Network Working Group
Internet-Draft
Updates: 6781 (if approved)
Intended status: Informational
Expires: January 22, 2017

M. Pounsett
Rightside Group, Ltd.

July 21, 2016

Change of Operator Procedures for Automatically Published DNSSEC Zones
draft-pounsett-transferring-automated-dnssec-zones-00

Abstract

Section 4.3.5.1 of [RFC6781] "DNSSEC Operational Practices, version 2" describes a procedure for transitioning a DNSSEC signed zone from one (cooperative) operator to another. The procedure works well in many situations, but makes the assumption that it is feasible for the two operators to simultaneously publish slightly different versions of the zone being transferred. In some cases, such as with TLD registries, operational considerations require both operators to publish identical versions of the zone for the duration of the transition. This document describes a modified transition procedure which can be used in these cases.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 22, 2017.

Copyright Notice

Table of Contents

1. Introduction

The process described in "DNSSEC Operational Practices, version 2" ([RFC6781]), section 4.3.5.1 for cooperating DNS operators to move a DNSSEC signed zone cannot be followed in all cases. When operators are moving a zone that is automatically published and/or changes rapidly, such as with a TLD or any other zone published from a registration database, it may not be feasible for the operators to publish different versions of the same zone.

In these cases, it would be necessary for one or both operators to have the capability to add, remove, or alter arbitrary records inline along the zone transfer path (such as modifying the NSSet, and stripping RRSIGs). It cannot be assumed that this capability exists, since few (if any) common DNS implementations include these functions, and many custom implementations exist whose feature sets cannot be predicted.

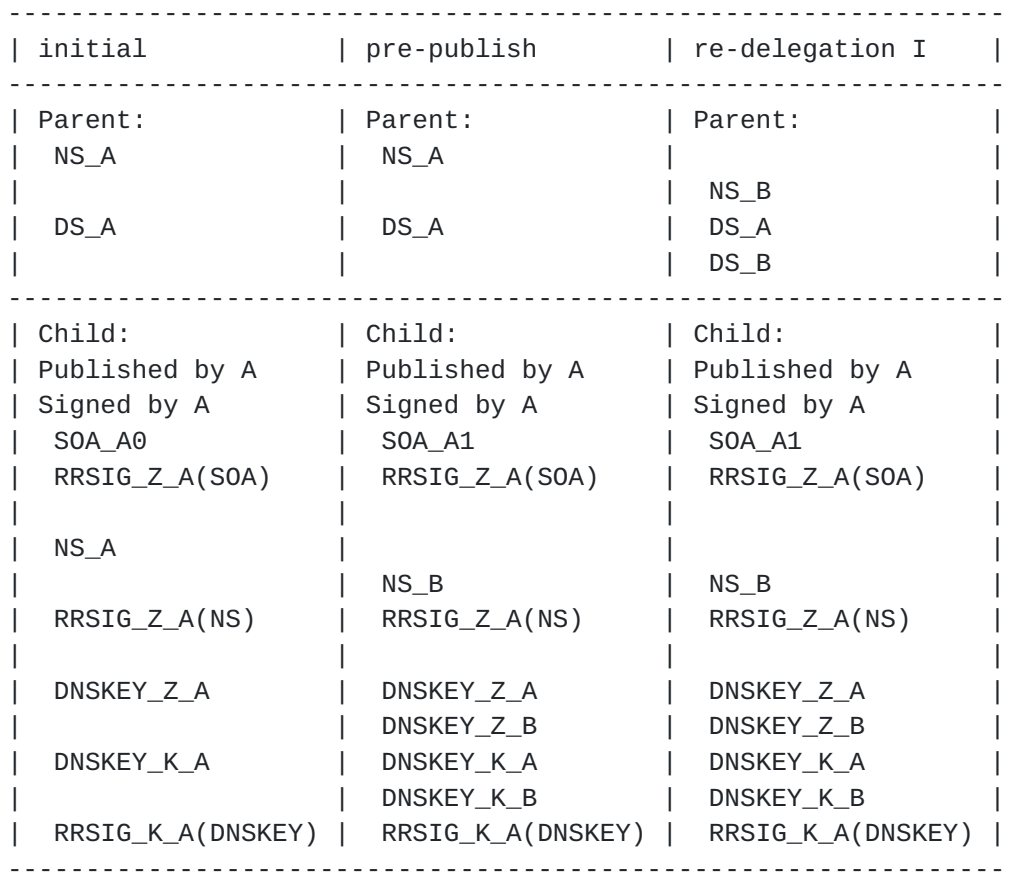
As a result, it must be assumed that operators moving an automatically generated or frequently updated zone must be able to publish an identical zone while transitioning it from one operator to another.

2. Changing Between Cooperating DNS Operators

In this scenario, it is assumed that the operators will not exchange any private key material, but are otherwise fully cooperative. It is also assumed that the zone publishing process will be transferred between operators independently of the DNS operations. The simplest case is to transition the publishing process after the DNS operations move has been completed, and is the order that is assumed in this document, although the reverse order is possible. During the transition, the losing operator will provide the zone contents to the gaining operator by some automatic means (typically zone transfer).

The transition uses a pre-publish KSK and ZSK rollover, whereby the losing operator pre-publishes the public KSK and ZSH of the gaining operator. Partway through the transition, the losing operator stops signing the zone and begins providing an unsecure zone to the gaining operator, who begins signing. Once that is done, the gaining operator continues to post-publish the public keys of the losing operator until the TTLs of the original RRSIGs expire.

In the timeline below, the losing operator is operator A, and the gaining operator is operator B. Records representig data generated by each operator are appended with the operator letter. DNSKEY_Z is a ZSK, and DNSKEY_K is a KSK. RRSIG_K is the RRSIG generated with DNSKEY_K.



Rollover for Cooperating Operators, Steps 1-3

signing-migration	re-delegation II	post-migration
Parent: NS_B DS_A DS_B	Parent: NS_B DS_B	Parent: NS_B DS_B
Child: Published by A Signed by B SOA_A2 RRSIG_Z_B(SOA) NS_B RRSIG_Z_B(NS) DNSKEY_Z_A DNSKEY_Z_B DNSKEY_K_A DNSKEY_K_B RRSIG_K_B(DNSKEY)	Child: Published by A Signed by B SOA_A2 RRSIG_Z_B(SOA) NS_B RRSIG_Z_B(NS) DNSKEY_Z_A DNSKEY_Z_B DNSKEY_K_A DNSKEY_K_B RRSIG_K_B(DNSKEY)	Child: Published by B Signed by B SOA_B0 RRSIG_Z_B(SOA) NS_B RRSIG_Z_B(NS) DNSKEY_Z_B DNSKEY_K_B RRSIG_K_B(DNSKEY)

Rollover for Cooperating Operators, Steps 4-6

3. Informative References

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <http://www.rfc-editor.org/info/rfc6781>.

Author's Address

Matthew Pounsett
Rightside Group, Ltd.

Email: matt@conundrum.com