The DRIP DET Key Infrastructure

draft-moskowitz-drip-dki-09
November 7, 2023
Robert Moskowitz

Of DKIs and PKIs

Why?

- I tried to implement a test environment based on draft-ietf-drip-registries-09 and couldn’t
  - Lots of unknowns
  - No tools
  - And potential security risks
    - That become apparent when you work through actual use

Why?

- Thus two documents
  - DIME technical matters in drip-registries
    - Has a likely endpoint for publishing
  - DKI for implemenational matters
    - Items will take time to resolve
    - At some point should be “done enough” for historical records

Objectives

- What it takes to deploy DET support
- Present the full DET Endorsement trust tree
  - And alternative deployment strategies
- Define X.509 “shadow” PKI
  - Many places where X.509 is preferred
    - Compatibility with ICAO PKI
  - Lite-PKI and PKIX-like profiles
  - c509 encoding for reduced A2X packet overhead

Objectives

- DNS deployment
  - ip6.arpa. tree
  - HID forward tree
- Open python scripts
  - DET generation
  - DNS RR generation
  - Endorsements
    - DET RR

Relation to Charter

- Drip-registers is inadequate to deploy
  - More is needed as shown in DKI draft
  - Need to interact with ICAO PKI
  - ASTM and A2X workgroup
    - Certificate-based broadcasts

Relation to Charter

- In particular
  - “leverage Internet standards … and infrastructure … well as domain name registration business”
    - What are the DNS RR in what domains?
    - PKIX used by others (civil aviation) and ASTM/Mitre A2X
  - Or “require existing protocols to be extended”
    - DRIP-specific X.509 profile and integration to ICAO Certificate Policy

Value in Workgroup adoption

- Content of drip-dki will used outside of IETF
  - ICAO TFP PKI and RPAS/UTM Panels
  - ASTM
  - UTM/UAS industry groups
- Industry has matured since DRIP started
  - Need to stay current and relevant
- Inform drip-registries of needed tech content

Value in Workgroup adoption

- Start out as “live” record of implementation
- Potential to evolve to guidance to new entrants
  - Adopt as a support document
    - i.e., the WG might decide to not publish as an RFC

Questions?