

Distribution of Oblivious Configurations via Service Binding Records

draft-pauly-ohai-svcb-config

Tommy Pauly, Tiru Reddy
OHAI
IETF 113, March 2022, Vienna

What does this document do?

Sends configs and paths for OHTTP targets through DNS records

Defines new SVCB / HTTPS record parameters

Explains usage for generic HTTP services

Explains usage for accessing Oblivious DNS servers

Integrates with DDR / DNR from ADD WG

Also explains use with previous version of ODoH

What does this document not do?

Doesn't cover oblivious proxy discovery

Could be added, but isn't necessarily something that should be discovered in the same way

Proxies get to see a client's IP and identity directly, and thus can require more trust/validation

...more on this later

Examples

Advertising an Oblivious DNS service config

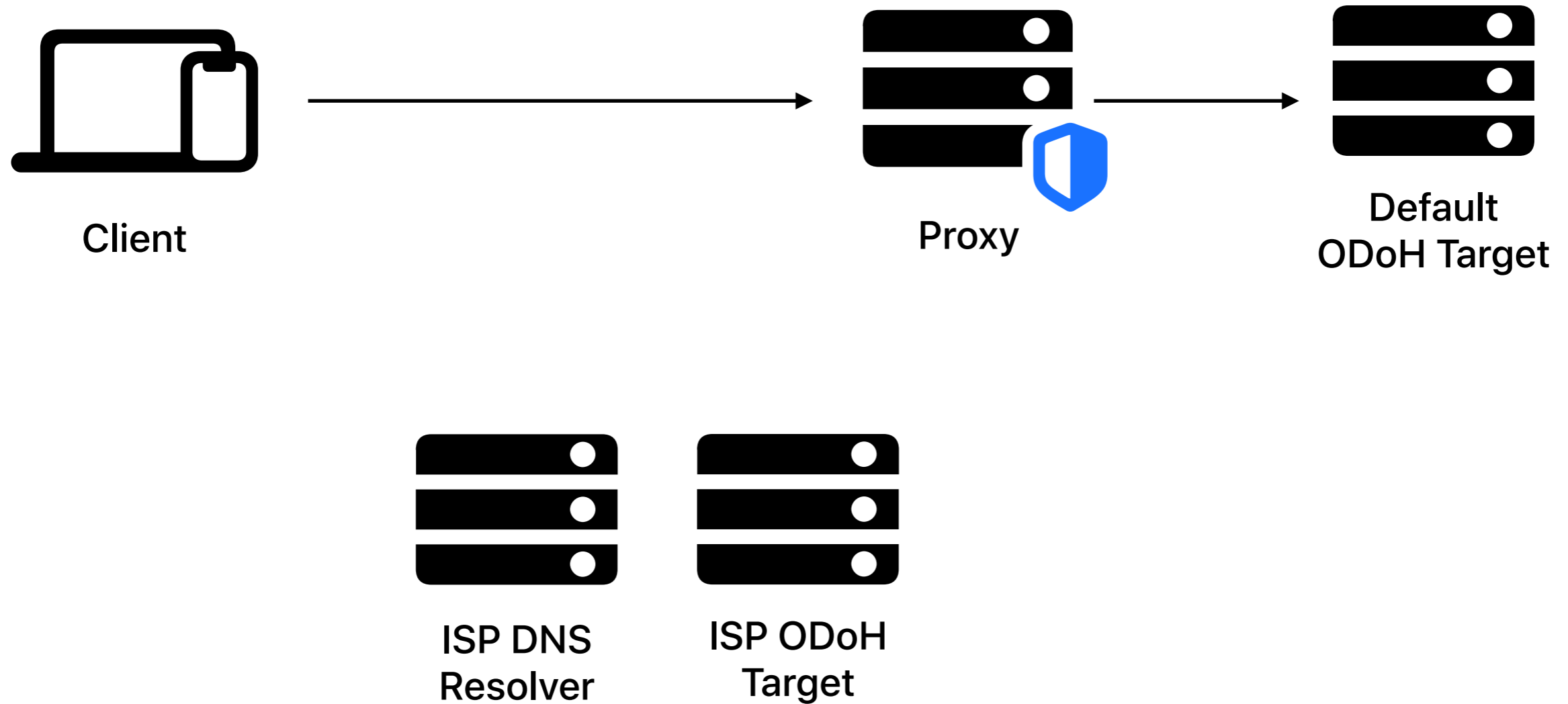
```
_dns.resolver.arpa 7200 IN SVCB 1 odoh.example.net.  
( mandatory=ohttp-configs alpn=h2 dohpath=/dns-query{?dns} ohttp-  
configs=... )
```

