

Homenet
Internet-Draft
Intended status: Standards Track
Expires: April 25, 2021

D. Migault
Ericsson
R. Weber
Akamai
T. Mrugalski
Internet Systems Consortium, Inc.
C. Griffiths

W. Cloetens
Deutsche Telekom
October 22, 2020

DHCPv6 Options for Home Network Naming Authority
draft-ietf-homenet-naming-architecture-dhc-options-08

Abstract

This document defines DHCPv6 options so any agnostic Homnet Naming Authority (HNA) can automatically proceed to the appropriate configuration and outsource the authoritative naming service for the home network. In most cases, the outsourcing mechanism is transparent for the end user.

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 April 25, 2021.

Copyright Notice

Copyright (c) 2020 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1. Terminology](#) [2](#)
- [2. Introduction](#) [3](#)
- [3. Protocol Overview](#) [4](#)
- [4. Payload Description](#) [5](#)
 - [4.1. Client Public Key Option](#) [5](#)
 - [4.2. Registered Homenet Domain Option](#) [5](#)
 - [4.3. Distribution Master Option](#) [6](#)
 - [4.3.1. Supported Transport](#) [6](#)
 - [4.4. Reverse Distribution Master Server Option](#) [7](#)
- [5. DHCP Behavior](#) [8](#)
 - [5.1. DHCPv6 Server Behavior](#) [8](#)
 - [5.2. DHCPv6 Client Behavior](#) [8](#)
 - [5.3. DHCPv6 Relay Agent Behavior](#) [8](#)
- [6. IANA Considerations](#) [8](#)
- [7. Security Considerations"](#) [9](#)
- [8. Acknowledgments](#) [9](#)
- [9. References](#) [9](#)
 - [9.1. Normative References](#) [9](#)
 - [9.2. Informative References](#) [10](#)
- [Appendix A. Scenarios and impact on the End User](#) [11](#)
- [Appendix B. Base Scenario](#) [11](#)
 - [B.1. Third Party Registered Homenet Domain](#) [11](#)
 - [B.2. Third Party DNS Infrastructure](#) [12](#)
 - [B.3. Multiple ISPs](#) [12](#)
- Authors' Addresses [13](#)

1. 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, as shown here.

The reader is expected to be familiar with [[I-D.ietf-homenet-front-end-naming-delegation](#)] and its terminology section. This section defines terms that have not been defined in [[I-D.ietf-homenet-front-end-naming-delegation](#)]:

- o Client Public Key: designates a public key generated by the HNA and used as an authentication credential for the HNA.

2. Introduction

[[I-D.ietf-homenet-front-end-naming-delegation](#)] describes how Homenet Naming Authority (HNA) outsources the Public Homenet Zone to an Outsourcing Infrastructure.

This document shows how an ISP can provision automatically the HNA with an DNS Outsourcing Infrastructure (DOI). Most likely the DOI will be - at least partly be - managed or provided by its ISP, but other cases may envision the ISP storing some configuration so the homenet becomes resilient to HNA replacement.

The ISP delegates the home network an IP prefix it owns as well as the associated reverse zone.

The ISP is well aware of the owner of that prefix, and as such becomes a natural candidate for hosting the Homenet Reverse Zone - that is the Reverse Distribution Master (RDM) and potentially the Reverse Public Authoritative Servers.

In addition, the ISP often identifies the home network with a name. In most cases, the name is used by the ISP for its internal network management operations and is not a name the home network owner has registered to. The ISP may thus leverage such infrastructure and provide the homenet a specific domain name designated as per [[I-D.ietf-homenet-front-end-naming-delegation](#)] a Homenet Registered Domain. Similarly to the reverse zone, the ISP is well aware of who owns that domain name and may become a natural candidate for hosting the Homenet Zone - that is the Distribution Master (DM) and the Public Authoritative Servers.

This document describes DHCPv6 options so the HNA can advertise the ISP its identity via a Client Public Key. The ISP internally associates the Registered Homenet Domains with that key - that is to the DM and RDM. The ISP provides the Registered Homenet Domain, necessary information on the DM and the RDM so the HNA can manage and upload the Public Homenet Zone and the Reverse Public Homenet Zone as described in [[I-D.ietf-homenet-front-end-naming-delegation](#)].

