DNSOP Working Group J. Stenstam
Internet-Draft L. Fernandez
Intended status: Standards Track E. Bergstr旦m
Expires: 25 December 2025 The Swedish Internet Foundation
23 June 2025

Authoritative DNS Transport Signaling
draft-johani-dnsop-transport-signaling-01

Abstract

This document proposes a mechanism for authoritative DNS servers to opportunistically signal their support for alternative transport protocols (e.g., DNS over TLS (DoT), DNS over HTTPS (DoH) and DNS over QUIC (DoQ)) directly within the Additional section of authoritative DNS responses. This "hint-based" approach aims to enable resolvers to discover and upgrade transport connections more efficiently, thereby improving privacy, security, and performance for subsequent interactions.

The mechanism is designed to not require any protocol change. It is safe, backward-compatible, and effective even when DNSSEC validation of the hint is not possible or desired.

This document proposes an improvement on the opportunistic (but blind) testing of alternative transports suggested in RFC9539 by providing a mechanism by which a responding authoritative server may signal what alternative transports it supports.

TO BE REMOVED: This document is being collaborated on in Github at: https://github.com/johanix/draft-johani-dnsop-transport-signaling (https://github.com/johanix/draft-johani-dnsop-transport-signaling). The most recent working version of the document, open issues, etc, should all be available there. The authors (gratefully) accept pull requests.

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."

This Internet-Draft will expire on 25 December 2025.

Copyright Notice

Copyright (c) 2025 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

1. 1. Introduction

The Domain Name System (DNS) primarily relies on UDP and TCP for communication between resolvers and authoritative servers. While these protocols are well-established, there is a growing interest in leveraging modern transport protocols like DNS over TLS (DoT) [RFC7858], DNS over HTTPS (DoH) [RFC9461] and DNS over QUIC (DoQ) [RFC9250] to enhance privacy, security, and performance.

Existing efforts to signal service connection information, such as the SVCB and HTTPS DNS records [RFC9460] [RFC9461], primarily focus on service discovery mechanisms where a client explicitly queries for these records, often from a parent zone. While robust, this approach can introduce additional latency and requires explicit configuration at the parent zone level.

This document proposes an "DNS Opportunistic Transport Signaling" (DNS OTS) mechanism. DNS OTS, aka an "OTS Hint" allows an authoritative DNS nameserver to directly convey its transport capabilities as a hint within the Additional section of responses to queries where it identifies itself as an authoritative nameserver for the requested zone. This direct, in-band signaling provides a low-latency discovery path, even when a formal, validated signal is not available. Furthermore, this is achieved without any changes to the DNS Protocol.

1.1. 1.1. Prior Art

An attempt at utilizing more modern, and in particular, more private transports between resolvers and authoritative nameservers was introduced in [RFC9539]. The idea there was to opportunistically try to send the query to the authoritative nameserver over multiple transports with no prior knowledge of whether a transport was supported in the receiving end or not.

The drawback with that approach is that without any significant deployment of authoritative support the resolver end will mostly spend cycles and traffic on a wasted effort. For this reason there seems not to be any known implementations.

Furthermore, in Appendix B of [RFC9539] requirements for improving the defense against an active attacker are listed. The first requirement is:

* A signaling mechanism that tells the recursive resolver that the authoritative server intends to offer authenticated encryption.

This document aims to provide exactly such a mechanism while staying within the current DNS protocol. Therefore the transport signaling provided will be opportunistic, and as such fit well as an improvement to [RFC9539].

1.2. Rationale for Using the Additional Section

Note to the RFC Editor: Please remove this entire section before publication.

When designing a mechanism that rely on sending new information in DNS responses without changing the current DNS protocol, the Additional section has the major advantage of being ignored by legacy software. This property makes it possible to essentially deploy the proposed mechanism immediately, as it will not cause problems with existing DNS infrastructure.

* Existing authoritative nameservers will not provide any OTS Hint in the Additional section.

* Existing resolvers will actively ignore any OTS Hint in the Additional section.

Only DNS nameservers (authoritative or recursive) that are aware of the proposed mechanism will use it.

The downside is that it is not possible to strictly rely on anything specific being present in the Additional section, as it may be stripped off by a middle man or even by the sending nameserver (eg. due to packet size constraints). For this reason it is not possible to provide more than an opportunistic transport signal.

Another issue is whether the data provided may be trusted or not. This is usually a major issue and the primary reason that data in the Additional section is actively ignored by resolvers. In this particular case, though, even an untrusted transport signal is better than no signal at all. Furthermore, the only effect of a forged or otherwise incorrect transport signal is a, typically failed, connection attempt to an authoritative nameserver that does not support the advertised transport. This will cause immediate fallback to "Do53", i.e. traditional DNS over UDP/TCP and the non-availability of the advertised transport will be remembered by the resolver (for some suitable time).

