ICANN 78 ANNUAL GENERAL MEETING

ICANN 25 1998–2023

IANA Stewardship Transition 7 2016–2023

SSAC Activities Update

Rod Rasmussen, SSAC Chair
October 2023

Agenda

- SSAC Overview
- SSAC Chair and Vice Chair Elections for 2023
- Name Collision Analysis Project
- SSAC Work Parties
- Tracking ICANN Top Priorities
- SSAC New Member Outreach
- Q&A

Security and Stability Advisory Committee (SSAC)

Who We Are

- **38** Members
- Appointed by the ICANN Board

What We Do

Role: Advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

What is Our Expertise

- Addressing and Routing
- Domain Name System (DNS)
- DNS Security Extensions (DNSSEC)
- Domain Registry/Registrar Operations
- DNS Abuse & Cybercrime
- Internationalization (Domain Names and Data)
- Internet Service/Access Provider
- ICANN Policy and Operations

How We Advise

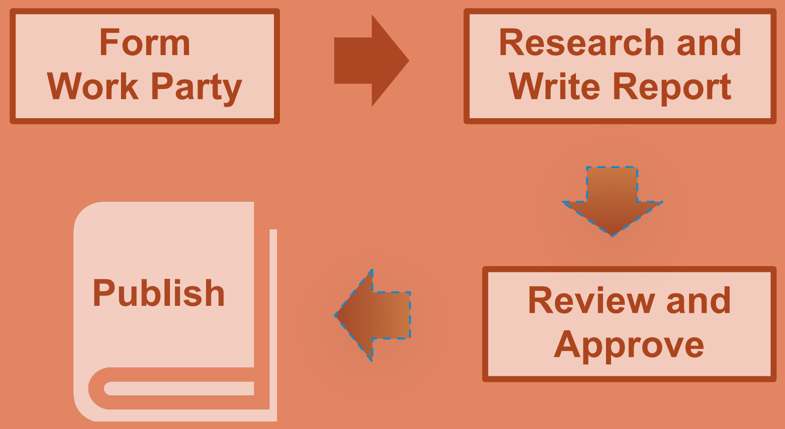
121 Publications since 2002

Security and Stability Advisory Committee (SSAC)

ICANN’s Mission & Commitments

- Ensure the stable and secure operation of the Internet's unique identifier systems.
- Preserve and enhance the administration of the DNS and the operational stability, reliability, security, global interoperability, resilience, and openness of the DNS and the Internet.

SSAC Publication Process



Form Work Party

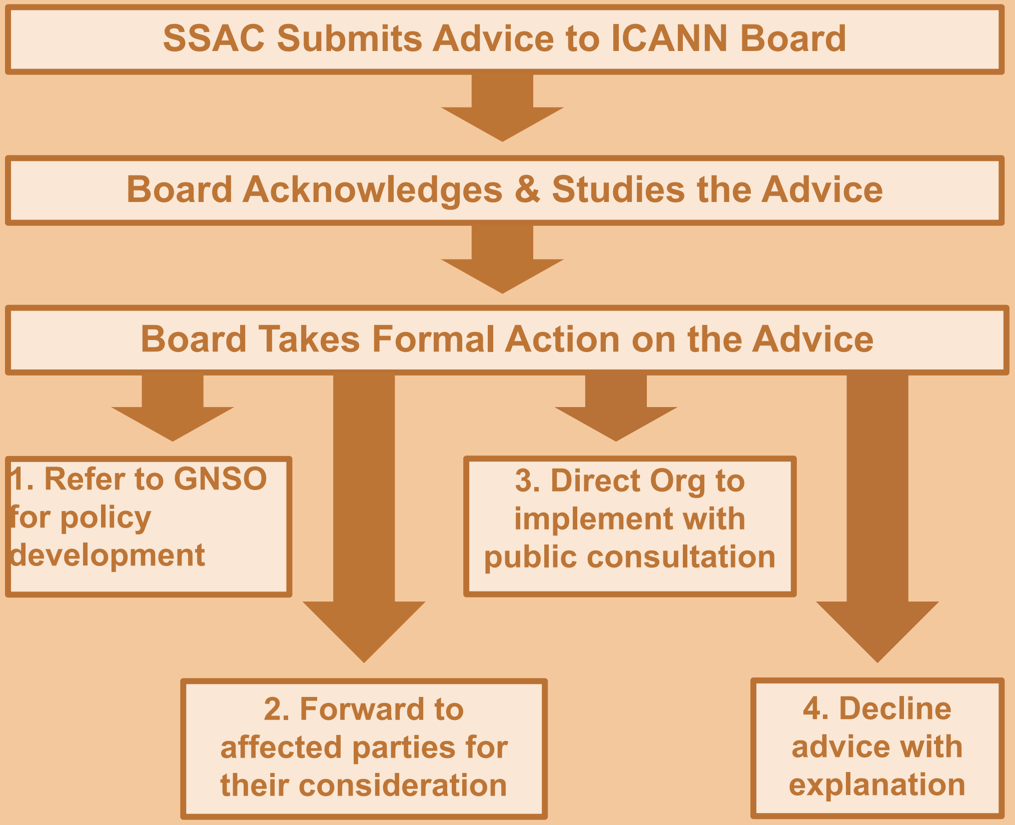
Research and Write Report

Review and Approve

Publish

Consideration of SSAC Advice

(to the ICANN Board)



