Automating Multiple Signers

Shumon Huque

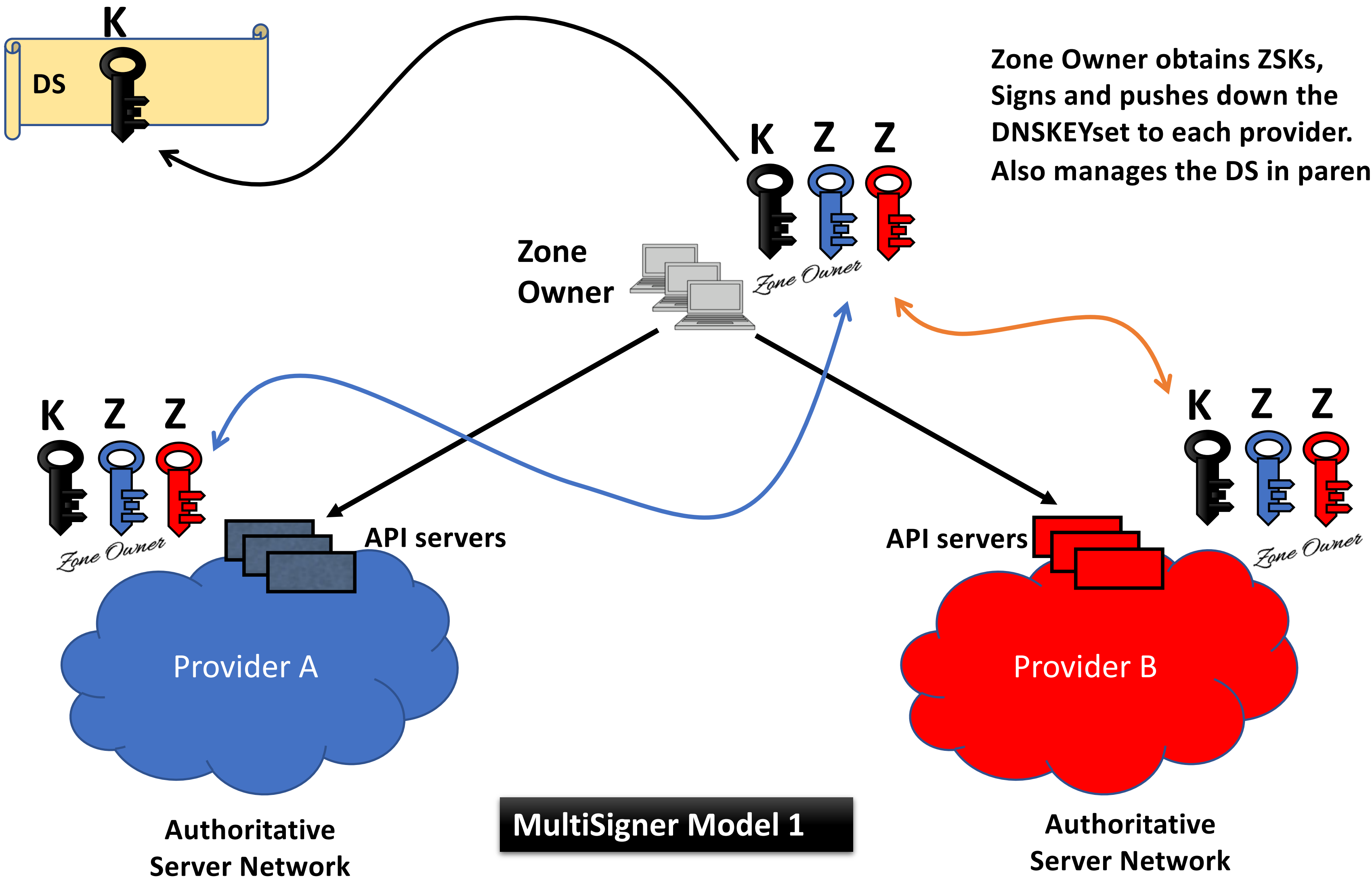
21st October 2020

ICANN’69 DNSSEC Workshop (virtual)

Multi-Signer DNSSEC update

- RFC 8901 has been published:
  - https://www.rfc-editor.org/rfc/rfc8901.html

- Vendor Support
  - NS1
  - Neustar (in progress)



Zone Owner obtains ZSKs,
Signs and pushes down the
DNSKEYset to each provider.
Also manages the DS in parent.

