

RDAP at IANA; Security Audits at IANA

Kim Davies
VP, IANA Services & President, PTI

Seattle
March 2024

PTI | An ICANN Affiliate

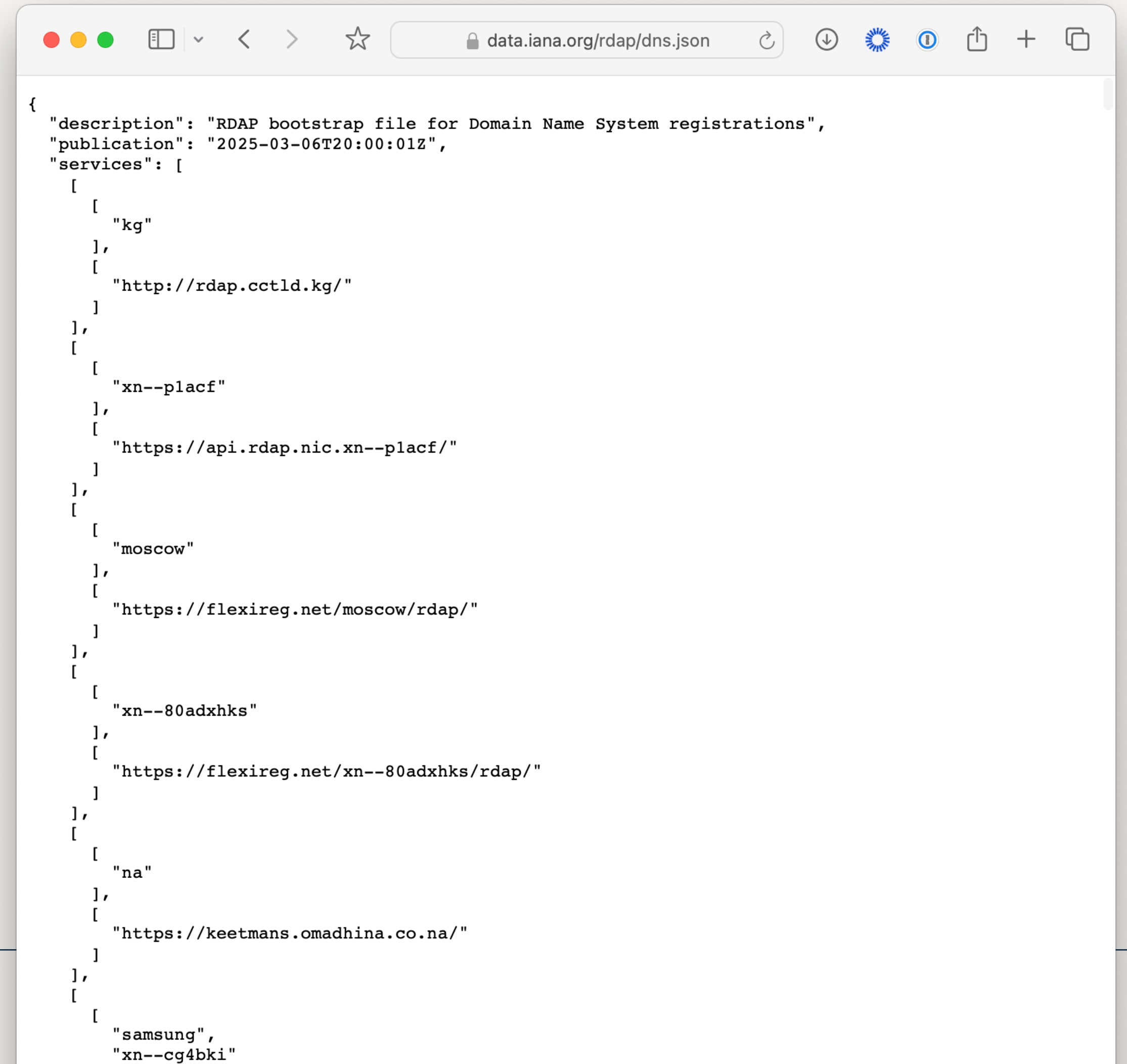


Agenda

- **RDAP at IANA**
 - Our deployment experience
 - Tips for TLD managers
- **System and organizational control (SOC) audits**
 - Our audit program
 - Upcoming changes

IANA's role in RDAP

- IANA operates the RDAP bootstrap, which is where RDAP clients obtain an initial set of pointers to high-level RDAP servers
- Operational since 2015
- This presentation isn't about that (much)

A screenshot of a web browser window showing the content of the file data.iana.org/rdap/dns.json. The browser's address bar shows the URL. The page content is a JSON object representing the RDAP bootstrap file. The JSON structure includes a description, a publication timestamp, and a list of services. Each service entry contains a domain identifier and a corresponding RDAP server URL.

```
{
  "description": "RDAP bootstrap file for Domain Name System registrations",
  "publication": "2025-03-06T20:00:01Z",
  "services": [
    [
      "kg",
      "http://rdap.cctld.kg/"
    ],
    [
      "xn--placf",
      "https://api.rdap.nic.xn--placf/"
    ],
    [
      "moscow",
      "https://flexireg.net/moscow/rdap/"
    ],
    [
      "xn--80adxhks",
      "https://flexireg.net/xn--80adxhks/rdap/"
    ],
    [
      "na",
      "https://keetmans.omadhina.co.na/"
    ],
    [
      "samsung",
      "xn--cg4bki"
    ]
  ]
}
```

