Authentication, Identity and Social Web

蕭景燈
中央研究院資訊科技創新研究中心

chsiao@citi.sinica.edu.tw
chsiao.myid.tw
@chsiao

有些一樣又有些不一樣

- Single sign-on
- Third party authentication
- Federated login/Federated identity
- User-centric identity

SSO不是新玩意

1994	**Yahoo!** Initiates Single Sign-On **Yahoo!ID**
1998	**MSN** Announces **MSN Passport** after acquiring HotMail
2004	**Google** Starts its own Single Sign-On: Gmail and Google Accounts
2005	**OpenID** Initiates single sign-on for independent sites
2005	**MSN** Launches Live.com and MSN Passport is renamed to **Windows Live ID**

2008/1	**Yahoo!** Supports OpenID 2.0
2008/2	Microsoft, Yahoo, IBM, VeriSign, and Google joined OpenID Foundation board
2008/7	**Facebook Connect** is announced on Facebook's developer conference F8
2009/4	**Facebook** announcs that they will become **OpenID RP**
2010/8	All third-party applications are required to use **OAuth** to connect to **Twitter**
2010/9	**Google services** accept **Yahoo!ID** via **OpenID** standard
2012/8	**Microsoft Account** is the new name for what was **Windows Live ID**

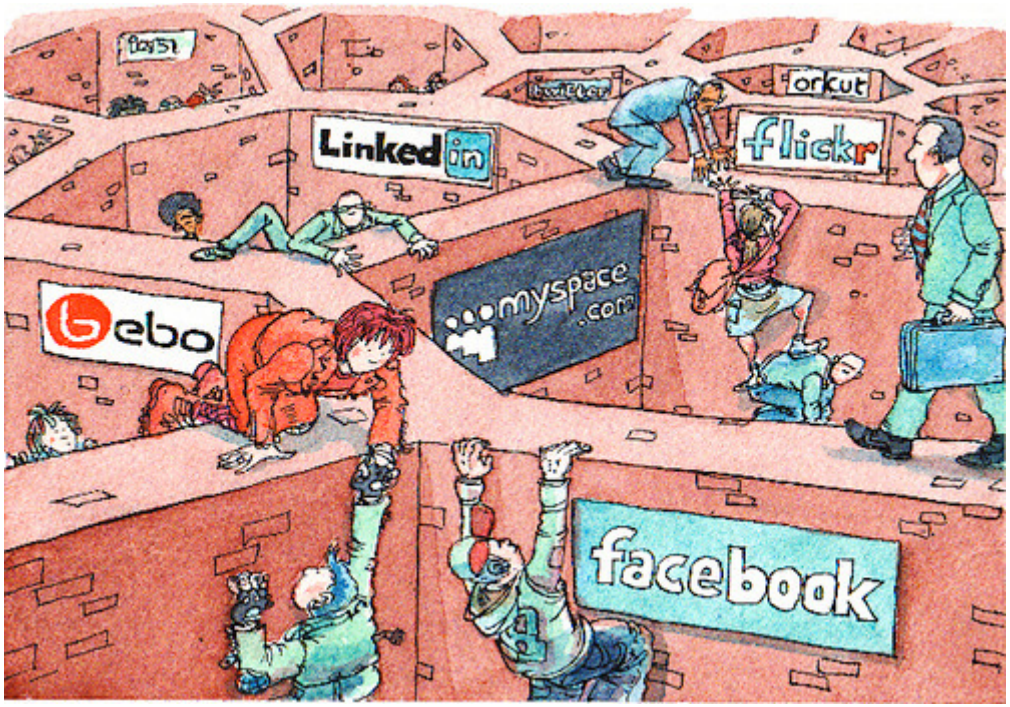
SSO目的不一樣，選擇不一樣

偏向安全與內部管控	偏向溝通與平台開放
LDAP, Active Directory, SAML	OpenID, Yadis, SAML
Network-oriented/IP-based	Web-oriented/HTTP-based
不對第三方認證開放	對第三方認證開放
集中認證伺服器	分散認證伺服器
使用者名錄功能方便瀏覽查詢	不強調使用者名錄之功能
很安全	安全
固定的Trust Boundary	彈性的Trunt Boundary
擴充性達百萬使用者	擴充性達千萬使用者