MultiSigner Model 1

Multi-Signer Model 1 Testbed

```
multisigner1.com.   43200  IN     NS     adns1.dnskensa.com.
multisigner1.com.   43200  IN     NS     adns2.dnskensa.com.
```

BIND

```
multisigner1.com.   43200  IN     NS     dns1.p01.nsone.net.
multisigner1.com.   43200  IN     NS     dns2.p01.nsone.net.
multisigner1.com.   43200  IN     NS     dns3.p01.nsone.net.
multisigner1.com.   43200  IN     NS     dns4.p01.nsone.net.
```

NS1

Multi-Signer Model 1 Setup

```
multisigner1.com.   7200 IN    DNSKEY 256 3 13 (
                                     pn6akhatf5l0TALuIee6Y2lor9BhI/bGrAivKC6xE582
                                     7q4jwkFSwiTlaZxkHHL9sMI40p97+rOiO5kj121e1Q==         BIND ZSK
                                     ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 37543
multisigner1.com.   7200 IN    DNSKEY 256 3 13 (
                                     pxEUulkf8UZtE9fy2+4wJwM44xncypgGVps4hE4kQGA5
                                     TuC/XJPoKBX6e3B/QL9AmwFCgyFeC4uRNxoqxK0xOg==         NS1 ZSK
                                     ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 44688
multisigner1.com.   7200 IN    DNSKEY 257 3 13 (
                                     jzdtUtdi8X6u0c8Hg1LtI2QnHPq6mhbTqiM+6ytuczNG
                                     bLWmm77edw2F7OFJwxGgZIxX1lUY90/oKPnY83pqkw==          KSK
                                     ) ; KSK; alg = ECDSAP256SHA256 ; key id = 42744       (Zone Owner)
multisigner1.com.   7200 IN    RRSIG DNSKEY 13 2 7200 (
                                     20201114025912 20201015025912 42744 multisigner1.com.
                                     nQLheKJ+pJacUV38yh6ObU93WHHsTpbI60V8FaWYukQh          KSK
                                     Lz0sjltJDZDV1IPNg07VexG9kb1oBHqt1v/8KfvB3Q== )        Signature
```

