78 ANNUAL GENERAL MEETING

ICANN 1998–2023

IANA Stewardship Transition 2016–2023

Joint Meeting:
SSAC and GNSO Council

Agenda

- Update on Name Collision Analysis Project report
- Current SSAC work topics that may be of interest to the GNSO and/or may be of relevance to policy activities
  - DS Automation
  - Registrar NS Management
- Discussion on ICANN home for underrepresented groups
- Fit for purpose

Name Collision Analysis Project

Matt Thomas and Suzanne Woolf

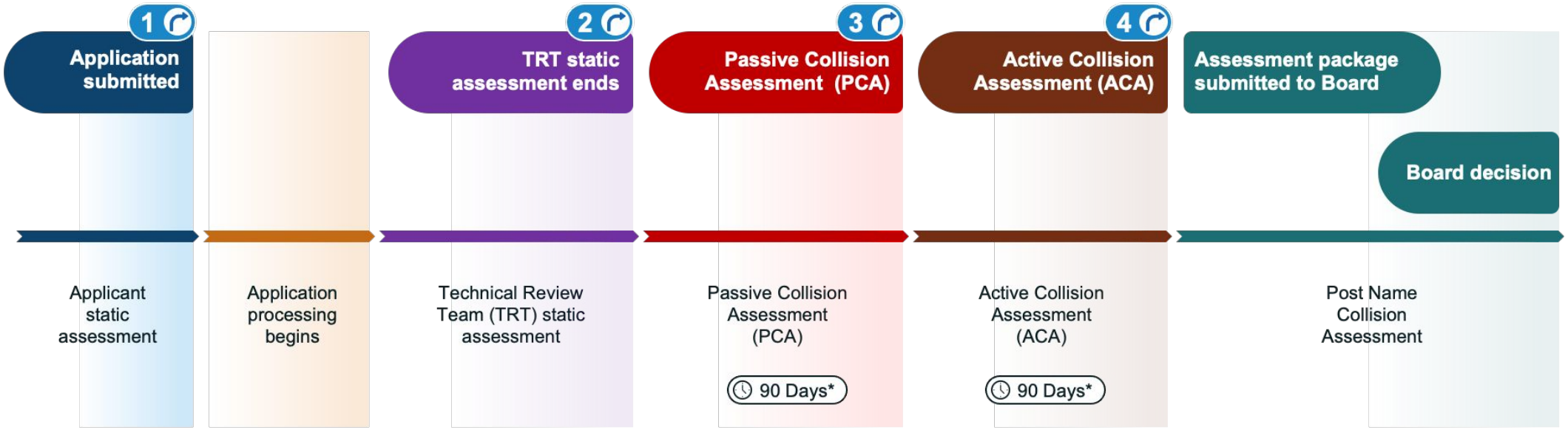
Recent Publications from Completed Work

- Case Study of Collision Strings
  - Case studies of CORP, HOME, and MAIL indicates the potential for *impact* has increased
  - Critical Diagnostic Measurements help predict the *impact* of name collisions
  - Leaking collision strings differ from delegated TLD queries
  - DNS-SD protocols and suffix search lists are a major problem
  - Potential for significant collision strings still occurs
- A Perspective Study of DNS Queries for Nonexistent Top-Level Domains
  - Study shows similarities and differences of RSIs and PRR
  - Existing measurement platforms could be extended to help inform applicants
- Root Cause Analysis - New gTLD Collisions
  - Private use of DNS suffixes is widespread
  - Name collision reports are supported strongly by measured data
  - The impact of TLD delegation ranged from no impact to severe impact
- **Name collisions are and will continue to be a difficult problem to identify and remediate**

Workflow Goals

- To ensure that name collisions can be assessed
  - Requires name collisions to be visible, if they exist
- To ensure there is an opportunity for a mitigation or remediation plan to be developed and assessed
  - Requires understanding the cause of name collisions such that a mitigation or remediation plan (or both) can be developed and assessed

