YADIS Position Paper
for the W3C Workshop on Toward a More Secure Web Transparency and Usability of Web Authentication

Co-authors:
Johannes Ernst LID, YADIS   http://netmesh.info/jernst
Kaliya Hamlin, Identity Woman http://www.identitywoman.net

Since its announcement at the Internet Identity Workshop in October '05, the YADIS.org project has rapidly become a focal point for a variety of organizations and open source developers to create interoperable, decentralized identity technologies that use URLs as identifiers.(**)

As decentralized identity is an area of rapid innovation, YADIS fosters innovation and interoperability at the same time by answering the question: "given an identity URL, which of the ever-growing list of identity-related capabilities does it support?" For example, if a user enters an identity URL at a website, should the website attempt OpenID or LID/GPG-based single-sign-on? Can profile information be obtained about the user with this identity, and using which server? Can we send an authenticated message to the user with this URL?

YADIS was initiated by the LID and OpenID projects, which had been working simultaneously on decentralised identity. Subsequently, many other developers have joined in, including folks working on XRI and a variety of applications that make use of decentralized identity. From both a technical and an organizational perspective, YADIS is applicable to any URL-based identity system, by no means is it tied to OpenID, LID, or XRI, and can be extended by anybody without requiring permission from anybody and without stepping on anybody else's toes.

A number of YADIS implementations already exist and make an incremental improvement to the existing login experience. It enables sites to easily add authentication from a variety decentralized protocol options. This is a candidate technology for technical infrastructures to support user-facing improvements to web authentication.

Identity servers (aka identity brokers or home-sites) will use YADIS to declare what authentication mechanisms are supported. Relying parties (aka identity consumers or member-sites) will need to support each mechanism that their users might want to use. YADIS simply assists the relying party in selecting the appropriate mechanism.

Supporting only OpenID authentication or only LID authentication is fine, as long as it is acceptable to the site that certain users may not be able to authenticate with their YADIS ID. YADIS itself doesn't really add to or reduce security; the integrated identity systems (such as LID, OpenID) are responsible for security including anti-phishing measures.

All over the 'net, we are experiencing end users asserting their own place on the net: blogging is one of its most visible signs. As a consequence, it is much more natural for users to use their own, independently asserted and hosted identity to identify themselves at sites that wish to identity users. User-facing tools to support individuals declaring their "independent" identity to websites has great potential to improve the trustworthiness of the net. We believe YADIS provides an important stepping stone towards the vision of the workshop and hope to participate.

(**) For our purposes here, we define "URL" as "REST-ful URI".