Hence, using the Additional section for opportunistic transport signaling has vastly more benefits than drawbacks.

2. 2. Terminology

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.

* *Authoritative Nameserver (Auth Server):* A DNS server that holds the authoritative zone data for a specific domain.

* *Recursive Nameserver (Resolver):* A DNS server that processes user queries, performing iterative lookups to authoritative servers to resolve domain names.

* *OTS Hint:* An SVCB record included opportunistically in the Additional section of an authoritative DNS response, intended to signal the responding authoritative nameserver’s transport capabilities.

* *SVCB Record:* Service Binding record, as defined in [RFC9460].

3. 3. The Opportunistic Signaling Mechanism

The core of this proposal is for an authoritative nameserver to include an SVCB record in the Additional section of its responses under specific conditions.

This consists of three parts. The first two are the behaviour of the authoritative nameserver receiving the query and the rehaviour of the recursive nameserver receiving the response. The final part is a new EDNS(0) option that defines an OPT-OUT capability.

4. 4. Authoritative Nameserver Behaviour

4.1. 4.1. Trigger Conditions for Including the OTS Hint

An authoritative nameserver SHOULD include an OTS Hint when _all_ of the following conditions are met:

1. *NS RRset Presence:* An NS Resource Record Set (RRset) for the queried zone is present in either the Answer section or the Authority section of the DNS response.

2. *Self-Identification:* The responding authoritative nameserver's own Fully Qualified Domain Name (FQDN) (or one of its configured aliases/identities) is found within the NS RRset mentioned in condition 1.

3. *Transport Capability:* The responding authoritative nameserver supports one or more alternative transport protocols (e.g., DoT, DoH, DoQ) and is configured to advertise these capabilities.

4. *Absence of the No-OTS Option:* The query does not include an EDNS(0) No-OTS option from the resolver.

5. *Availability of RRSIG SVCB:* If the zone in which the nameserver name is located is signed, only include the SVCB record if it is possible to also include the corresponding RRSIG SVCB. If the zone with the nameserver name is unsigned, then include the SVCB even without the RRSIG.

4.2. 4.2. Multiple Server Identities

An authoritative nameserver may be known by multiple FQDNs (e.g., ns1.example.com, dns.customer.org, ns.cdnprovider.net). To facilitate condition 2 ("Self-Identification"), authoritative server implementations MAY include a configuration mechanism (e.g., an identities list) where operators can list all FQDNs by which the server is known. This allows the server to correctly identify itself regardless of the specific name used in the NS RRset.

4.3. 4.3. Format of the OTS Hint

The OTS Hint MUST be an SVCB record with the following characteristics:

* *OWNER:* The owner name of the SVCB record MUST be the FQDN of the authoritative nameserver itself, as identified in the NS RRset that triggered its inclusion (e.g., ns.dnsprovider.com.).

* *CLASS:* IN (Internet).

* *TYPE:* SVCB.

* *TTL:* The TTL of the SVCB record SHOULD be chosen by the authoritative server operator. Choice of TTL is a local configuration decision, but unless the supported transports are subject to frequent change a value on the order of 24h or more is suggested.

* *SVCB_PRIORITY:* 1. The specific priority value is not critical for this hint mechanism, but 1 indicates the highest priority for the service.

* *SVCB_TARGET:* . (root). This indicates that the DNS transport capabilities described by the SVCB record refer to the owner name of the record.

* *SVCB_PARAMS:* A set of Service Parameters indicating the supported transport protocols. In this document only the "alpn" parameter [RFC9460] is defined, as relevant for signaling DoT (alpn=dot), DoH (alpn=doh) and DoQ (alpn=doq).

  If any other parameter, including "ipv4hint" and "ipv6hint", is present in the SVCB parameter list then it SHOULD be ignored.

Example 1:

If ns.dnsprovider.net. responds to a query for www.example.com. and ns.dnsprovider.net is listed in the NS RRset, it may respond with a DNS message that contains: ~~~ Header: ...

Answer: www.example.com. IN A 1.2.3.4

Authority: example.com. IN NS ns1.example.com. example.com. IN NS ns.dnsprovider.net.

Additional: ns.dnsprovider.net. IN A 5.6.7.8 ns.dnsprovider.net. IN RRSIG A ... ns.dnsprovider.net. IN SVCB 1 . "alpn=doq,dot,do53" ns.dnsprovider.net. IN RRSIG SVCB ... ~~~ *Example 2:*

If the unsigned zone example.com uses ns.dnsprovider.net., but under the vanity name "ns2.example.com." (with the same IP addresses), then a possible response from ns.dnsprovider.net (aka ns2.example.com) may be: ~~~ Header: ...