Multi-Signer Model 1 Setup

NS1

* Ask NS1 to turn on multi-signer for zone in question

BIND

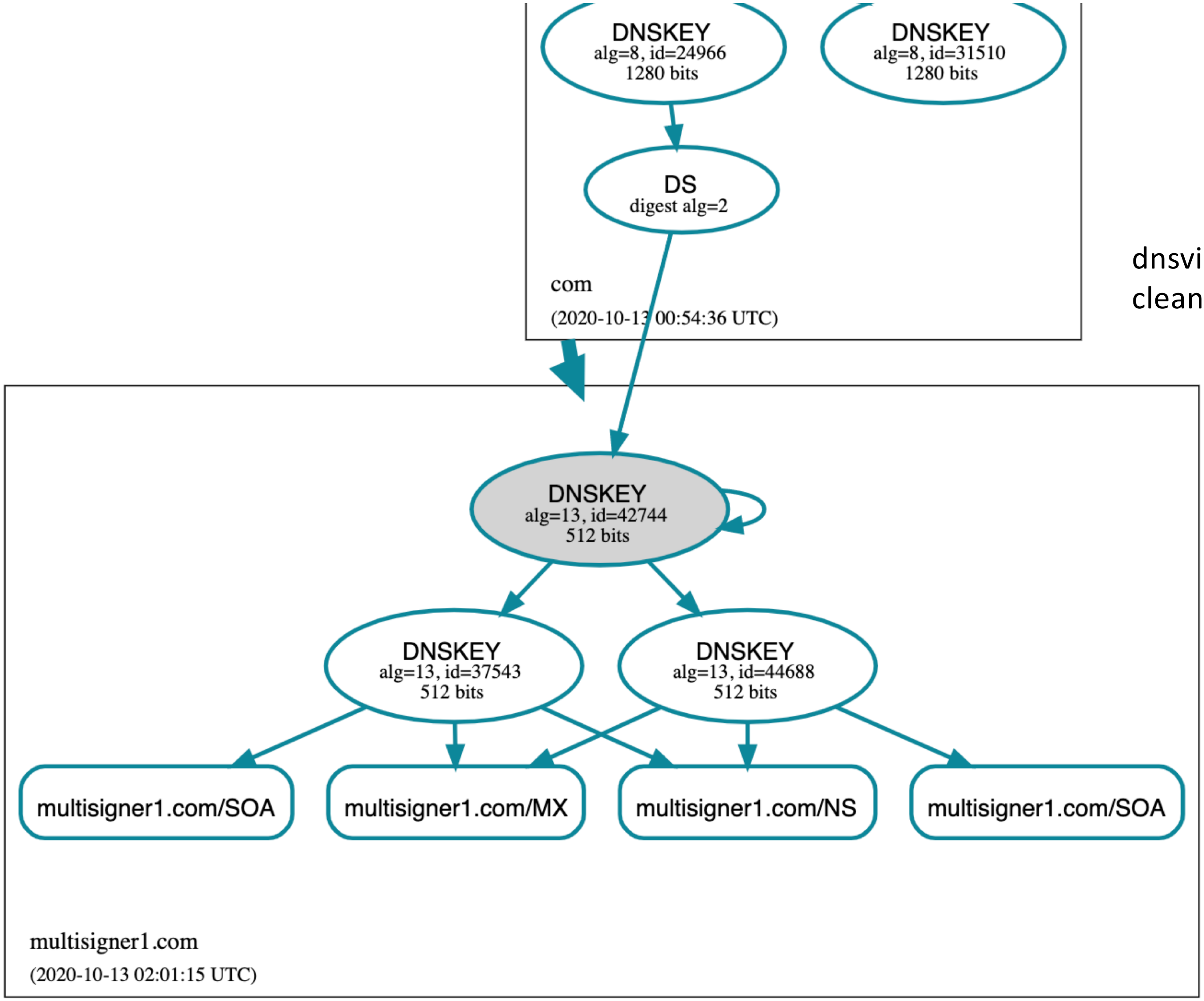
* Does not naturally support this model; Need some quick&dirty hacks
* Generate ZSK manually

Zone Owner

* Generate KSK
* Use NS1 API function to retrieve DNSKEY set (only has ZSK)
* Obtain DNSKEY set manually from BIND provider
* Sign DNSKEY Rrset
* Use NS1 API to update the DNSKEY set & DNSKEY Rrsig
* Manually take DNSKEY set to BIND Provider and stitch it into the rest of the zone that was signed offline with dnssec-signzone; reload zone file.

