MUSIC : Multi-Signer Controller

Status Update

Johan Stenstam Roger Murray

The Swedish Internet Foundation

September 19, 2022

MUSIC: A Multi-Signer Controller

Since autumn 2021 we have been working on a project that what we call **MUSIC**.

This is a Proof of Concept implementation of the processes described in the "multi-signer" Internet-Draft by Shumon Huque and Ulrich Wisser. For an introduction, please see the presentation, "Making Music with DNSSEC", from the DNSSEC Workshop during the March 2022 ICANN meeting.

MUSIC has been working for sometime, both in a "manual" and a "automatic" mode, but as always when you do something the first time you run into issues and learn.

Handling Combined Signing Keys (CSKs)

As described in the multi-signer draft, **MUSIC** synchronizes ZSKs between multiple "signers".

- The KSK is not needed, since it doesn't sign the data in the zone, only some RRsets at the zone apex. I.e. the KSKs are only needed to ensure that the correct CDS records are published for subsequent publication of the correct DS records in the parent zone.

Problem: However, this logic does not cater to the existence of signers that don't use the KSK/ZSK split but rather use a single CSK, i.e. a combined signing key.

Handling CSKs, cont'd

There are basically two ways to deal with this issue.

Alternative 1: Instead of assuming a KSK/ZSK split (and only synchronizing the latter), do a careful, intelligent analysis of what DNSKEY is used for what purpose.

Alternative 2: Just synchronize all DNSKEYs across all signers.

Handling CSKs, cont'd

We implemented **Alternative 2**, with the following reasoning:

- Pro: this is simple.
- Pro: it works.
- Pro: it makes DNSViz happy ;) .
- Con: leads to a larger `DNSKEY` RRset than necessary.

DNSKEY RRset Size Considerations

As observed already in RFC8901 on Multi-Signer DNSSEC Models the use of any multi-signer process will lead to a DNSKEY RRset with more keys than otherwise.

- This is one of the reasons for only synchronizing ZSKs and not KSKs.

This prompts the question of whether the current implementation of MUSIC (where all DNSKEYs are synchronized) will have issues due to the DNSKEY RRset becoming large enough to be "problematic".

We do not believe this to be the case, because:

- The migration to using elliptic curve DNSKEYs, which are significantly smaller.
- The KSK/ZSK split is essentially an artifact of the DS update in the parent being "complicated". With the emergence of automated DS updates (via CDS/CDNSKEY) it seems likely that over time CSK will replace KSK/ZSK as the primary DNSKEY semantic.

Handling CDS Digest Algorithms

Some signers generate their own CDS records which can be problematic.

Current status: MUSIC creates a CDS RRset including both SHA-256 and SHA-384 and updates the signers.

The signers are then polled for consistency before continuing.

Rewrite of Database Layer

The database code has been rewritten to allow for simultaneous changes.

Next Steps

- testing
- bug fixes
- testing
- rinse
- repeat

Code: https://github.com/DNSSEC-Provisioning/music.git

Contact: music@internetstiftelsen.se

Thanks!

Johan and Roger