



SSAC Activities Update

Patrik Fältström, SSAC Chair | ICANN-53 | June 2015

Agenda

1

Overview

2

Recent
Achievements

3

Work in Progress
and Future
Milestones

4

SAC070 and
SAC071

5

Registrant
Protection/
Credential
Management

6

Community
Interaction

Security and Stability Advisory Committee (SSAC)

WHO WE ARE



35 Members

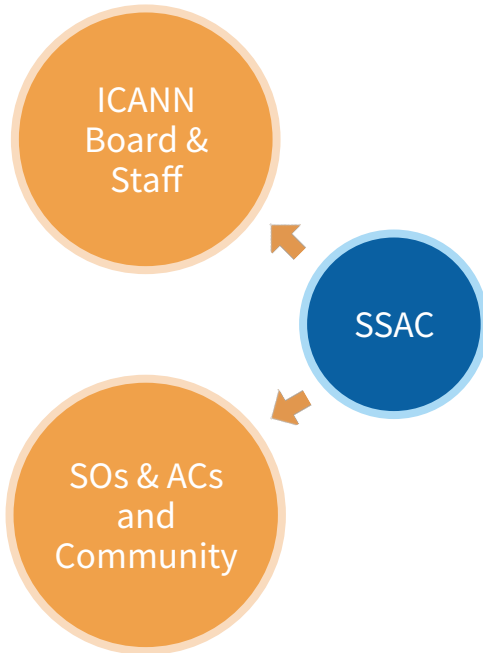


Appointed by the ICANN Board

WHAT WE DO

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

WHO WE ADVISE



HOW WE ADVISE

71 Publications since 2002



Reports



Advisories



Comments

OUTREACH

Security and Stability Advisory Committee (SSAC)

PUBLICATIONS PROCESS

Form Work Party



Research & Writing



Review & Approve



Publish



CURRENT WORK PARTIES

New gTLDs Program Review
Registrant Protection
DNSSEC Workshops
Document Management Solutions
Tracking Board Advice
Membership Committee

RECENT PUBLICATIONS

[SAC071]: SSAC Comments on Cross Community Working Group Proposal on ICANN Accountability Enhancements (08 June 2015)
[SAC070]: SSAC Advisory on the Use of Static TLD / Public Suffix Lists (29 May 2015)
[SAC069]: SSAC Advisory on Maintaining the Security and Stability of the IANA Functions Through the Stewardship Transition (10 Dec 2014)

OUTREACH



<https://ssac.icann.org>



<https://www.facebook.com/pages/SSAC/432173130235645>



SSAC Intro: <https://www.icann.org/news/multimedia/621>



SAC067 & 68: <https://www.icann.org/news/multimedia/729>

A world map composed of a network of white dots and lines on an orange background. The dots represent nodes and the lines represent connections, forming a complex web that outlines the continents.

Work in Progress and Future Milestones

Patrik Fältström

Current Work in Progress

- ⦿ New gTLDs: Mid-Course Correction, Collisions, Timing of Next Round
- ⦿ Registrant Protection/Credential Management
- ⦿ Cross-Community Working Group on Auction Proceeds (with GNSO)
- ⦿ DNSSEC Sessions at ICANN Meetings (Ongoing)
- ⦿ Document Management Tools (Internal Guidance)
- ⦿ Board Advice Tracking (Ongoing)
- ⦿ Membership Committee (Ongoing)

Future Milestones



- DNSSEC Workshop at ICANN 53
 - ✓ SAC070: SSAC Advisory on the Use of Static TLD/Suffix Lists
 - ✓ SAC071: Comments on Cross Community Working Group Proposal on ICANN Accountability Enhancements
- Advisory on Registrant Protection/Credential Management
- Advisory on New gTLDs Program Review
 - DNSSEC Workshop at ICANN 54



**SAC070: SSAC Advisory on
the Use of Static TLD / Public
Suffix Lists**

Patrik Fältström

What is Public Suffix List?

