draft-ietf-sidrops-signed-tal
Lessons from RFC5011
So, what can we learn?

- Standardise this before we have a dozen RPs
- Lots of DNS specific timing (TTLs)
- Back-up keys?
- Bootstrapping!
Objectives

- Planned rolls
- Automatable process
- Leave a trail
TA Roll – Before
TA Roll – During

MUST ignore AIA!
TA Roll – After

TA TAL -> TA.CER -> TA.MFT, TA.CRL, TA*.TAL


CA.MFT, CA.CRL, GC.CER

Graph showing the relationships between TA TAL, TA*.TAL, TA.CER, TA*.CER, and the certificates CA.MFT, CA.CRL, and GC.CER.
Comments?
TA Roll – With strict AIA

TA TAL → TA.CER → TA.MFT

TA* TAL → TA*.CER → TA*.MFT

CA.CER

CA.MFT

CA.CRL

GC.CER
TA Roll – Cleanup (strict AIA)