Proposed Application Assessment Workflow and Timeline



Offramp Options

1 – Applicant decision only

2,3, & 4 – TRT identifies risk in its written report; notifies Board and Applicant who consider mitigation, remediation, or withdrawal; OR no risk concerns and assessment proceeds to next step

*: 90 days of data collection followed by time for report and decision

Proposed Assessment Workflow and Technical Review Team

- Need to be independent and neutral experts
- Technical expertise must include:
  - Knowledge and understanding of DNS specifications, provisioning, and operation
  - Knowledge and understanding of Internet infrastructure
    - Where it intersects with the DNS
    - Where it intersects with the usage of the DNS by applications and services
  - Ability to review and understand data collected (e.g., CDMs)
  - Ability to understand and assess risk
- Four responsibilities
  - Assess the visibility of name collisions
  - Document data, findings, and recommendation(s)
  - Assess mitigation and remediation plan
  - Emergency response

NCAP - Workflow and Neutral Service Provider

- Responsible for operation of the servers that will collect the CDMs
  - Data privacy concerns are still under discussion
  - Is this part of the Technical Review Team or a separate team?
  - If a separate team, could there be more than one?
- Four responsibilities
  - Operate Passive Collision Assessment environment
  - Operate Active Collision Assessment environment
  - Log processing and analysis preparation for TRT
  - Emergency response

NCAP - How to Participate

- Join the discussion group
  - https://docs.google.com/forms/d/1PDIX6sMIdP4vLn1LLuefxsup78mLM0iDb8ybWhIw2T4/edit

- Study 2 report nearing completion
  - Findings and Recommendations still in progress
  - Target is Public Comment before end of 2023

DNSSEC DS Automation Work Party

Steve Crocker and Peter Thomassen

Motivation

- **Registries and registrars play a critical role in the DNSSEC ecosystem**
  - Their internal DNSSEC operations are mostly automated today
- However: **not much progress for automation of DS record provisioning**
  - **Especially** when the child uses a **third-party DNS service**
  - **Critical functionality** for glitch-free provider transfer + multi-signer setups → **missing piece**
- About 10 ccTLDs / 2 registrars / 1 RIR maintain DS records automatically
  - Also, authenticated bootstrapping (child: 3 DNS operators; parent: 2 ccTLDs, 1 registrar)
- There is a gap in the gTLD space: **no automation** which leads to disparate and ad hoc processes
- **Note:** The scope of the SSAC's work is facilitating efficient DS provisioning **for signed zones**
  - not: signing all zones

Key Findings (draft)

- In the registry-registrar-registrant (RRR) model, **when DNS service is provided by the registrar, the key change and subsequent DS update can be administered "internally"**, such as in direct interaction by the registrar with the registry via EPP.
- [... Otherwise], **DS records are typically deployed using the manual deployment method**, i.e., *Registrant Pull & Push*. This particularly applies to cases where the RRR model is in use, and **DNS service is not provided by the Registrar**.
- The manual method usually involves registrants submitting key information to their registrar, who in turn submits it to the registry. This first part of this process can be **onerous and error-prone**, and is often perceived as **frustrating and difficult**.

Current Thinking

- The SSAC is working on a report that will encourage the creation of **industry best practices for DNSSEC DS automation**
- ICANN Org and thought leaders in the gTLD Ry/Rr community should **begin studying how to support DS automation**
  - There are potential policy implications for uniform adoption of DS automation
- For automation to work smoothly, several aspects need to be considered:
  - Scalability (Are parent-side scans impractical? Can notifications from the child improve it?)
  - Safety measures (e.g., acceptance checks, DS TTL policies)
  - Resolving submissions by multiple parties (e.g., CDS/CDNSKEY vs. manual submission)
  - Automation in the presence of locks
  - Reporting of significant changes and errors
  - Consistency (e.g., CDS vs. CDNSKEY)
- These should be addressed, and ideally be handled consistently across TLDs
  - Above issues starting to get addressed by IETF (e.g., draft-ietf-dnsop-generalized-notify)