- Public suffix: “a domain under which multiple parties that are unaffiliated with the owner of the Public Suffix domain may register subdomains.”
- Examples:

www.icann[org] www.bbc[co.uk]

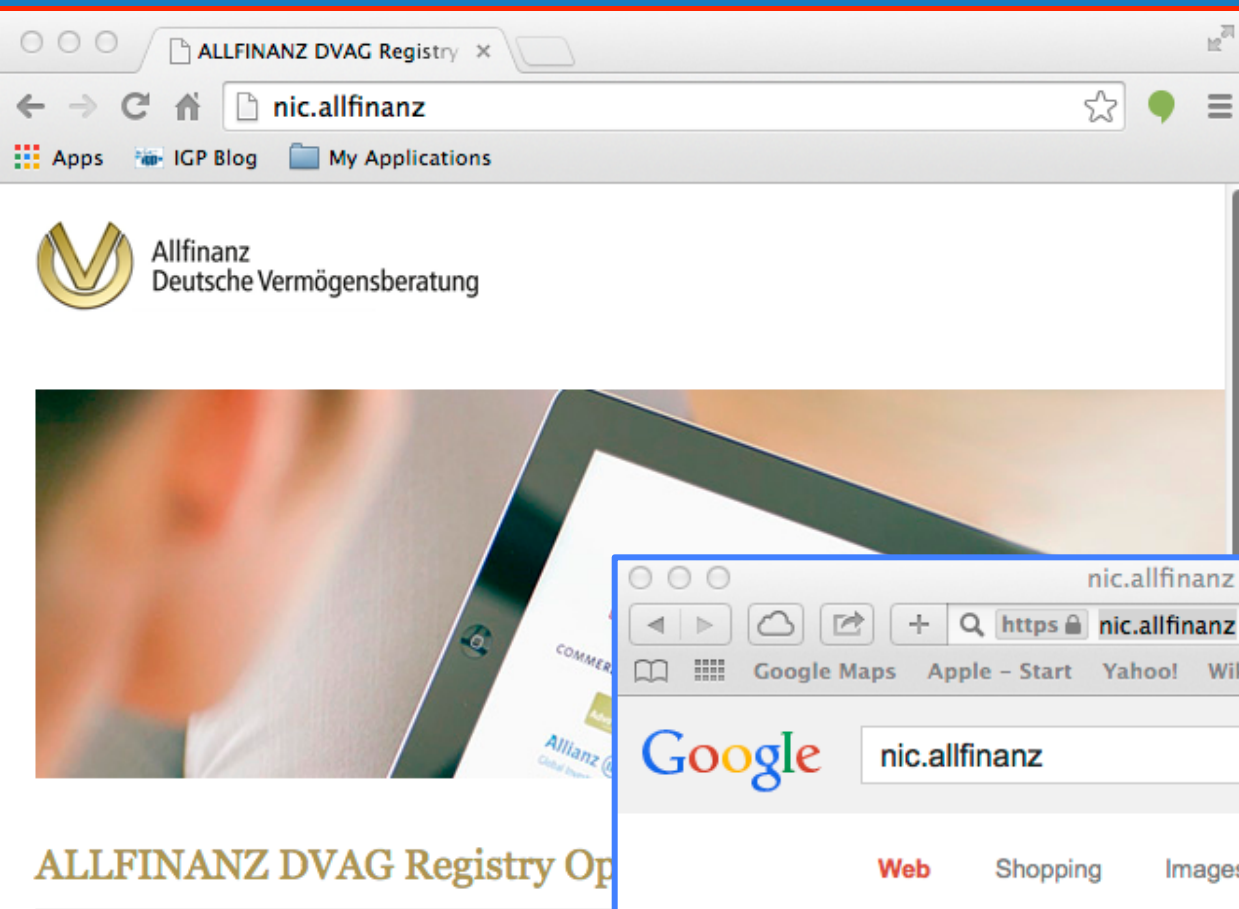
www.pps[k12.pa.us]

- No programmatic way to determine the boundary where a Domain Name System (DNS) label changes stewardship from a public suffix.
- Tracking the boundary accurately is critically important for security, privacy, and usability issues in many systems and applications, such as web browsers.