SSAC Submits Advice to ICANN Board

Board Acknowledges & Studies the Advice

Board Takes Formal Action on the Advice

1. Refer to GNSO for policy development

2. Forward to affected parties for their consideration

3. Direct Org to implement with public consultation

4. Decline advice with explanation

Security and Stability Advisory Committee (SSAC)

Recent Publications

[SAC121]: SSAC Briefing on Routing Security

[SAC120]: SSAC Input to GNSO IDN EPDP on Internationalized Domain Name Variants

Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References

ICANN | SSAC

Security and Stability Advisory Committee

Outreach

🌐 ssac.icann.org and SSAC Intro: www.icann.org/news/multimedia/621

f www.facebook.com/pages/SSAC/432173130235645

▶ SAC067 SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition and SAC068 SSAC Report on the IANA Functions Contract: www.icann.org/news/multimedia/729

SSAC Chair and Vice Chair Elections for 2023

- SSAC has selected Ram Mohan as the next SSAC Chair, to be confirmed by the Board at the AGM

- SSAC has also selected Tara Whalen as the next SSAC Vice Chair

- Barry Leiba and Jeff Bedser will also be serving on the SSAC Admin Committee in addition to Ram and Tara

- Chair and Vice Chair terms officially begin on 1 January 2024 and last through 31 December 2026

Name Collision Analysis Project

Matt Thomas and Suzanne Woolf

NCAP Background

- ICANN Board tasked SSAC to conduct studies to present data, analysis and points of view, and provide advice to the Board on name collisions
  - Specific advice regarding .home/.corp/.mail
  - General advice regarding name collisions going forward
- Studies to be conducted in a thorough and inclusive manner that includes other technical experts
  - 25 discussion group members, including 14 SSAC work party members
  - 23 community observers

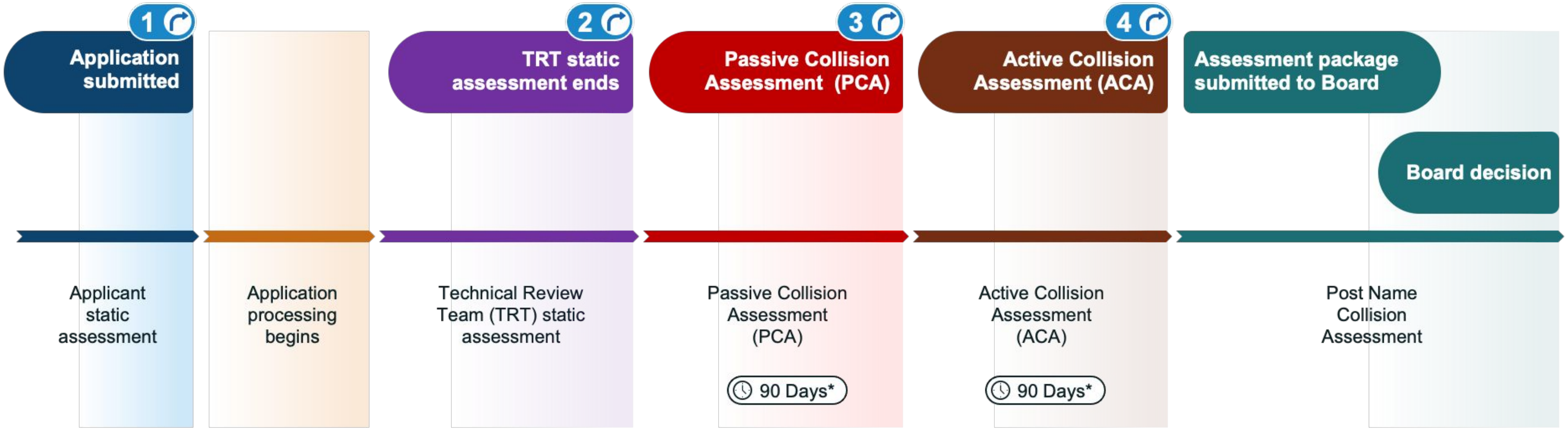
Recent Publications from Completed Work

- 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



1 Application submitted

2 TRT static assessment ends

3 Passive Collision Assessment (PCA)

4 Active Collision Assessment (ACA)

Assessment package submitted to Board

Board decision

Applicant static assessment

Application processing begins

Technical Review Team (TRT) static assessment

Passive Collision Assessment (PCA)

90 Days*

Active Collision Assessment (ACA)

90 Days*

Post Name Collision Assessment

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 - How to Participate

- Join the discussion group
  - https://docs.google.com/forms/d/1PDIX6sMldP4vLn1LLuefxsup78mLM0iDb8ybWhlw2T4/edit

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

Updates on SSAC Work Parties

Current Work Parties

- Name Collision Analysis Project
- DS Automation
- Evolution of DNS Resolution
- Registrar NS Management
- DNSSEC and Security Workshops (Ongoing)
- Membership Committee (Ongoing)

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
- **<u>Note</u>:** 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**.

