Discovery of Oblivious Services via Service Binding Records

draft-ietf-ohai-svcb-config-00

Tommy Pauly, Tiru Reddy
OHAI
IETF 115, November 2022, London
Discovery model

*Client wants to use a target service, and also has a trusted Oblivious Relay it works with*
Discovery model

Target service works with an Oblivious Gateway for OHTTP access (may be co-located)
Discovery model

*Goal is to let the client use its relay to reach the target through the cooperating Oblivious Gateway*
Mechanisms

DNS SVCB/HTTPS parameter for gateway discovery (effectively a boolean parameter)

Well-known URI for gateway requests

Key configuration lookup on gateway URI

These mechanisms are designed to ensure that a discovered gateway and its config are bound to the target
Examples

DNS response (SVCB/HTTPS)

svc.example.com. 7200 IN HTTPS 1. (alpn=h2 oblivious)

Oblivious gateway location

https://svc.example.com/.well-known/oblivious-gateway

Key configuration query

GET /.well-known/oblivious-gateway HTTP/1.1
Host: svc.example.com
Accept: application/ohttp-keys
SVCB Parameter Name
Issue #30

Current parameter name is "oblivious"

Suggestion to change this to "ohttp" to avoid future ambiguity
Media type for DNS
Issue #29
One use case is for \_dns SVCB records (not HTTPS) to discover Oblivious DoH gateways
Currently not clearly written, however
Path forward:

Inner media type: message/bhttp
Outer media type: message/ohttp-*
Target is a DoH resolver
DDR Verification
Issue #28

For DNS resolver discovery, discovery from _dns.resolver.arpa normally requires clients to validate an IP address in the target certificate

Text describes that the client either checks directly, or uses a separate proxied (CONNECT) request to the target

Is this sufficient?