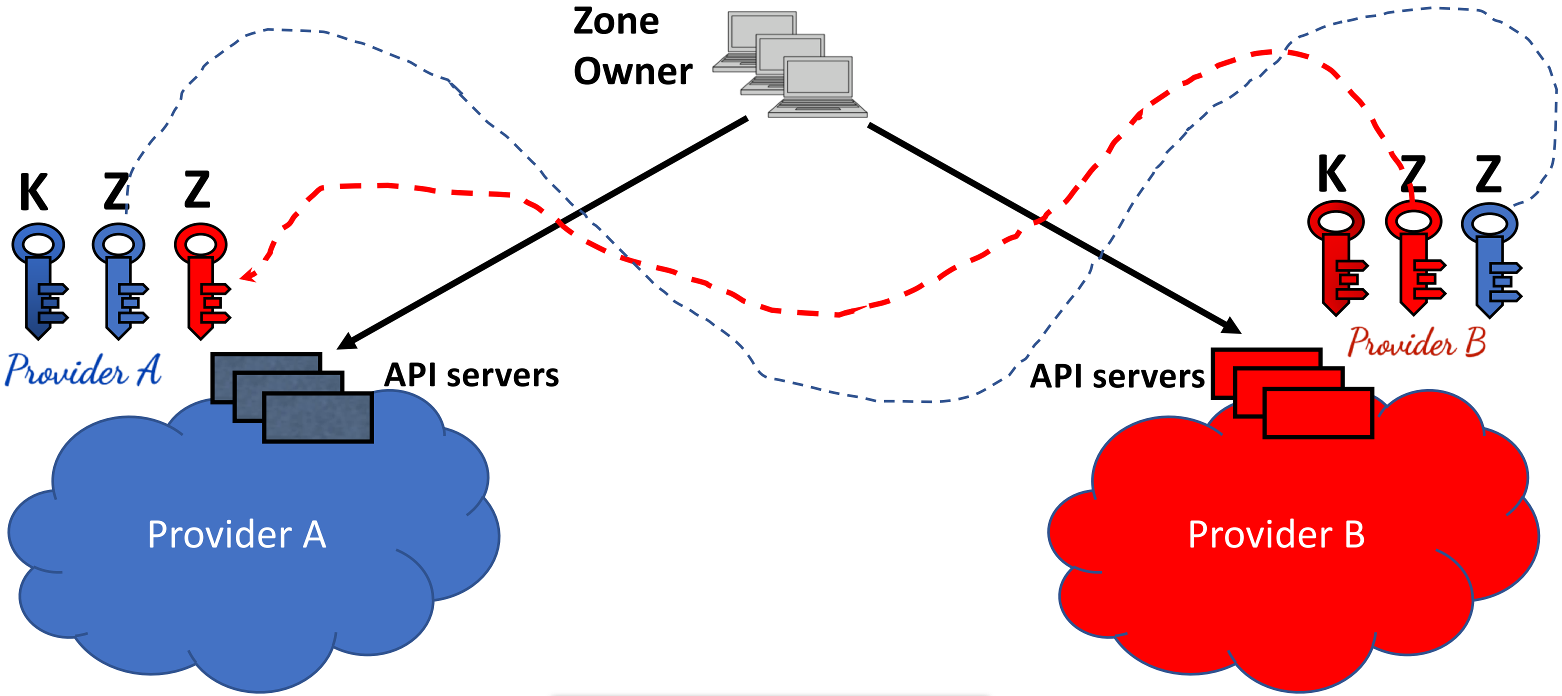
Multi-Signer Model 1 Setup

```
# Obtain current NS1 DNSKEY configuration
$ curl -X GET -H x-nsone-key:${NS1_API_KEY}
https://api.nsone.net/v1/zones/multisigner1.com/dnssec

# Update NS1 DNSKEY Rrset
$ curl -X POST -H x-nsone-key:${NS1_API_KEY}
https://api.nsone.net/v1/zones/multisigner1.com/multisigner1.com/dnssec
{post data}

# Update NS1 DNSKEY RRsig
$ curl -X POST -H x-nsone-key:${NS1_API_KEY}
https://api.nsone.net/v1/zones/multisigner1.com/multisigner1.com/rrsig
{post data}
```



dnsviz assesses this cleanly.

