SAC119
Feedback to the GNSO Transfer Policy Review PDP WG

A Comment from the ICANN Security and Stability Advisory Committee (SSAC)
5 August 2021

Preface

The Security and Stability Advisory Committee (SSAC) focuses on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., pertaining to the correct and reliable operation of the root zone publication system), technical administration matters (e.g., pertaining to address allocation and Internet number assignment), and registration matters (e.g., pertaining to registry and registrar services). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no authority to regulate, enforce, or adjudicate. Those functions belong to other parties, and the advice offered here should be evaluated on its merits. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any dissenting opinions or alternative views that are included at the end of the document.

Table of Contents

1 Introduction

The SSAC appreciates the opportunity to provide early input into the GNSO Transfer Policy Review Policy Development Process (PDP) Working Group (WG).[1] The SSAC believes that it is important for registrants to experience a secure, stable, and smooth transition when transferring registrations between registrars.

There are two specific security risks the SSAC would like to highlight.

- A registrant's domain name is at risk of experiencing a discontinuity of DNS resolution, and when DNSSEC is in use, a discontinuity of validation, during a registration transfer if the transfer of DNS services is not considered during the process.

- A registrant's domain name is at increased risk of being hijacked if the authInfo code is not managed according to best practice security principles.

2 Ensuring DNSSEC Operational Continuity

When a registrant bundles their DNS service with their registration, then it is essential that the transfer of DNS service be coordinated between the DNS service providers (who are most often the registrar when services are bundled) in order to ensure there is no discontinuity in DNS resolution (i.e., the registrant does not lose the ability to use their domain name).

When the domain name is DNSSEC-signed in the bundled scenario, there is an additional risk of failure to validate if the transfer is not properly coordinated. Best practice security principles would ordinarily treat a security failure more harshly than a non-existent domain, the consequences of which will vary by application.

These risks are substantially reduced during a registration transfer if a registrant uses a third party DNS service provider, one who is independent of the registration service provider. It is important to note that these risks are not specific to registration transfers; they are present whenever there is a change in DNS service providers.

The SSAC recommends the Transfer Policy Review Team consider these concerns and seek the necessary enhancements to the current process that will ensure a secure, stable, and resilient transfer solution in the best interest of the registrant.

[1] See GNSO Transfer Policy Review Policy Development Process Working Group (PDP WG) - Request for Early Input, https://community.icann.org/download/attachments/167543988/Transfer%20Policy%20Review%20PDP%20-%20Request%20for%20Early%20Input%20-%2030%20June%202021.pdf?version=1&modificationDate=1625057999000&api=v2

3 Uniform Use of authInfo Code

The role and significance of the authInfo code was changed dramatically with the introduction of the Temporary Specification for gTLD Registration Data.[2] The SSAC notes that it now functions predominantly as the sole authentication credential used to authorize an inter-registrar transfer. While the process appears to have been working for the past three years, it unfortunately exposes registrants to a domain hijacking vulnerability because the credential is not supported with best practice security principles, processes, or procedures. The SSAC recommends the Transfer Policy Review Team consider this concern and seek the necessary enhancements to the current process that will ensure a secure, stable, and resilient transfer solution in the best interests of the registrant.

The SSAC has previously spoken about registrants and the issues they face when using an authInfo code and transferring between registrars in SAC007,[3] SAC040,[4] SAC044,[5] and SAC074.[6]

In SAC007 the SSAC stated that, "Registrars have an obligation and strong business incentives to reduce the risk of domain hijacking and loss due to mishandling of names and registration information." As part of this obligation registrars should make the use of the Extensible Provisioning Protocol (EPP) authInfo code more uniform, and establish a uniform default setting of domain locks across registrars. The SSAC is supportive of these discussions being in scope and looks forward to a consensus resolution on these important issues from the GNSO Transfer Policy Review PDP WG.

The SSAC again talked about transfer policy in SAC040 in the context of measures registrars should take to protect registrants against account hijacking. SAC040 reiterated the advice given in SAC007.

SAC044 reiterated much of what the SSAC had already said on the subject in SAC007 and SAC040, yet directed towards registrants. Where SAC040 provided advice to registrars on what they should implement, or make more uniform, SAC044 provided similar advice to registrants on how best they can protect their domain names from hijacking. The Transfer Policy Review PDP WG may find this advice helpful as they consider the benefits to, and role of, registrants in a secure, stable, and resilient transfer process.

---

[2] See Temporary Specification for gTLD Registration Data, https://www.icann.org/resources/pages/gtld-registration-data-specs-en
[3] See SAC007: Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Actions
[4] See SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse
[5] See SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts
[6] See SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle

In SAC074, the SSAC built upon its previous work by providing additional advice to registrars. Specifically that registrars and registries follow Section 5 of ICANN's 2015 Inter-Registrar Transfer Policy for handling an authInfo code.[7] This report documents specific and anecdotal security concerns at registrars. Although not specifically stated in SAC074, it motivates a need for more uniform handling of the authInfo code. The Transfer Policy Review PDP WG may find issues highlighted in this report helpful as they consider changes to the handling of the authInfo code to create a more secure, stable, and resilient transfer process for registrants.

4 Acknowledgments, Statements of Interest, Dissents and Alternative Views, and Withdrawals

In the interest of transparency, these sections provide the reader with information about four aspects of the SSAC process. The Acknowledgments section lists the SSAC members and outside experts who contributed directly to this particular document, as well as ICANN org staff who facilitated the work. The Statements of Interest section points to the biographies of all SSAC members and invited guests, which disclose any interests that might represent a conflict—-real, apparent, or potential—-with a member's or invited guest's participation in the preparation of this Report. SSAC members participate as individuals, not as representatives of their employers or other organizations. SSAC consensus on a document occurs when the listed authors agree on the content and recommendations with no final objections from the remainder of the SSAC, with the exception of any dissenting opinions or alternative views.[8]

The Dissents and Alternative Views section provides a place for those individual members to describe any disagreement that they may have with the content of this document or the process for preparing it. The Withdrawals section identifies individual members who have withdrawn and recused themselves from discussion at any stage during the development of this report. Except for members listed in the Dissents and Alternative Views and the Withdrawals sections, this document has the consensus approval of all of the members of SSAC.

4.1 Acknowledgments

The committee wishes to thank the following SSAC members for their time, contributions, and review in producing this Comment.

SSAC members
Greg Aaron
Joe Abley
Steve Crocker
Patrik Fältström
John Levine

[7] See Policy on Transfer of Registrations between Registrars, https://www.icann.org/resources/pages/policy-transfers-2014-07-02-en
[8] See SSAC Operational Procedures v9.0, Section 1.1, https://www.icann.org/en/system/files/files/ssac-operational-procedures-v9.0-05jan20-en.pdf

James Galvin
Jonathan Spring

ICANN staff
Andrew McConachie (editor)
Danielle Rutherford
Kathy Schnitt
Steve Sheng

4.2 Statements of Interest

SSAC member biographical information and Statements of Interest are available at: https://www.icann.org/resources/pages/ssac-biographies-2021-01-07-en

4.3 Dissents and Alternative Views

There were no dissents or alternative views.

4.4 Withdrawals

There were no withdrawals.