Answer: www.example.com. IN A 1.2.3.4

Authority: example.com. IN NS ns1.example.com. example.com. IN NS ns2.example.com.

Additional: ns2.example.com. IN A 5.6.7.8 ns2.example.com. IN SVCB 1 . "alpn=doq,dot,do53" ~~~ This requires that "ns2.example.com." is a name that ns.dnsprovider.net. is aware of as one of its identities. Furthermore, as the zone example.com is unsigned it is not possible to provide a DNSSEC signed OTS Hint in the second example.

5. 5. Recursive Nameserver Behavior

Recursive nameservers adopting this mechanism SHOULD implement the following logic:

5.1. 5.1. When Sending Queries

1. *OPT-OUT Possibility:* If the resolver already thinks that it knows the transport capabilities of the authoritative nameserver it is about to send a query to it may opt out from DNS transport signaling by including an EDNS(0) "No-OTS" option in the query.

5.2. 5.2. When Receiving Responses

1. *Opportunistic Parsing:* When receiving an authoritative DNS response, the resolver SHOULD parse the Additional section for SVCB records.

2. *Owner Check:* If an SVCB record is found whose owner name matches an authoritative nameserver identified in the Authority or Answer sections of the _current_ response, the resolver MAY consider this an OTS Hint.

3. *DNSSEC Validation (Optional but Recommended):* * The resolver SHOULD attempt to DNSSEC validate the OTS Hint. This involves validating the SVCB record itself and its corresponding RRSIG (if present) against the DNSSEC chain of trust for the zone that owns the SVCB record (e.g., dnsprovider.com for ns.dnsprovider.com).

* If validation succeeds: The OTS Hint is considered a *trusted signal*. The resolver MAY then prefer the signaled alternative transports for subsequent queries to that specific authoritative nameserver.

* If validation fails, or no RRSIG is present: The OTS Hint MUST be treated as an *unvalidated hint*. The resolver MAY still opportunistically attempt to use the signaled alternative transports, but MUST be prepared for immediate fallback to traditional transports (UDP/TCP) if the connection fails. This is particularly relevant for scenarios like vanity names (e.g., ns.customer.com where customer.com is an unsigned zone, but the underlying server ns.dnsprovider.com is capable).

1. *Prioritization:* * Any DNSSEC-validated SVCB record found via explicit query (e.g., ns.example.com for a queried domain MUST take precedence over any unvalidated OTS Hint.

* The OTS Hint is a mechanism to _discover_ capabilities opportunistically, not to override trusted delegation or service configuration.

1. Fallback: Resolvers MUST always be prepared to fall back to traditional UDP/TCP transport if an attempt to use an alternative transport based on an OTS Hint (especially an unvalidated one) fails or times out.

5.3. 5.3. Authentication of the Authoritative Nameserver

Authentication of the authoritative nameserver is not an explicit goal. The reason is that as an opportunistic mechanism it will not always be possible to do such authentication. Some of the options that do exist are listed below.

Authentication of the authoritative nameserver may be done either by validation of a DNSSEC RRSIG over the SVCB record containing the OTS Hint or by verification of the server certificate presented in the set up of the communication (be it over DoT, DoQ or DoH).

As there will not always be a DNSSEC signature to validate that option is opportunistic at best. Likewise, while it may sometimes be possible to validate the server cert against a DNSSEC-signed TLSA record, it will not always be an option.

Finally, validating the server cert against a list of well-known public Certificate Authorities is possible, but there is no standardized way to determine which CAs are appropriate for DNS server certificates.

However, even without strong authentication of the authoritative server the proposed mechanism still provides benefits (privacy, potential performance improvements) and for that reason cryptographic verification of the server identity is not a requirement.

5.4. 5.4. Resolver Caching Strategies

Resolvers implementing the DNS OTS Hint mechanism have several options for caching the transport signals received via OTS Hints.

A suggested primary strategy is to set the EDNS(0) No-OTS option when no transport signaling information is needed (because the resolver already knows the authoritative nameservers transport capabilities from a previous response or for some other reason).

Three example caching strategies are listed below. Other strategies are possible. Each strategy has different trade-offs in terms of efficiency, responsiveness to changes, and resource usage:

1. *Standard DNS Cache:* Treat the SVCB record like any other DNS record, caching it according to its TTL. This is the simplest approach and will simply cause the resolver to fall back to UDP for one query if the transport signal data has expired.

