

Oblivious HTTP Application Intermediation  
Internet-Draft  
Intended status: Informational  
Expires: 6 January 2023

T. Pauly  
Apple Inc.  
T. Reddy  
Akamai  
5 July 2022

Discovery of Oblivious Services via Service Binding Records  
draft-pauly-ohai-svcb-config-02

## Abstract

This document defines a parameter that can be included in SVCB and HTTPS DNS resource records to denote that a service is accessible using Oblivious HTTP, with an indication of which Oblivious Gateway Resource to use to access the service (as an Oblivious Target Resource). This document also defines a mechanism to learn the key configuration of the related Oblivious Gateway Resource.

## About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-pauly-ohai-svcb-config/>.

Discussion of this document takes place on the Oblivious HTTP Application Intermediation Working Group mailing list (<mailto:ohai@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/ohai/>.

Source for this draft and an issue tracker can be found at <https://github.com/tfpaully/draft-ohai-svcb-config>.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Internet-Draft

Oblivious Services in SVCB

July 2022

This Internet-Draft will expire on 6 January 2023.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Conventions and Definitions . . . . .	<a href="#">3</a>
<a href="#">3.</a>	The oblivious-gateway SvcParamKey . . . . .	<a href="#">3</a>
<a href="#">3.1.</a>	Use in HTTPS service records . . . . .	<a href="#">4</a>
<a href="#">3.2.</a>	Use in DNS server SVCB records . . . . .	<a href="#">5</a>
<a href="#">3.2.1.</a>	Use with DDR . . . . .	<a href="#">5</a>
<a href="#">3.2.2.</a>	Use with DNR . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Key Configuration Fetching . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Security and Privacy Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">6.1.</a>	SVCB Service Parameter . . . . .	<a href="#">7</a>
<a href="#">7.</a>	References . . . . .	<a href="#">8</a>
<a href="#">7.1.</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">7.2.</a>	Informative References . . . . .	<a href="#">9</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

## [1.](#) Introduction

Oblivious HTTP [[OHTTP](#)] allows clients to encrypt messages exchanged with an Oblivious Target Resource (target). The messages are encapsulated in encrypted messages to an Oblivious Gateway Resource (gateway), which gates access to the target. The gateway is accessed via an Oblivious Relay Resource (relay), which proxies the encapsulated messages to hide the identity of the client. Overall, this architecture is designed in such a way that the relay cannot

inspect the contents of messages, and the gateway and target cannot discover the client's identity.

Since Oblivious HTTP deployments will often involve very specific coordination between clients, relays, and gateways, the key configuration can often be shared in a bespoke fashion. However, some deployments involve clients discovering oblivious targets and their associated gateways more dynamically. For example, a network may want to advertise a DNS resolver that is accessible over Oblivious HTTP and applies local network resolution policies via mechanisms like Discovery of Designated Resolvers ([[DDR](#)]). Clients can work with trusted relays to access these gateways.

This document defines a mechanism to advertise that an HTTP service supports Oblivious HTTP using DNS records, as a parameter that can be included in SVCB and HTTPS DNS resource records [[SVCB](#)]. The presence of this parameter indicates that a service can act as an oblivious target, and indicates an oblivious gateway that can provide access to the target.

This document also defines a way to fetch an oblivious gateway's key configuration by sending a request to the gateway ([Section 4](#)).

This mechanism does not aid in the discovery of oblivious relays; relay configuration is out of scope for this document.

## [2](#). Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

## [3](#). The oblivious-gateway SvcParamKey

The "oblivious-gateway" SvcParamKey ([Section 6](#)) is used to indicate that a service described in an SVCB record can be accessed as an oblivious target using the specified gateway. The service that is

queried by the client hosts one or more target resources. The gateway is a separate resource that is indicated by the SVCB record parameter, which allows oblivious access to any target resource hosted by the service described in the SVCB record.

In order to access the service's target resources obliviously, the client needs to send encapsulated messages to the gateway resource using the gateway's key configuration (which can be retrieved using the method described in [Section 4](#)).

The presentation format of the "oblivious-gateway" parameter is a comma-separated list of one or more gateway URIs. URIs MUST be encoded as escaped items if they include "," or "\"", replacing these with "\", and "\", respectively.

The wire format consists of one or more URIs encoded in UTF-8 [[RFC3629](#)], each prefixed by its length as a single octet, with these length-value pairs concatenated to form the SvcParamValue. These pairs MUST exactly fill the SvcParamValue; otherwise, the SvcParamValue is malformed.

The "oblivious-gateway" parameter can be included in the mandatory parameter list to ensure that clients that do not support oblivious access do not try to use the service. Services that mark the oblivious-gateway parameter as mandatory can, therefore, indicate that the service might not be accessible in a non-oblivious fashion. Services that are intended to be accessed either with an oblivious gateway or directly SHOULD NOT mark the "oblivious-gateway" parameter as mandatory. Note that since multiple SVCB responses can be provided for a single query, the oblivious and non-oblivious versions of a single service can have different SVCB records to support different names or properties.

