Authentication / Registries

draft-drip-ietf-auth-30, draft-drip-ietf-registries-08

Adam Wiethuechter; AX Enterprize, LLC
Authentication: Blocker

• ASTM/ICAO relationship still TBD

• Plans to move forward

  1. Give ASTM fallback to IANA
     • Chatted with IANA this week. They are willing to do the work, but need ASTM to give them the OK
     • We can draft the letter for ASTM to deliver to IANA to start process if they wish to do so
  
  2. Use "Experimental/Private Use" SAM Type code points of F3411-22a
     • Mark document as Experimental
     • Get -auth published and go back in -bis to:
       • Get proper allocations from TBD registrar (assigned by ASTM)
       • Move document into standard track
       • Change **nothing** else in document during -bis
Authentication: Clean Up

• Cleaned up
  • Text in various places
  • Formats (field ordering and definition of terms [to match Endorsements])

• Soften the reference on –registries as much as possible
  • Document now much more stand-alone with informative reference to –registries

• See atw branch on GitHub for latest, not merged in yet but ¬30 pushed to datatracker
  • Lots of closed issues associated with branch
Registries: what we want to support

• New section in document (Section 2.1: Supported Scenarios)
• DETs (obviously) - the primary goal of the document
  • for [Single-Use] [Specific] Session IDs
• Serial Numbers
  • "Bare" – generic interoperability and support
  • "Linked" – for after-market DRIP support
  • "Generated" – for fully integrated DRIP support
Serial Numbers

- ANSI/CTA 2063-A ("bare")
  - `<mfr-code><length><id>`
  - 34-character set (0-9, A-Z [except O, I])

- DRIP Serial Number ("linked")
  - Use DNS to point "bare" Serial to valid DET
  - Could be manufacturer or USS doing this!

- DRIP Serial Number ("generated")
  - Subset of "bare" Serial Number
  - 32-character set (0-9, A-Y [except O, I, S, Z])
  - `<id>` generated using methods defined in RFC9374 Section 4.2
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

• Serial Numbers need some apex in DNS
  • Proposed: "sn.uas.icao.arpa"
    • Requires creation of "uas.icao.arpa" and its allocation to some entity (probably ICAO)
    • Other ID formats could be used under this
      • UTM Assigned (UUID), CAA Assigned, etc.
      • Definition of other than Serial Numbers = out of Scope
  • Format as domains already in document
HHIT/DET Resource Record

• New RRTYPE

• Superset of HIP RR, with new additions for HHITs
  • What do we want in it?
    • OGA ID, HI, list(RVS), list(Endorsements), URI
    • HID field abbreviations? (to enable Section 4.4)

• Formatted in CBOR?

• This removes the large open question of how to get Endorsements into CERT RR
  • Was using OIDs – was very messy

• Consolidates everything into one RRTYPE instead of 3
Endorsements

• CDDL updated to reflect current models
• Parred down formats specified to those essential
  • Several were currently unused, why define if no current use?
• Want to be sure it aligns with X.509 and others (i.e., RATS)
  • Terminology, structure, etc.
• Does it make sense for it to be separate document instead of part of – registries?
  • Would be STD track (not INFO as currently is in document)
  • -registries would be bi-directional "informative" reference
Next Steps & Timeline

• Clean up text in Section 6
  • Due to Endorsement changes / clean up

• Review and word-smith Section 7 and move it after DNS section
  • Logically better place

• Develop and get RRType allocated (separate draft to define)
  • Jim starting process, WG needs to confirm contents of RRType good

• Break out Endorsements into own draft?
  • Applicable elsewhere than just this area in future

• Break out X.509 items into own draft?
  • Bob was leading this and is driven by ICAO work – timeline unknown

• IANA registries for various items
  • Mainly keys for data models in CDDL for aircraft info, session info, etc.

• Have something for WGLC by 117/118