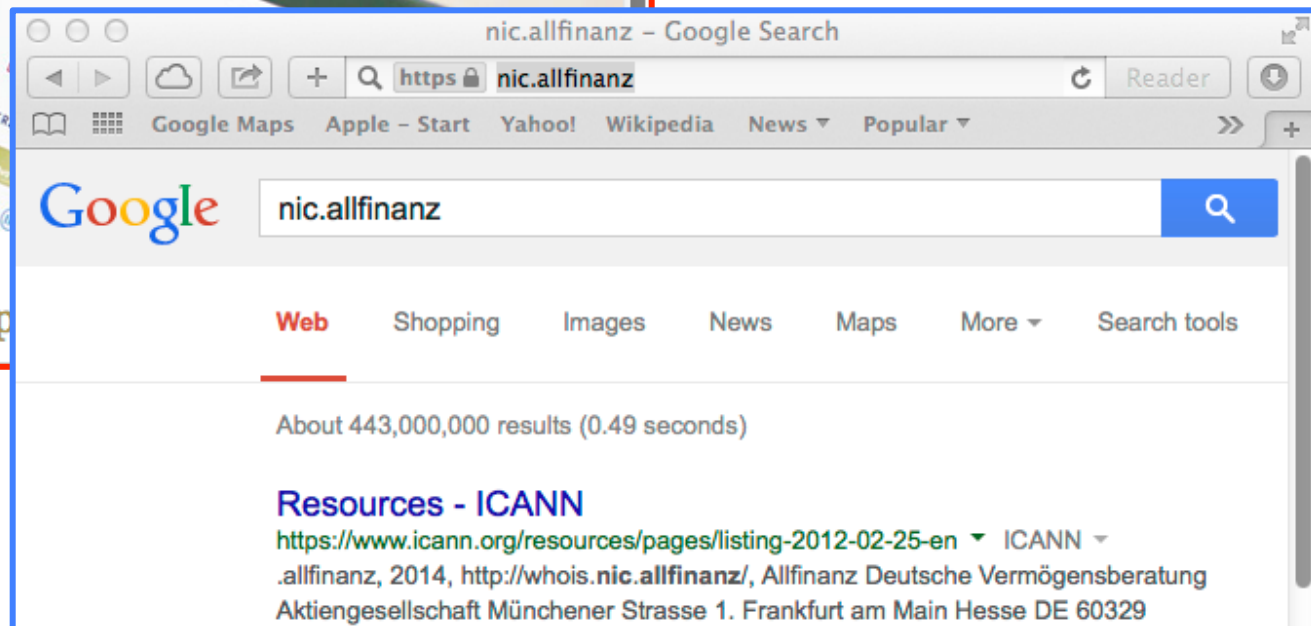
Why Are Public Suffix Lists Important?

| Use Case | Descriptions | Applications |
|---------------------|---|---|
| Cookie Setting | Decide whether a cookie should be allowed to set for a suffix of a given domain | Mozilla Firefox, Google Chrome, Safari, Opera |
| SSL Certificates | Decide whether to issue or accept an SSL wildcard certificate for *.public.suffix. | Certificate Authorities |
| Navigability | Decide whether a browser should attempt to navigate to a given URL without consulting DNS | Google Chrome |
| TLD Validation | Determine the validity of TLDs in a domain name | Web forms, programming language libraries |
| Domain Highlighting | Decide which part of a domain to highlight | Mozilla Firefox |

Inconsistent Suffix Lists Usage



← Google Chrome
37.0.2062.124



Apple Safari
7.0.6 9537.78.2 →

SAC070 Findings

PSL is a design compromise between convenience of use and accuracy of its contents

No consensus definition of “public suffix” and associated terms and PSL is used for several purposes having to do with administrative boundaries in the DNS

Lack of accountability mechanisms for ensuring PSLs are produced in a consistent, fair, unbiased manner with recourse for individuals or organizations that may have an issue

Knowledge gap exists between registries and maintainers of the public suffix lists regarding the processes and responsibilities for changes and additions to the Mozilla PSL and other PSLs

No universal library, framework, tool, etc. for PSL use and implementers do not use PSL entries consistently in software or other services

SAC070 Findings, Cont.

No universal library, framework, tool, etc. for PSL use and implementers do not use PSL entries consistently in software or other services

Great variation of latency for implementing PSL changes in software applications and Internet services

General lack of authentication and other standard security controls for the content and transmission of PSLs from maintainers to users

Due to the wide variety of use cases for PSLs, it may be difficult to create a one-size-fits-all PSL for all audiences covering any application or usage

If new gTLDs use public suffixes similarly to some ccTLDs, which may include more than one public subdomain, the impact to any PSL could be significant

SAC070 Recommendations

| Parties to take Action | Recommendation |
|----------------------------|--|
| IETF | Standardize PSL alternatives (IETF DBOUND WG) |
| IETF | Develop consensus definition of “public suffix” and other associated terminology |
| ICANN & Mozilla Foundation | Collaboratively create informational materials that can be given to TLD registry operators about Mozilla PSL |
| ICANN | Encourage the software development community to develop and distribute programming and operating system libraries for PSL. |

SAC070 Recommendations, cont.

| Parties to take Action | Recommendation |
|------------------------|---|
| Application developers | Use canonical file format and modern authentication protocols as specifications |
| Application developers | Replace proprietary PSLs with Mozilla PSL and the proposed IANA PSL |
| IANA | Host a PSL containing information about the domain within the registries with which IANA has direct information |
| ICANN | Explicitly include the use and actions related to the PSL as part of the work related to universal acceptance |



**SAC071: SSAC Comments on Cross
Community Working Group Proposal
on ICANN Accountability
Enhancements**

Patrik Fältström

SSAC Charter: The SSAC advises “the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.”

