



IDENTITY & ACCESS MANAGEMENT

Executive Briefing Paper

A View of OpenID

The underlying principle of OpenID and InfoCard is that citizens will be able to fully control how much or how little personal information they share with the service provider.

It is the point of control that should concern organisations. Ask the question, “who holds the keys?” Is the person holding the keys the right person for your business to trust?

In addition, are the processes that manage the registration of citizens sufficiently robust so the identity may be unequivocal and unique (that is, properly verified) and is the integrity of the credentials such that the credentials would be difficult to compromise?

The basics of how OpenID and InfoCard work are that under the OpenID Foundation (OIDF) and Information Card Foundation (ICF) open trust frameworks, any organisation that meets the technical and operational requirements of the trust framework may be certified as an identity provider (IDP).

Citizens can choose identity provider and preferred credential (only those credential types supported by the IDP). Open trust framework service providers, i.e. websites, are able to accept and trust the credential offered by the user, subject to any rules the service provider may have regarding the minimum level of information it requires from the credential.

For some activities these credentials will enable the user to be completely anonymous; for others they may require personal information such as name, age, gender, and so on. Service Providers need to determine what they require and citizens need to accept that for some services they may be required to disclose more than they might think necessary.

Open trust frameworks create some complexity, possibly confusion, over the choice the citizen makes in handing over what they think is the appropriate level of information for authentication purposes. What happens if the service provider asks for more than seems reasonable? The trust level is given a new dimension: the user not only has to trust the identity provider but also has to trust the service provider. It is not clear how OpenID and InfoCard set up trust relationships with service providers beyond the service provider being ‘enabled’: I suspect that there would be implied liabilities, if they did.

OpenID and InfoCard are user centric and, arguably, at the “wrong end of the telescope”, for enterprises looking for a suitable approach to providing corporate identity management solution.

Given the amount of time the open trust community has taken to get this far, as much time again might be used to bring a solution suitable for corporate use.

Author:
John McIntosh
Lakebridge Limited
2009