draft-ietf-sidrops-signed-tal-02
Goals

- Allow RPKI Trust Anchor Key Rolls
- Learn from DNSSEC (RFC 5011)
- Soft landing into existing standards
- Leave a trail for outdated clients
Changes in -02

- Allow multiple active keys as in DNSSEC (recommended to use just two)
- Supports both planned and unplanned rolls
- No time and intent of next key included, because of unplanned rolls
Next steps!

• Speak now, or forever hold your peace!

• Running code at IETF 104

• Do people want a hackaton?
Current situation

TA TAL → TA.CER → TA.MFT → CA.MFT
      |            |            | CA.CRL
      |            | TA.CRL    | CA.CRL
      |            | CA.CER    | GC.ROA
Opt-in, using 1 key
Using 2 keys

```
TIM@NLNETLABS.NL | SIDROPS | IETF103
```

```
TA TAL → TA.CER → CA.CER → CA.MFT

TA2 TAL → TA2.CER → TA2.TAK
```

```
TA.TAK → CA.CER → CA.CRL

CA.CRL

GC.ROA
```
Rolling to keys 2 & 3