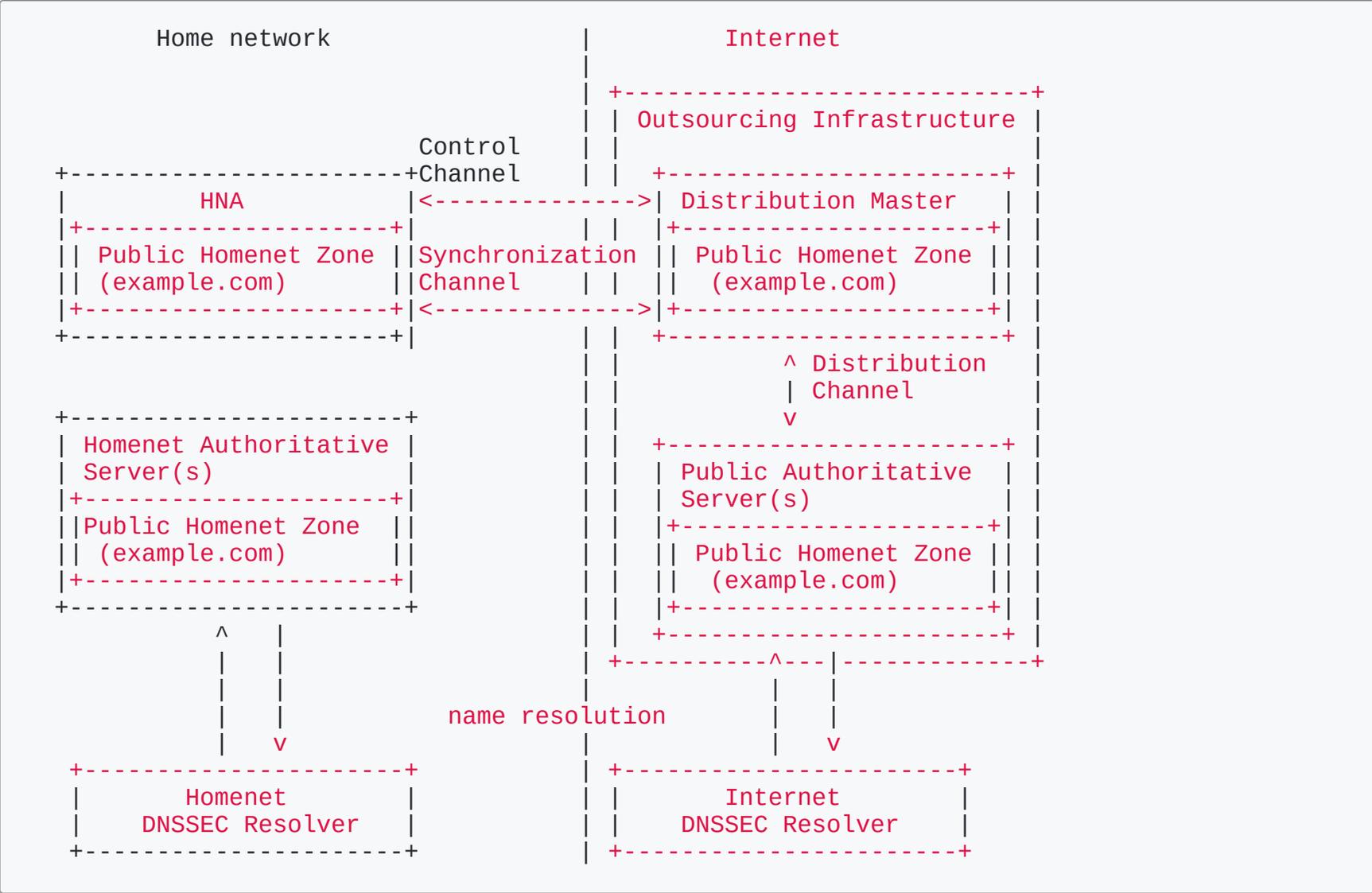


# **Outsourcing Home Network Authoritative Naming Service**

draft-ietf-front-end-naming-delegation-10

**Migault, Richardson, Hunter, Weber, Griffith, Cloetens**



# Channels between the HNA and the DM

Synchronization Channel uses DNS

Control Channel runs over DNS over TLS

- HNA retrieves AXFR responses from the DM (NS, AAAA, A, SOA)
- HNA sends DNS updates to the DM (secondary, DS, STOP)

We have a proof of concept developed by Ray.

Motivation for using DNS:

- DNS libraries are installed anyway
- HTTP libraries are not necessarily installed:
  - code complexity (multiple libraries, various versions...)
  - increases attack surface

Downside:

- May make hard the usage of OAUTH.

# WHY using OAUTH ?

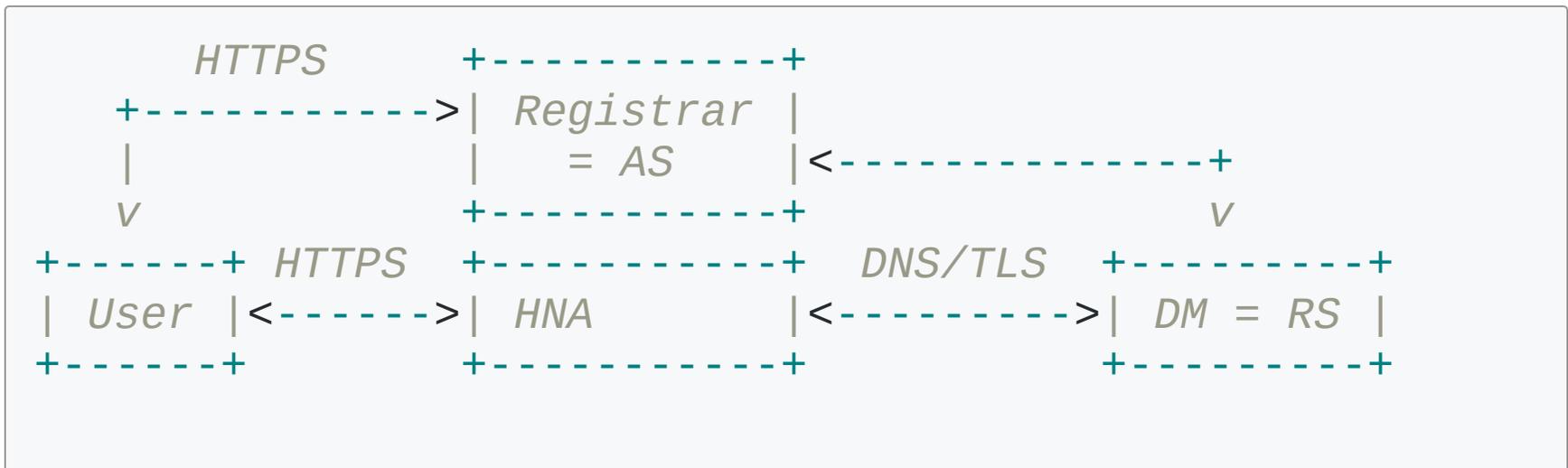
Currently the expected procedure for registration is based on:

1. User would go to the web interface of the home router,
2. Select a compatible DNS provider,
3. buy the domain, process payment
4. get a link and copy /paste that link on the web interface

OAUTH improves automation:

1. User would go to the web interface of the home router,
2. Select a compatible DNS provider,
3. buy the domain, process payment
4. redirect back to the home router

# How to take advantage of OAUTH ?



How DNS over TLS could carry authorization from AS ?

- using DNS over HTTPS
- Maybe: RFC8705 OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens

Thanks!