An RDAP server at IANA

- IANA operates a WHOIS service at whois.iana.org
- Seeking to replicate comparable functionality in RDAP
- IANA's use case is unique and not well suited to an off the shelf solution
 - IANA runs the root zone zone
 - IANA operates two top-level domains that contain organizational delegations
 - IANA runs an ICANN registrar
 - IANA runs reverse DNS
 - IANA operates number resource space
- We developed our own from scratch RDAP implementation to handle our unique use case

Toes in the water

- .INT
 - Deployed and added to the bootstrap registry in April 2024
- IN-ADDR.ARPA and IP6.ARPA
 - Generally, seeking to provide redirects to RIR RDAP servers with more specific results
 - Difficult to navigate due to the different provenances of different allocations; plus significant chunks are reserved out of otherwise normal unicast allocations
 - In beta and under dialogue with RIRs before deployment
- IP address and AS space
 - Not yet deployed
 - Intend to provide answers where IANA is authoritative for the final block (e.g. multicast, reserved) with remarks on space purpose

Toes in the water

- Root zone
 - RFC 9224 is current guidance that is relevant
 - “authoritative registration data service is found by doing the label-wise longest match of the target domain name”
 - “The entry for the root of the domain name space is specified as
‘.’”
 - Challenges due to client behavior
 - RDAP lookup for “com” will match “com”, not the root zone RDAP service
 - Longest match for a TLD without RDAP, reserved TLD or non-existent TLD, will match the root zone
 - e.g. “example.eu”, “printer.internal”
 - Would become a sinkhole for RDAP traffic - undesirable
 - Some clients have special matching rules or TLDs
 - It is there, just not linked to, e.g. <https://rdap.iana.org/domain/us>

```
-bash
{
  "rdapConformance": [
    "rdap_level_0"
  ],
  "objectClassName": "domain",
  "ldhName": "us",
  "nameservers": [
    {
      "objectClassName": "nameserver",
      "ldhName": "b.cctld.us",
      "ipAddresses": {
        "v4": [
          "156.154.125.70"
        ],
        "v6": [
          "2001:502:ad09::29"
        ]
      }
    },
    {
      "objectClassName": "nameserver",
      "ldhName": "f.cctld.us",
      "ipAddresses": {
        "v4": [
          "209.173.58.70"
        ],
        "v6": [
          "2001:500:3682::11"
        ]
      }
    }
  ],
  {
```

RDAP at the TLD level

- Noticed RDAP is sometimes impacted by RSP changes
- Bootstrap data for TLDs is derived from our root zone management processes
- Changes to the RDAP server for a TLD must be coordinated as a root zone change, this means
 - Consider time needed: approvals, staff review and implementation
 - If tied to an NS change, can be delayed by technical check remediation and time to publish root zone changes
- Recently made optimizations to purge CDNs to make changes faster
- Much like with name servers, plan your migration
 - Strive to maintain new and old RDAP servers for some time
 - Use HTTP redirects from the old server
 - Consider clients may access the old server for some time, that may have out-of-date information
 - Impact on TLS certificate issuance, for example

IANA's audit program

- Evaluates key systems that support the IANA functions to ensure they operate securely, reliably, and in accordance with industry best practices.
- Through this process, IANA maintains transparency and accountability while continuously refining its security and operational controls.
- Performed by a third party auditor on an annual basis
- SOC3 reports are public reports posted on IANA's website
- SOC2 reports are confidential reports provided to key community stakeholders



Framework

- IANA uses the System and Organizational Control (SOC) audit framework, set by the American Institute of Certified Public Accountants (AICPA)
- Descendent from “SysTrust” audits we first started performing
- SOC audits can be performed at multiple levels, the relevant ones:
 - SOC 2 — Focused detailed reporting, intended for limited audience
 - SOC 3 — Summarizes the SOC 2 for a general audience
- Current reporting criteria
 - Security (Standard for all SOC 2 reports)
 - Availability (Ensuring systems are operational as expected)
 - Processing Integrity (Ensuring requests are processed accurately and completely)



System Scope

- Systems and processes for KSK management
- Key systems used to perform transactions
 - RZMS (Root Zone Management System): Main system for process naming function requests; community input drives improvements.
 - Request Tracker (RT): Ticketing system for tracking requests from all three functions.
 - GitHub: Repository storage and updates for protocol parameter registries.



Annual process

- The audits are conducted annually in a continuous cycle. Overlapping audit periods ensure IANA maintains ongoing compliance.
- Planning (March-May):
 - Defining timelines, deliverables and expectations with external auditors and internal stakeholders.
 - Updating controls when processes change or new processes are introduced (ex: KYC and OTE environment)
- Testing (July-December):
 - Documentation is collected to test the operating effectiveness of controls.
 - Conducted twice a year due to the number of controls (~75 controls).
 - Involves participation from multiple departments (HR, E&IT, Finance, Legal, Facilities).



Improvements

- IANA will now publish a SOC 3 report for transparency and broader stakeholder assurance. First SOC3 report will be available late April.
- Scope Expansion:
 - Evaluating the inclusion of additional systems used to perform the IANA functions.
 - Evaluating the inclusion of additional SOC Criteria (Confidentiality): to address the handling of PII as part of IANA's evolving responsibilities.



Takeaways

- Community-driven development (as seen with RZMS and related processes) can contribute to process and audit maturity outside of framework updates.
- Reminder that the RIR CEOs receive the detailed SOC2 report and are encouraged to ask follow-up questions regarding controls or testing procedures.
- Reach out to ask IANA questions about audits or other compliance any time!
- More info:
<https://www.iana.org/about/audits>

