

# Bootstrapping Weirds

draft-blanchet-weirds-bootstrap  
draft-blanchet-weirds-bootstrap-ianaregistries

Marc Blanchet  
Viagénie  
marc.blanchet@viagenie.ca

Berlin IETF, July 2013

# Context

- 2 bootstrap solutions being discussed:
  - DNS-based (draft-blanchet-weirds-bootstrap)
  - IANA registry based (draft-blanchet-weirds-bootstrap-ianaregistries)
- Different approaches. Pros and Cons. Domains and numbers have different contexts.
- Goal: to reach consensus on the approach (could be mixed?)
- Drafts are in good shape to get the idea, but not fully specified (on purpose). When consensus reached, will revise the draft(s)

# DNS-based solution

- draft-blanchet-weirds-bootstrap
- names:
  - rdap query for example.com will result in DNS query of example.com.domain.rdap.arpa
- numbers:
  - rdap query for 192.9.200.0/24 generates a DNS request to 200.9.192.ip4.rdap.arpa.
  - rdap query for 2001:db8::/32 generates a DNS request to 8.b.d.0.1.0.0.2.ip6.rdap.arpa.
- requested RR are A and AAAA.
  - (could be CNAME/SRV/NAPTR, but kept simple for now, more later on DNS RR...)

# DNS-based solution

- can be secured with DNSSEC
- highly scalable
- has expiration, caching, ...
- infrastructure already in place

# IANA Registries based Solution

- draft-blanchet-weirds-bootstrap-ianaregistries
- names:
  - rdap query for example.com results in matching and fetching the content of the cell corresponding to the row for “com” in the IANA registry. The content is the rdap server url (<http://rdap.mytld/rdap/...>)
- numbers:
  - rdap query for 192.9.200.0/24 results in matching and fetching the content of the cell corresponding to the row for “192/8” in the IANA registry..

# IANA Registries based Solution

- Creation of new IANA registries
  - but based on current data and relationships
- Registries:
  - tld => rdap server url
    - similar to the current root zone database registry with a new “column”.
  - numbers => rdap server url
    - similar to the current IP address registries with a new column.
  - small single XML files
    - can be fetched in advance, locally cached, ...

# ASN

- AS numbers are not hierarchical numberspace. flat.
- IANA allocations are done by ranges to RIR
- Both solutions can be mapped into the allocations
  - IANA registry-based solution would be identical to the addresses: match, column with the rdap url
  - DNS-based solution would be mostly a single flat space to a single entity (the RIR may agree to run a joint server/proxy for these.

# Addresses

- Currently, RIR (only 5) usually:
  - know each other
  - know ranges for each RIR
  - therefore, redirect to the other server when they receive a request not for their own range.
- But:
  - we need to specify the list of these servers somewhere. (not in the RFC, IANA registry?)

# Comparing solutions

- Possible requirements/decision/differentiation points (was sent to the list)
  - require use of https on every request
  - specify per registry which of http/https is to be used by clients
  - provide delegation below the tld
  - same solution for both names and numbers
  - don't route all traffic through one point of attack (which is not the same as one point of failure)
  - base URL may have a prepended path (i.e. http://domain/my/own/path/query)
  - if DNS is used, only terminating DNS RR can be used (i.e. no CNAME, SRV, NAPTR)
  - constrained to what Javascript offers in browsers
  - simplicity/easy to implement
  - does the client have a cache of "servers" to start with?
  - if a cache, how/when does it refresh the data?

# HTTP vs HTTPS

- Support for both requires some signaling
  - DNS: “advanced” records (SRV/NAPTR)
  - IANA registries: a field saying which one is available.
- Single transport is easier for client. But https is heavier on servers and require one cert per TLD. But https gives us data integrity (and confidentiality and source verification)

# Base URL and DNS

- If we want “http://example.com/rdap/mytld/” (instead of http://rdap.mytld), then
  - For DNS-based solution:
    - basic DNS RR (A, AAAA, CNAME) do not fill this
    - need to use SRV/NAPTR records which are more complex.
      - SIP had these records (as non mandatory) but almost nobody use them.
  - For IANA registry:
    - the base url is in the IANA registry.

# Javascript

- Almost no DNS requests in the browser.
- But most JS use external APIs/AJAX/... to complement their code.
- JS in browsers should then, as typical, use some external API/AJAX for the purpose of bootstrapping.
  - could be a private service by the JS app provider
  - or a public service.
- Shall we restrict the specification to the only capabilities of the intersection of features on all JS browser implementations?

# Impact on IANA

- We need IANA work for both solutions.
- IANA has already relationship with TLDs.
- DNS-based:
  - tlds tell IANA the RDAP DNS records for their tld. IANA put it in the related arpa zone.
  - DNS infrastructure already setup for this service.
- IANA registry-based:
  - tlds tell IANA the rdap server url for their tld. IANA put it in the IANA registry
  - IANA has to put some caching infrastructure to handle the load. (IANA is (preliminary) ok if this is what we need)

# ICANN EWG Considerations

- ICANN EWG considering a centralized repository of (copied) registration data (copy received from the registries).
- Bootstrap
  - shall support this if that recommendation is put forward.
  - but also support at the same time other registration data repository (for example, cctld not going into EWG).
- DNS and IANA registries based approaches both support ICANN EWG direction.

# Comparing Solutions

- DNS-based:
  - is more constrained (http-https, base url) if kept simple.
  - can be flexible if using more complex DNS records (SRV, NAPTR)
  - infrastructure already in place, scales, ...
- IANA-registry-based:
  - more flexible (full url with choice of http\*)
  - infrastructure to be put in place

# Comparing Solutions

- Mixed solution?
  - one solution for names, another solution for numbers
  - not simpler...

# WG Direction

- Looking for consensus on direction to update the draft and to add more details (on the chosen solution).
- DNS-based? IANA-registry-based? Both?