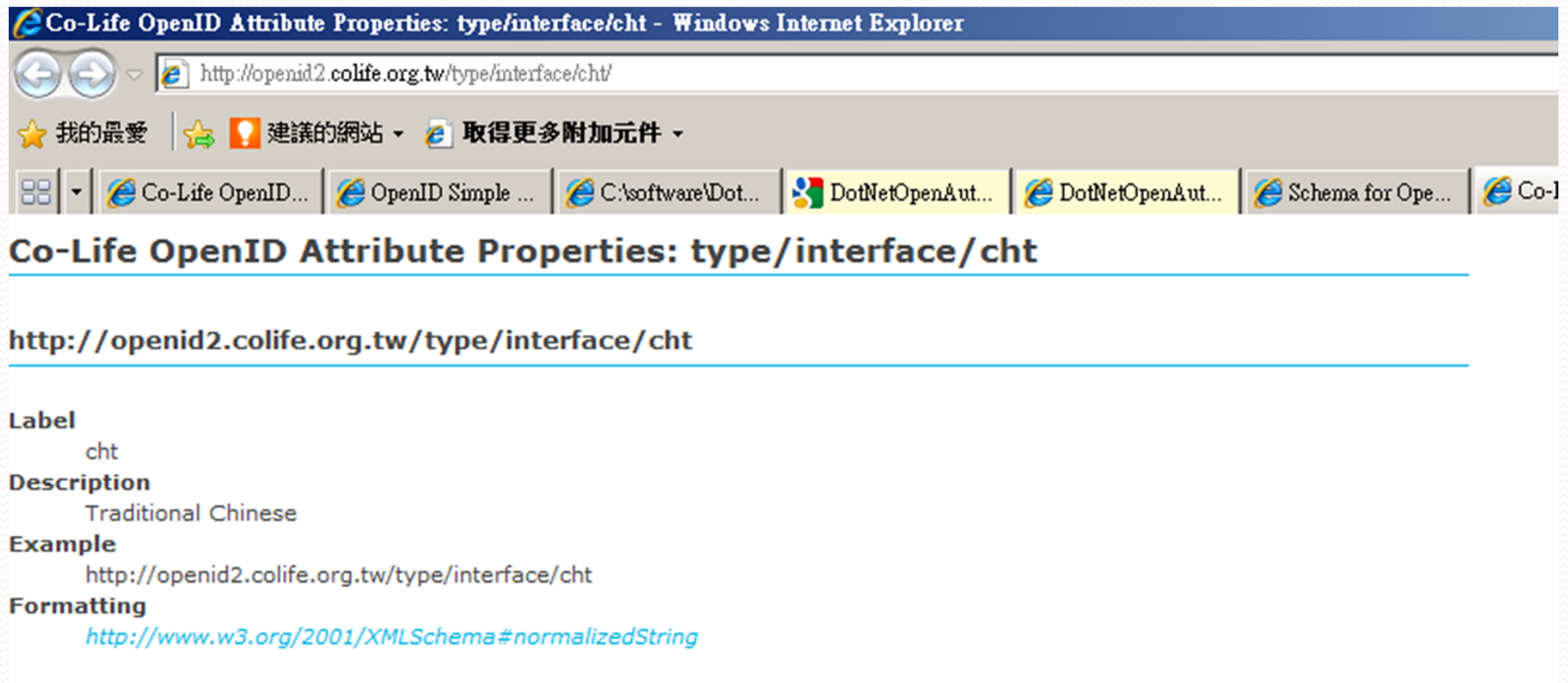
http://axschema.org/birthDate	Birth date
http://axschema.org/birthDate/birthYear	Birth year
http://axschema.org/birthDate/birthMonth	Birth month
http://axschema.org/birthDate/birthday	Birth day

Telephone

http://axschema.org/contact/phone/default	Phone (preferred)
http://axschema.org/contact/phone/home	Phone (home)
http://axschema.org/contact/phone/business	Phone (work)
http://axschema.org/contact/phone/cell	Phone (mobile)
http://axschema.org/contact/phone/fax	Phone (fax)

不存在的 Attribute

- http://openid2.colife.org.tw/type/interface/cht
- http://openid2.colife.org.tw/type/interface/eng

To be a RP – 記錄帳號的欄位變更

- MyOpenID URI
  - http://tmchuang.myopenid.com
- Google OpenID URI
  - https://www.google.com/accounts/o8/id?id=AItO awlWm3dFpddNJ0TWllz0h9J7-ImdMh_MPsI
- Yahoo Openid URI
  - https://me.yahoo.com/a/ZsXnzPUImcDMIJ6oMN 422pIP6GXxOrDXQw--#bf1b4

To be a RP – 結合多個 OpenID帳號

OpenID RP 驗證設定 by OP

登入頁 **http://rp.colife.org.tw/login.aspx**

http://rp.colife.org.tw 首頁內容
```
<html>
<head>
 <title>Openid Login</title>
 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
 <meta http-equiv="X-XRDS-Location" content="http://rp.colife.org.tw/xrds.aspx"/>
</head>
<body>
.....................
```
xrds.aspx
```
<?xml version="1.0" encoding="UTF-8"?>
<xrds:XRDS xmlns:xrds="xri://$xrds " xmlns:openid=http://openid.net/xmlns/1.0  xmlns="xri://$xrd*($v*2.0)">
<XRD>
 <Service>
   <Type>http://specs.openid.net/auth/2.0/return_to</Type>
  <URI priority="1">http://rp.colife.org.tw/loginprogrammatic.aspx</URI>
  <URI priority="2">http://rp.colife.org.tw/login.aspx</URI>
 </Service>
</XRD>
</xrds:XRDS>
```