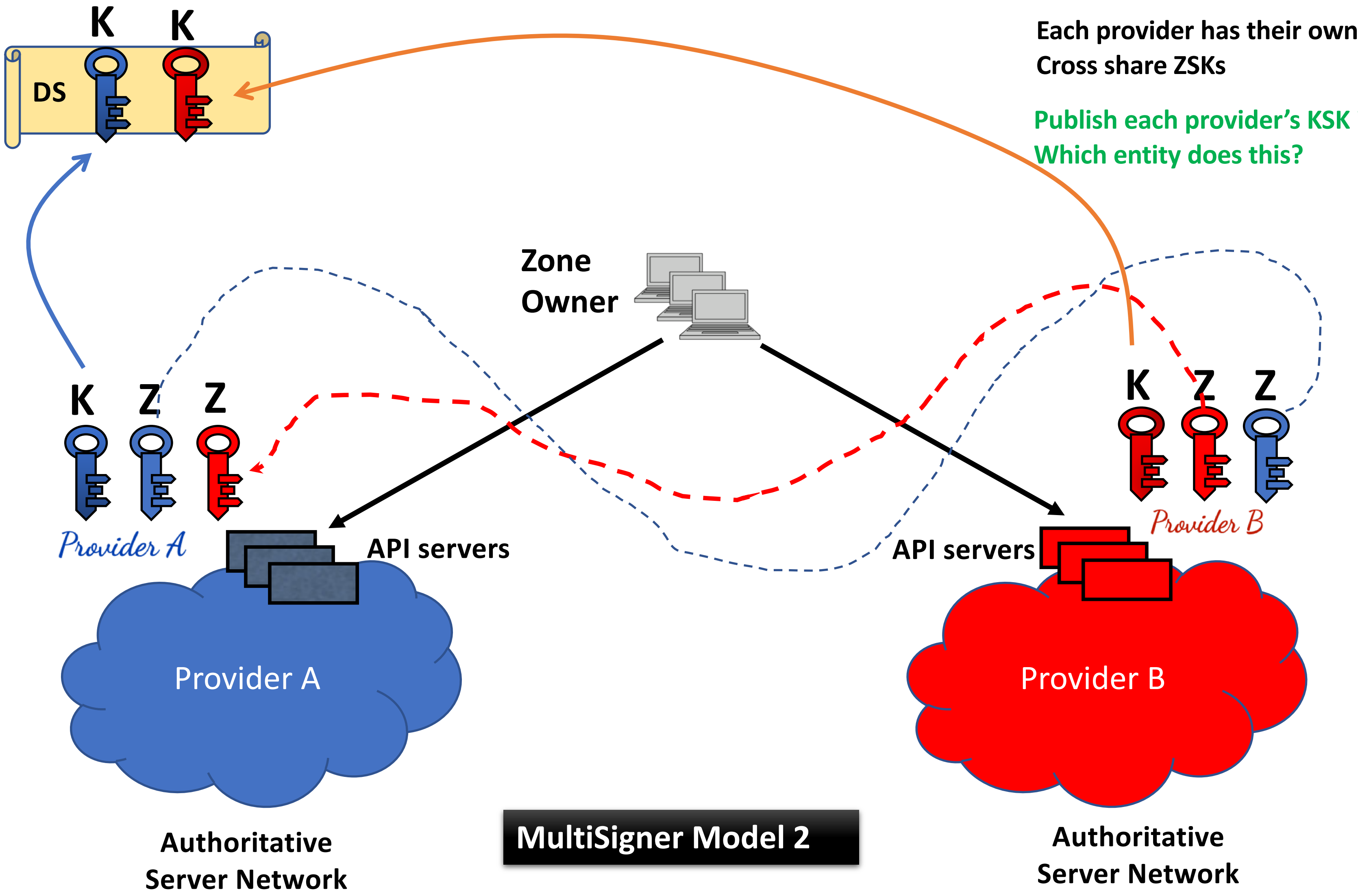
Each provider has their own KSK/ZSK
Cross share ZSKs and sign with KSK



Authoritative
Server Network

Authoritative
Server Network

MultiSigner Model 2



Each provider has their own KSK/ZSK
Cross share ZSKs

Publish each provider's KSK in DS.
Which entity does this?

MultiSigner Model 2

Multi-Signer Model 2 Testbed

```
multisigner2.com.    21599    IN    NS    adns1.dnskensa.com.
multisigner2.com.    21599    IN    NS    adns2.dnskensa.com.
```

Provider A

```
multisigner2.com.    21599    IN    NS    adns3.dnsrakuda.com.
multisigner2.com.    21599    IN    NS    adns4.dnsrakuda.com.
```

