

# OpenID and SAML

Fiona Culloch, EDINA

EuroCAMP, Stockholm, 7 May 2008

## What is OpenID for?

- In principle, an OpenID is a universal username, valid across multiple, unrelated services
- E.g., I have `fculloch.protectnetwork.org`  
That is an identifier for me
- Original idea: avoid creating new accounts for every blog, wiki, etc. Use same OpenID for all
- Driver: blogs, wikis etc. starting to require authN because of comment spam

## How it works (1)

- Login page provides “OpenID” edit box in addition to traditional username/password
- Standardised logo identifies this box to the user
- User types OpenID, eg, `fculloch.protectnetwork.org`
- Converted to `http://fculloch.protectnetwork.org`
- User redirected to authentication page at `protectnetwork.org`, enters password there
- `Protectnetwork.org` confirms to original web site that user entered correct password. User now logged in.

- *Relying Party (RP)*, uses OpenID to authenticate users
  - Analogous to SAML *Service Provider (SP)*
- *OpenID Provider (OP)*, is a server identified by an OpenID.
  - OP invoked by RP to find out if the user sitting at the browser knows the password for claimed OpenID
  - Analogous to SAML *Identity Provider (IdP)*

## What is OpenID?

- Conventions for form field name, logo
- “An” OpenID is the “username” I type, e.g.,  
fculloch.protectnetwork.org
- The protocols used between the RP and the OP  
(all layered on top of HTTP, versions: 1, 2)
- Transport for user attributes from OP to RP
- A movement (or bandwagon)
- A political programme

## What is OpenID *not*?

- No association of OpenID with real-world person (bgates.myopenid.org could be anyone)
  - So more like a traditional username (bgates) than...
  - ...an X.509 personal certificate, where a trusted 3<sup>rd</sup> party (the CA) vouches for a real-world name, org.
- No association of user with any organisation
  - c.f. eduPersonScopedAffiliation in SAML feds
- Not authoritative source of organisational

## Political goals

- “User-centric” identity
  - OpenID used should be the *user’s* choice, not the RP’s (or the OP’s)
- An OpenID should remain usable if the OP goes out of business, changes its name, DNS reassigned etc.
- Ultimately, it must be possible to operate your own OP rather than relying on an infrastructure provider (e.g., a commercial or campus OP)
  - Lightweight open-source implementations

## How realistic are those goals?

- Those “user-centric” properties are what mainly distinguish the way OpenID is used, but...
- If anyone can create their own OpenIDs, the original problem (comment spam) isn't solved
- My [fculloch.protectnetwork.org](http://fculloch.protectnetwork.org) “Open”ID is tied to a particular provider. I could set up [fculloch.org](http://fculloch.org) instead (indirection is allowed) but
  - It's harder to set up (vs. AOL, Yahoo! free OpenIDs)

## \$64,000 question

- Will important RPs want to deal with (trust) arbitrary OPs?
  - To date, many more orgs want to be OPs than RPs
  - SourceForge may change this, too soon to tell, note:
    - They require additional registration details
    - You must still create a trad. username/password, for use with non-web services
  - Some potential campus RPs say they *won't* trust arbitrary OPs, want to restrict user to campus OP,

## Restricting OP choice breaks model

- RPs restricting user choice of OP breaks “user-centricity”
- RP blacklisting or whitelisting of OPs or individual OpenIDs starts to look a bit like a federation
- Without free choice, OpenID is just an alternative authN/attribute transfer protocol to SAML (protocol war, yawn!) and a much criticised one at that:
  - Phishing weaknesses

## How OpenID differs from federations

Trusted 3 <sup>rd</sup> party (federation) enrolls/verifies members from specific community	Any OP in the world to any RP
SP can authZ on user's org. affiliation (ePSA) verified by fed	No way to verify any claimed org. affiliation attribute
(Usually) rules of membership, attribute standards.	anarchic
Org. verification enables privacy-preserving temp ids	Inherently discloses persistent, cross-service id

## But what if...?

- Groups of RPs, OPs get together to:
  - agree minimum practices
  - Whitelist only OPs that meet them (prob. big names)
  - Standardise the attributes used
- That looks more like a federation. I.e., difference is more social than technical (protocol)
- If my current OP is not on whitelist, I must move. Can keep same OpenID only if I have set up indirection (unusual, non-trivial). Will users

## What are we (and others) doing?

- EDINA & University of Kent awarded 7-month study into OpenID, to cover:
  - What OpenID is and is not (also CardSpace)
  - What institutions are doing / plan to do (survey, limited UK-only results to date, European input good)
  - How OpenID relates to SAML feds (specifically UK)
  - Whether OpenID may be relevant to services using licensed data

## Integrate OpenID with a SAML fed

- A UK federation IdP using OpenID (any OP) to authenticate its users:
  - eduPersonPrincipalName attribute conveys OpenID, e.g.,  
fculloch.protectnetwork.org@openidbridge.ac.uk
  - authN only; no user attributes at present
  - Can SP trust bridge IdP? History of trusted national services in UK.
- Example SP using licensed data, e.g., EDINA LLL
  - An ACL of allowed ePPNs (so not just OpenIDs)

## Why integrate OpenID & SAML?

- To allow experimentation with OpenID authN against already deployed SAML SPs
  - To discover appropriate uses for OpenID (e.g., trial user accounts)
- To avoid diversion of effort into adding OpenID RP support to existing SAML SPs where not required
- Non-proprietary alternative to existing open-access IdPs (e.g., ProtectNetwork, TypeKey) for

## Initial survey feedback

- Relatively little OpenID familiarity in campuses
- Few concrete plans for early deployment
- More interest in “campus OP” that would allow users *outgoing* access to blogs etc. + some level of trust at campus RPs (which would only allow campus OP)
  - N.B.: *not* user-centric!
- Less interest in correlating arbitrary OpenIDs to real users (e.g. at matriculation or via account linking)
  - “I can see what’s in it for students, but not for institution”

## What are others doing?

- Significant interest in adding campus OpenID support as plug-in for Shibboleth 2.0 IdP, similarly to other id platforms (ProtectNetwork, OpenAthens,...)
  - Again, note not user-centric
  - Use case is internal access to already OpenID-enabled RP software packages
- Shibboleth, OpenAthens etc. viewed as protocol-neutral platforms, leaving SAML vs OpenID as protocol war
  - OpenID can be configured w/whitelists (like a federation); SAML can be configured to be promiscuous (like OpenID)
  - Question is how each community will evolve

## OpenID Momentum

- Momentum was large part of OpenID appeal
- Perhaps some easing of late as “user-centric” meets RP requirements
- Many large, credible commercial OPs:
  - VeriSign, Yahoo!, AOL, Blogger, ...
- Fewer large RPs (SourceForge may change game)

## More survey feedback

- Views on whether OpenID is more or less secure than traditional passwords are not consistent
- Generally even less familiarity with CardSpace, even at mainly Microsoft shops
- You can help! Contact us for survey form.

- [s.shaw@ed.ac.uk](mailto:s.shaw@ed.ac.uk)
- [fiona.culloch@btinternet.com](mailto:fiona.culloch@btinternet.com)