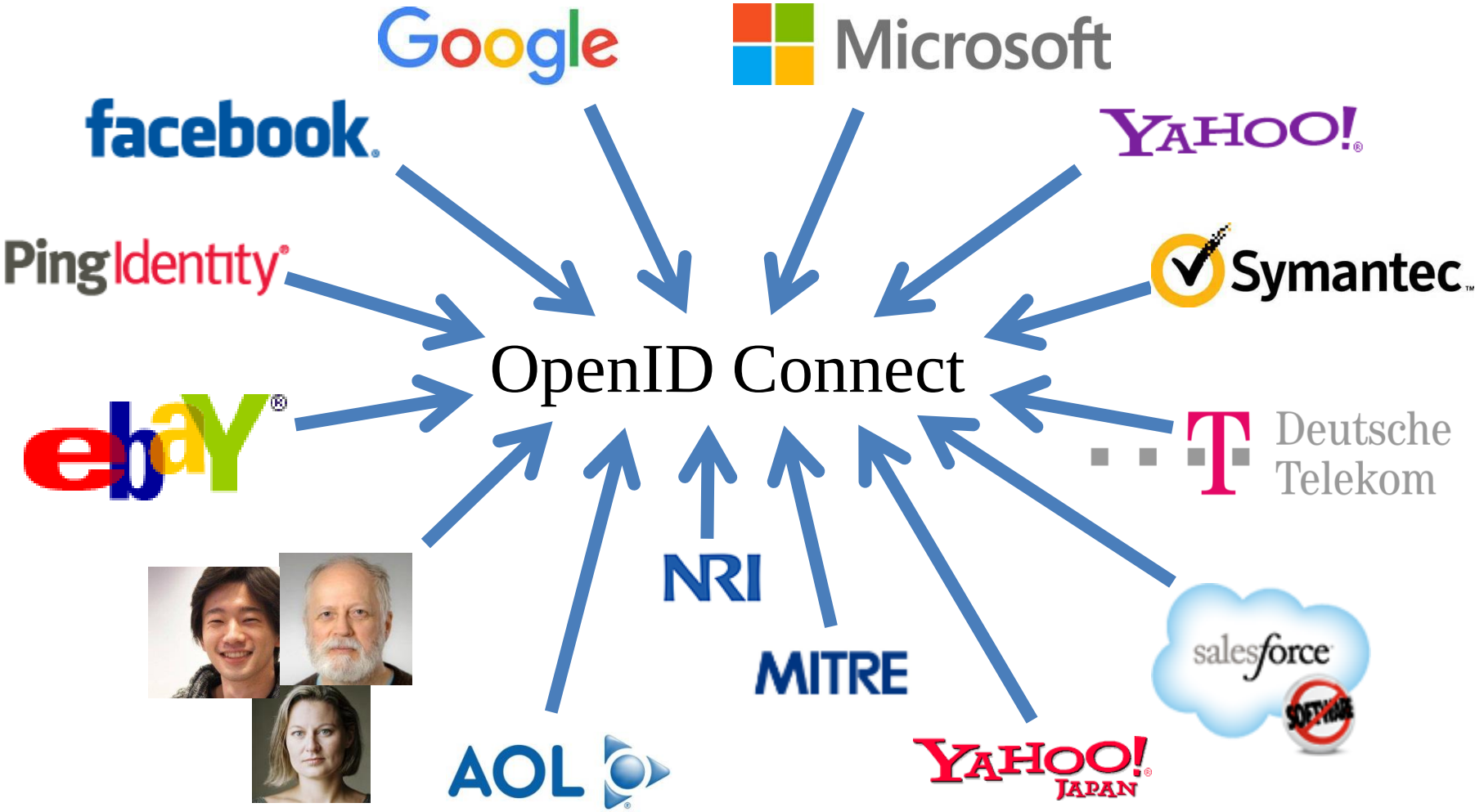
OpenID Connect Working Group

May 10, 2016

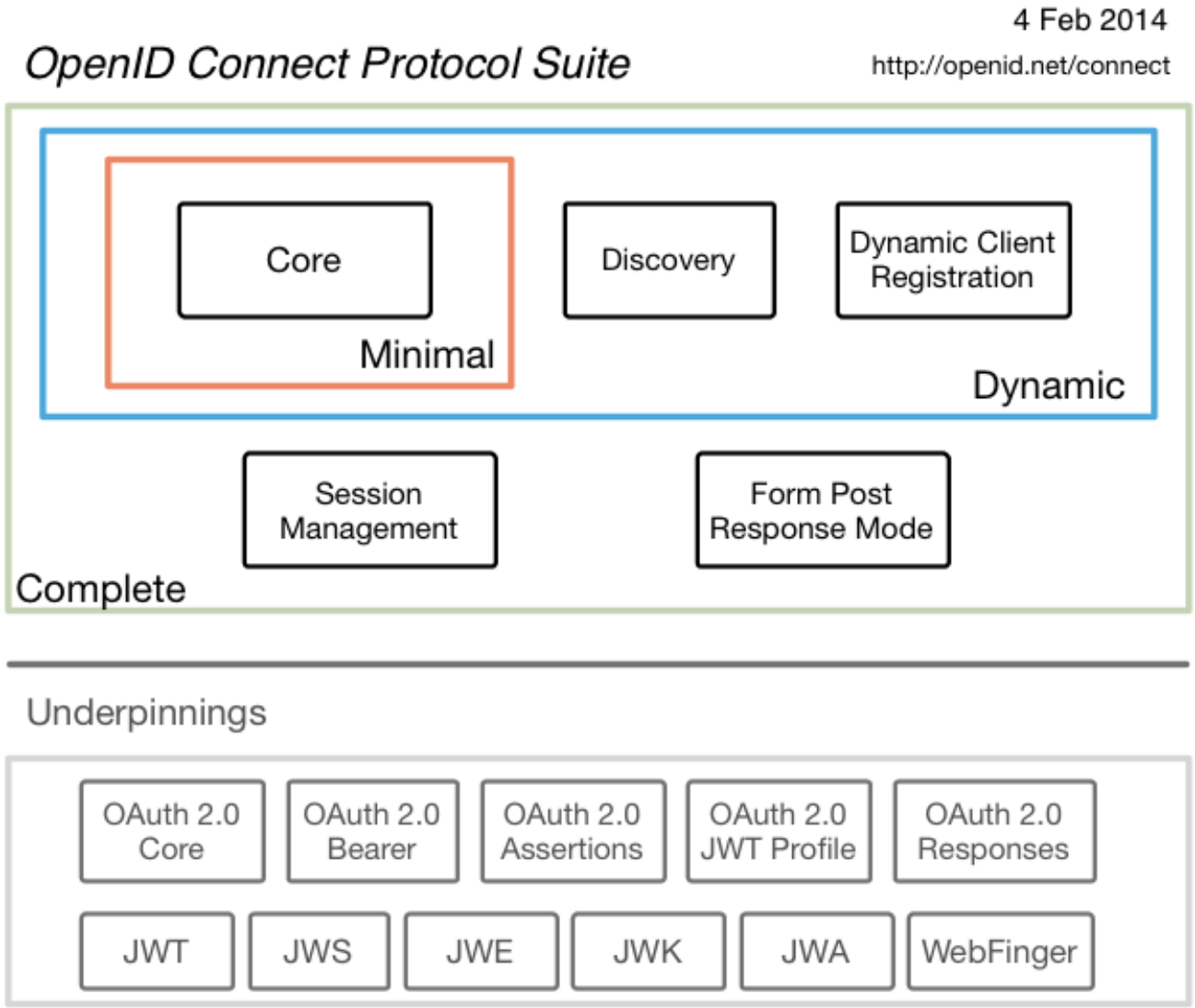
Mike Jones

Identity Standards Architect – Microsoft

Working Together



OpenID Connect



Topics

- Most Recently Completed Specifications
- Session Management / Logout
- Second Errata Set
- New Related Work
- OpenID Connect Certification

Most Recently Completed Specifications (1 of 2)

- OpenID 2.0 to OpenID Connect Migration
  - Defines how to migrate from OpenID 2.0 to OpenID Connect
    - Has OpenID Connect identity provider also return OpenID 2.0 identifier, enabling account migration
  - http://openid.net/specs/openid-connect-migration-1_0.html
  - Completed April 2015
  - Google shut down OpenID 2.0 support in April 2015
  - Yahoo, others also plan to replace OpenID 2.0 with OpenID Connect

Most Recently Completed Specifications (2 of 2)

- OAuth 2.0 Form Post Response Mode
  - Defines how to return OAuth 2.0 Authorization Response parameters (including OpenID Connect Authentication Response parameters) using HTML form values that are auto-submitted by the User Agent using HTTP POST
  - A “form post” binding, like SAML and WS-Federation
    - An alternative to fragment encoding
  - http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html
  - Completed April 2015
  - In production use by Microsoft, Ping Identity