Provider B

Provider A’s DNSKEY RRset

```
multisigner2.com.     86400 IN DNSKEY       256 3 13 (
                              ffO2/RnlIMbC5GtDk5wgr7Yu14/enGzsUfd9f3/wp1sR
                              yVR40Sp+hdqOKPX7uiwrWPnBjynArilvGb8OuIs3dw==
                              ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 6178
multisigner2.com.     86400 IN DNSKEY       256 3 13 (
                              ndO6peYkx6M0TiSYVoKAWVlE8COHo60eeqwb6FgviJXR
                              FmvlqaKrJbii+SeT8YiBRRkTcgKtraFUMGvEcKlbow==
                              ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 9395
multisigner2.com.     86400 IN DNSKEY       257 3 13 (
                              DS7+/N9M+NkcY4ryglXMq/rvyDHJI3meqhhcgssVTGMB
                              YEFkgPPTh7W0TZritRlicA7QmI6TUCnZRWu+zqbjnQ==
                              ) ; KSK; alg = ECDSAP256SHA256 ; key id = 45058
multisigner2.com.     86400 IN RRSIG DNSKEY 13 2 86400 (
                              20201031222331 20201016212352 45058 multisigner2.com.
                              dxc1MwZihYO9gxhIn2g9klWpEJ8TXCXq4m99e8ulwMOK
                              p8yDJluJiPM3qgrttYfSXy9yH+EXafk6/i/blSfY/A== )
```

B’s ZSK

A’s ZSK

A’s KSK

RRSIG by A’s KSK

Provider B’s DNSKEY RRset

```
multisigner2.com.      86400 IN DNSKEY       256 3 13 (
                              ffO2/RnlIMbC5GtDk5wgr7Yu14/enGzsUfd9f3/wp1sR
                              yVR40Sp+hdqOKPX7uiwrWPnBjynArilvGb8OuIs3dw==
                              ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 6178
multisigner2.com.      86400 IN DNSKEY       256 3 13 (
                              ndO6peYkx6M0TiSYVoKAWVlE8COHo60eeqwb6FgviJXR
                              FmvlqaKrJbii+SeT8YiBRRkTcgKtraFUMGvEcKlbow==
                              ) ; ZSK; alg = ECDSAP256SHA256 ; key id = 9395
multisigner2.com.      86400 IN DNSKEY       257 3 13 (
                              1DZ7QVWyGLjCxyVdy9wZG0xfLekfsZBGH9IsDNjSLfVG
                              04NRQmosS2kk/WMH2PrOqWL2TuaWB6snIaTLZwWftA==
                              ) ; KSK; alg = ECDSAP256SHA256 ; key id = 3736
multisigner2.com.      86400 IN RRSIG DNSKEY 13 2 86400 (
                              20201031212739 20201016205723 3736 multisigner2.com.
                              RCK52++B9srOnWEL43V0+QlUkuAOk3Wu6CScQdIylY0P
                              sb/Qq25G6DsAeKKUQZaotCFJAJscJSKjZLIEjZn0WQ== )
```

