# Why TAR for Resolvers

- Why use a TAR
  - The resolver operator outsources configuration
    - Easy for operator
    - Trust in the anchor selection
      - provide security
      - also managed properly (the zone 'works')
- Why not use a TAR
  - Root is signed
  - Concerns over malice or bad management
  - Denial of service
    - No timely updates of key material
    - No availability of TAR contents

# How to use a TAR

- TAR is allowed to configure resolver
  - Trust anchors
  - Domain-insecure statements
    - "Ignore DNSSEC here; treat as insecure"
    - Like unknown algorithm keys in the DS
- End user may want to use multiple TARs
  - default add up trusted keys
    - TARs have keys for same name
      - Use all keys together, any one will do
    - Fix conflicts between TARs
  - Too much work: outsource the merge to a TAR

# TAR key is the new Secure Entry Point

- TAR key must be as strong as contents
  - As secure as the DNSSEC keys
    - Gives idea of acceptable key size
    - Support TAR key rollover by resolver and TAR
      - Like 5011 on dlv.isc.org DNSKEY
      - Or tar-key-list that is signed by all PGP keys
        - » 5011 or 1ofN on TAR-key
- HTTPS for TAR protection has problems
  - Cycle in DNS->TLS->DNS dependencies
  - Certificates not rolled over
  - 1024b cert to protect 2048b .gov would not be smart