DS Provisioning: Registrant Pull & Push Method

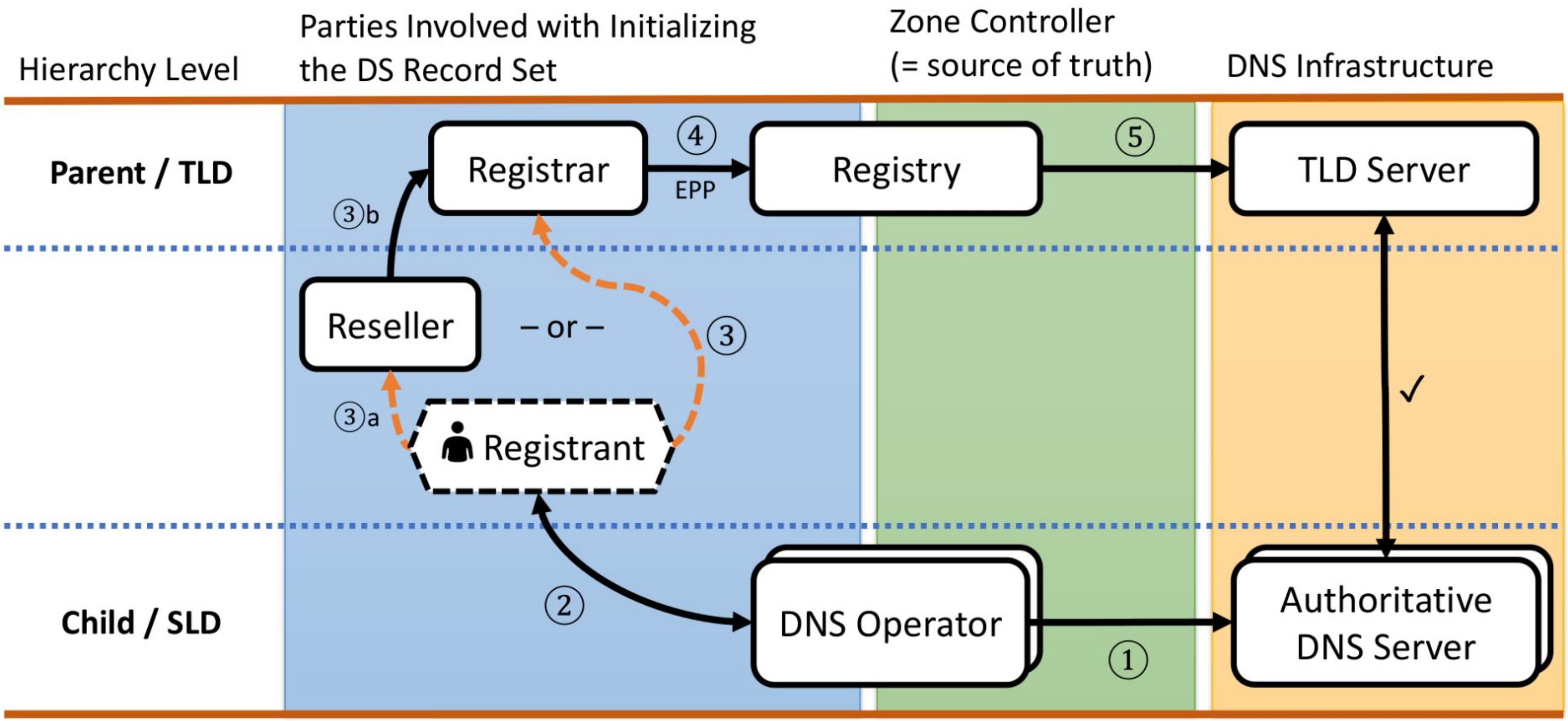
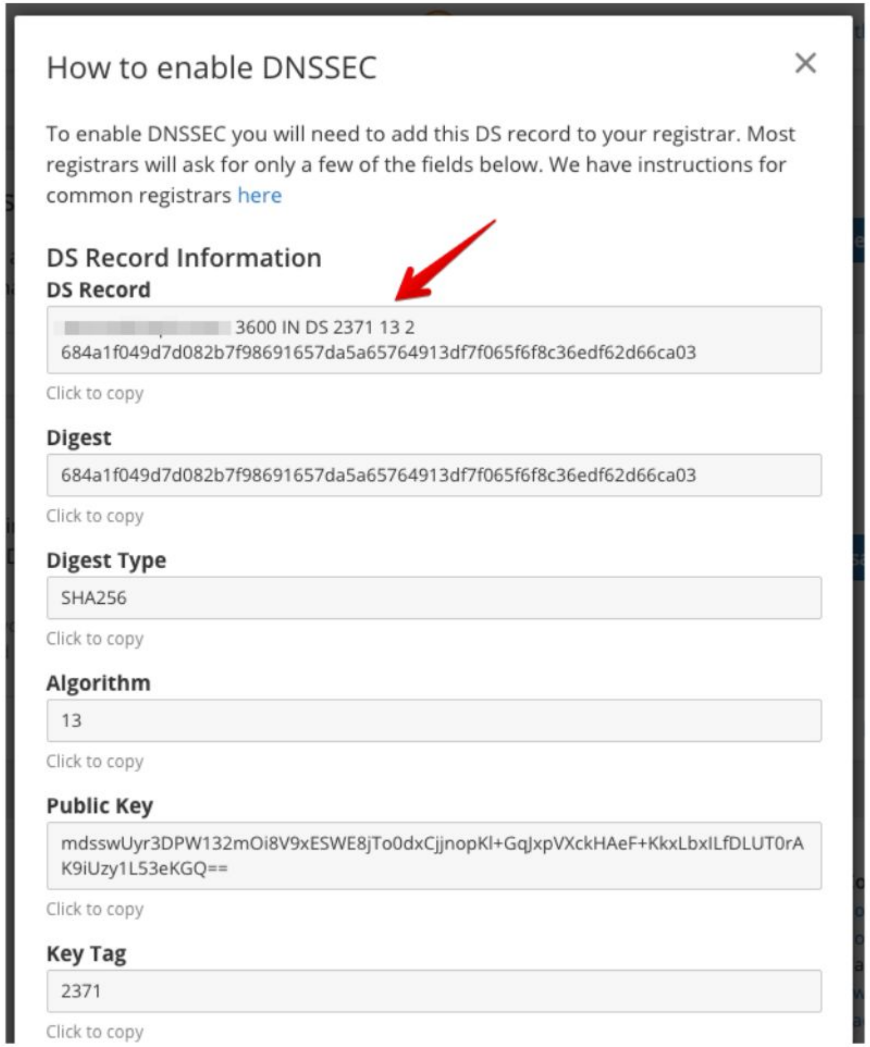


