INTERNET STIFTELSEN

Multi-Signer Overview and Status

Ulrich Wisser, DNS-Labs - The Swedish Internet Foundation

Shumon Huque, Salesforce

Name Server Software Capabilities

(Command line/ Dynamic DNS/ Rest API)

Capability	Bind	Knot	PowerDNS
Add DNSKEY records (without access to private key)	Yes/?/?	Yes/No/No	Yes/Yes/Yes
Remove (previously added) DNSKEY record(s)	Yes/?/?	Yes/No/No	Yes/Yes/Yes
Add CDS/CDNSKEY record for keys not in the DNSKEY set	Yes/No/No	No/No/No	Yes/Yes/Yes
Remove CDS/CDNSKEY records	Yes/No/No	Yes/No/No	Yes/Yes/Yes
Add CSYNC record	Yes/Yes/No	Yes/No/No	Yes/Yes/Yes
Remove CSYNC record	Yes/Yes/No	Yes/No/No	Yes/Yes/Yes

Source: https://github.com/DNSSEC-Provisioning/Multi-signer/blob/main/capabilities_sw.md

DNS Service Provider Capabilities

(Dynamic DNS / Rest API / Web User Interface)

Capability	deSEC.io	NS1	Neustar
Add DNSKEY records (without access to private key)	No/Yes/Yes	Work In Progress	Work In Progress
Remove (previously added) DNSKEY record(s)	No/Yes/Yes		
Add CDS/CDNSKEY record for keys not in the DNSKEY set	No/Yes/Yes		
Remove CDS/CDNSKEY records	No/Yes/Yes		
Add CSYNC record	PDNS4.5		
Remove CSYNC record	PDNS4.5		

Source: https://github.com/DNSSEC-Provisioning/Multi-signer/blob/main/capabilities_saas.md

Algorithm Testing

Tested on PowerDNS, Bind and Knot

The algorithm holds

Workarounds are currently needed (like importing KSK)

Not tested:

- ZSK/KSK rollover
- Algorithm rollover

Multi-Signer Controller

Plugin architecture

Version one supports Dynamic Updates with PowerDNS and deSEC Rest API

Under active development, currently supporting PowerDNS 4.5

IETF draft

https://github.com/DNSSEC-Provisioning/draft-wisser-dnssec-automation

Work in Progress

Since IETF 110:

- clarifications and better explanations
- added ZSK-/KSK-rollover algorithm
- added section explaining why all signers need a common set of algorithms

Status: Standards Track, BCP, Informational?

Can this work be adopted?