The use of DHCPv6 options makes the configuration completely transparent to the end user and provides a similar level of trust as the one used to provide the IP prefix. The link between the HNA and the DHCPv6 server may benefit from additional security for example by using [[I-D.ietf-dhc-sedhcpv6](#)].

3. Protocol Overview

This section illustrates how a HNA receives the necessary information via DHCPv6 options to outsource its authoritative naming service to the DOI. For the sake of simplicity, and similarly to [\[I-D.ietf-homenet-front-end-naming-delegation\]](#), this section assumes that the HNA and the home network DHCPv6 client are collocated on the CPE. Note also that this is not mandatory and specific communications between the HNA and the DHCPv6 client only are needed. In addition, this section assumes the responsible entity for the DHCPv6 server is able to configure the DM and RDM. In our case, this means a Registered Homenet Domain can be associated to a Client Public Key.

This scenario has been chosen as it is believed to be the most popular scenario. This document does not ignore scenarios where the DHCP Server does not have privileged relations with the DM or RDM. These cases are discussed latter in [Appendix A](#). Such scenarios do not necessarily require configuration for the end user and can also be zero-config.

The scenario considered in this section is as follows:

1. The HNA is willing to outsource the Public Homenet Zone or Homenet Reverse Zone and configures its DHCP Client to provide its Client Public Key to the DHCP Server using a Client Public Key Option (OPTION_PUBLIC_KEY).
In addition, it also requests the DHCP Client to include in its Option Request Option (ORO) the Registered Homenet Domain Option (OPTION_REGISTERED_DOMAIN), the Distribution Master Option (OPTION_DIST_MASTER) and the Reverse Distribution Master Option (OPTION_REVERSE_DIST_MASTER) option codes.
2. The DHCP Server updates as indicated by the ORO, the DM and RDM, and associate the Registered Domain with the Client Public Key.
3. The DHCP Server responds to the HNA with the requested DHCPv6 options, i.e. OPTION_DIST_MASTER) and OPTION_REVERSE_DIST_MASTER. The DHCP Client transmits the information to the HNA.
4. The HNA is able to get authenticated by the DM and the RDM. The HNA builds the Homenet Zone (resp. the Homenet Reverse Zone) and proceed as described in [\[I-D.ietf-homenet-front-end-naming-delegation\]](#).

4. Payload Description

This section details the payload of the DHCPv6 options.

4.1. Client Public Key Option

The Client Public Key Option (OPTION_PUBLIC_KEY) indicates the Client Public Key that is used to authenticate the HNA. This option is also defined in [I-D.ietf-dhc-sedhcpv6].

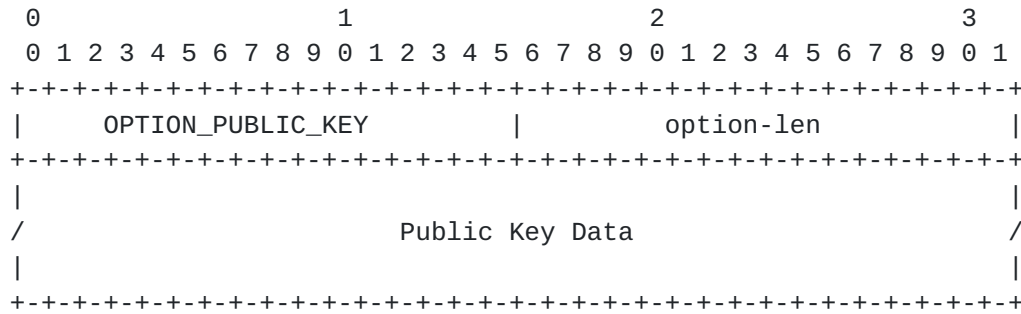


Figure 1: Client Public Key Option

- o option-code (16 bits): OPTION_PUBLIC_KEY, the option code for the Client Public Key Option (TBD1).
- o option-len (16 bits): length in octets of the option-data field as described in [RFC3315].
- o Client Public Key Data: contains the Client Public Key. The format is the DNSKEY RDATA format as defined in [RFC4034].