Figure 2. Entities and their relationships during DS provisioning.

DNS Provider Interface



How to enable DNSSEC

To enable DNSSEC you will need to add this DS record to your registrar. Most registrars will ask for only a few of the fields below. We have instructions for common registrars here

DS Record Information

DS Record

[redacted] 3600 IN DS 2371 13 2
684a1f049d7d082b7f98691657da5a65764913df7f065f6f8c36edf62d66ca03

Click to copy

Digest

684a1f049d7d082b7f98691657da5a65764913df7f065f6f8c36edf62d66ca03

Click to copy

Digest Type

SHA256

Click to copy

Algorithm

13

Click to copy

Public Key

mdsswUyr3DPW132mOi8V9xESWE8jTo0dxCjjnopKl+GqJxpVXckHAeF+KkxLbxILfDLUT0rA K9iUzy1L53eKGQ==

Click to copy

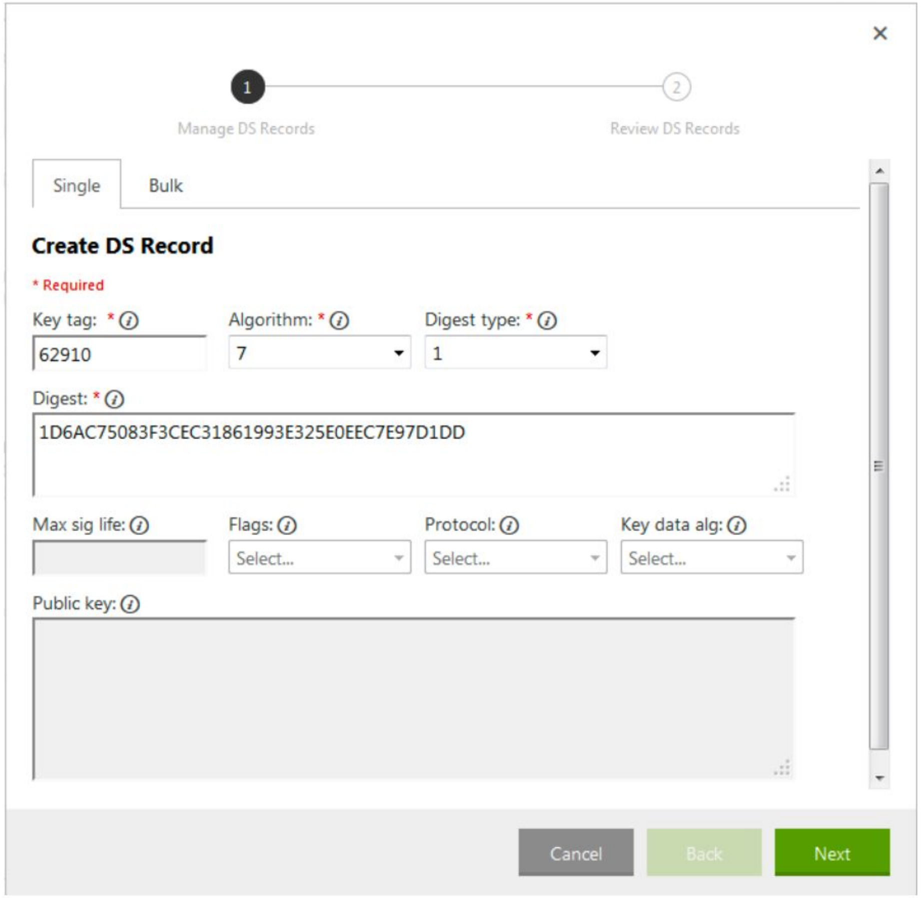
Key Tag

2371

Click to copy

Figure 5. A DNS Operator's Interface for Registrant to Retrieve DS Record Information

Registrar Interface



Create DS Record

* Required

Key tag: * ⓘ 62910

Algorithm: * ⓘ 7

Digest type: * ⓘ 1

Digest: * ⓘ 1D6AC75083F3CEC31861993E325E0EEC7E97D1DD

Max sig life: ⓘ

Flags: ⓘ Select...

