

# DET Identity Management Architecture

-registries-13

Adam Wiethuechter -- AX Enterprize, LLC

Jim Reid – RTFM, LLP

# Changes since -12

- Information to Standard Track
- drip-arch to RFC9434
- Proposal to remove Serial Numbers
- Prefix delegation in IANA Considerations
  - Guidance for discussion
- Endorsement key values registry

Full diff: [https://author-tools.ietf.org/diff?doc\\_1=draft-ietf-drip-registries-12&doc\\_2=draft-ietf-drip-registries-13](https://author-tools.ietf.org/diff?doc_1=draft-ietf-drip-registries-12&doc_2=draft-ietf-drip-registries-13)

# Proposed: Serial Number Removal

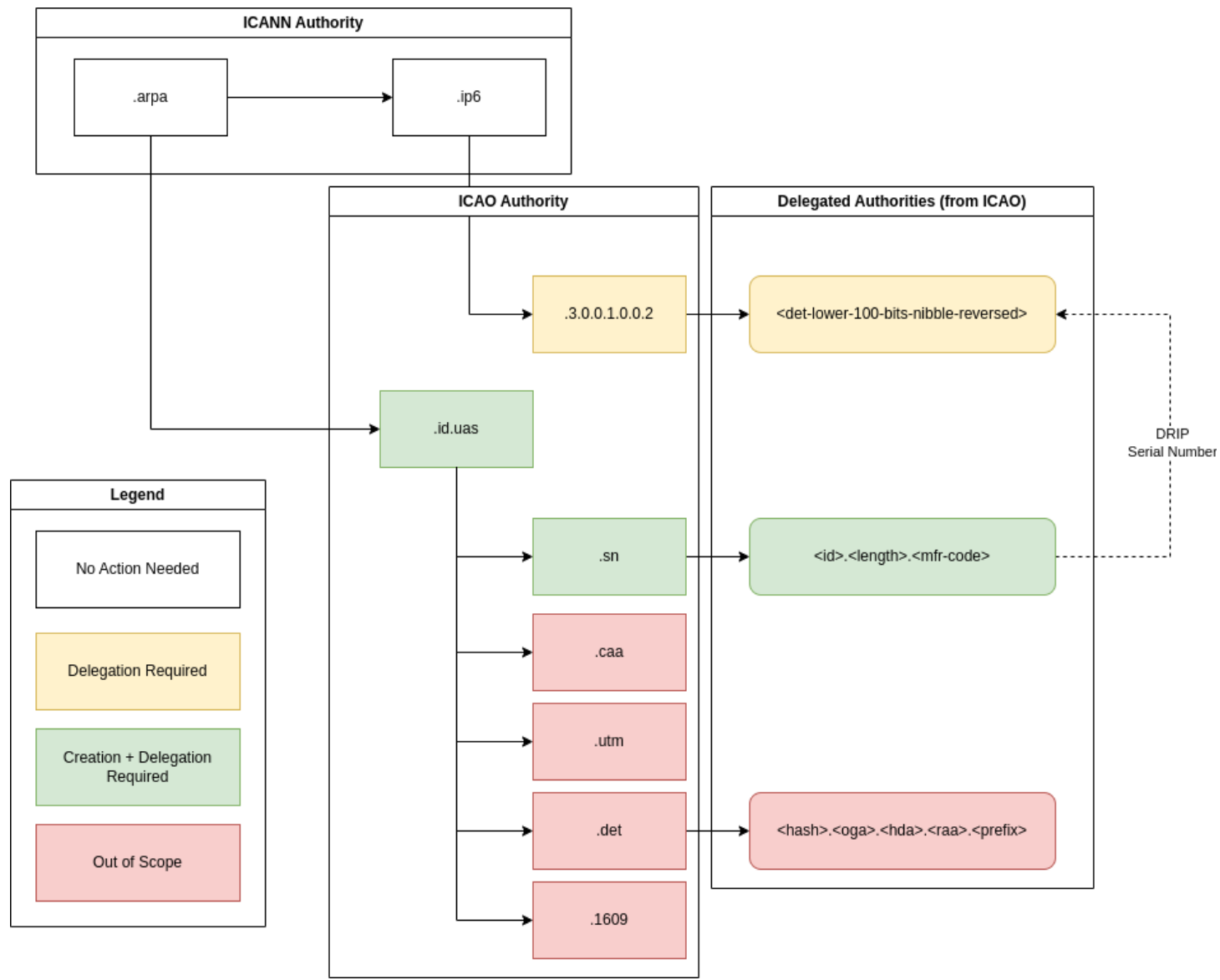
- Document (as is titled) focuses on DET's in DNS
  - `ip6.arpa` is well defined as apex point
  - DET lookup is a MUST for interoperability
- Serial Numbers in DNS are recommended but optional
  - requires a new apex point raising lots of questions
  - Other than for DRIP Serial Numbers [1] orthogonal to DET in DNS discussion
- New document created to separate them [2]
  - -13 has Author Notes pointing out sections for removal that are copied into new document

[1] <https://www.rfc-editor.org/rfc/rfc9374.html#section-4.2>

[2] <https://datatracker.ietf.org/doc/draft-wiethuechter-drip-uas-sn-dns/>

# Apexes

- "ip6.arpa" required home for RRs of DETs
  - Other domains can be specified and use standard DNS mechanism of "ip6.arpa" to redirect
    - Use of other domain apexes for DETs = **out of scope**
  - Format as domains already in document
- With proposed Serial Number removal, the "arpa" leg of diagram is out of scope for this document
- ICAO may not be authority until later (TBD)



# In Progress (-14)

<https://github.com/ietf-wg-drip/draft-ietf-drip-registries/pull/42>

# DET Resource Record

- DET RR is now more of a metadata record containing DRIP specific information
  - Use of other RRs for other functions
    - HIP = Public Key (HI), RVS
    - TLSA = Certificates & DTLS
    - URI = Private Information Registry pointer
- Cleaned up, added subsection for fields
- IANA sections for TYPE and STATUS
- Updating examples to reflect change
- There is issue on GitHub [1] about this being its own document?

domain IN DET ( DET TYPE STATUS HID SN BROADCAST\_ENDORSEMENT )

[1] <https://github.com/ietf-wg-drip/draft-ietf-drip-registries/issues/38>

# Other Changes

- Added text from Bob for C.509 Certificates (CBOR)
- Security Consideration section on Public Key Exposure
  - Was originally in rough form in –auth making a recommendation to registries so moved here
- Add Appendix A: HID Abbreviation
  - Moved and rework of previous Section 8.1.1.1
  - Unsure if stepping into client domain so changed to a recommendation
  - Moved to appendix and weakened requirements language

# Open Issues

- IANA Registry for RAA Values
  - Country Code range should be avoided
    - Pseudocode in draft for how to encode and decode them
- CERT RR use (OID Allocation / CBOR in CERT RR)
  - This may be deprecated?
- Lots of issues from OPSDIR and DNSDIR
  - Many of them done in –12, but with SN changes may require a relook
  - Safe to close them?

<https://github.com/ietf-wg-drip/draft-ietf-drip-registries/issues>



# DNS Prefix Delegation

Outcome of side meeting discussion with IANA

# Discussion

Questions, Comments, Concerns?