The media type to use for encapsulated requests made to a target service depends on the scheme of the SVCB record. This document defines the interpretation for the "https" [[SVCB](#)] and "dns" [[DNS-SVCB](#)] schemes. Other schemes that want to use this parameter MUST define the interpretation and meaning of the configuration.

### [3.1.](#) Use in HTTPS service records

For the "https" scheme, which uses the HTTPS RR type instead of SVCB, the presence of the "oblivious-gateway" parameter means that the target being described is an Oblivious HTTP service that uses the default "message/bhttp" media type [[OHTTP](#)] [[BINARY-HTTP](#)].

For example, an HTTPS service record for svc.example.com that supports an oblivious gateway could look like this:

```
svc.example.com. 7200 IN HTTPS 1 . (  
    alpn=h2 oblivious-gateway=https://osvc.example.com/gateway )
```

A similar record for a service that only support oblivious connectivity could look like this:

```
svc.example.com. 7200 IN HTTPS 1 . (  
    mandatory=oblivious-gateway  
    oblivious-gateway=https://osvc.example.com/gateway )
```

### [3.2.](#) Use in DNS server SVCB records

For the "dns" scheme, as defined in [[DNS-SVCB](#)], the presence of the "oblivious-gateway" parameter means that the DNS server being described is an Oblivious DNS over HTTP (DoH) service. The default media type expected for use in Oblivious HTTP to DNS resolvers is "application/dns-message" [[DOH](#)].

In order for DNS servers to function as oblivious targets, their associated gateways need to be accessible via an oblivious relay. Encrypted DNS servers used with the discovery mechanisms described in this section can either be publicly accessible, or specific to a network. In general, only publicly accessible DNS servers will work as oblivious DNS servers, unless there is a coordinated deployment with an oblivious relay that is also hosted within a network.

#### [3.2.1.](#) Use with DDR

Clients can discover an oblivious DNS server configuration using DDR, by either querying `_dns.resolver.arpa` to a locally configured resolver or querying using the name of a resolver [[DDR](#)].

For example, a DoH service advertised over DDR can be annotated as supporting oblivious resolution using the following record:

```
_dns.resolver.arpa 7200 IN SVCB 1 doh.example.net (
  alpn=h2 dohpath=/dns-query{?dns}
  oblivious-gateway=https://odoh.example.net/gateway )
```

Clients still need to perform some verification of oblivious DNS servers, such as the TLS certificate check described in [DDR]. This certificate check can be done when looking up the configuration on the gateway as described in [Section 4](#), which can either be done directly, or via the relay or another proxy to avoid exposing client IP addresses.

Clients also need to ensure that they are not being targeted with unique key configurations that would reveal their identity. See [Section 5](#) for more discussion.

### [3.2.2](#). Use with DNR

The SvcParamKeys defined in this document also can be used with Discovery of Network-designated Resolvers (DNR) [DNR]. In this case, the oblivious configuration and path parameters can be included in DHCP and Router Advertisement messages.

While DNR does not require the same kind of verification as DDR, clients still need to ensure that they are not being targeted with unique key configurations that would reveal their identity. See [Section 5](#) for more discussion.

## [4](#). Key Configuration Fetching

Clients that know a service is available as an oblivious target via discovery through the "oblivious-gateway" parameter in a SVCB or HTTPS record need to know the key configuration of the gateway before sending oblivious requests.

In order to fetch the key configuration of an oblivious gateway discovered in this manner, the client issues a GET request to the URI of the gateway specifying the "application/ohttp-keys" ([OHTTP])

media type in the Accept header.

For example, if the client receives the following record:

```
svc.example.com. 7200 IN HTTPS 1 . (  
    alpn=h2 oblivious-gateway=https://osvc.example.com/gateway )
```

It could fetch the key configuration with the following request:

```
GET /gateway HTTP/1.1  
Host: osvc.example.com  
Accept: application/ohttp-keys
```

Oblivious gateways that coordinate with targets that advertise oblivious support SHOULD support GET requests for their key configuration in this manner, unless there is another out-of-band configuration model that is usable by clients. Gateways respond with their key configuration in the response body, with a content type of "application/ohttp-keys".

Clients can either fetch this key configuration directly, or do so via a proxy in order to avoid the server discovering information about the client's identity. See [Section 5](#) for more discussion of avoiding key targeting attacks.