Protocol: ⓘ Select...

Key data alg: ⓘ Select...

Public key: ⓘ

Figure 8. Another registrar's interface for registrants to create DS Record. It requires separate input of the various DS record components. Note that the numerical value of the Digest Type can be selected from a drop-down field (current selection: 1), whereas the Child DNS operator's interface used a mnemonic ("SHA256") for this field. The registrant would have to know that the correct choice in this case is 2. – The input fields in the lower half of the screenshot are all irrelevant.

Additional Key Findings (draft)

- The need for human intervention for setting up a domain name is **not aligned with registrants' expectations**, and **does not scale** sufficiently well when maintaining large domain portfolios.
- Non-automatic DS management has emerged as a major obstacle for broad deployment of DNSSEC. For example, studies have shown that **40% of registrants** who actively **requested zone signing** [...] did **not subsequently configure DS records** for their domain. As the number of domains [...] increased by a factor of three during the observation period [...], the fraction without DS records **remained stagnant at about 40%**.*

* See Figure 8 of https://conferences.sigcomm.org/imc/2017/papers/imc17-final53.pdf and related discussion.

DS Provisioning: Direct Interaction of Child & Parent (I)

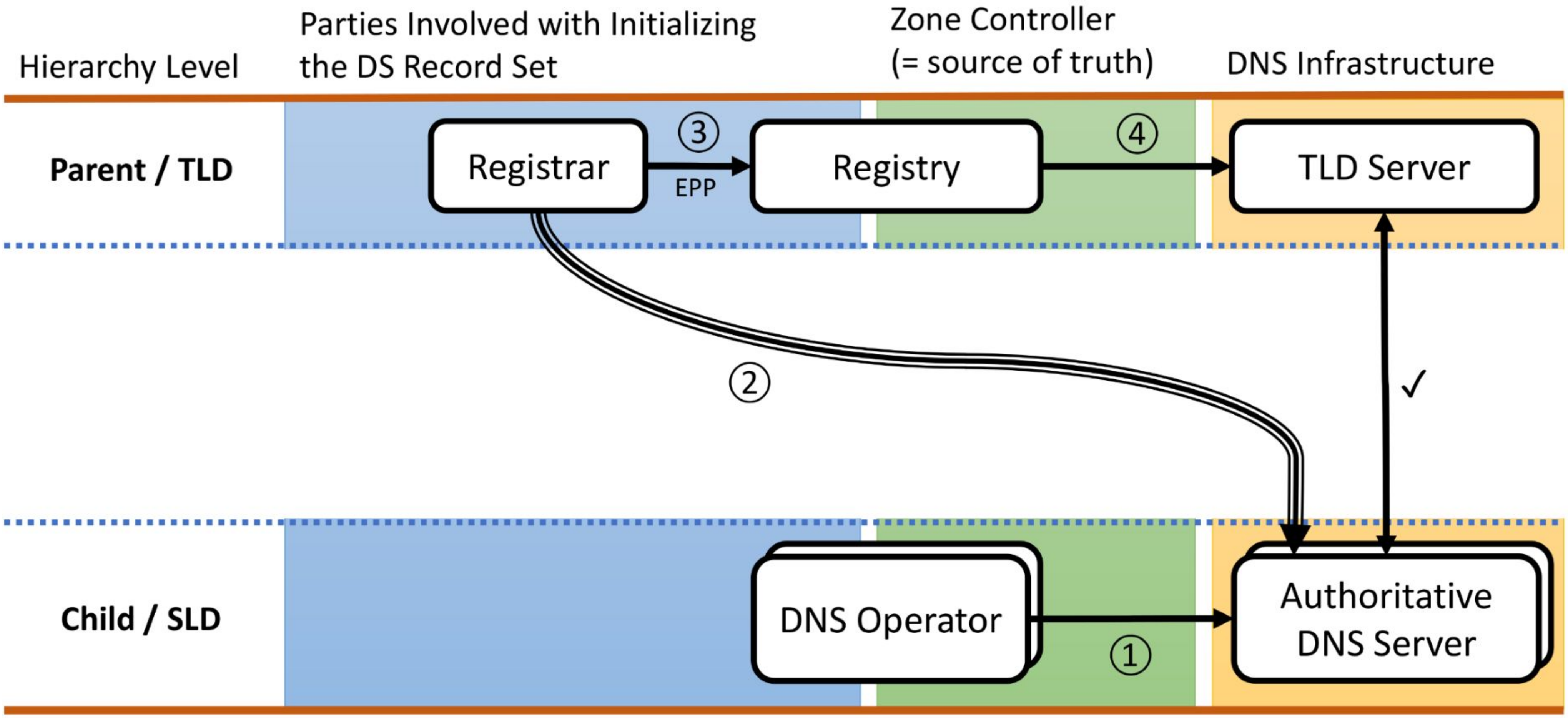


Figure 3. Simplified entity relationships during DS initialization with CDS/CDNSKEY