網路服務認證 **Authentication** 的目的

- 確認使用者身分，以確保線上交易過程有效
- 確認使用者身分，分別使用者權限，提供可用的資訊與資源
- 確認使用者身分，以提供客製化服務
- 確認使用者身分，以利社群活動的參與

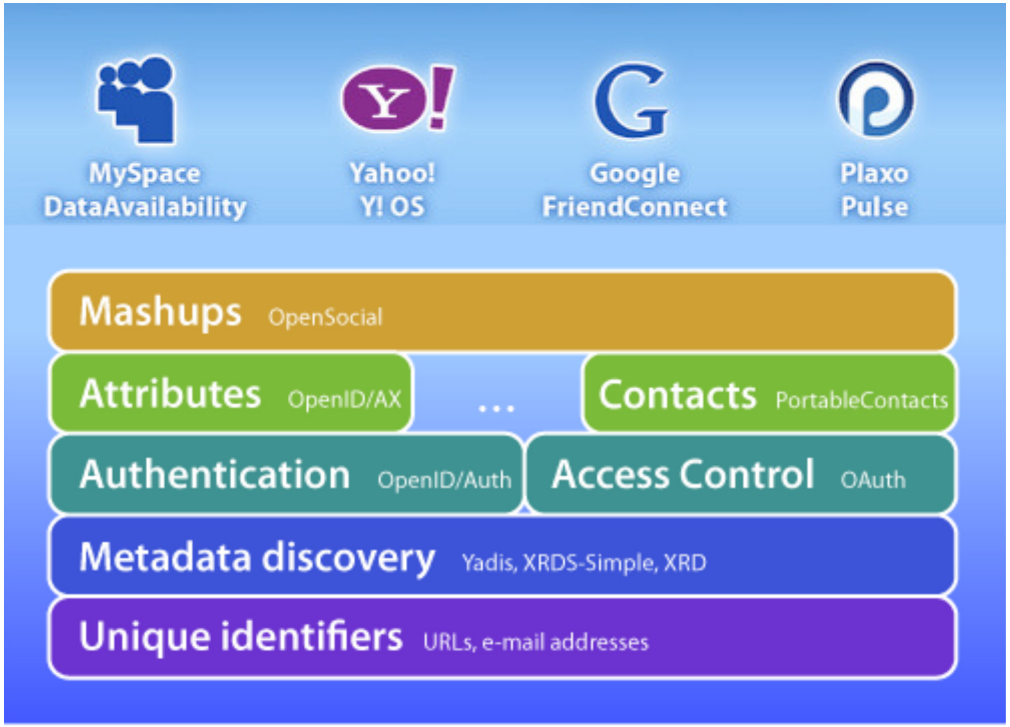
不相往來的 **Walled Gardens** 社群網路



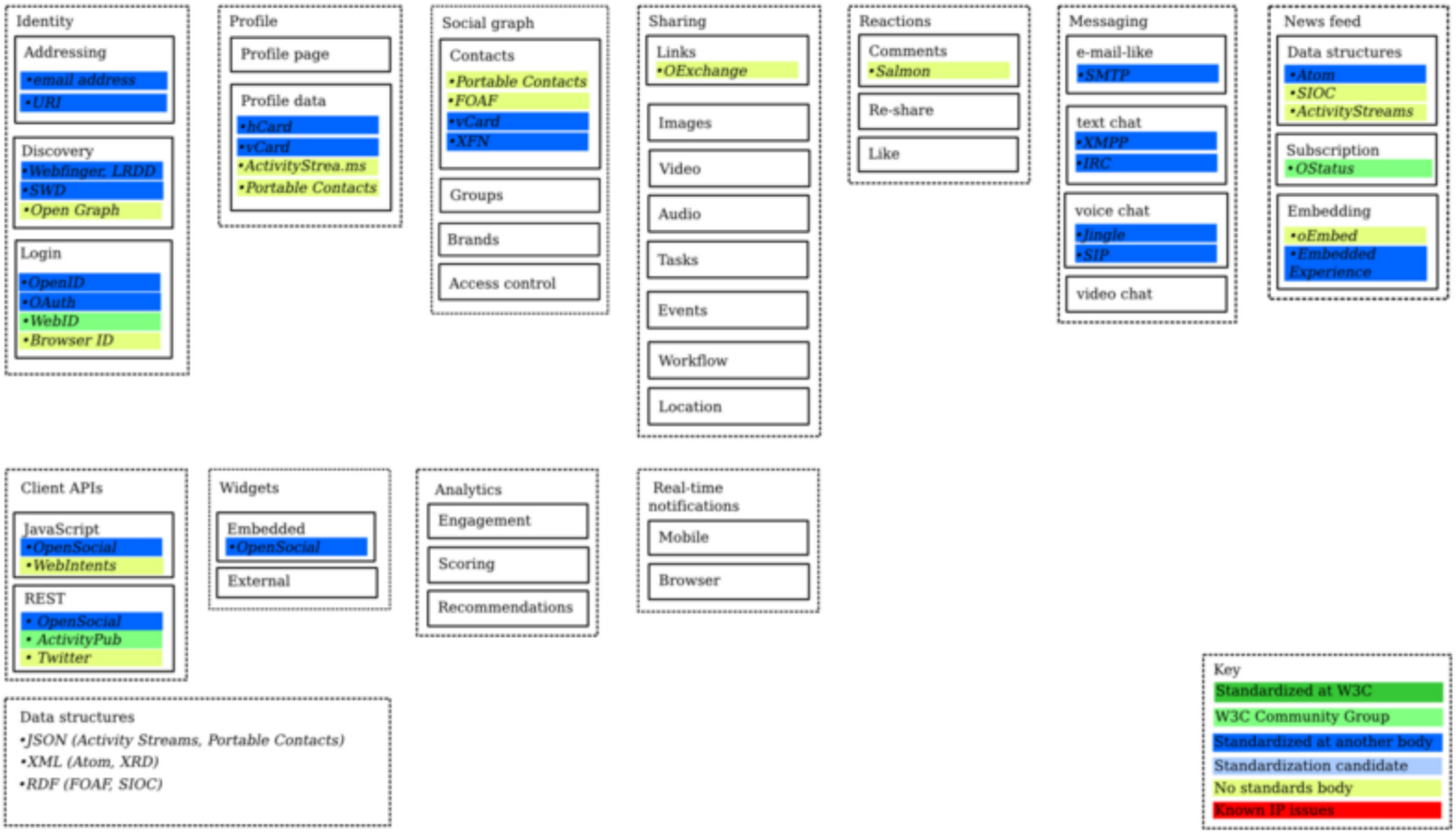
原圖出處 經濟學人 The Economics May 19, 2008

跨網站認證的公開標準

業界提出的 Open Stack



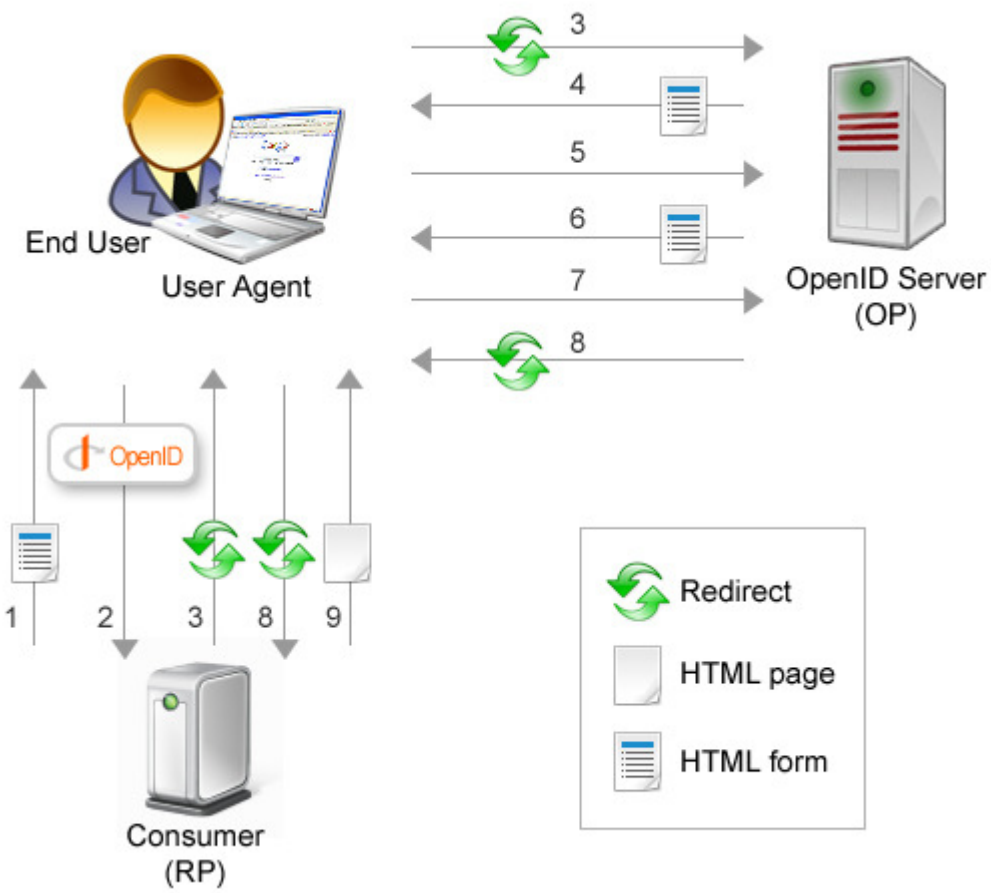
W3C 整合與擴充


Identity
Addressing
•email address
•URI
Discovery
•Webfinger, LRDD
•SWD
•Open Graph
Login
•OpenID
•OAuth
•WebID
•Browser ID
Profile
Profile page
