DRIP UAS RID

draft-ietf-drip-uas-rid-01.txt
September 23, 2020
Robert Moskowitz
etal.

From the DRIP Charter

- DRIP’s goal is to specify how RID can be made trustworthy and available in both Internet and local-only connected scenarios,

Design Goals

- 20 characters maximum
- Deterministically globally unique
  - With distributed Registry Services
- Non-spoofable
  - Provable ownership without Internet lookup in 200 bytes
  - Much less is better for performance
    - With Internet lookup

Design Sub-Goals

- Use Public Key as UA ID
  - HASH with hierarchy to create RID
- DRIP UAS RID is an IPv6 address
  - Not necessary for Broadcast or Network Remote ID, but of value for access policies and UAS applications
- Provide ID Privacy
- Thus a Hierarchical Host Identity Tag (HHIT)

DRIP Requirements Supported

- GEN 1 – 3
  - Provable Ownership, Binding, and Registration
- ID 1 – 5
  - Length, Registry ID, Entity ID, Uniqueness, non-spoofability
- REG 1 & 2
  - Public and Private Lookup

Draft Updates

- Since moskowitz-drip-uas-rid-06
  - Cleaned up definitions
  - Removed hhit-registries for EPP
  - Nit changes in DNS examples
  - Added ASTM message type for reference
  - Added self-claim (84 bytes) example

Work to Do

- Clean up text that HHITs are IPv6 addresses that can be stored in FQDN for data retrieval
  - Is this HHIT really registered?
  - What is the HI?
  - Other?

Work to Do

- Add to Intro on value of non-transferable/duplicatable Identifier
  - Very hard for others to duplicate Identifier claim
    - Identifier can potentially exist in only one place in 3rd party assertions by *definition* not just by policy
  - Consequences of non-transferable in electronics replacement

Work to Do

- Further parameterize ORCHID algorithm
  - Support different sizes
  - Prefix, RAA|HDA, Hash
- More text on self-claim
  - What is signed by private key
    - Include MAC?
    - Should check this out over at cfrg

Work to Do

- Add sample HDA signed claim (200 byte?)
  - For offline proof
  - Cleans up sec 9.1
- Add both self and HDA claims to sec 3.4
  - But does not remove draft-wiethuechter-drip-auth

Questions ?