DS Provisioning: Direct Interaction of Child & Parent (II)

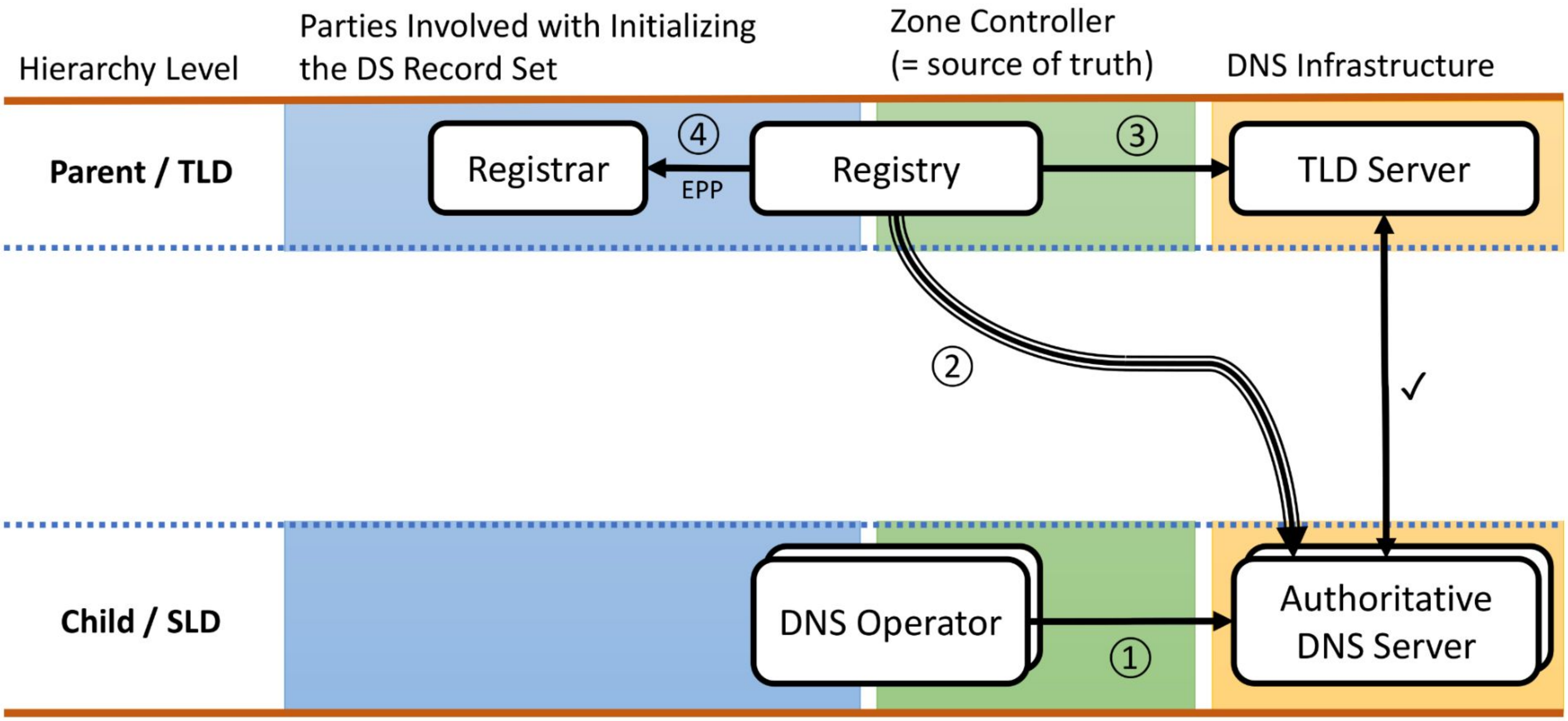


Figure 4. Simplified entity relationships during DS initialization with CDS/CDNSKEY

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**
- 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

James Galvin

Registar NS Management - Problem Statement

- **The Problem:**
  - Unintended byproduct of longstanding undocumented registrar practices
  - Use of third-party name servers whose domain expires
  - EPP + Registry policies prevent removal of such expired domains
    - Goal was to protect other domains that depend on this expired domain
- **Registrar Workaround**
  - Rename NS host objects that are subordinate to expired domain
  - Rename NS using a new non-existent domain name in another TLD operated by a different registry
    - Allows removal of domain
  - Creates new attack surface: someone could register the nonexistent domain name
  - Over the last 9 years: > 512K domains have been implicitly exposed to resolution hijacking

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.

Evolution of DNS Resolution Work Party

Barry Leiba

Evolution of DNS Resolution Work Party

- **Goal:** Discuss technologies that are changing the nature of DNS resolution and the implications of these changes on the DNS namespace, provisioners, and operators of DNS infrastructure
- **Scope:** Explore the current state and evolving nature of DNS resolution with a focus on SSR issues related to alternative naming technologies (e.g., blockchain)
- **Deliverable:** An SSAC report that analyzes the effects of relevant new technologies. The report may also suggest methods to measure the implications of these technologies, and possibly propose instrumentation to provide measurements where there may be instrumentation gaps.
- **Intended Audience:** The ICANN community and the greater Internet community. This includes network operators, DNS software implementers, policy makers, and concerned Internet users.

