Authors: U. Wisser   S. Huque
         The Swedish Internet Foundation   Salesforce
                    DNSSEC automation

Abstract

   This document describes an algorithm and a protocol to automate
   DNSSEC multi-signer [RFC8901] "Multi-Signer DNSSEC Models" setup,
   operations and decomissioning. It primarily deals with Model 2 of
   the Multi-Signer specification, where each operator has their own
   distinct KSK and ZSK sets (or CSK sets). It makes use of [RFC8078]
   "Managing DS Records from the Parent via CDS/CDNSKEY" and [RFC7477]
   "Child-to-Parent Synchronization in DNS" to accomplish this.

Status of This Memo

Copyright Notice

Section 4.e of the Trust Legal Provisions and are provided without
warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

[RFC8901] describes the necessary steps and API for a multi-signer
DNSSEC configuration. In this document we will combine [RFC8901]
with [RFC8078] and [RFC7477] to define a fully automatable algorithm
for setting up, operating and decomissioning of a multi-signer
DNSSEC configuration.

One of the special cases of multi-signer DNSSEC is actually the
secure change of DNS operator.

1.1. Out-Of-Scope

In order for any multi-signer group to give consistent answers
across all nameservers, the data contents of the zone also have to
be synchronized (in addition to infrastructure records like NS,
DNSKEY, CDS etc). This content synchronization is out-of-scope for
this document.

1.2. Notation

Short definitions of expressions used in this document

signer An entity signing a zone

multi-signer group A group of signers that sign the same zone

1.3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Use Cases

2.1. Running a multi-signer setup

As described in [RFC8901] a multi-signer DNSSEC configuration has some challenges that can be overcome with the right infrastructure and following a number of steps for setup and operation.

In this document we describe how all of the steps in the multi-signer DNSSEC setup can be automated. That is, all except the initial trust between involved signers.

2.2. Secure change of name server operator

Changing the name server operator of a DNSSEC signed zone can be quite a challenge. Currently the most common method is temporarily "going insecure". This is a bad choice for security, and a bad choice for users relying on the security of the zone.

Changing name server operators can be considered to be a transient special case of multi-signer DNSSEC operations. A new operator joins the old operator in a temporary multi-signer setup. Once that is completed, the old operator leaves the multi-signer setup.

3. Algorithm

3.1. Setting up a new multi-signer group

The zone is already authoritatively served by one DNS operator and is DNSSEC signed. For full automation both the KSK and ZSK or CSK must be online.

This would be a special case, a multi-signer group with only one signer.

3.2. Configuration

The following configuration has to be made for any signer of the
multi-signer group before joining the group. These steps are not
automated by this draft.

1. The signers own keys (the keys the signer has the private part
   of)

2. The NS records in the zone

3. An established trust to the multi-signer group

3.3. A new signer joins the multi-signer group

3.3.1. Prerequisites

The new signer

1. has a working setup of the zone, including DNSSEC signing.

2. uses the same algorithm for DNSSEC signing as the multi-signer
   group uses.

3.3.2. Steps for joining

1. a new signer joins the group

2. Exchange of keys, after this step all signers must have the
   DNSKEY set of all other signers of the group

3. Calculate CDS/CDNSKEY set

4. All signers put the ZSK of all other signers in their DNSKEY
   set.

5. All signers publish their CDS/CDNSKEY set

6. Wait for parent to pick up DS updates

7. Remove CDS/CDNSKEY set from all signers

8. Wait 2 time maximum TTL of DS at parent and DNSKEY at all
   children

9. Exchange of NS set, after this step all signers must have the
   NS set of all other signers

10. Compile new complete NS set with NS records from all signers

11. Compare to NS set at parent

12. If parent is different, publish CSYNC record with NS and A and
    AAAA bit set.

13. Wait for parent to pick up changes

14. Remove CSYNC record from all signers

3.4. A signer leaves the multi-signer group

1. Signal to all other signers to remove the leaving signer's NS
   records

2. Compile new complete NS set with NS records from all signers

3. Compare to NS set at parent

4. If parent if different, publish CSYNC record with NS and A and
   AAAA bit set.

5. Wait for parent to pick up changes

6. Remove CSYNC record from all signers

7. Wait 2 times TTL of maximum NS TTL from parent and all signers

8. Signal all other signers leaving of multi-signer group

9. Stop answering queries

10. Remaining signers remove ZSK of leaving signer from their
    DNSKEY set

11. Remaining signers recalculate DNSKEY set

12. Calculate CDS/CDNSKEY set

13. All signers put the ZSK of all other signers in their DNSKEY
    set.

14. All signers publish their CDS/CDNSKEY set

15. Wait for parent to pick up DS updates

16. Remove CDS/CDNSKEY set from all signers

4. Automation

Automation of the necessary steps described in the last section can
be divided into two main models, centralized and decentralized. Both
have pros and cons and any zone operator should chose wisely.

4.1. Centralized

In a centralized model the zone operator will run software that
executes all steps necessary and controls all signers.

4.2. Decentralized

In the decentralized models all signers will communicate with each
other and execute the necessary steps on their instance only. For
this signers need a specialized protocol to communicate
configuration details that are not part of the zone data.

5. Acknowledgements

6. IANA Considerations

7. Security Considerations

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
           RFC2119, March 1997, <https://www.rfc-editor.org/info/
           rfc2119>.

[RFC7477] Hardaker, W., "Child-to-Parent Synchronization in DNS",
           RFC 7477, DOI 10.17487/RFC7477, March 2015, <https://
           www.rfc-editor.org/info/rfc7477>.

[RFC8078] Gudmundsson, O. and P. Wouters, "Managing DS Records from
           the Parent via CDS/CDNSKEY", RFC 8078, DOI 10.17487/
           RFC8078, March 2017, <https://www.rfc-editor.org/info/
           rfc8078>.

9. Informative References

[RFC8901] Huque, S., Aras, P., Dickinson, J., Vcelak, J., and D.
           Blacka, "Multi-Signer DNSSEC Models", RFC 8901, DOI
           10.17487/RFC8901, September 2020, <https://www.rfc-
           editor.org/info/rfc8901>.

Authors' Addresses

Ulrich Wisser
The Swedish Internet Foundation
Box 92073
SE-12007 Stockholm
Sweden

Email: ulrich@wisser.se

URI: https://www.internetstiftelsen.se

Shumon Huque
Salesforce
415 Mission Street, 3rd Floor
San Francisco, CA 94105
United States of America

Email: shuque@gmail.com