draft-ietf-regext-rdap-openid
Federated Authentication for the Registration Data Access Protocol (RDAP) using OpenID Connect

Scott Hollenbeck
shollenbeck@verisign.com
IETF-104 REGEXT Working Group
• Purpose
  • Add support for federated authentication to RDAP

• Approach
  • Based on OpenID Connect and OAuth
  • Leverage independent Identity Providers
  • RDAP operators are Relying Parties
  • Use identity and authentication information to make requestor authorization and access control decisions
Implementations

• Servers
  • [https://rdap.verisignlabs.com](https://rdap.verisignlabs.com)
    • “Thin” experiment with .cc and .tv
  • [https://vtrdap.verisignlabs.com](https://vtrdap.verisignlabs.com)
    • “Virtual thick” experiment with .cc and .tv
  • [https://rdap-pilot.verisignlabs.com](https://rdap-pilot.verisignlabs.com)
    • “Thick” experiment with .career (.com and .net, too)
  • Verisign servers support credentials issued from [https://www.mojeid.cz/](https://www.mojeid.cz/)

• Identity Providers
  • [https://auth.viagenie.ca](https://auth.viagenie.ca)
  • [https://testprovider.rdap.verisignlabs.com/](https://testprovider.rdap.verisignlabs.com/)
Discussion Points

• Ongoing policy development
  • ICANN context in particular
  • Direct impact on needed claims

• Non-browser clients
  • Is the device flow needed?

• Path segments
  • Correct? More needed?

• Custom claims returned in ID token or via UserInfo endpoint?

• Query parameters vs. HTTP headers
  
  .../domain/example.com?id_token=eyJ0...EjXk&access_token=eyJ0...NiJ9
  vs.
  .../domain/example.com?id_token=eyJ0...EjXk and
  Authorization: Bearer <access_token>