Profile data
•hCard
•vCard
•ActivityStrea.ms
•Portable Contacts
Social graph
Contacts
•Portable Contacts
•FOAF
•vCard
•XFN
Groups
Brands
Access control
Sharing
Links
•OExchange
Images
Video
Audio
Tasks
Events
Workflow
Location
Reactions
Comments
•Salmon
Re-share
Like
Messaging
e-mail-like
•SMTP
text chat
•XMPP
•IRC
voice chat
•Jingle
•SIP
video chat
News feed
Data structures
•Atom
•SIOC
•ActivityStreams
Subscription
•OStatus
Embedding
•oEmbed
•Embedded Experience
Client APIs
JavaScript
•OpenSocial
•WebIntents
REST
• OpenSocial
• ActivityPub
• Twitter
Widgets
Embedded
•OpenSocial
External
Analytics
Engagement
Scoring
Recommendations
Real-time notifications
Mobile
Browser
Data structures
•JSON (Activity Streams, Portable Contacts)
•XML (Atom, XRD)
•RDF (FOAF, SIOC)
Key
Standardized at W3C
W3C Community Group
Standardized at another body
Standardization candidate
No standards body
Known IP issues

第三方認證與身分2.0

- 將實體社會的認證方式複製到網路世界
- 符合Web 2.0的使用情境
- 使用者完全掌握自己的身分
- 認證與授權分離
- 使用者以單一帳號登入，解決帳號密碼的管理