Session Management / Logout

- Three approaches being pursued by the working group:
  - Session Management
    - http://openid.net/specs/openid-connect-session-1_0.html
    - Uses HTML5 postMessage to communicate state change messages between OP and RP iframes
  - Front-Channel Logout
    - http://openid.net/specs/openid-connect-frontchannel-1_0.html
    - Uses HTTP GET to load image or iframe, triggering logout
    - Similar to options in SAML, WS-Federation
  - Back-Channel Logout
    - http://openid.net/specs/openid-connect-backchannel-1_0.html
    - Server-to-communication not using the browser
    - Can be used by native applications, which have no active browser
- All support multiple logged in sessions from OP at RP
- Unfortunately, no one approach best for all use cases

Second Errata Set

- Errata process corrects typos, etc. discovered
- Errata process makes no normative changes
- Edits under way for second errata set
- See http://openid.net/specs/openid-connect-core-1_0-23.html for current Core errata draft

New Related Work

- International Government Profile (iGov) Working Group
  - Developing OpenID Connect profile for government & high-value commercial applications
- Enhanced Authentication Profile (EAP) Working Group
  - Will enable use of TLS token binding with OpenID Connect
  - Will enable integration with FIDO authentication

OpenID Certification

- OpenID Connect Certification launched in April 2015
  - Google, Microsoft, Ping Identity, ForgeRock, PayPal, and NRI were the launch participants
    - Their OpenID Provider implementations were certified
  - Deutsche Telekom, Salesforce, Dominick Baier, and others also “tested the tests” prior to the launch
- See http://openid.net/certification/ and http://openid.net/certification/faq/

What is OpenID Certification?

- OpenID Certification enables OpenID Connect implementations to be certified as meeting requirements of defined conformance profiles
- Current conformance profiles defined by the OpenID Connect working group are:
  - Basic OpenID Provider
  - Implicit OpenID Provider
  - Hybrid OpenID Provider
  - OpenID Provider Publishing Configuration Information
  - Dynamic OpenID Provider

Use of Self-Certification

- OpenID Certification uses self-certification
  - Party seeking certification does the testing
  - (rather than paying a 3rd party to do the testing)
- Simpler, quicker, less expensive, more scalable than 3rd party certification
- Results are nonetheless trustworthy because:
  - Testing logs are made available for public scrutiny
  - Organization puts its reputation on the line by making a public declaration that its implementation conforms to the profile being certified to