2. *Cache-Until-Fail:* Cache the transport signal until a connection attempt fails, then invalidate the cached entry. This approach uses more aggressive caching based on the assumption that changes to transport capabilites are expected to be rare, and there is no risk of presenting any data that is no longer correct. The possible downside is that the resolver will not learn about possible new transports that become available. E.g., with an "alpn=doq", the resolver will not learn that the authoritative server later started to support DNS-over-TLS (in addition to DoQ) if it is successfully using the DNS-over-QUIC connection.

3. *Success-Based Refresh:* Refresh the transport signal cache entry each time a successful connection is made using that transport. This provides a balance between efficiency and responsiveness but requires additional bookkeeping.

For a more detailed analysis of possible caching logic, see [RFC9539], section 4.

Note that the resolver always has the option of not using the EDNS(0) No-OTS option whenever the cache entry is getting close to expiry.

Given the variety of deployment scenarios and operational requirements, this document does not mandate a specific caching strategy. Implementers SHOULD choose a strategy that best fits their operational needs, considering factors such as:

* The importance of minimizing connection attempts

* The impact of failed connection attempts

* The computational cost of different caching strategies

* The memory requirements of maintaining cache state

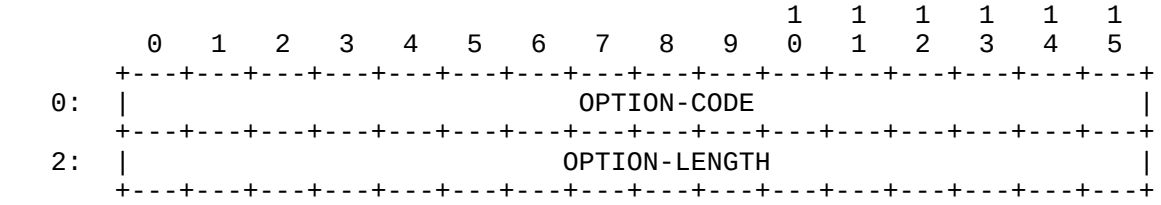
The chosen strategy SHOULD be documented in the implementation’s configuration options to allow operators to make informed decisions about its use.

6. 6. The EDNS(0) No-OTS Option

To provide a mechanism for resolvers to explicitly opt out of receiving transport signals, this document defines a new EDNS(0) option called "No-OTS" (NOTS). When included in a query, this option signals to the authoritative server that the resolver does not want to receive any transport signals in the response.

The typical use case is to set the EDNS(0) No-OTS option when the resolver already has the transport information it needs.

The EDNS(0) No-OTS option is structured as follows:



Field definition details:

OPTION-CODE: 2 octets / 16 bits (defined in [RFC6891]) contains the value TBD for No-OTS.

OPTION-LENGTH: 2 octets / 16 bits (defined in [RFC6891]) contains the length of the payload in octets. For the No-OTS option, this value MUST be 0 as there is no payload.

When an authoritative server receives a query containing the EDNS(0) No-OTS option, it SHOULD NOT include any OTS Hints in the response, regardless of whether it would normally do so based on the conditions described in Section 3.1.

This option provides a clean way for resolvers to opt out of receiving transport signals, which may be useful in scenarios where:

* The resolver has already established transport preferences for a particular authoritative server
* The resolver does not support or does not want to use alternative transports
* The resolver wants to minimize response sizes
* The resolver is operating in an environment where transport signals are not needed or desired

The No-OTS option is designed to be a simple, lightweight mechanism that can be used to disable transport signaling without affecting the normal operation of DNS resolution.

7. 7. Comparison with DELEG

The idea to use an SVCB alpn parameter for transport signaling originated with the work on DELEG [I-D.draft-ietf-deleg]. The current document uses the same data format, but as an opportunistic addition to the Additional section rather than as integral part of a changed delegation mechanism.

Both mechanisms have distinct use cases, and pros and cons. The major advantage of the DELEG mechanism is that it cannot be spoofed or filtered, as it is an integral part of an upcoming protocol change.

The opportunistic mechanism described here has the major advantage of being available immediately without any changes to the DNS protocol. Furthermore, as it is a signal directly from an authoritative nameserver, a single OTS Hint may allow the recipient recursive nameserver to upgrade the transport used for all the zones served by that authoritative nameserver (which may be millions) without the need to make any changes to the zones, nor to the parent zones.

Given the current DNS landscape with a limited number of very large providers of authoritative DNS service and a limited number of large providers of recursive DNS service the opportunistic model described here has the potential of enabling upgrading the transport for a significant fraction of the DNS traffic with a limited amount of effort.

