# Homenet Naming And Service Discovery Architecture

Ted Lemon, Nominum Inc <ted.lemon@nominum.com>

# Goals of this presentation

- Clarify things for people who have already read it
- Get people who have not up to speed
- Are there things in here that are too ambitious?
- Are there things missing?

# What I know is missing

- Forgot to document multiple namespace case, will add
- Forgot to document remote device registration case, will add
- No support for device renaming from homenet management UI
  - This is not possible with mDNS
  - Can be done with DNS update as envisioned
- Otherwise I think this document addresses the requirements in the Homenet Architecture.

# Aspects of the Architecture

- Namespace databases
  - Forward
  - Reverse
  - Does not support mDNSh human-readable subdomain idea
- Public versus local
  - Public is limited (requires user input)
  - Private contains everything
  - Guest namespace?
- Global name versus ".homenet"
  - '.homenet' (or some other name) is fallback if no global name

# The Database

- The database is essentially some DNS zones for which “the homenet” is primary.
- Public and private views of this database are derived from an ideal version of the database
- Updates can be done with DNS protocol and DNS updates
- The same data, with automatic subsetting, will appear in public, private and ‘.homenet’ namespaces.
- Reverse zones are public/private and appear whether delegated or not.

# Database Updates

- Current mDNS Hybrid mechanism is not quite what we want
- We have to define something new
- Has to work for mDNS, would like to preserve mDNS behavior (not chatty), but need to make some effort to have complete information using startup announcements, connection failures, etc.
- In the long term we really want DNS updates with SIG(0) and secure claiming of names

# Global Domain Names

- The homenet should have a global name
- Requires either manual registration or a new service
- New service: GNRP (Global Name Registration Provider)
  - Default way homenet gets global name
  - Does (is required to do) secure delegation
  - Provides working PKI cert (homenet generates key)
  - Can be ISP but not required
  - ISP has to do reverse zone delegation
  - GNRP mechanism must be specified to avoid ad hoc solutions and lock-in
  - Delegation of reverse requires spec

# DNSSEC

- Global zones are all securely delegated and signed
- Public and private zones are signed, and private zone always has higher serial number than public zone
- Local zones can’t have secure delegation, so we use TOFU
    - This uses a per-homenet UUID so that clients can trust more than one homenet and know which homenet they are talking to
    - If two homenets have the same UUID, the second one seen will fail to validate
    - This requires a spec, and I don’t know if people will want it in their resolvers

# Management

- User management
  - Via Browser: requires working PKI.   How do we do management before we have a global name?   Can we use local TOFU + DANE?
  - Phone application - this is a popular solution at the moment, but requires a standard API or else we’ll get lock-in and non-interop
- Central management
  - Desirable for users who want it as a service
  - Netconf/YANG or REST API
  - Need a way to turn it on and provision it, should be standard
- This is really part of the larger management problem

# Comments?

Please review the next version of the document when it comes out.

Thanks!

# Other Issues

- For disconnected operation we really want local consumers of service to use the ULA. So if we have a ULA, only the ULA should be published in the local zone. Right?
-