DRIP UAS RID

draft-moskowitz-drip-uas-rid-03.txt
July 30, 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 Considerations

• Registered String ==> Non-spoofable
  - E.G. ANSI/CTA serial # and RFID EPC
  - Expect lying and stealing
  - No confidence in lookup/retrieval for actionable information
Design Considerations

• Digital Certificates ==? Non-spoofable
  - Certificates non-spoofable
    • But Name is spoofable
  - Multiple roots
    • Who to trust on Name
  - Simultaneous Name registrations in different roots
    • Who ‘wins’
Design Considerations

• To be Trusted/Non-Spoofable, an Identity needs to be self-asserting
  - Identity is derived from trustable information
    • e.g. a Public Key
  - Algorithm on Trusted information yields Identity
    • Hash the Public Key into the Identity
      • Fixed length result is best
Design Considerations

• Global Uniqueness implies an assigning hierarchy
  - Statistical Uniqueness not sufficient
  - Include Hierarchy into Identity
  - Include in hash algorithm for non-spoofable hierarchy
Possible Approaches

• Host Identity Tag – RFC7401
  - Lacks Hierarchy which is an ‘easy’ add

• Cryptographically Generated Addresses – RFC3972
  - Difficult crypto agility – hard to fix, RFC4982
  - Loose Hierarchy in IPv6 prefix
    • Hard to limit and control for Remote ID
Chosen Approach

• Host Identity Tag with added Hierarchy
  • draft-moskowitz-hip-hierarchical-hit
  • Open to discuss on ‘better’ defining 96 bit partitioning
  • Can debate choice of EdDSA25519/cSHAKE128 suite choice
    • Public key is 32 bytes WITHOUT patent issues
    • cSHAKE is NEAT!
      • NIST SP800-185
Chosen Approach

• Global Uniqueness through Registration
  - draft-moskowitz-hip-hhit-registries
  - Or see EPP presentation
    • Probably the better choice

• Lookup via DNS
  - Either IPv6 reverse lookup
  - Or specific reverse lookup design of HHITs
  - Or RDAP
DRIP Requirements met

• 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
DRIP Workgroup Action

CALL FOR WORKGROUP ADOPTION
At August Interim
Questions