Evolution of DNS Resolution - Findings

- Names that are syntactically equivalent to DNS names are being used in alternate protocols and different contexts. This is partly because applications written for DNS names easily support syntactically equivalent names, and also because users are already comfortable with this naming syntax.

- There are motivations to evolve Internet naming just as there are motivations to maintain the status quo. Wholesale replacement of the DNS as the default naming system for the Internet is very unlikely, therefore any successful alternative naming system must coexist with it for the foreseeable future.

- Relatively few users appreciate that a top-level domain can sometimes signal a change from the default naming system (i.e., global DNS). For example, many Tor users know that .ONION designates resolution via Tor, but very few users are aware of more than a couple of top-level domain names that signal a different resolution context should be used. It is likely that more will come over time.

Evolution of DNS Resolution - Findings (continued)

- Alternative protocols are increasingly using overlapping names. Therefore the same name will yield a different response depending on which resolution context is used.

- Mechanisms are being implemented at ICANN and the IETF to facilitate coordinated use of the domain namespace on a voluntary basis.

- Ambiguity in Internet name resolution can give unexpected results and therefore undermines trust in the integrity of services on the Internet.

- As domain names become less visible and less conspicuous, they become less a part of the user experience. Users still have a reliance on the underlying names to connect to expected services.

Tracking ICANN Top Priorities

Rod Rasmussen

Tracking ICANN Top Priorities

- **DNS Abuse**
  - See SAC115: SSAC Report on an Interoperable Approach to Addressing Abuse Handling in the DNS
- **Access to registration data**
  - See SAC118v2: SSAC Comments on Initial Report of the Expedited Policy Development Process (EPDP) on the Temporary Specification for gTLD Registration Data Team – PHASE 2A
  - See SAC101v2: SSAC Advisory Regarding Access to Domain Name Registration Data
  - SSAC sent active representatives to participate in the GNSO's EPDP on the Temp Spec
  - SSAC is working on a pending comment regarding Urgent Requests in the gTLD Registration Data Policy
- **Adding new gTLDs**
  - See SAC114: SSAC Comments on the GNSO New gTLD Subsequent Procedures Draft Final Report
  - See Addendum to SAC114: Additional Context for Recommendation 1, Recommendation 3, Recommendation 7, and Additional References

Topics of Interest/Possible New Work

- DNSSEC Assessment and examining the potential for DNSSEC as a universal trust anchor
- Long-term implications of namespace expansion
- Technical implications of forced removal or transfer of a TLD
- Examining datasets available from ICANN for use in the investigation of SSR-related issues that fall within SSAC's remit
- Assess the effectiveness of the eventual DAAR 2.0 in detecting and reporting domain abuse
- Assess the role of PSL in domain name security, privacy, and DNS operations
- Review and update advice on EBERO
- Review of the number of allocatable variants in the LGR

SSAC Skills and Potential New Member Outreach

Julie Hammer

SSAC Member Skills

- The skills of SSAC members span the following categories:
  - Domain Name System
  - Security
  - Abuse
  - Root Server System
  - IP Addressing/Routing
  - Registration Services
  - Internationalized Domain Names
  - Information Technology
  - Non-Technical (e.g., legal, risk management, business skills)
- The SSAC Skills Survey is used to document the skills of all existing and potential SSAC Members

SSAC New Member Outreach – Important Priorities

- SSAC is looking for motivated professionals who have skills in the SSAC skills categories and, in particular, expertise or background in:
  - ISP operations
  - Large-scale network architecture and design
  - Large-scale Registrar Operations
  - Cloud/hosting experience
  - Browser Development/Testing
  - Mobile Apps Development/Testing
  - Low bandwidth resource constrained Internet connectivity (eg IoT, SCADA)
  - Red Team experience
- The SSAC is interested in increasing membership from Africa, Latin America, and Asia-Pacific
- The SSAC is interested in increasing membership from an academic background

