

Towards Distributed Multi-Signer Control

Steve Crocker

Edgemoor Research Institute

A Quick Look Back

- Automation of transfers
- Continuous operation of multiple DNS signers (RFC 8901)
- Let's build it
- .SE design and implementation of MUSIC
- Multi-signer ad hoc group meeting weekly/biweekly
- And then...

Multiple hurdles

- No one found time and interest to try out MUSIC. Why?
- DS Automation also struggling

DS Automation Hurdles

- DS Automation based on publishing CDS/CDNSKEY records
- Coordination very loose and inefficient
 - Scanning
 - No error control
 - Used in a few ccTLDs
 - No use in gTLDs due to process hurdles (despite interest) -> need to address ICANN operational concerns

Potential Advance re DS Automation

- Generalized Notify
- Generalized Notifications IETF draft: draft-ietf-dnsop-generalized-notify
 - Allows Child operator to wake up Parent and ask for DS action
 - Child operator lookup Parent-side listener in the DNS, at \$child._dsync.\$parent
 - Also allows including EDNS0 Report-Channel option (indicates where to send errors)
 - Working Group Last Call coming up

Back to MUSIC

- Music is a centralized control
- Who runs it?
- How do you configure it to have access to each Signer?

Distributed Design (looks like it) solves the problems

- Each party controls and approves all zone changes
- A distributed design requires the different parties to be able to notify each other and communicate state