4.2. Registered Homenet Domain Option

The Registered Domain Option (OPTION_REGISTERED_DOMAIN) indicates the FQDN associated to the home network.

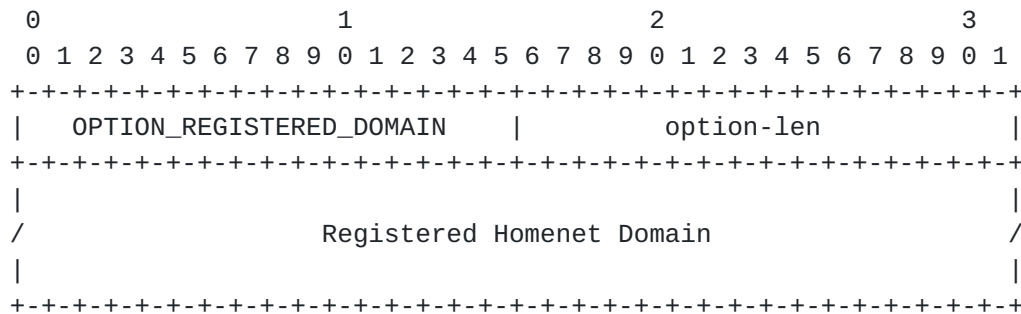


Figure 2: Client Public Key Option

- o option-code (16 bits): OPTION_REGISTERED_DOMAIN, the option code for the Registered Homenet Domain (TBD2).
- o option-len (16 bits): length in octets of the option-data field as described in [RFC3315].
- o Registered Homenet Domain (variable): the FQDN registered for the homenet

4.3. Distribution Master Option

The Distributed Master Option (OPTION_DIST_MASTER) provides the HNA to FQDN of the DM as well as the transport protocol for the transaction between the HNA and the DM.

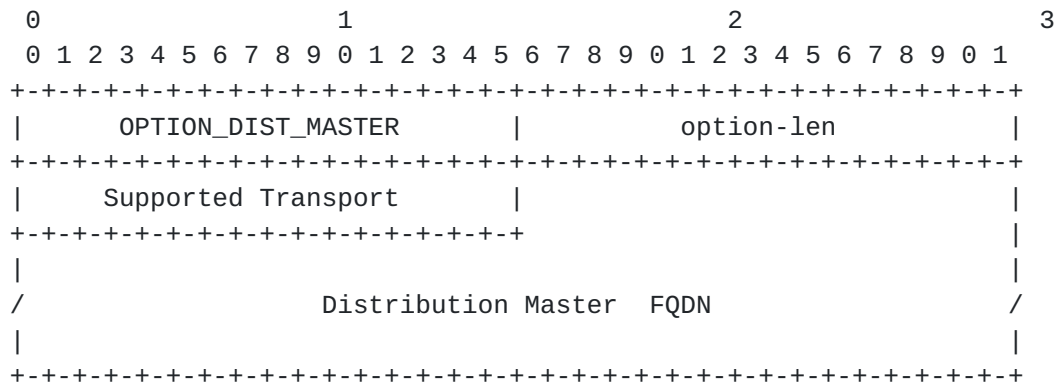


Figure 3: Distribution Master Option

- o option-code (16 bits): OPTION_DIST_MASTER, the option code for the DM Option (TBD3).
- o option-len (16 bits): length in octets of the option-data field as described in [RFC3315].
- o Supported Transport (16 bits): defines the supported transport by the DM. Each bit represents a supported transport, and a DM MAY indicate the support of multiple modes. The bit for DoT MUST be set.
- o Distribution Master FQDN (variable): the FQDN of the DM.

4.3.1. Supported Transport

The Supported Transport field of the DHCPv6 option indicates the supported transport protocol. Each bit represents a specific transport mechanism. The bit sets to 1 indicates the associated

transport protocol is supported. The corresponding bits are assigned as described in Figure 4.

Bit	Transport Protocol	Reference
0	DNS over TLS	
1	DNS over HTTPS	
2-7	unallocated	

Figure 4: Supported Protocols

4.4. Reverse Distribution Master Server Option

The Reverse Distribution Master Server Option (OPTION_REVERSE_DIST_MASTER) provides the HNA to FQDN of the DM as well as the transport protocol for the transaction between the HNA and the DM.