8. 8. Security Considerations

* *Spoofing of Unvalidated Hints:* An OTS Hint that cannot be DNSSEC validated (e.g., for ns.example.com where example.com is unsigned) is susceptible to spoofing by an on-path attacker. Such an attacker could insert a fake SVCB record advertising a non-existing transport, thereby denying connection over that transport. However, since the hint is opportunistic and not required for DNS resolution, the worst-case scenario is that the resolver attempts a connection that fails and then falls back to traditional transports. Security for the actual DNS data remains unaffected. The cryptographic validation of TLS/QUIC (via X.509 certificates) for DoT/DoQ would still protect the integrity and privacy of the connection itself.

* *DNSSEC Validation:* When a OTS Hint is signed by DNSSEC (e.g., the ns.dnsprovider.net SVCB record from a signed dnsprovider.net zone), it provides a trusted signal. Resolvers SHOULD leverage DNSSEC validation to distinguish between trusted and unvalidated hints.

* *No New Attack Vectors:* This mechanism does not introduce new attack vectors for DNS data itself, as it primarily concerns transport discovery. It relies on the existing security properties of DoT, DoH and DoQ for actual session security.

* *Safe Rollout:* As existing recursive nameservers carefully avoid data in the Additional section that they do not need, the OTS Hint will be ignored by everyone except recursive nameservers that understand the OTS Hint.

* *No-OTS enables a downgrade attack:* If an attacker is able to inject a No-OTS option to an outbound query then no transport signal will be provided. However, this is a consequence of the opportunistic nature of the OTS Hint and not worse than not being able to do transport signaling at all.

9. 9. Operational Considerations

* *Response Size:* Including an SVCB record in the Additional section will increase the size of UDP responses. Authoritative server operators should consider the potential for UDP fragmentation or TCP fallback if responses become excessively large, though a single SVCB record is typically small. Recursive nameservers should usually set the EDNS(0) No-OTS when they already have the transport signaling information.

* *Server Configuration:* Authoritative server implementations will need configuration options to enable this feature and manage the identities list.

* *Rollout Strategy:* This mechanism supports a gradual rollout. Authoritative servers can begin sending hints without requiring changes from resolvers, and resolvers can begin processing hints without requiring all authoritative servers to implement the feature.

* *Monitoring:* As there is extremely limited data on effects of alternative DNS transports for communication resolver to authoritative nameserver it is strongly suggested that monitoring (of use, resource consumption, etc) is considered.

10. 10. IANA Considerations

10.1. 10.1. No-OTS EDNS(0) Option

This document defines a new EDNS(0) option, entitled "No-OTS", assigned a value of TBD in the "DNS EDNS0 Option Codes (OPT)" registry.

Value	Name	Status	Reference
TBD	No-OTS	Standard	(This document)

Note to the RFC Editor: In this section, please replace occurrences of "(This document)" with a proper reference.

11. 11. Implementation Status

Note to the RFC Editor: Please remove this entire section before publication.

The TDNS Framework of experimental DNS servers developed and maintained by the Swedish Internet Foundation implements this draft (see https://github.com/johanix/tdns (https://github.com/johanix/tdns)). TDNS has support for both the authoritative nameserver and recursive nameserver parts of the draft.

12. 12. Acknowledgments

* The participants of the DELEG Working Group, Peter Thomassen and Christian Elmerot.

13. References

13.1. Normative References

[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>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/rfc/rfc6891>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[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>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

[RFC9461] Schwartz, B., "Service Binding Mapping for DNS Servers", RFC 9461, DOI 10.17487/RFC9461, November 2023, <https://www.rfc-editor.org/rfc/rfc9461>.

[RFC9539] Gillmor, D. K., Ed., Salazar, J., Ed., and P. Hoffman, Ed., "Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS", RFC 9539, DOI 10.17487/RFC9539, February 2024, <https://www.rfc-editor.org/rfc/rfc9539>.

13.2. Informative References

[I-D.draft-ietf-deleg] April, T., paek, P., Weber, R., and Lawrence, "Extensible Delegation for DNS", Work in Progress, Internet-Draft, draft-ietf-deleg-00, 6 May 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-deleg-00>.

Appendix A. Change History (to be removed before publication)

Initial public draft

Authors' Addresses

Johan Stenstam
The Swedish Internet Foundation
Sweden
Email: johan.stenstam@internetstiftelsen.se

Leon Fernandez
The Swedish Internet Foundation
Sweden
Email: leon.fernandez@internetstiftelsen.se

Erik Bergstrm
The Swedish Internet Foundation
Sweden
Email: erik.bergstrom@internetstiftelsen.se