OpenID Delegation as a Service

Hands-on experiences with hosted
OpenID delegation & the identifier lifecycle

Background

Boris Erdmann:

https://my.xlogon.net/ OpenID Provider

recently: http://jimdo.com/ Web Page Creator

Issue „Web Hoster“

Not neccessarily an OpenID Provider (Protocol)

Definitely a place to host aspects of Identity
(HTML header, XRDS, XFN, FoaF, RSS)

OpenID Delegation as a Service?

Standards too wide-ranging

No common practices

Update liability

Care for working Discovery

Several variants:

HTML header: no service discovery
(Sreg, AX, PAPE - and broken, see „identifier lifecycle“)

XRDS: proxy, cache, X-XRDS-Location

Service: discover and republish?

Support „broken“ Yadis libs (e.g. Plaxo/libopkele)

?

>>>

Identifier Lifecycle

http://boris.jimdo.com/

upgrade

http://boris.de/

One Identifier or Two?

ONE: redirect *boris.de* to *boris.jimdo.com* => :-(

(other sites still know me as *boris.jimdo.com*)

TWO: announce *boris.de* to all other sites?

(please see rp3.sxip.com)

Overloading and Bad Signalling

Content spam:
redirect *boris.jimdo.com* => *boris.de*

HTML discovery: broken beyond repair
(I lose boris.jimdo.com as identifier)

HTTP GET: same goes for X-XRDS-Location

Overloading and Good Signalling

Content spam:
redirect *boris.jimdo.com* => *boris.de*

Yadis discovery:
if request.headers.accept.preference is XRDS

HTTP HEAD request: send X-XRDS-Location

My Plea:

Hey, relying parties: „fix“ your libs!

Identifier Recycling

Delegation is discovery only:

can't make use of OpenID 2.0 fragment identifiers