



# draft-ietf-regext-rdap-reverse-search

Mario Loffredo, Maurizio Martinelli  
Registro.IT/IIT-CNR

# The proposal in a nutshell



<RDAP server URL>/{resource-type}/reverse/{role}?{property}=<search pattern>

- **resource-type:** it MUST be one of resource type path segments defined in Section 3.2 of RFC 9082:
  - "domains", "nameservers" or "entities" for now;
  - maybe "ips" and "autnums" in the future ?
- **role:** it MUST be one of the roles described in Section 10.2.4 of RFC 9083;
  - for role independent searches, the value "entity" MUST be used;
- **property:** it identifies the entity property to be used in matching the search pattern:
  - a pre-defined list of possible properties includes: *fn, handle, email, city, country, cc*;
  - servers MAY implement additional properties.

# Accomplishments



- RegExt has mainly focused on privacy implications:
  - both "Privacy Considerations" and "Security Considerations" sections have been updated repeatedly
  - the reverse search path has been designed to let the RDAP providers to implement different authorization policies on a per-role basis
- Discussion about privacy concerns seems to be concluded

# Next steps



- Move the focus on technical issues:
  - define likely use cases
    - should we extend the reverse search to accomplish other cases ?
    - should we obfuscate the private information in the query string ?
  - review the query model accordingly
  - add implementations