Registrar NS Management Work Party

Gautam Akiwate

Registar NS Management - Scope

- Building on the risks identified in the paper ***Risky BIZness: Risks Derived from Registrar Name Management***
- Exploring the risks that emerge from the expiration of domains that other domains rely on for authoritative name service
- The SSAC is also investigating options for detection, remediation for domains that are currently exposed, and operational practices that will prevent new exposures
- For each options to mitigate current exposures and prevent new exposures the SSAC is reviewing
  - ***Benefits*** of each option to registrars, registries, and registrants
  - ***Burdens*** to registrars, registries, and registrants
  - ***Residual risk*** if the option is implemented

Registar NS Management - Options to Remediate Currently Exposed Domains

- Registrants:
  - Can directly update name server records through their registrar.
  - The main challenge is unawareness of their domain's exposure.
- Registrars:
  - Equipped to identify and bulk remediate exposed domains.
  - Can perform periodic checks and reconcile nameservers used.
  - Faces challenges like legal liability and the massive scale of operations.
- Registries:
  - Capable of making bulk changes but generally reluctant unless the request comes from the sponsoring registrar.
- Third Party:
  - Might defensively register vulnerable name server domains.
  - ICANN could potentially facilitate this type of defensive registration.

Registar NS Management - Options to Prevent New Exposure

Delete Host Object:

- Relax registry requirements to allow host object deletion and the registrar would issue an EPP request to delete the host object

Rename to empty.as112.arpa:

- Involves using a shared sacrificial name server in empty.as112.arpa.
- Doesn’t necessitate coordination among zones.
- Ensures that specific name server domains won’t be registered by others.

Special Use TLD (e.g., .invalid):

- Utilize a reserved TLD, such as .invalid, for naming sacrificial name servers.
- ICANN might create a dedicated TLD like .sacrificial for this use.

Sinkhole Name Server Names (Per-Registrar):

- Registrars create sinkhole domains for hosting a sacrificial name server.

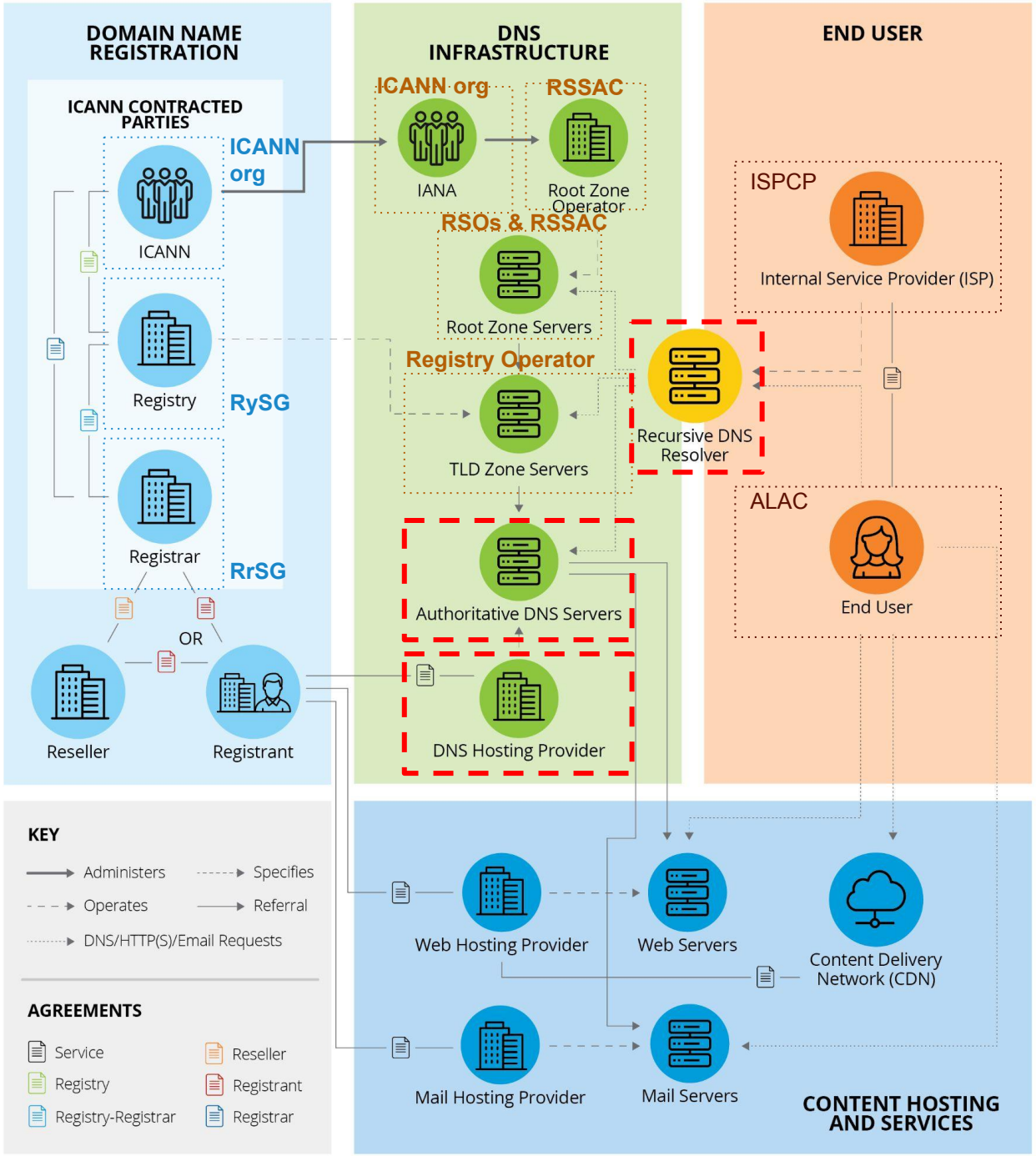
Sinkhole Name Server Names (Global/Community):