Certification Workflow

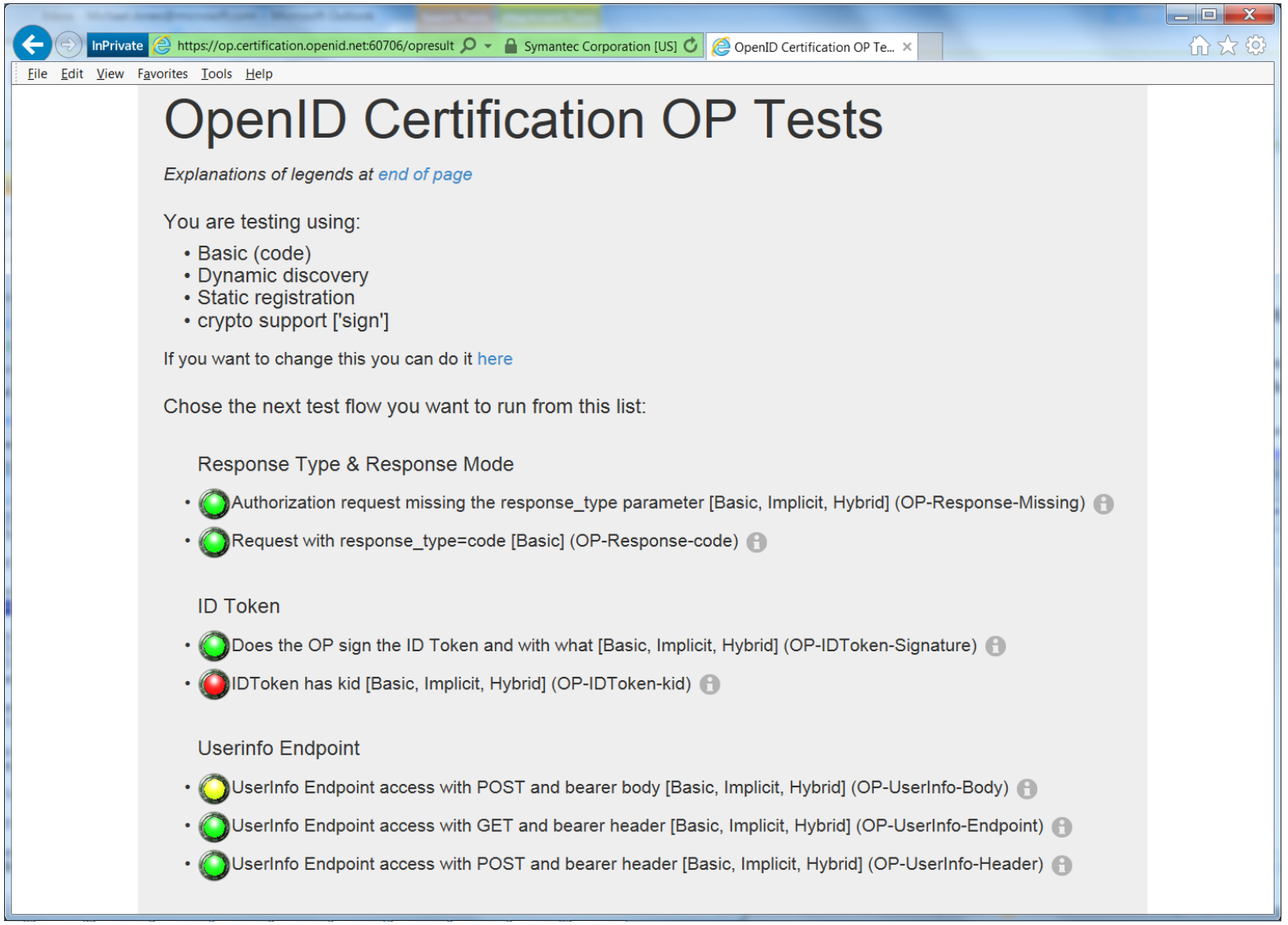
- Organization decides what profiles it wants to certify to
  - For instance, “Basic”, “Config”, and “Dynamic”
- Runs conformance tests publicly available at http://op.certification.openid.net/
- Once all test for a profile pass, org submits certification request to OIDF containing:
  - Logs from all tests for the profile
  - Signed declaration that implementation conforms to the profile
- OpenID Foundation verifies application is complete and grants certification
- OIDF lists certification at http://openid.net/certification/ and registers it in OIXnet at http://oixnet.org/openid-certifications/