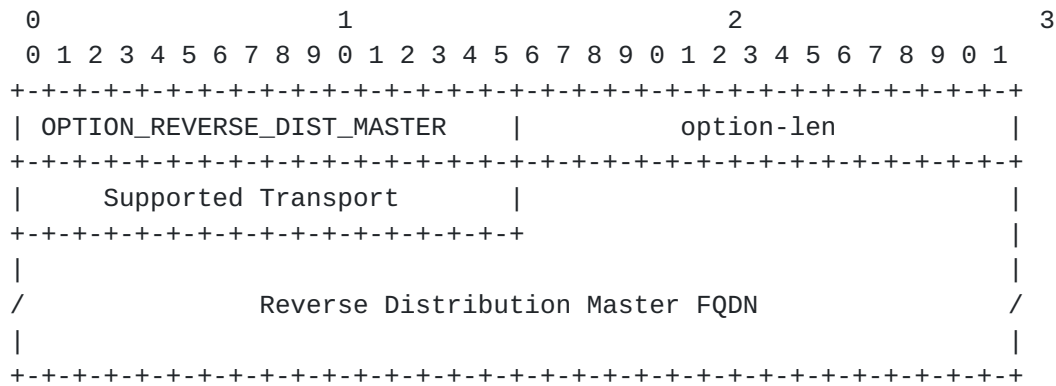


Figure 5: Reverse Distribution Master Option

- o option-code (16 bits): OPTION_REVERSE_DIST_MASTER, the option code for the Reverse Distribution Master Option (TBD4).
- o option-len (16 bits): length in octets of the option-data field as described in [RFC3315].
- o Supported Transport (16 bits): defines the supported transport by the DM. Each bit represents a supported transport, and a DM MAY indicate the support of multiple modes. The bit for DoT MUST be set.
- o Reverse Distribution Master FQDN (variable): the FQDN of the RDM.

5. DHCP Behavior

5.1. DHCPv6 Server Behavior

Sections [17.2.2](#) and [18.2](#) of [[RFC3315](#)] govern server operation in regards to option assignment. As a convenience to the reader, we mention here that the server will send option foo only if configured with specific values for foo and if the client requested it. In particular, when configured the DHCP Server sends the Registered Homenet Domain Option, Distribution Master Option, the Reverse Distribution Master Option when requested by the DHCPv6 client by including necessary option codes in its ORO.

The DHCP Server may receive a Client Public Key Option (OPTION_PUBLIC_KEY) from the HNA. Upon receipt of this DHCPv6 option, the DHCP Server SHOULD acknowledge the reception of the Client Public Key Option as described and communicate this credential to the available DM and RDM unless not configured to do so.

A HNA may update its Client Public Key by sending a new value in the Client Public Key Option (OPTION_PUBLIC_KEY) as this document assumes the link between the HNA and the DHCP Server is considered authenticated and trusted. The server SHOULD process received Client Public Key Option sent by the client unless not configured to do so.

5.2. DHCPv6 Client Behavior

The DHCPv6 client SHOULD send a Client Public Key Option (OPTION_PUBLIC_KEY) to the DHCP Server. This Client Public Key authenticates the HNA.

The DHCPv6 client sends a ORO with the necessary option codes: Registered Homenet Domain Option, Distribution Master Option, the Reverse Distribution Master Option.

Upon receiving a DHCP option described in this document in the Reply message, the HNA SHOULD proceed as described in [[I-D.ietf-homenet-front-end-naming-delegation](#)].

5.3. DHCPv6 Relay Agent Behavior

There are no additional requirements for the DHCP Relay agents.