- Registrars utilize a third-party service provider for a global sinkhole name server to cut costs and potentially reduce risks.
- ICANN Org may select an entity or itself manage this name server.

Notification + Delete Host Object:

- Leverage a pull-based DNS protocol and provide a notification method.
- Enable notifications for changes to the database affecting domains to avoid dangerous inconsistencies.

Discussion on ICANN home for underrepresented groups



- How can ICANN ensure that all relevant voices have adequate representation within policymaking bodies?
  - ***DNS operators (see diagram):*** DNS operations often are run by entities not typically represented by ICANN constituencies - evolution from primarily being operated by ISPs
  - ***Security practitioners:*** currently in PSWG and SSAC. PSWG and SSAC are not policymaking bodies.
  - ***Other technological stakeholders:*** e.g. Internet of Things (IOT) operators, cloud computing vendors. These groups may have different interests in how identifier systems evolve and impact others in the DNS

Underrepresented group

Discussion on ICANN home for underrepresented groups

- Is there a place for these groups in the GNSO?
- Should their voices be part of the policymaking process?
- What proactive steps can ICANN take to reach out to the 'missing' stakeholders and ensure they have a seat at the table?

Achieving fit-for-purpose outcomes in the ICANN multistakeholder model

Fit-for-purpose Outcomes

Topic for SSAC's joint meeting with the ICANN Board: achieving fit-for-purpose outcomes in a multistakeholder model environment

- The SSAC is considering how to effectively integrate SSR considerations into the global public interest framework.
- The goal is to equip the ICANN community with useful, relevant guidelines to incorporate SSR considerations early and throughout the policy development lifecycles.

Brainstorming Questions

- Are there objective ways to answer the questions in the Global Public Interest toolkit?
- Should the assessment that a policy recommendation aligns with the public interest be included in the duties of any working group making policy recommendations?
- What happens when policy outputs from the multistakeholder model result in programs or policies that are not effective?
- The current public interest categories for ICANN policy and practices are “Neutral, Objective, Responsive, Accountable, and Fair. Would it make sense to add “effective” to this list?
- Should there be a dedicated entity or judge within ICANN to ascertain if a policy recommendation aligns with the public interest?