Interim Trust Anchor Repository

- Commenced limited testing at RIPE meeting in Dubai
- Launched to public in January 2009 at itar.iana.org
- Open to any TLD operator to submit their trust anchors
- Simple transaction model
  - Submit via website
  - Admin and Tech contact for domain must approve
  - Won’t list until matching DNSKEY appears in the zone
Stats to date

- 61 change requests submitted
- 42 trust anchors approved and listed
- 12 rejected by domain contacts
- 7 approved by domain contacts, but a matching DNSKEY never appeared in the DNS
- Approximately 10,000 downloads per month
Observations

- Administrative and Technical contacts must approve changes, but clearly some do not check what they are approving.
  - Have approved invalid trust anchors
  - My guess is they know a request is coming, and just blindly click to approve
- Useful to gather real-world experience with TLD managers to help instruct how we handle DS for the root zone proper.
Future work

- More pro-active notifications of events of interest
  - “Psst.. your key is about to expire and you haven’t listed a replacement yet.”
  - “Psst.. you seem to have entered the wrong algorithm code, because everything else checks out. Want to change it?”
- Discussion on IETF dnsop list about recommending a refresh period
- Killing it with fire
  - Once root signing is in the rear-view mirror, investigate decommissioning.
Fair warning

- We are working on DS record handling procedure for a signed root zone.
- As this is predicated on the current process for root zone changes, we can’t just directly transplant the ITAR model.
- Example:
  - **ITAR**: one transaction to list a TA, which includes an expiry date
  - **Root zone**: adding and removing DS records are two discrete acts that are done independently
- We’ll be proposing procedures on this early next year.
Thanks!