## [5](#). Security and Privacy Considerations

Attackers on a network can remove SVCB information from cleartext DNS answers that are not protected by DNSSEC [[DNSSEC](#)]. This can effectively downgrade clients. However, since SVCB indications for oblivious support are just hints, a client can mitigate this by always checking for oblivious gateway information. Use of encrypted DNS along with DNSSEC can be used as a mitigation.

When discovering designated oblivious DNS servers using this mechanism, clients need to ensure that the designation is trusted in lieu of being able to directly check the contents of the gateway server's TLS certificate. See [Section 3.2.1](#) for more discussion, as well as the Security Considerations of [[I-D.ietf-add-svcb-dns](#)].

As discussed in [[OHTTP](#)], client requests using Oblivious HTTP can only be linked by recognizing the key configuration. In order to

prevent unwanted linkability and tracking, clients using any key configuration discovery mechanism need to be concerned with attacks that target a specific user or population with a unique key configuration.

There are several approaches clients can use to mitigate key targeting attacks. [CONSISTENCY] provides an analysis of the options for ensuring the key configurations are consistent between different clients. Clients SHOULD employ some technique to mitigate key targeting attack. Oblivious gateways that are detected to use targeted key configurations per-client MUST NOT be used.

When clients fetch a gateway's configuration ([Section 4](#)), they can expose their identity in the form of an IP address if they do not connect via a proxy or some other IP-hiding mechanism. In some circumstances, this might not be a privacy concern, since revealing that a particular client IP address is preparing to use an Oblivious HTTP service can be expected. However, if a client is otherwise trying to obfuscate its IP address or location (and not merely decouple its specific requests from its IP address), or revealing its IP address will increase the risk of a key targeting attack (if a gateway service is trying to differentiate traffic across client IP addresses), a proxy or similar mechanism can be used to fetch the gateway's configuration.

## [6.](#) IANA Considerations

### [6.1.](#) SVCB Service Parameter

IANA is requested to add the following entry to the SVCB Service Parameters registry ([\[SVCB\]](#)).



Number	Name	Meaning	Reference
TBD	oblivious-gateway	Defines an oblivious HTTP gateway to use to access this resource	(This document)

Table 1

## 7. References

### 7.1. Normative References

#### [BINARY-HTTP]

Thomson, M. and C. A. Wood, "Binary Representation of HTTP Messages", Work in Progress, Internet-Draft, [draft-ietf-httpbis-binary-message-05](https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-binary-message-05), 9 June 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-binary-message-05>>.

#### [DDR]

Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, [draft-ietf-add-ddr-08](https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-08), 5 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-ddr-08>>.

#### [DNR]

Boucadair, M., Reddy, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, [draft-ietf-add-dnr-09](https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-09), 24 June 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-dnr-09>>.

#### [DNS-SVCB]

Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, [draft-ietf-add-svcb-dns-06](https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-06), 5 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-06>>.

#### [DOH]

Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", [RFC 8484](https://www.rfc-editor.org/rfc/rfc8484), DOI 10.17487/RFC8484, October 2018, <<https://www.rfc-editor.org/rfc/rfc8484>>.

#### [OHTTP]

Thomson, M. and C. A. Wood, "Oblivious HTTP", Work in Progress, Internet-Draft, [draft-ietf-ohai-ohttp-01](https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-01), 15 February 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-ohai-ohttp-01>>.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/rfc/rfc2119>>.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, [RFC 3629](#), DOI 10.17487/RFC3629, November 2003, <<https://www.rfc-editor.org/rfc/rfc3629>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/rfc/rfc8174>>.
- [SVCB] Schwartz, B., Bishop, M., and E. Nygren, "Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)", Work in Progress, Internet-Draft, [draft-ietf-dnsop-svcb-https-10](#), 24 May 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-svcb-https-10>>.

## [7.2.](#) Informative References

- [CONSISTENCY] Davidson, A., Finkel, M., Thomson, M., and C. A. Wood, "Key Consistency and Discovery", Work in Progress, Internet-Draft, [draft-wood-key-consistency-02](#), 4 March 2022, <<https://datatracker.ietf.org/doc/html/draft-wood-key-consistency-02>>.
- [DNSSEC] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", [RFC 4033](#), DOI 10.17487/RFC4033, March 2005, <<https://www.rfc-editor.org/rfc/rfc4033>>.
- [I-D.ietf-add-svcb-dns] Schwartz, B., "Service Binding Mapping for DNS Servers", Work in Progress, Internet-Draft, [draft-ietf-add-svcb-dns-06](#), 5 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-add-svcb-dns-06>>.

## Authors' Addresses

Tommy Pauly  
Apple Inc.  
Email: [tpauly@apple.com](mailto:tpauly@apple.com)

Pauly & Reddy

Expires 6 January 2023

[Page 9]

---

Internet-Draft

Oblivious Services in SVCB

July 2022

Tirumaleswar Reddy  
Akamai  
Email: kondtir@gmail.com

