

DIME Architecture

Adam Wiethuechter - AX Enterprize, LLC

Jim Reid - RTFM LLP

ICAO / ASTM Updates

- Have been assured that the portal and requests being accepted by end of week
- Have updated the initial allocation for the Specific Session ID
 - Org Name: IETF
 - More specific like IETF DRIP?
 - Org Address: somewhere in DE
 - Contact Name: DRIP WG Chairs
 - Contact Email: drip-chairs@ietf.org
 - Support Email: draft-ietf-drip-rid@ietf.org
 - Update to something with RFC9374? (rfc9374@ietf.org?)
 - Specification: datatracker link to RFC9374
- Specific Authentication Method (SAM) requests should be ready to process soon

Recent Reviews

Review from Dnsdir (Tim Wicinski)

- Creation/delegation of domain(s) needs request to IAB (RFC3172)
- RRType needs IANA section asking for creation of such
- Appendix A: Catch of protentional error on prefix
 - 2001:30/28 and "2001003"
- Section 10: very hand wavy (X.509 and certificates)
 - Most text from Bob and more in line with DK1, which Bob pointed to in reply
- Section 4.5: move to terminology section
 - Some terms not defined and should be added
- Figure 2: expanded names, but should use acronyms
 - A clearer marking of each interface marked with protocols (second version of figure?)
- Need examples of what goes into registries (as appendix)

Review from Bob M.

- Lots of text cleanup items and clarification questions
 - Lots of text fixes in -10 but need to go back and review for clarifications
- Handling of interactions between this document and DKI document
 - How to remove burden of ICAO delegations to a minimum
- RAA allocation scheme?
 - Added in -10
- Manufacturer code allocation scheme?
 - Added in -10

Review from Opsdir (Joel Jaeggli)

- Section 5.3: under specified
 - Resolution is potentially life-critical
- Section 6.1: hard to parse
 - Already worked on in -10, needs re-review
- Section 7: incomplete?
 - key management problem should be elucidated
- Section 8
 - ICAO domain sounds like a type of TLD; action for ICANN if so
 - Other DNS related items should be looked at by DNS SME (dnsdir)

Working Items

RAA Allocations

- Justification: ICAO process long -> predefine what we can, and can catch up as IATF and other work moves forward
- RAA space carved up
 - Apex = 0 - 3
 - ISO 3166-1 Numeric Codes = 4 - 3999
 - Manufacture Code Authorities (MCA) = 4000 - 4095
 - Reserved = 4096 - 16375
 - Experimental = 16376 - 16384
- RAAs are allocated in groups of 4 to keep on nibble boundaries
 - Makes DNS delegation easier
 - MCA region does not follow this rule

ISO 3166-1 Numeric Codes

- Three digits, can convert to base RAA value
 - $\text{raa_code} = \text{iso_code} * 4$
 - Allocated range(raa_code , $\text{raa_code} + 4$)
 - $\text{iso_code} = \text{floor}(\text{raa_code} / 4)$
- Well defined, already in use for Text Abbreviations
- Can jump start deployments when using cross-certificates
 - See DKI for details
- Examples
 - United States (US) = 840, $840 * 4 = 3360$, RAAs = 3360, 3361, 3362, 3363
 - RAA = 1105, $\text{floor}(1105 / 4) = 276$, 276 = Germany (DE)

Manufacturer Code Authorities (MCAs)

- Formally ICAO Authority of Manufacturers (IAM)
 - Removed ICAO to not cause confusion
- 4000 – 4095
 - Only need 82 so each Manufacturer Code has one HDA
- Can derive HID (RAA/HDA) from Manufacturer Code
 - $HID = 65536000 + \text{base34_decode}(\text{mfr_code})$
 - $\text{mfr_code} = \text{base34_encode}(HID - 65536000)$
- Examples
 - MFR = 1648; RAA = 4002, HDA = 13616
 - RAA = 4005, HDA = 0; MFR = 22VD

Experimental

- Last 2 RAA allocations in range
- Very last (16381-16384) setup by DRIP experts (i.e. WG) to act as RAAs for HDAs wishing to test
 - 16384 special as used for MAA testing
- Rest of range (16376 – 16380) owned by DRIP WG and temporary handed to parties wishing to test as an RAA

New RR Type (Section 8.1.1)

- CBOR encode entire object?
 - Endorsement is expected to be CBOR already
- Fields from HIP RR
 - OGA ID, DET, HI, RVS
- Fields added for DET RR
 - HID Abbrev., URI, Broadcast Endorsement, Active[, Serial Number]
- How does Endorsement get marked as expired?
 - Added active flag to fields - does this help?
- All other Endorsements and/or X.509s in CERT RRs

Section 6.1 Rework

- Subsections for each Serial Number support scenario
 - Plain Text (no DET)
 - Associated w/DET
 - DET source is MAA (either static or dynamic)
 - DET source is HDA (dynamic)
 - Linked w/DET
 - SN is made from DET
- Figures for each scenario and explanatory text
- Some debate as to how this fits in DNS due to unknowns of domains
 - Who owns apex?
 - Who runs apex?
 - Delegation to MFRs is straightforward, once apex is known