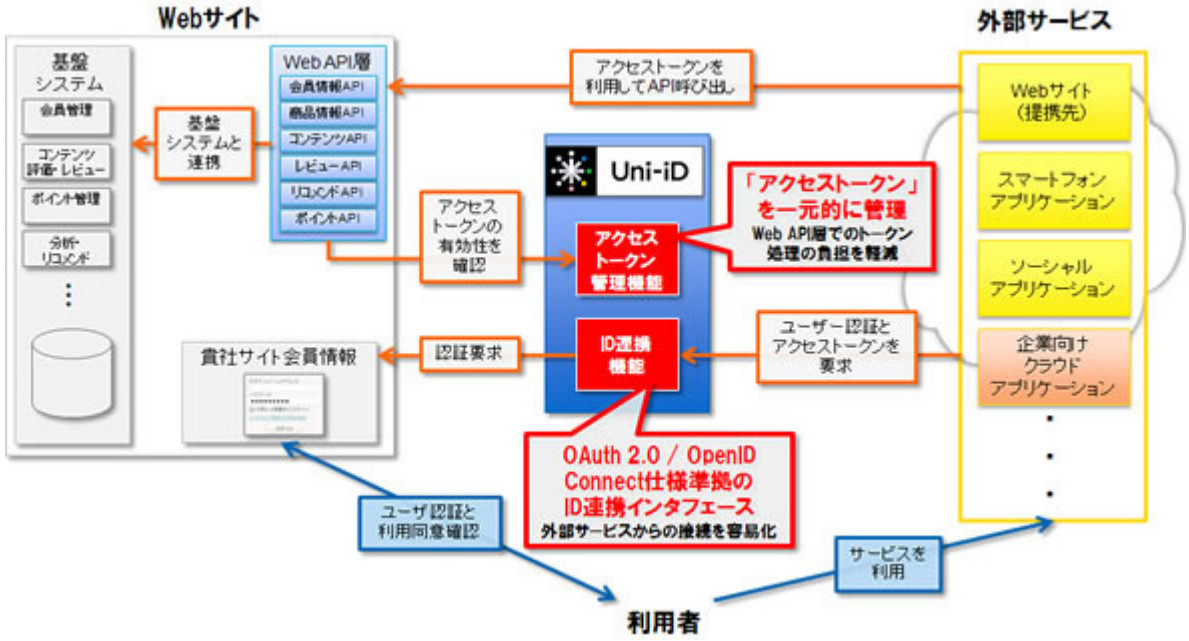
以OpenID實作第三方認證



OAuth

- OAuth官方的稱呼在2012/5從OAuth 2.0 **Authorization** Protocol改爲OAuth 2.0 **Authorization** Framework
- OAuth是授權協定，但間接可以用爲認證目的(使用者未經過認證就無法取得授權)
- OAuth可以與認證機制OpenID, SAML, LDAP等整合(integration)
- OAuth 2.0內建(built-in)於下一版的OpenID標準OpenID Connect之中