6. IANA Considerations

The DHCP options detailed in this document are: * OPTION_CLIENT_KEY: TBD1 * OPTION_REGISTERED_DOMAIN: TBD2 * OPTION_DIST_MASTER: TBD3 * OPTION_REVERSE_DIST_MASTER: TBD4

The document also requests a Supported Transport Registry:

Bit	Transport Protocol	Reference
0	DNS over TLS	
1	DNS over HTTPS	
2-7	unallocated	

7. Security Considerations"

8. Acknowledgments

We would like to thank Marcin Siodelski and Bernie Volz for their comments on the design of the DHCPv6 options. We would also like to thank Mark Andrews, Andrew Sullivan and Lorenzo Colliti for their remarks on the architecture design. The designed solution has been largely been inspired by Mark Andrews's document [[I-D.andrews-dnsop-pd-reverse](#)] as well as discussions with Mark. We also thank Ray Hunter for its reviews, its comments and for suggesting an appropriated terminology.

9. References

9.1. Normative References

- [RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), DOI 10.17487/RFC1034, November 1987, <<https://www.rfc-editor.org/info/rfc1034>>.
- [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/info/rfc2119>>.
- [RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", [RFC 2181](#), DOI 10.17487/RFC2181, July 1997, <<https://www.rfc-editor.org/info/rfc2181>>.
- [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), DOI 10.17487/RFC3315, July 2003, <<https://www.rfc-editor.org/info/rfc3315>>.
- [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", [RFC 4034](#), DOI 10.17487/RFC4034, March 2005, <<https://www.rfc-editor.org/info/rfc4034>>.

- [RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the DNS", [RFC 6672](#), DOI 10.17487/RFC6672, June 2012, <<https://www.rfc-editor.org/info/rfc6672>>.
- [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/info/rfc8174>>.

[9.2.](#) Informative References

- [I-D.andrews-dnsop-pd-reverse]
Andrews, M., "Automated Delegation of IP6.ARPA reverse zones with Prefix Delegation", [draft-andrews-dnsop-pd-reverse-02](#) (work in progress), November 2013.
- [I-D.ietf-dhc-sedhcpv6]
Li, L., Jiang, S., Cui, Y., Jinmei, T., Lemon, T., and D. Zhang, "Secure DHCPv6", [draft-ietf-dhc-sedhcpv6-21](#) (work in progress), February 2017.
- [I-D.ietf-homenet-front-end-naming-delegation]
Migault, D., Weber, R., Richardson, M., Hunter, R., Griffiths, C., and W. Cloetens, "Outsourcing Home Network Authoritative Naming Service", [draft-ietf-homenet-front-end-naming-delegation-11](#) (work in progress), April 2020.
- [I-D.sury-dnsex-t-cname-dname]
Sury, O., "CNAME+DNAME Name Redirection", [draft-sury-dnsex-t-cname-dname-00](#) (work in progress), April 2010.

[Appendix A](#). Scenarios and impact on the End User

This section details various scenarios and discuss their impact on the end user. This section is not normative and limits the description of a limited scope of scenarios that are assumed to be representative. Many other scenarios may be derived from these.

[Appendix B](#). Base Scenario

The base scenario is the one described in [Section 3](#) in which an ISP manages the DHCP Server, the DM and RDM.

The end user subscribes to the ISP (foo), and at subscription time registers for example.foo as its Registered Homenet Domain example.foo.

When the HNA is plugged (at least the first time), it provides its Client Public Key to the DHCP Server. In this scenario, the DHCP Server, DM and RDM are managed by the ISP so the DHCP Server and as such can provide authentication credentials of the HNA to enable secure authenticated transaction with the DM and the Reverse DM.

The main advantage of this scenario is that the naming architecture is configured automatically and transparently for the end user. The drawbacks are that the end user uses a Registered Homenet Domain managed by the ISP and that it relies on the ISP naming infrastructure.

[B.1](#). Third Party Registered Homenet Domain

This section considers the case when the end user wants its home network to use example.com not managed by her ISP (foo) as a Registered Homenet Domain.

This section still consider the ISP manages the home network and still provides example.foo as a Registered Homenet Domain.

When the end user buys the domain name example.com, it may request to redirect the name example.com to example.foo using static redirection with CNAME [[RFC2181](#)], [[RFC1034](#)], DNAME [[RFC6672](#)] or CNAME+DNAME [[I-D.sury-dnsext-cname-dname](#)].

