Augmenting HIP Registration to Register Hierarchical HITs

Draft-moskowitz-hip-hhit-registries
IETF 106 TM-RID BOF
Nov 19, 2019
Robert Moskowitz

HHIT Registries

- Service provided by the Hierarchical HIT Domain Authority (HDA)
  - And RAA for HDA's HHIT
- All HHITs for a domain MUST be registered
  - Prevents duplicate HHITs
  - HI associated with HHIT
- Collects other information based on HDA policy

HHIT Registries

- Provides retrieval based on HHIT and authorization
  - RFC 8005 DNS HIP RR
    - HI and optional RVS (if authorized)
  - Other registered information
    - Based on authorization

HHIT Registration

- Expansion to RFC 8003 Registration Extension
- Registration of HHIT is always authenticated
  - “Know your clients”
    - No support for opportunistic registration
  - Support for X.509 cert or PSK
  - PSK could be delivered in sideband (SMS) after failed registration
    - PSK ONLY used in initial registration

HHIT Registration

- I2 can contain a PKIX CSR
  - R2 would contain client's X.509 certificate
  - Provides client with cert to use as needed
- New parameter, CLIENT_INFO for Registry specific information requests and responses
  - Content defined by Registry

HHIT Registration Operation

- RAAs MUST have a HHIT with HDA=0
  - HDAs MUST have a HHIT and register it with RAA
    - RAA uses its HHIT in HDA registration
  - RAA lookup service confirms validity of HDA
- RAA MAY provide a PKI for HHITs
  - e.g. RFC 8002 for HITs in certs
  - HHIT cert used to sign HDA’s client registrations

HHIT Registration Operation

- RAAs MAY provide other signed objects for HDA validity
  - draft-wiethuechter-tmrid-auth provides information on UAS RemoteID signed objects
- HDA HHIT used in client HHIT registration
  - HDA should provide proof of registration
    - X.509, or other signed object like above

Questions?