Is OAuth2 In Your Future

Is OAuth2 In Your Future?

Whether it becomes a protocol or a framework, OAuth2 certainly deserves another look. In fact, I revisit the nascent worlds of OAuth2 and OpenID Connect often, regularly testing the waters and gauging the current state-of-the-art. At this point, AFAICT there's really nothing to latch on to unless you're a bleeding edge developer, researcher, or technology pundit.

People whose opinion I respect predict OAuth2 and friends have a very positive future indeed. Personally I think it's too early to tell, but from the perspective of a federation operator, are there use cases that would benefit from OAuth2 now?

We are faced with at least one burning use case at the moment. That is, the use case of a low to moderate value federated webapp with very modest attribute requirements. This use case requires near 100% penetration yet should have near zero boarding requirements, that is, Level of Assurance (LoA) is minimal while the barriers to interoperability should be as close to zero as possible.

Relatively speaking, this is a very old use case. It has remained unsolved for so long, it now threatens to unravel the federated approach by marginalizing the hard won successes realized over years of deployment. Thus the opportunity for a young framework (like OAuth2) to step in and make significant inroads is very real. This is of course the way it should be, a kind of survival of the fittest. So let the user beware: OAuth2 may be in your future sooner than you think!

Let me outline the use case in slightly more detail so we know what we're up against. A typical federated Service Provider (SP) has the following requirements:

- Roughly LoA-1, that is, a basic level of assurance with optional identity (if there is a claim of positive identity, the Identity Provider (IdP) should assert it)
- Globally unique, persistent, non-reassigned identifier
- One or more so-called personal identifiers (e-mail address, person name, and/or human-readable principal name)
- A discovery interface with an 80% success rate (minimum)
- No manual IdP boarding requirements

Expanding on the latter pair of requirements: Assume at least 80% of the users that visit the SP are presented with a discovery interface that includes one of their preferred IdPs, and moreover, the IdP selected by the user meets the assurance and attribute requirements without further human interaction. Remember, this must result in a positive user experience *at least 80% of the time*!

Today of course we are far from meeting the needs of this use case. SPs either manually board IdPs one-by-one, leading to a relatively small group of trusted IdPs, or SPs present the user with a broad selection of IdPs, few of which meet the designated assurance and attribute requirements. In either case, the SP realizes roughly a 20% success rate (at best). Not good.

Solutions anyone? Do OAuth2 and friends play a role here?