Advertising a generic OHTTP config

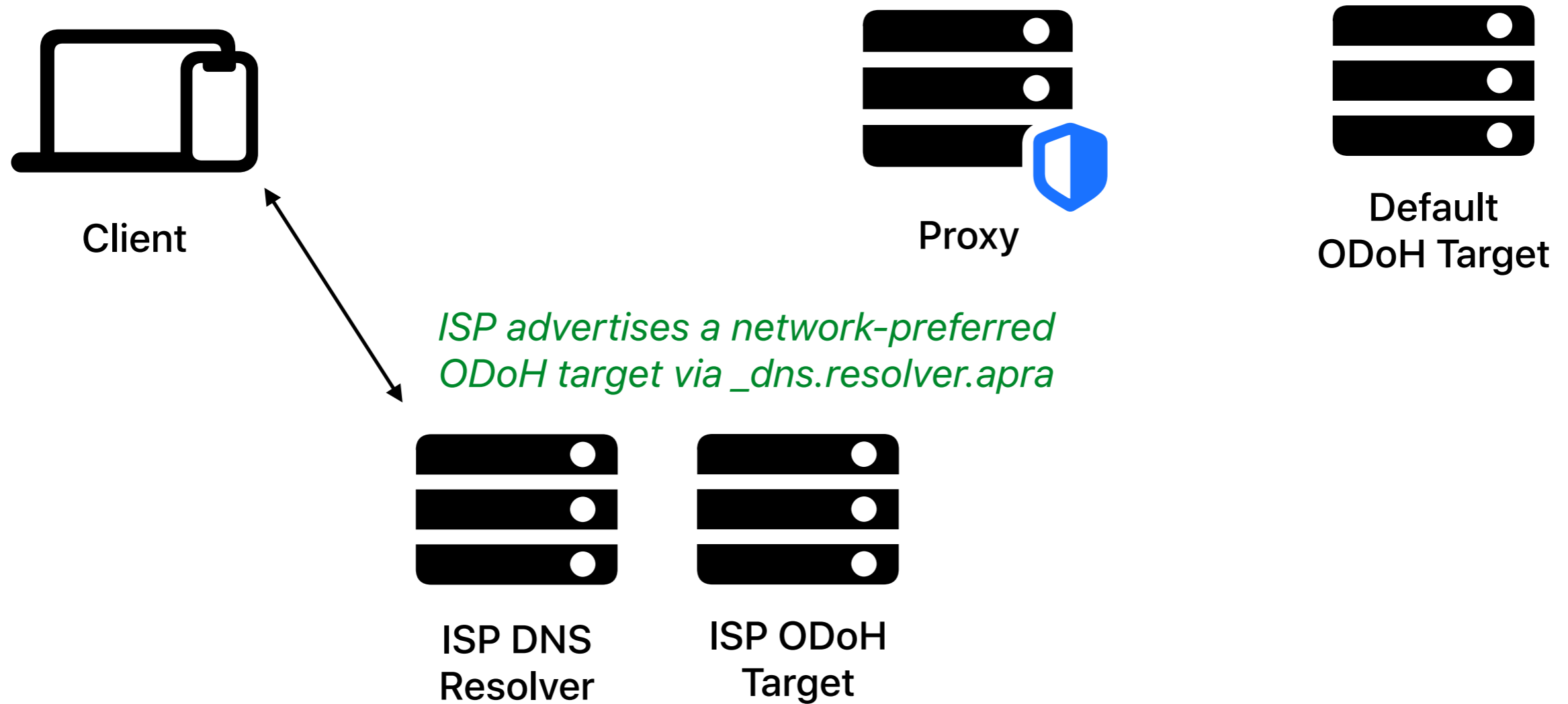
```
metrics-upload.example.net. 7200 IN HTTPS 1 . ( mandatory=ohttp-  
configs alpn=h2 ohttp-path=/oblivious-upload ohttp-configs=... )
```