B’s ZSK

A’s ZSK

B’s KSK

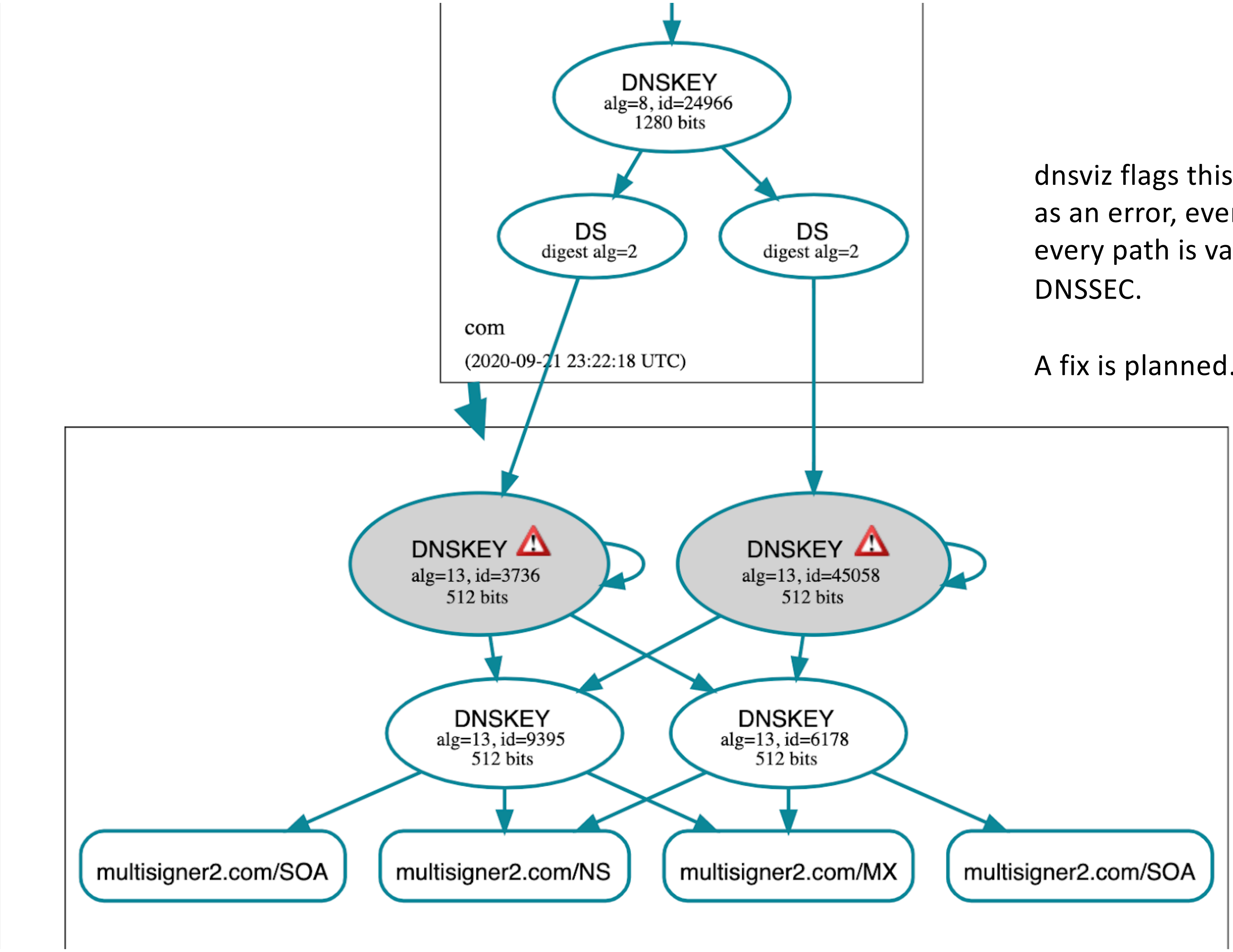
RRSIG by B’s KSK

Multi-Signer Model 2 Setup

2 set of BIND servers
Works with “auto-dnssec” and dynamic signing.