This configuration is performed once when the domain name example.com is registered. The only information the end user needs to know is the domain name assigned by the ISP. Once this configuration is done no additional configuration is needed anymore. More specifically, the HNA may be changed, the zone can be updated as in [Appendix B](#) without any additional configuration from the end user.

The main advantage of this scenario is that the end user benefits from the Zero Configuration of the Base Scenario [Appendix B](#). Then, the end user is able to register for its home network an unlimited number of domain names provided by an unlimited number of different third party providers.

The drawback of this scenario may be that the end user still rely on the ISP naming infrastructure. Note that the only case this may be inconvenient is when the DNS Servers provided by the ISPs results in high latency.

[B.2.](#) Third Party DNS Infrastructure

This scenario considers that the end user uses example.com as a Registered Homenet Domain, and does not want to rely on the authoritative servers provided by the ISP.

In this section we limit the outsourcing to the DM and Public Authoritative Server(s) to a third party. The Reverse Public Authoritative Server(s) and the RDM remain managed by the ISP as the IP prefix is managed by the ISP.

Outsourcing to a third party DM can be performed in the following ways:

1. Updating the DHCP Server Information. One can imagine a GUI interface that enables the end user to modify its profile parameters. Again, this configuration update is done once-for-ever.
2. Upload the configuration of the DM to the HNA. In some cases, the provider of the CPE hosting the HNA may be the registrar and provide the CPE already configured. In other cases, the CPE may request the end user to log into the registrar to validate the ownership of the Registered Homenet Domain and agree on the necessary credentials to secure the communication between the HNA and the DM. As described in [\[I-D.ietf-homenet-front-end-naming-delegation\]](#), such settings could be performed in an almost automatic way as to limit the necessary interactions with the end user.

[B.3.](#) Multiple ISPs

This scenario considers a HNA connected to multiple ISPs.

Suppose the HNA has been configured each of its interfaces independently with each ISPS as described in [Appendix B](#). Each ISP provides a different Registered Homenet Domain. The HNA Client Public Key may be shared between the HNA and the multiple ISPs.

The protocol and DHCPv6 options described in this document are fully compatible with a HNA connected to multiple ISPs with multiple Registered Homenet Domains. However, the HNA should be able to handle different Registered Homenet Domains. This is an implementation issue which is outside the scope of the current document.

If a HNA is not able to handle multiple Registered Homenet Domains, the HNA may remain connected to multiple ISP with a single Registered Homenet Domain. In this case, one entity is chosen to host the Registered Homenet Domain. This entity may be one of the ISP or a third party. Note that having multiple ISPs can be motivated for bandwidth aggregation, or connectivity fail-over. In the case of connectivity fail-over, the fail-over concerns the access network and a failure of the access network may not impact the core network where the DM Server and Public Authoritative Primaries are hosted. In that sense, choosing one of the ISP even in a scenario of multiple ISPs may make sense. However, for sake of simplicity, this scenario assumes that a third party has been chosen to host the Registered Homenet Domain. Configuration is performed as described in [Appendix B.1](#) and [Appendix B.2](#).

With the configuration described in [Appendix B.1](#), the HNA is expect to be able to handle multiple Homenet Registered Domain, as the third party redirect to one of the ISPs Servers. With the configuration described in [Appendix B.2](#), DNS zone are hosted and maintained by the third party. A single DNS(SEC) Homenet Zone is built and maintained by the HNA. This latter configuration is likely to match most HNA implementations.

The protocol and DHCPv6 options described in this document are fully compatible with a HNA connected to multiple ISPs. To configure or not and how to configure the HNA depends on the HNA facilities. [Appendix B](#) and [Appendix B.1](#) require the HNA to handle multiple Registered Homenet Domain, whereas [Appendix B.2](#) does not have such requirement.

Authors' Addresses

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent, QC 4S 0B6
Canada

E-Mail: daniel.migault@ericsson.com

Ralf Weber
Akamai

E-Mail: ralf.weber@akamai.com

Tomek Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City 94063
US

E-Mail: tomasz.mrugalski@gmail.com

Chris Griffiths

E-Mail: cgriffiths@gmail.com

Wouter Cloetens
Deutsche Telekom

E-Mail: wouter.cloetens@external.telekom.de