The SSAC:

- ⦿ Has neither been given nor sought any standing for its advice other than that it be evaluated on its merits and adopted (or not) according to that evaluation by the affected parties.

SSAC Comments, Cont.

The SSAC:

- ⦿ Has no comment at this time on whether or not a legal structure is required or desirable to compel ICANN and the Board to respond to the SSAC's advice.
- ⦿ Is concerned about the way in which the proposed new SO/AC Membership Model might affect the way in which the SSAC operates, considering its narrow focus on security and stability matters and its reluctance to become involved in issues outside that remit.

The SSAC:

- ⦿ Expects that the community will adopt an organizational structure that recognizes the role and importance of high-quality expert advice on security and stability.
- ⦿ Notes the relatively short time available for consideration of the draft proposal and reserves the right to make additional comments as further details are developed.

A world map composed of a network of white dots and lines on an orange background. The dots represent nodes and the lines represent connections, forming a complex web that outlines the continents.

Registrant Protection/ Credential Management

Ben Butler and Merike Kaeo

- ⦿ Augment previous work done in SAC040 and SAC044 by defining best practice guidelines for comprehensive credential lifecycle management of domain names.
- ⦿ Target audience:
 - ⦿ Wider ICANN community;
 - ⦿ Registrars, registries, registrants;
 - ⦿ Software developers of applications/tools;
 - ⦿ DNS service providers; and
 - ⦿ Webhosting and email service providers.

⦿ Will address:

- ⦿ Credential lifecycle best practices for creating, distributing, storing, renewing, transferring, revoking and recovering name credentials;
- ⦿ All credentials used to provide authentication of an identity (registrant or authorized administrator of registrar or registry); and
- ⦿ Any relevant policy issues that can support or hinder credential management.

Document Content

- ⦿ What is the problem?
- ⦿ Recent attack issues
- ⦿ Credential types
- ⦿ Credential use:
 - ⦿ Entity using credential;
 - ⦿ Credential validator;
 - ⦿ Purpose of credential.
- ⦿ Credential management life cycle today
- ⦿ Practical checklist/credential management life cycle best current practices
- ⦿ Recommendations

Timeline

Q1 &
Q2
2015

- Develop first draft
- Consult with community at ICANN 52
- Consult with community at ICANN 53

Q3
2015

- Develop Final draft
- Possible further consultation
- Publish Advisory

Ongoing Validation

- ⦿ Review of Sections 4 and 5 (use of credentials and how current lifecycle is managed)
- ⦿ What issues or problems do you encounter?
 - ⦿ Successes/challenges with password requirements and 2FA
 - ⦿ Successes/challenges with registrant engagement
 - ⦿ Successes/challenges with storage and backups of credentials
 - ⦿ Successes/challenges with distribution of credentials
 - ⦿ Successes/challenges of re-issuing/renewing/revoking credentials
- ⦿ Are there areas where tools or software development would aid in credential security/management?
- ⦿ What are the challenges for small registrars?



Community Interaction

Patrik Fältström

Questions from the Community

- ⦿ How does the SSAC prioritize new work?
- ⦿ How does the SSAC address requests from the ICANN Board and the community?
- ⦿ How does the SSAC track the Board's response to SSAC advice?
- ⦿ How does the SSAC inform the community of its work?

Questions to the Community

- ⦿ Are the SSAC publications accessible and understandable:
 - ⦿ How is the length (long, short, just right?)
 - ⦿ How is the level of detail?
 - ⦿ Do the publications reach their audience?
- ⦿ How can the SSAC do a better job for the community?
- ⦿ What can the SSAC do differently?
- ⦿ What topics are missing from the current list of work parties?

A world map where the continents are defined by a complex network of white nodes and connecting lines, set against a dark blue background. The nodes vary in size and are densely packed in some areas, creating a digital or network-like appearance of the globe.

Thank you