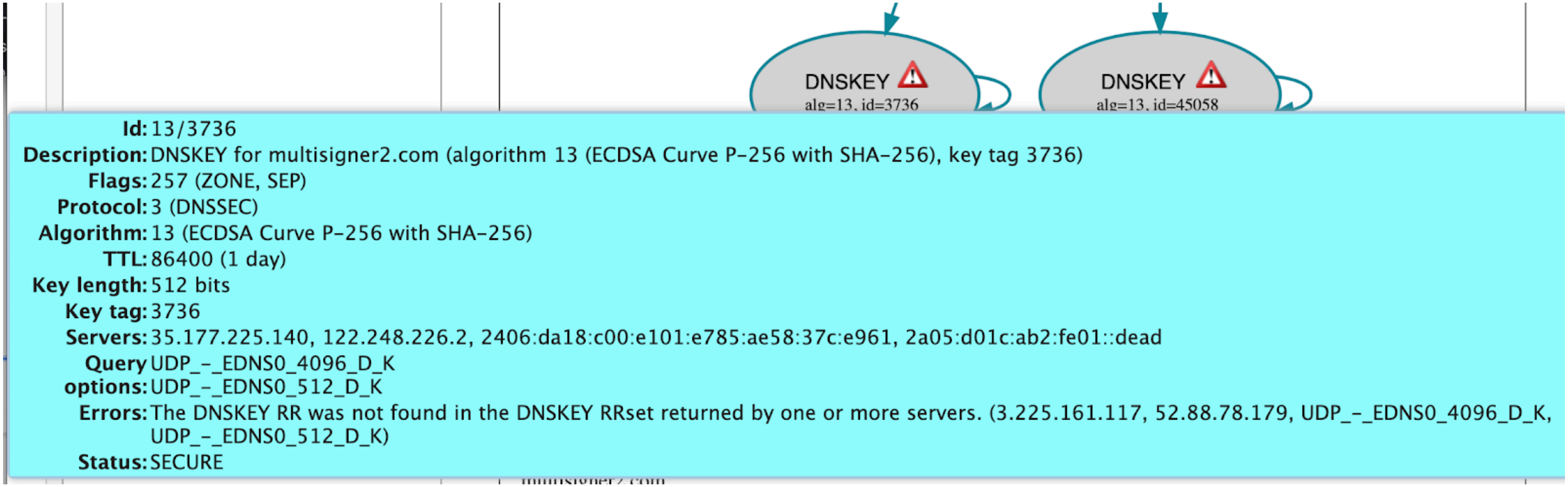
Obtain foreign ZSK
Use “**dnssec-importkey**”, e.g.

```
# Import the foreign ZSK into the zone’s key directory, using a publish time of 5 minutes from now
# This will cause BIND to import the key into its DNSKEY set
$ sudo -u named dnssec-importkey -P +5mi -K /usr/local/bind/zones/multisigner2.com
Kmultisigner2.com.+013+09395.key
/usr/local/bind/zones/multisigner2.com/Kmultisigner2.com.+013+09395.key
/usr/local/bind/zones/multisigner2.com/Kmultisigner2.com.+013+09395.private
```



dnsviz flags this configuration as an error, even though every path is validatable by DNSSEC.

A fix is planned.



Id: 13/3736
Description: DNSKEY for multisigner2.com (algorithm 13 (ECDSA Curve P-256 with SHA-256), key tag 3736)
Flags: 257 (ZONE, SEP)
Protocol: 3 (DNSSEC)
Algorithm: 13 (ECDSA Curve P-256 with SHA-256)
TTL: 86400 (1 day)
Key length: 512 bits
Key tag: 3736
Servers: 35.177.225.140, 122.248.226.2, 2406:da18:c00:e101:e785:ae58:37c:e961, 2a05:d01c:ab2:fe01::dead
Query options: UDP_-_EDNS0_4096_D_K
UDP_-_EDNS0_512_D_K
Errors: The DNSKEY RR was not found in the DNSKEY RRset returned by one or more servers. (3.225.161.117, 52.88.78.179, UDP_-_EDNS0_4096_D_K, UDP_-_EDNS0_512_D_K)
Status: SECURE

Use of CDS and CDNSKEY with Multi-Signer

From RFC 8901:

8. Use of CDS and CDNSKEY

CDS and CDNSKEY records [RFC7344][RFC8078] are used to facilitate automated updates of DNSSEC secure-entry-point keys between parent and child zones. Multi-signer DNSSEC configurations can support this, too. In Model 1, CDS/CDNSKEY changes are centralized at the zone owner. However, the zone owner will still need to push down updated signed CDNS/DNSKEY RRsets to the providers via the key-management mechanism. In Model 2, the key-management mechanism needs to support cross-importation of the CDS/CDNSKEY records, so that a common view of the RRset can be constructed at each provider and is visible to the parent zone attempting to update the DS RRset

Testbed Next Steps

- Recruiting more vendors & implementations
- Key rollovers and continuous validatability tests
- Writing better automation tools
- Looking for volunteers who can help

OpenSource DNS Software Support

- ISC BIND
  - Model 2: dnssec-importkey
- CZ.NIC Knot DNS
  - Model 1: offline-ksk feature
- Nlnet Labs NSD?
- PowerDNS?

Extending Multi-Provider DNS toolkits

- DS update support
- Multi-Signer support

- Candidates
  - OctoDNS
  - Denominator
  - Terraform
  - [Others?]