James Gannon

Dublin, Ireland

28 August 2015

Root Zone KSK Rollover Plan
Comments of James Gannon

Introduction

James Gannon is a Security and Privacy expert based in Dublin, Ireland. With over 10 years experience in the Telecommunications, Media and Technology sector he advises clients on complex policy and implementation issues in international settings. Mr Gannon is current a member of the Non-Commercial Stakeholders Group (NCSG) in ICANN, however these comments are submitted in an individual capacity.

Overview

We thank the design team for their effort on this critical issue. We note that a KSK rollover scenario was discussed by Design Team L of the CWG-Stewardship effort, this scenario was based on the recommendations of the KSK Operator Function Termination Plan that was the subject of a DIDP request in March 2015. The DIDP can be viewed at the following location https://www.icann.org/resources/pages/20150312-1-2015-03-25-en.

While the work of the KSK Rollover Design Team was a separate effort we note that this document will be a valuable addition to the work of Design Team L and the CWG-Stewardship.

The following comments are as a result of an analysis primarily in the context of the IANA Stewardship and its potential impact on the plan developed by the design team and is not intended to constitute a technical analysis of the content of the document.

Summary

We agree with the substance of the recommendation of the Design Team however we note that in the recommendations at a high level have not accounted for the potential role of the Post Transition IANA (PTI) entity that is envisioned by the CWG-Stewardship. However we understand the the design team has chosen not to account for this potential change in the

IANA structure prior to the CWG-Stewardship recommendations being adopted by the ICANN board and the NTIA.[1] Out of an abundance of caution we offer the following suggestions for the Design Team to consider in their continued planning:

1. We suggest that the following risk scenario may be considered by the Design Team:

   1.1. Risk: Concerns over the stability of the root zone KSK system in the event that the IANA functions are no longer performed by ICANN or its PTI subsidiary and instead are performed by an independent IANA Functions Operator as a result of the outcome of a separation process in the future.

2. We suggest that the design team set out a clear differentiation between the responsibilities of ICANN and the responsibility of the IFO in any rollover plan, this will allow for the plan to be interchangeable and would represent a plan that will endure the potential implementation of PTI and also any future change in the IANA functions operator.

3. SSR Department staff and a new IFO? We note that a number of responsibilities are assigned to the SSR department staff of ICANN, we suggest that the design team may wish to examine if any issues may arise in the event that the IFO is no longer an internal department of ICANN (i.e PTI) or if the IFO is an independent entity from ICANN entirely. The design team may come to the conclusion that the roles and responsibilities of the SSR staff may remain as proposed however until such an analysis is documented there may be uncertainty as to this matter.

4. SSAC/RSSACs relationship with a new IFO? While potentially a matter for the SSAC/RSSAC and not for the design team we note that similar to our concerns about the SSR Department staff that the SSAC and RSSACs roles with regards to the PTI or a future IFO have not been identified and that the design team may wish to consider the roles and responsibilities of these groups in a post transition environment.

---

[1] §1 Overview, of the report.

5.   With regards to Recommendation 7 of the design team we wish to thank the teams for their caution in adopting new crypto standards in such a critical area, we note our agreement with the 5 year timeline proposed by the design team.

6.   For the purposed of clarity we suggest that Recommendation 9 of the design team be modified to read "…ICANN in cooperation with the RZM partners *and the IANA Functions Operator,* should…"

Finally we wish to thank the design team for a comprehensive and well constructed plan which places the security, stability and resiliency of the root at the core of the process.

Regards,
James Gannon
Security and Privacy Policy
Cyber Invasion Ltd
Dublin, Ireland