CLOUDFLARE

Provisioning Multi-Signer DNSSEC with Cloudflare

Christian Elmerot
Systems Engineer

Briefly about DNSSEC at Cloudflare

- DNSSEC live signing at scale on the edge
- Use ECDSA256 DNSKEYs
- Providing zone privacy through “minimal lies” NSEC (formerly known as black lies*)
- Presigned DNSSEC with Cloudflare as secondary provider supported (NSEC only)
- Supports DNSSEC live signing on secondary zones with hidden primary
- Enabling DNSSEC is single API call / button in UI

* https://blog.cloudflare.com/black-lies/

Multi-Signer DNSSEC Implementation

Current state of Multi-Signer DNSSEC with Cloudflare

Multi-Signer DNSSEC at Cloudflare

- Support both multi-signer models 1 and 2 as described in RFC 8901
- Ready in beta today

Common characteristics between the multi-signer models

- Currently only supporting external ZSKs, not adding CSK or KSK

Supported modes of Multi-Signer DNSSEC with Cloudflare

Model 1 and 2 with Cloudflare as primary

- External DNSKEYs managed through API or UI

```
# curl -X POST "https://api.cloudflare.com/client/v4/zones/abcd…………7980/dns_records" \
  -H "X-Auth-Email: admin@example.net" \
  -H "X-Auth-Key: 12345678907abcdefc90222" \
  -H "Content-Type: application/json" \
  --data '{
              "type":"DNSKEY",
              "name":"example.net",
              "ttl":3600,
              "data": {
                  "flags": 256, "protocol":3, "algorithm": 13,
                  "public_key": "oJMRESz5E4gY………………fRx8fGAa2XhSA==" }
             }'
```

Model 1 and 2 with Cloudflare as secondary

- External DNSKEYs managed through transfer from primary

Provisioning Multi-Signer DNSSEC with Cloudflare

1. Enable zone DNS settings to indicate desired model

   REST API call
   Required to have external DNSKEYs
   included in signed set

```
# curl -X PATCH \
  "https://api.cloudflare.com/client/v4/zones/abcd…………7980/dnssec" \
  -H "X-Auth-Email: admin@example.net" \
  -H "X-Auth-Key: 12345678907abcdefc90222" \
  -H "Content-Type: application/json" \
  --data '{"dnssec_multi_model":2}'
```

2. Enable DNSSEC on zone with Cloudflare

   REST API or UI

3. Add external ZSK DNSKEY(s)

   REST API or UI

4. Verify

5. Update DS (model 2)

6. Update NS set

Feature gaps - or why we still call it beta

- CDS / CDNSKEY management through API / UI
- Simplified NS rrset management
- Simplify zone activation when multiple providers are used
- Improve UI and API documentation

Looking Ahead

A bit about upcoming and work in progress

CDS scanning of delegated child zones

- Signed zones with delegations require manual DS update by zone owner
- Scan signed zones delegations for CDS/CDNSKEY to allow automatic management of DS records
- Encourage more use of CDS / CDNSKEY
- Required for automating Multi-Signer DNSSEC for child zones
- Soon(™)

Authenticated Bootstrapping of DNSSEC Delegations

- https://datatracker.ietf.org/doc/draft-ietf-dnsop-dnssec-bootstrapping/
- Encourage more use of CDS / CDNSKEY, faster and secure DS provisioning
- Support all signed zones using standard Cloudflare NS
- Support for current draft currently in production
- Intending to implement any draft changes compatible with current architecture

Thank you!

Questions?