To be an OP

- 需要一個 RP for 測試
- What is your OpenID URI format ?
  ex: http://tmchuang.myopenid.com → Need DNS
      http://openid2.colife.org.tw/user.aspx?tmchuang
- 決定所需的註冊欄位資料
  - **Simple Registration**
    - **FullName、Nickname、Email、BirthDate、Gender、Country、PostalCode、Language、TimeZone**
    - Require (需要,可選擇)、Request (必需,一定要)
  - **Fetch Message**
    - **5.1. Fetch Request Format**
    - **5.2. Fetch Response Format**
  - **User Define**

To be an OP – 隱私權政策

- 個資法的通過...
- 什麼資料可以給、什麼資料不能給

OpenID 開發語言

http://openid.net/developers/libraries/

Apache 2

mod_auth_openid
mod_auth_openid is an authentication module for the Apache 2 webserver.
License: **MIT**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

C#

DotNetOpenId / DotNetOpenAuth
Supports OAuth, OpenID+OAuth extension, InfoCard. Includes easy ASP.NET controls.
License: **Ms-PL**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

Coldfusion

OpenID CFC
Consumer library for OpenID auth framework.
License: Apache v2   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

CFOpenID
CFOpenID is the Coldfusion implementation of OpenID consumer specification. It is intended to
details specific to OpenID and providing you with simple API to integrate it into your site.
License: Apache v2   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

CFKit OpenID
A hopefully easy to implement openid consumer component for coldfusion.
License: Apache v2   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **1.1**

OpenID 開發語言 (con't)

Java

JOpenID
JOpenID is an OpenID 2.0 Java 5 implementation for Google Federated Login.
License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

dyuproject
java REST framework, openid 2.0 relying party, oauth consumer and service provider, JSON IOC
License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

JOID
JOID lets you create both OpenID 2.0 relying parties and identity providers.
License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

OpenID4Java
This library allows you to OpenID-enable your Java webapp.
License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**   Mailing list:
OpenID4Java

OpenID 開發語言 (con't)

Perl

OpenID4Perl
This library allows you to OpenID-enable your Java webapp.
License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**   Mailing list:
OpenID4Perl

Net::OpenID::Consumer
Net::OpenID::Consumer - library for consumers of OpenID identities
License: **Perl**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

Net::OpenID::Server
Net::OpenID::Server - library for building your own OpenID server
License: **Perl**   Relying Party: **No**   Identity Provider: **Yes**   Compatibility: **2.0**

NetMesh InfoGrid LID
License: **Sleepycat**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

OpenID 開發語言 (con't)

PHP

An PHP 5 library for easy openid authentication. Works only as a consumer.
License: MIT License   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

PHP OpenID Library
The PHP OpenID library lets you enable OpenID authentication on sites built using PHP. It features the OpenID consumer, Store implementations, and an OpenID server.
License: Apache v2   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

Simple OpenID PHP Class
Authenticate users with OpenID single sign-on
License: **Unknown**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

OpenID component for CakePHP
An OpenID component for CakeP
License: **MIT**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

sfOpenIDPlugin for Symfony
Module to handle authentication via OpenID
License: **Unknown**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

EasyOpenID
A PEAR-free library for OpenID relying party.
License: **BSD/GPL**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **2.0**

OpenID 開發語言 (con't)

Python

Python OpenID Library
A Python library for verifying and serving OpenID identities. Python OpenID makes it easy to add OpenID authentication to your web applications.

License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

Google App Engine Django OpenID Library
OpenID Consumer/Relying Party (RP) for *Google App Engine Django* projects implemented as a Django app.

License: **GPLv3**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**   Mailing list: **google-app-engine-django-openid**

Ruby

Ruby OpenID Library
A Ruby library for verifying and serving OpenID identities. Ruby OpenID makes it easy to add OpenID authentication to your web applications.

License: **Apache v2**   Relying Party: **Yes**   Identity Provider: **Yes**   Compatibility: **2.0**

Squeak/Smalltalk

OpenID for Squeak
This is an implementation of OpenID consumer based on OpenID Authentication 1.1. The consumer can discover XRD or OpenID descriptions and establish DH-SHA1 association with the provider.

License: **Unknown**   Relying Party: **Yes**   Identity Provider: **No**   Compatibility: **1.1**

參考資料

- 10分鐘學會 OpenID OpenID 服務串接一路通 http://myid.tw
- OpenID.Net http://openid.net/
- OpenID WikiPedia http://en.wikipedia.org/wiki/OpenID
- OpenID Developer http://openid.net/developers/
- OpenID Libraries http://openid.net/developers/libraries/
- Google OpenID
  http://code.google.com/intl/zh-TW/apis/accounts/docs/OpenID.html
- Yahoo OpenID http://openid.yahoo.com/
- MyOpenID http://www.myopenid.com
- Twitter Feed http://twitterfeed.com/
- DotNetOpenAuth http://www.dotnetopenauth.net/

謝謝指教