DNS Server Example

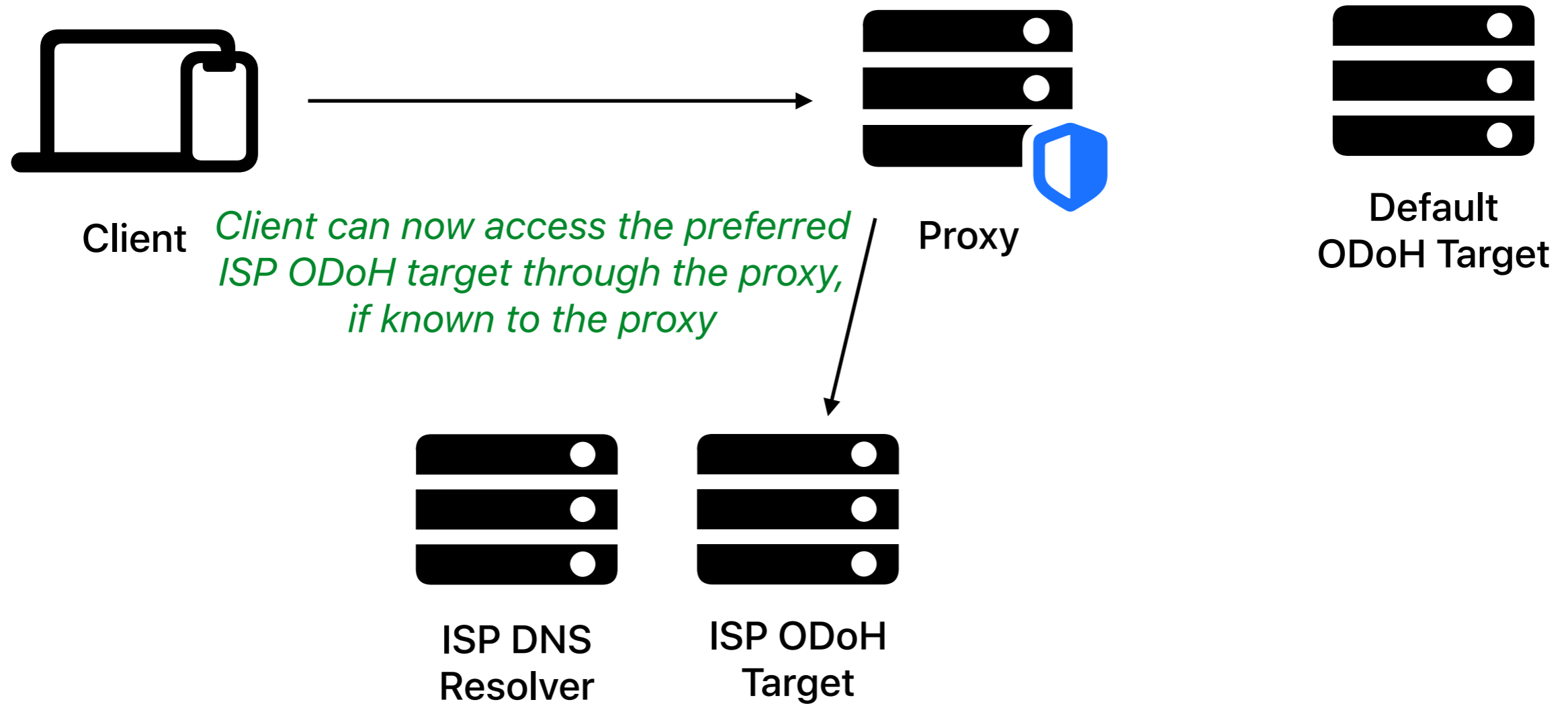
By default, client uses a public ODoH server



DNS Server Example



DNS Server Example



Proxy Usage

Deployment model that this works for:

- Client knows one or more proxies it trusts
- Client wants to be able to access oblivious targets that are published either by their ISP or in the public DNS
- Client can discover if a target is supported by a proxy, and what path to use
- Path mapping will be per-proxy; proxies might support URI-template paths (`/targethost={host},targetpath={path}`)

Unknown/untrusted proxy model is less clear for discovery

Does someone have a use case for that? Let's add it!

Next steps

Adopt?

Seems to be in scope for charter

Get SVCB parameters allocated