DRIP UAS RID

draft-ietf-drip-rid-08.txt
July 28, 2021
Robert Moskowitz
Etal.

Review of changes
And Todos

Target Audience

- This may well be the most important DRIP document read outside of the IETF
  - Regulators and manufacturers
    - Need to understand the technology
    - What is gained with HHIT Remote ID over alternatives
- Read this as an IETF outsider might
  - So help me where I get lost in the weeds.

Updates since 07

- Most appendices moved to core
  - Messes up rfcdiff tool
- Cleaned up IANA considerations
- Minor realignment with draft-ietf-drip-req
- X.509 comparison expanded
- Text clean up. A bit.

Appendices to core document

- For the most part this was cut and paste
    - Real easy in xml where you can collapse sections for easy moving.
- Consolidated HHITs into CTA 2063-A sections
- All these sections still need editorial review
    - I really need to work over the new section 6
    - And align appendix B.

IANA Considerations

- DRIP RID HHIT makes important changes to the HIP IANA registry
- Text in IANA considerations and throughout now better instructs IANA on what is needed.
- Please review
  - Note, I am one of the IANA HIP registry ‘expert reviewers’, so others eyeballs on this would be good.

EdDSA

- NIST FIPS 186-5 *still* draft
  - At least in my review of their web site
  - And yes, I made a negative comment on use of SHA512 instead of SHAKE
- This impacts discussions in ICAO Digital Identity WG IATF (Digital Identity Trust Framework, PKI)

Expand X.509 comparison

- Comments made it clear I was not clear!
  - Hopefully text in Introduction is better now.
  - I do not want to belabor the point, as this is a document on RID using HHIT, not X.509
    - But elsewhere in the USS/UTM ecosystem, X.509 certs are important so there will be a connection some way or another...

To Do

- Examples!
  - Check out DNS examples
  - Add HHITs as CTA 2063-A numbers
    - Desire Python script for that
  - Others?

To Do

- Really need to tighten up proofs sections
  - Or loosen up with more text!
- Open to other things I need to fix/expand
- Changes to align with ASTM F3411-21
  - When published.

To Do

- Add Python code?
  - hhit-gen.py, 249 lines
  - Collision resistant script (run to 1M)
  - TBD HHIT → CTA 2063A (Help!)
  - In draft or on Github?
    - How to reference Github in RFCs?
- Respond to Secdir review
  - Discuss HHIT on CFRG