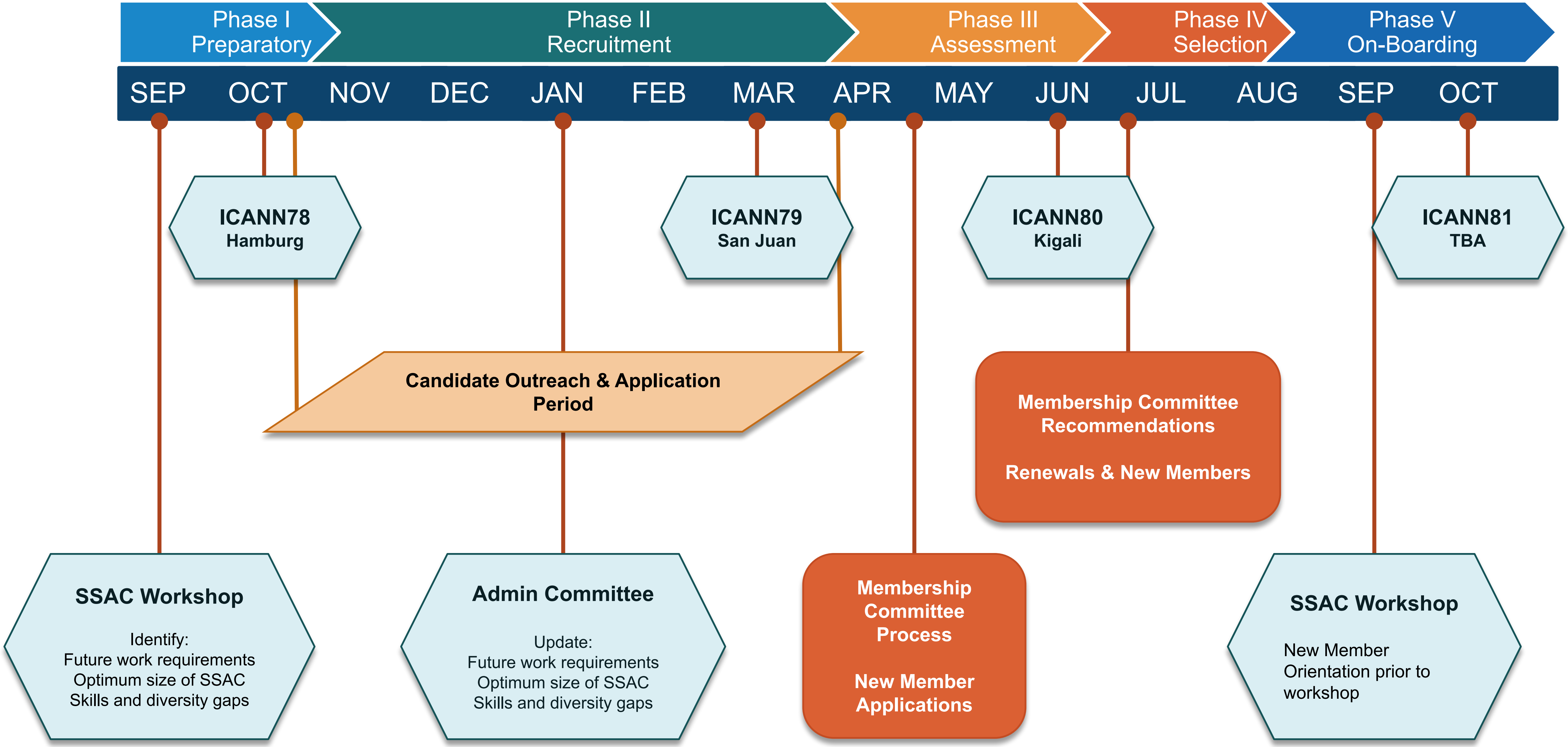
SSAC New Member Outreach – Other Priorities

- SSAC is also looking for professionals who have skills, expertise or background in:
  - Large-scale network operations
  - Large-scale open recursive resolvers
  - Large-scale measurement
  - Expertise in non-Latin based scripts
  - Innovators in new TLDs
  - Certificate Authority
  - Cryptography
  - Denial of Service
  - Root Server Operations
  - Software Engineering
  - Regulatory Legal Experience

SSAC Members - Expectations

- **Behave respectfully**
    - Interact with each other and with other members of the ICANN community with respect, honesty and open-mindedness
    - Be sensitive to all cultures
    - Be receptive to new or alternative ideas
- **Attend SSAC meetings**
    - Monthly teleconferences, work party meetings, ICANN meetings, and the annual SSAC workshop
- **Contribute in Work Parties** according to your skills in the subject area
        - ‘Expert’ or ‘High’: lead, draft text, contribute ideas and views
        - ‘Medium’: participation welcomed, review text
        - ‘Low’ or ‘None’: participation not expected
- **Volunteer for Representational Roles**
    - e.g. NomCom, Cross-Community Groups, Liaisons, etc.
- **Protect SSAC Confidentiality**
    - All SSAC deliberations are confidential unless explicitly made public

SSAC Membership Outreach – 2024 Timeline



Phase I Preparatory

Phase II Recruitment

Phase III Assessment

Phase IV Selection

Phase V On-Boarding

SEP OCT NOV DEC JAN FEB MAR APR MAY JUN JUL AUG SEP OCT

ICANN78
Hamburg

ICANN79
San Juan

ICANN80
Kigali

ICANN81
TBA

Candidate Outreach & Application Period

Membership Committee Recommendations

Renewals & New Members

SSAC Workshop

Identify:
Future work requirements
Optimum size of SSAC
Skills and diversity gaps

Admin Committee

Update:
Future work requirements
Optimum size of SSAC
Skills and diversity gaps

Membership Committee Process

New Member Applications

SSAC Workshop

New Member Orientation prior to workshop

SSAC Contact for Potential New Members

Individuals who are interested in enquiring about SSAC membership should:

- Review information on the SSAC Public Website: https://www.icann.org/groups/ssac,
- Contact any member of SSAC Support Staff, or
- Send an email to ssac-staff@icann.org