



Internet Identity Initiatives

RL "Bob" Morgan
University of Washington and Internet2
EMC2
Málaga, Spain
October 2006

- Internet identity buzzwords /projects :
user-centric, sxip, dix, openid, lid, yadis , xri/xdi, i-names ,
infocard, cardspace, identity metasytem, saml, ws-
federation, ws-trust, liberty, id-wsf, shibboleth, adfs ,
osis, heraldry, bandit, higgins , isso, saml-lite, identity
schemas, idcommons
- Internet identity and institutional identity



vast convergence of identity interests

the “read/write web” implies authentication everywhere

ordinary people as resource owners: blogs, wikis,
photos/music, RSS, social networks, blogspam, IM

so ordinary people face many many logins as users, and
have to do user management on their blogs

“identity gang” discussion since early 2005

“identity” is not just authentication

not even “attributes”, but everything “associated with me”
across myriad services, media, modalities, ...

INTERNET[®] Whose identity?

personal privacy, personal control: institutions of all kinds are the bad guys (including us!), since institutions claim ownership of users' "identities"

doing something about phishing ...
hence reducing password exposure

many technical/social solutions being promoted as "user-centric", meaning what exactly?

INTERNET² What is ‘user-centric’?

many not necessarily related characteristics

- identity rendered visible/manipulable to user

- IdP / SP as easy to install as blog package (or comes with)

- can use your ‘personal’ URL as identifier

- decentralized, i.e. no institutional power player

- all data passes through browser

 - no backdoor data exchanges between servers

 - user sees /approves exchanges

- identity data asserted by user, controlled by user

 - on client machine, or via online ‘identity agent’

see <http://openid.net/>

one example of “user-centric” system

developed in fight against blogspam

so blog commentors can be authenticated

user identifier is your URL (you have one, right?)

provide link to authn site via your URL

mechanism/assurance similar to email signup loop

can be installed without root/webserver access

operations crypto-protected, trust management is up to the participating parties (aka “reputation”)

anti-SAML? anti-XML ...

INTERNET² OpenID status

version 1.x

spreading through blogosphere, VeriSign labs promoting

version 2.0

almost finalized

includes XRI resolution, YADIS

moving into attribute exchange ...

“bounties” for app integration ...

has subsumed other SSO approaches ?

LID, SXiP, Passel, etc

Microsoft-promoted, much industry uptake
formerly InfoCard, aka “identity metasystem”
MS “identity selector” is CardSpace, in Vista
other selectors for other platforms, eg Higgins project
identities visible to users as “cards”
user-generated or third-party provided
typical signon, credit card purchase cases
protocol interactions are all WS-Trust
to IdP and to SP
solves “where are you from” problem ...

Cardspace in Vista betas

MS promises support for XP, also available?

will need AD IdP, IIS support, MS not saying much yet

Other platforms

Higgins project focus of Java implementors
though others are out there

MacOS X implementation demonstrated
though no official comment from Apple

Mozilla/Firefox? plugins happening

Linux? RedHat participating ...

OS IS

collaboration among open-source identity-system implementors, principally re CardSpace-compatibility
Microsoft “open specification promise”

Higgins

general framework for identity management
both client and server
big support from IBM, Novell, other vendors

Apache Heraldry

OpenID support, maybe CardSpace?

brand-new universal namespace

resolvable, privacy-supporting, individual-centric,
comprehensive, multi-registrar, etc

specified via OASIS

“link contracts” for DRM-style annotation on attributes

service infrastructure being deployed

Neustar acting as global root, many other registrars
you can buy an “i-name” now

three initial services: contact, web forwarding,
ISSO (i-name-enabled SSO, referenced in OpenID)

WS -*

WS -Trust being standardized in OASIS
only use case turns out to be CardSpace ...

WS -Federation still not submitted ...

SAML

responding to “user-centric” challenge

new profile with no XML signature (for PHP ...)

some lighter-weight implementations happening
eg zxid.org

<http://identityschemas.org/>

every identity system redefines ...

name, address, email, phone, homepage, ...

Higgins

common info-mgt requires schema mapping

developing OWL framework for representation

ad-hoc group assembled to help ...

schema repository, tools

not LDAP, but LDAP-clueful are participating

organizing via idcommons process

Microsoft

“live ID” is new Passport

“will be federated”, via WS -Fed

Yahoo, Google

both setting up to be IdPs to the world, using proprietary methods

will they federate? unclear

AOL

longtime Liberty/AML participant ...

INTERNET[®] Whither institutional identities?

the compliance driver

for high-value/formal relationships we need high-security, high-trust, high-value, high-cost, institutionally-controlled and -licensed, audited IdM

the community driver

to be a valuable and popular player in Internet identity communities we need easily obtained, portable, low-barrier, adaptable, multi-protocol IdM

can we do both?

institutional IdM will need to support many faces, interactions, partners, can't be protocol-evangelical

what can institutional ID be used for?

- users might already be hooking in to OpenID using institutional authentication, URLs

- random sites of interest to users might be SAML SPs?

institutional ID linkage?

- all people coming to our institutions for any purpose already (will) have online identities

- can we make use of them?

 - reputation? e-portfolio?

<http://openid.net/>

<http://cardspace.netfx3.com/>

<http://osis.netmesh.org/>

<http://identityschemas.org/>

<http://wiki.idcommons.net/>

<http://www.identitygang.org/>