A public identity infrastructure for the Internet

IETF 100, Singapore

Vittorio Bertola <vittorio.bertola@open-xchange.com>
Marcos Sanz <sanz@denic.de>

The state of online auth for the average user

- Most people just reuse usernames and passwords across hundreds of websites and services
  - Usability issues
  - Security issues

- Single-sign-on systems in private namespaces gaining ground
  - Users like them, but:
  - Fragmentation, lack of interoperability
  - Clients have to implement each of them separately
  - Users cannot choose their provider

Advantages of public, federated SSO

- Why can’t your online identity work like your email address?
- You only need one account to interoperate with everyone
- You get to choose and even to change your provider
  - You can keep your address if it is in your own domain name
- You only need to remember and secure one set of credentials
- Any additional security mechanisms can be implemented just once by a specialized party (not by any website operator)
- You have an easy way to control the sharing of your information and to keep it updated (a legal requirement in many countries)
- You don’t need to register for new websites, just identify yourself

Design principles for the solution

- Be public and federated
  - Prevent a chat-like mess of incompatible competing services
- Reduce the implementation effort
  - Build on widely used technologies: OpenID Connect/OAuth, DNS
  - Allow easy integration of existing OAuth-based sets of identities
- Flatten the user's learning curve
  - Users are already familiar with DNS-based identifiers (hostnames/emails)
- Not deal with real world identification
  - Users can have multiple identities, pseudonymous identities etc
  - Though you could build third-party certification as an option in the scheme

How it works

- We add a DNS-based discovery mechanism to OpenID Connect
  - Any hostname or email address can be mapped to an identity provider
  - A string with name-value couples in a TXT record specifying pointers
  - You only have to add the DNS piece, the rest is standard OpenID Connect
  - draft-ietf-oauth-discovery-07 leaves issuer discovery out of scope
- We use the OpenID distributed claims mechanism to separate roles
  - Distinction between an identity authority doing authorization and authentication, and an identity agent managing users and their data
  - Separating functions and data sets increases privacy and security
- We (plan to) add an ontology for any useful claim

Project status

- A joint project by three companies (codename “DomainID”)
- A prototype up and running
- Presented to several relevant companies in Europe
  - Interest by TLD registries willing to become identity authorities
  - Interest by domain name registrars willing to become identity agents
  - Interest by telcos / ISPs willing to supply identities to their users
- Two -00 drafts independently submitted in October
  - Still missing lots of stuff
- Looking for feedback and participation

draft-bertola-dns-openid-pidi-architecture

draft-sanz-openid-dns-discovery