Oauth 2.0/OpenID Connect實作



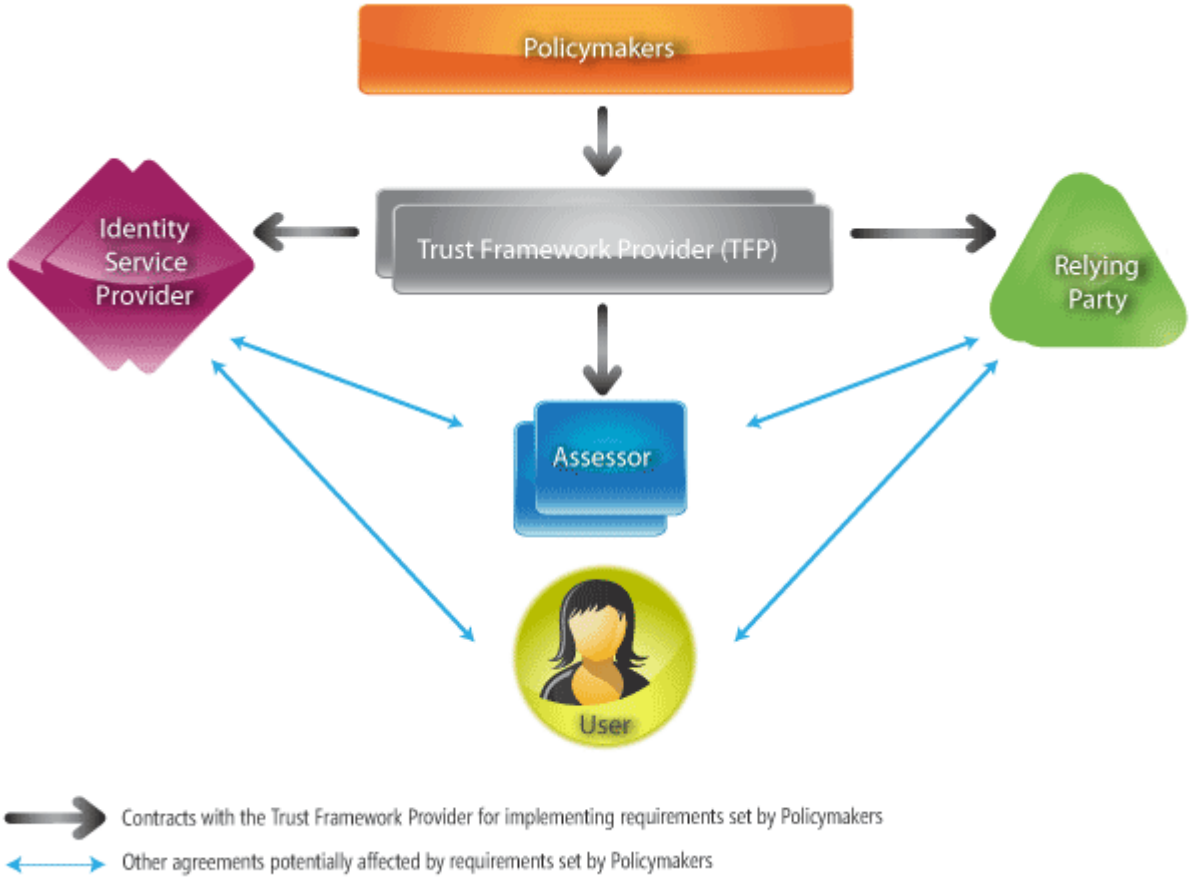
日本野村総合研究所的 Uni-ID

進一部要討論的問題

- 安全問題
- 隱私問題
- 網站間信任問題

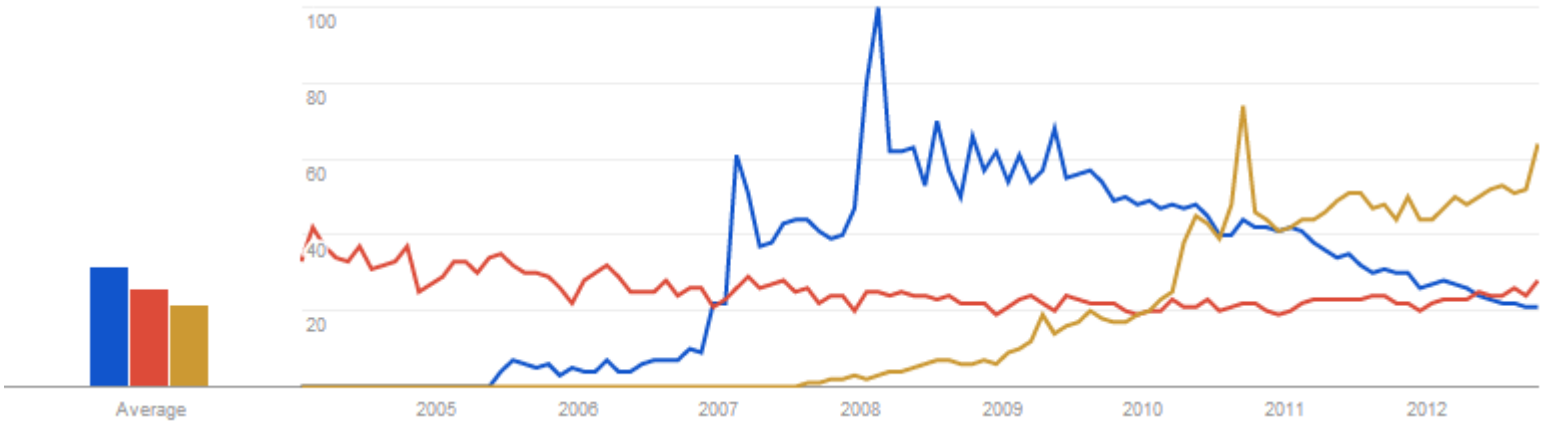
OIX Trust Framework

- OIX解決信任問題
  - 信任不是技術問題
  - 信任是商業、法律、社會問題
  - 仰賴實體社會的法律協議

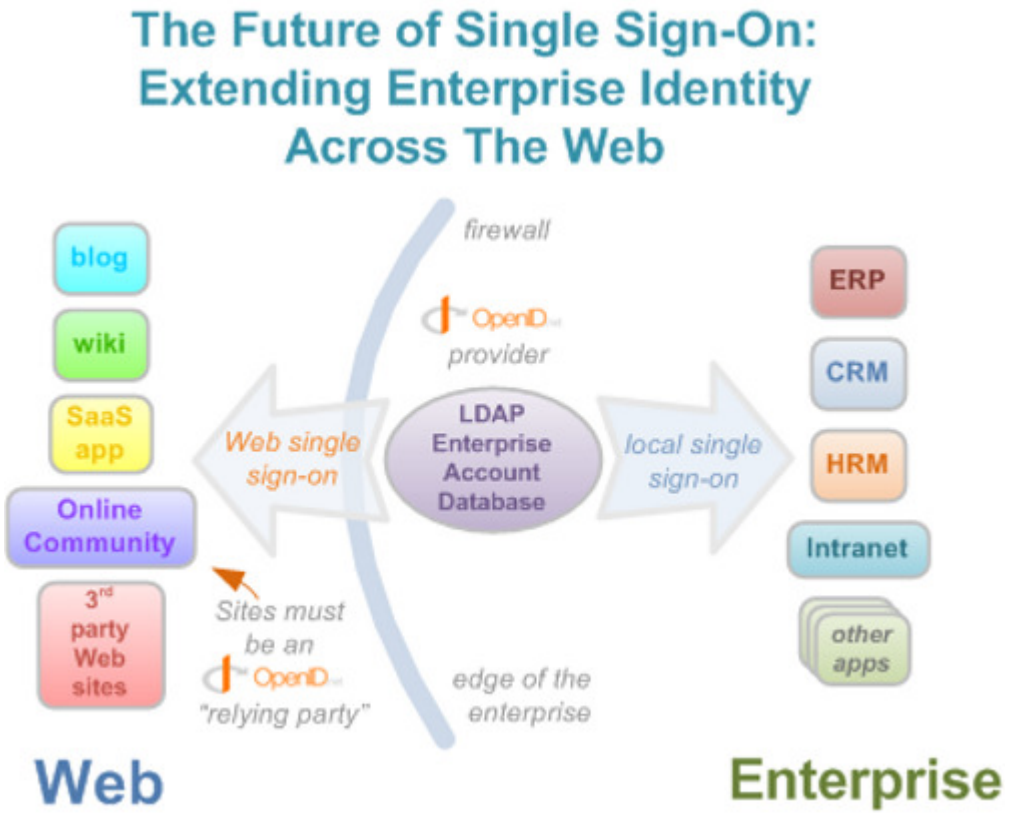


趨勢參考

- Internet Identity Workshop and Identity Commons
- Cloud Identity Workshop
- W3C Social Web TaskForce and WebID Community Group
- National Strategy for Trusted Identity in Cyberspace(NSTIC) and Open Identity Exchange(OIX)



內部LDAP帳號轉成OpenID示意圖



更遠大的想法

From http://blogs.zdnet.com/Hinchcliffe