Thoughts on Remaining Discovery Issues

Mike Jones

IETF Applications Area Working Group

November 5, 2012

Problem of Hosted Domains

- .well-known endpoint may not be able to be created for some domains
  - In hosted case, there may be no web server at all
- Discovery still desirable for such domains

Hosted Domain Options

- Use DNS SRV records
  - Positive: Arguably the "right way" to solve this
    - *But if workable, we wouldn't need .well-known either*
  - Negative: Not usable by many kinds of clients
  - Negative: Some Web hosters don't expose SRV records
- Use a domain name prefix
  - E.g., use "simple-web-discovery.example.com" for SWD discovery for domain "example.com"
  - Positive: Uses DNS A records, which all can use
  - Negative: Requires use of a specific hostname
  - Negative: Needs TLS certificate for subdomain name
- Decide that discovery can not be performed

Solution Chosen by OpenID Connect

- OpenID Connect WG chose domain prefix solution
  - Try .well-known at domain, then try at subdomain
- Simple Web Discovery draft just updated to incorporate this solution
  - draft-jones-simple-web-discovery-04
  - `SWD_service_redirect` JSON-based redirect removed, since no longer needed
- *We encourage WebFinger to also enable discovery when a .well-known endpoint cannot be created at the domain's host*

Discovery using non-default ports

- Services can be hosted at non-default ports
  - For instance, an IdP at https://example.com:8080/ rather than https://example.com/ (port 443)
  - Often done in test configurations
- Discovery service may need to be hosted at non-default ports for the same reasons
  - *Discovery spec should make it clear that it is legal to locate discovery endpoints at non-default ports (while still using TLS)*

Good Progress on WebFinger

- Consensus now seems to be apparent on WebFinger supporting these requirements:
  - Simple to implement
  - REST/JSON
  - Low latency
- Hopefully consensus soon on supporting this remaining requirement:
  - Supports hosted deployments

Finishing WebFinger in Timely Manner

- Stable spec critical for interop testing, deployment
- Timely completion critical to adoption
- *Encourage WG to identify, decide open issues*
- OpenID Connect can switch from SWD to WebFinger
  - If Connect requirements are met by WebFinger
  - If WebFinger spec stabilizes soon