Current Certifications

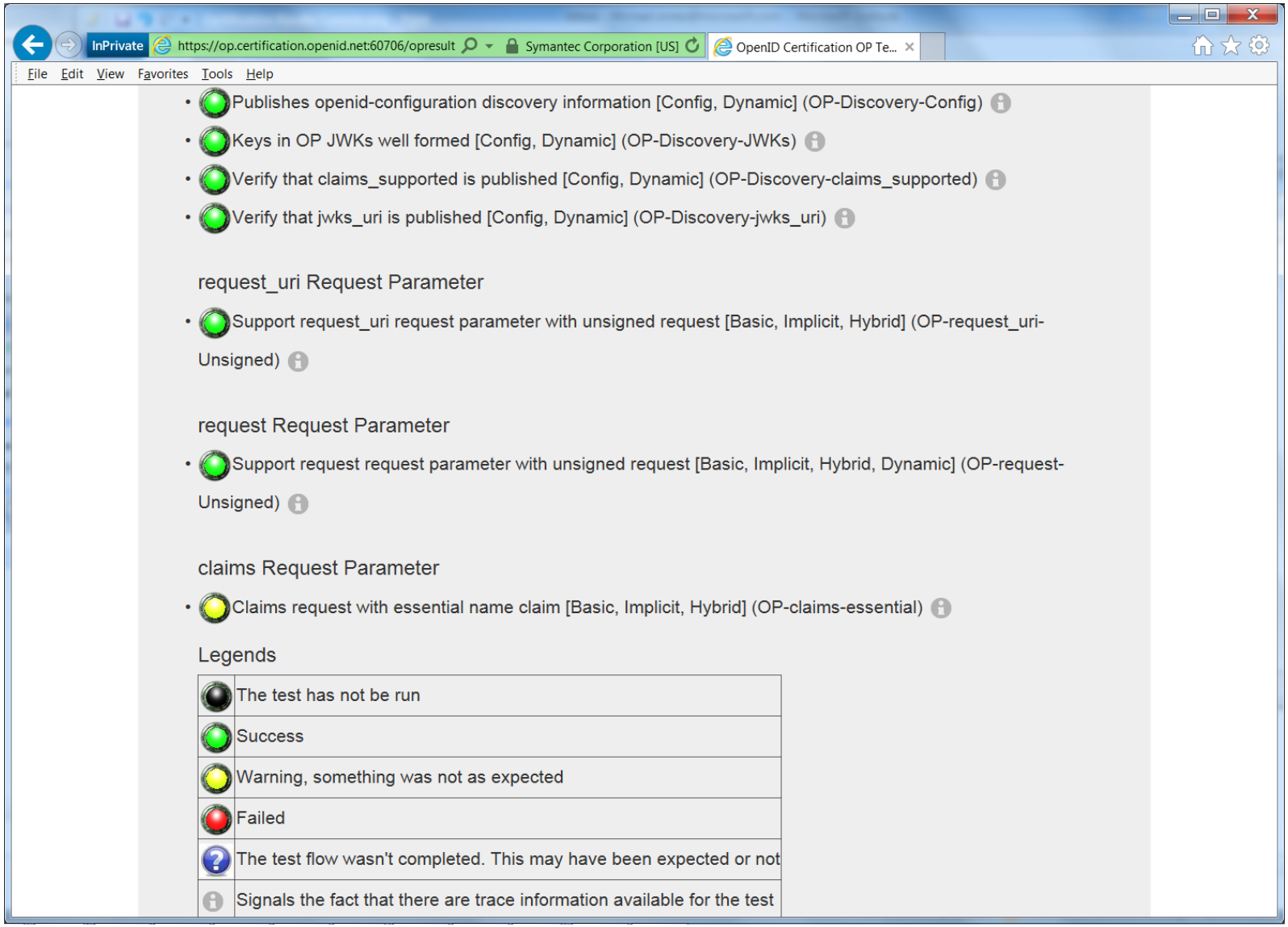
- Listed at http://openid.net/certification/
- 26 implementations presently certified by 24 organizations for 80 profiles
  - Recent additions Spark , Auth0, NEC, SecureAuth, University of Chicago (for Shibboleth overlay!)
- Each entry in table a link to zip file containing test logs and signed conformance statement
  - *Results available for public inspection*
- Also see http://openid.net/2015/11/04/openid-certification-momentum/

- ***Yours can be next!***

OpenID Example Testing Screen



Test Screen Legend



How does certification relate to interop testing?

- We held 5 rounds of OpenID Connect interop testing – see http://osis.idcommons.net/
  - Each round improved implementations and specs
  - By the numbers: 20 implementations, 195 members of interop list, > 1000 messages exchanged
- With interop testing, by design, participants can ignore parts of the specs
- Certification raises the bar:
  - Defines set of conformance profiles that certified implementations meet
  - Assures interop across full feature sets in profiles

OpenID Certification: How did we get here?

- Establishing a successful certification program didn't just happen
- Over a man-year of work:
  - Creating conformance profiles
  - Designing and implementing testing software
  - Testing and refining the tests
  - Testing implementations and fixing bugs found
  - Creating the legal framework for self-certification
  - Putting it all in place
- Special thanks to:
  - Roland Hedberg, Umeå, and GÉANT for the software
  - Don Thibeau for the simplicity of the approach
  - Engineers from Google, Microsoft, Ping Identity, ForgeRock, PayPal, and NRI for testing the OP tests

My Favorite Comment on OpenID Certification

- Eve Maler – VP of Innovation at ForgeRock
  - "You made it as simple as possible so every interaction added value"
- High praise! ☺

OpenID Certification: What's Next?

- Scope of OpenID Certification expanding
- RP certification beginning
  - Your involvement wanted to test the tests!
- Additional OP profiles are also planned:
  - Self-Issued
  - Refresh Token Profile
  - OP-Initiated Login
  - Front-Channel Logout
  - etc.

Call to Action

- Certify your OpenID Connect OP implementations now!
- Help us test the RP tests!
- Join the OpenID Foundation and/or the OpenID Connect working group

Open Conversation

- How are you using OpenID Connect?
- What would you like the working group to know?