DHCP Options for Homenet Naming Architecture
draft-mglt-homenet-naming-architecture-dhc-options-02.txt

Abstract

   CPEs are usually constraint devices with reduced network and CPU
   capacities. As such, a CPE hosting on the Internet the authoritative
   naming service for its home network may become vulnerable to resource
   exhaustion attacks. One way to avoid exposing CPE is to outsource
   the authoritative service to a third party. This third party can be
   the ISP or any other independent third party.

   Outsourcing the authoritative naming service to a third party
   requires setting up an architecture which may be unappropriated for
   most end users. To leverage this issue, this document proposes DHCP
   Options so any agnostic CPE can automatically proceed to the
   appropriated configuration and outsource the authoritative naming
   service for the home network. This document shows that in most
   cases, these DHCP Options make outsourcing to a third party (be it
   the ISP or any ISP independent service provider) transparent for the
   end user.

   This Internet-Draft will expire on January 3, 2015.

Copyright Notice

Table of Contents

1. Requirements notation

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in [RFC2119].

2. Terminology

   - Customer Premises Equipment: (CPE) is the router providing
         connectivity to the home network. It is configured and managed
         by the end user. In this document, the CPE might also hosts
         services such as DHCPv6. This device might be provided by the
         ISP.

   - Public Key: designates a public Key generated by the CPE. This
         key is used as an authentication credential for the CPE.

   - Registered Homenet Domain: is the Domain Name associated to the
         home network.

   - DNS Homenet Zone: is the DNS zone associated to the home network.
         This zone is set by the CPE and essentially contains the
         bindings between names and IP addresses of the nodes of the
         home network. In this document, the CPE does neither perform
         any DNSSEC management operations such as zone signing nor
         provide an authoritative service for the zone. Both are
         delegated to the Public Authoritative Server. The CPE
         synchronizes the DNS Homenet Zone with the Public Authoritative
         Server via a hidden master / slave architecture. The Public
         Authoritative Server might use specific servers for the
         synchronization of the DNS Homenet Zone: the Public
         Authoritative Name Server Set.

- DNS Homenet Zone Template: The template used as a basis to
     generate the DNS Homenet Zone.

- DNS Template Server: The DNS server that hosts the DNS Homenet
     Zone Template.

- DNS Homenet Reverse Zone: The reverse zone file associated to the
     DNS Homenet Zone.

- Public Authoritative Master(s):   are the visible name server
     hosting the DNS Homenet Zone. End users' resolutions for the
     Homenet Domain are sent to this server, and this server is a
     master for the zone.

- Public Authoritative Name Server Set: is the server the CPE
     synchronizes the DNS Homenet Zone. It is configured as a slave
     and the CPE acts as master. The CPE sends information so the
     DNSSEC zone can be set and served.

- Reverse Public Authoritative Master(s):   are the visible name
     server hosting the DNS Homenet Reverse Zone. End users'
     resolutions for the Homenet Domain are sent to this server, and
     this server is a master for the zone.

- Reverse Public Authoritative Name Server Set: is the server the
     CPE synchronizes the DNS Homenet Reverse Zone. It is
     configured as a slave and the CPE acts as master. The CPE
     sends information so the DNSSEC zone can be set and served.

3. Introduction

CPEs are usually constraint devices with reduced network and CPU
capacities. As such, a CPE hosting on the Internet the authoritative
naming service for its home network may become vulnerable to resource
exhaustion attacks. One way to avoid exposing CPE is to outsource
the authoritative service to a third party. This third party can be
the ISP or any other independent third party.

Outsourcing the authoritative naming service to a third party
requires setting up an architecture which may be unappropriated for
most end users. To leverage this issue, this document proposes DHCP
Options so any agnostic CPE can automatically proceed to the
appropriated configuration and outsource the authoritative naming
service for the home network. This document shows that in most
cases, these DHCP Options make outsourcing to a third party (be it
the ISP or any ISP independent service provider) transparent for the
end user.

When the CPE is plugged, the DHCP Options described in the document enable the CPE:

- 1. To build the DNS Homenet Zone: Building the DNS Homenet Zone requires filling the zone with appropriated bindings likes name / IP addresses of the different devices in the home networks. Such information can be provided for example by the DHCP Server hosted on the CPE. On the other hand, it also requires configuration parameters like the name of the Registered Domain Name associated to the home network or the Public Authoritative Master(s) the DNS Homenet Zone is outsourced to. These configuration parameters are stored in the DNS Homenet Zone Template. This document describes the DHCP Zone Template Option. This option carries a DNS Homenet Zone Template FQDN. In order to retrieve the DNS Homenet Zone Template, the CPE sends a query of type AXFR [RFC1034] [RFC5936]for the DNS Homenet Zone Template FQDN.

- 2. To upload the DNS(SEC) Homenet Zone to the appropriated server: This server is designated as the Public Authoritative Name Server Set. It is in charge of publishing the DNS(SEC) Homenet Zone on the Public Authoritative Master(s). This document describes the DHCP Public Authoritative Name Server Set Option that provides the FQDN of the appropriated server. Note that, in the document we do not consider whether the DNS(SEC) Homenet Zone is signed or not and if signed who signs it. Such questions are out of the scope of the current document.

- 3. To upload the DNS Homenet Reverse Zone to the appropriated server: This server is designated as the Reverse Public Authoritative Name Server Set. It is in charge of publishing the DNS Homenet Reverse Zone on the Reverse Public Authoritative Master(s). This document describes the DHCP Reverse Public Authoritative Name Server Set Option that provides the FQDN of the appropriated server. Similarly to item 2., we do not consider in this document if the DNS Homenet Reverse Zone is signed or not, and if signed who signs it.

- 4. To provide authentication credential (a public key) to the DHCP Server: Information stored in the DNS Homenet Zone Template, the DNS(SEC) Homenet Zone and DNS Homenet Reverse Zone belongs to the CPE, and only the CPE should be able to update or upload these zones. To authenticate the CPE, this document defines the DHCP Public Key Option. This option is sent by the CPE to the DHCP Server and provides the Public Key the CPE uses to authenticate itself. The DHCP Server is then responsible to provide the Public Key to the various DNS servers.

As a result, the DHCP Options described in this document enable an agnostic CPE to outsource its naming infrastructure without any configuration from the end user. The main reason no configuration is required by the end user is that there are privilege links first between the CPE and the DHCP Server and then between the DHCP Server and the various DNS servers (DNS Homenet Zone Server, the Reverse Public Authoritative Name Server Set, Public Authoritative Name Server Set). This enables the CPE to send its authentication credentials (a Public Key) to the DHCP Server that in turn forward it to the various DNS servers. With the authentication credential on the DNS servers set, the CPE is able to update the various zones in a secure way.

If the DHCP Server cannot provide the public key to one of these servers (most likely the Public Authoritative Name Server Set) and the CPE needs to interact with the server, then, the end user is expected to provide it manually or using other mechanisms. Such mechanisms are outside the scope of this document. In that case, the authentication credentials need to be provided every time the key is modified. Appendix A provides more details on how different scenarios impact the end users.

4. Protocol Overview

This section illustrates how a CPE configures its naming infrastructure to outsource its authoritative naming service. All configurations and settings are performed using DHCP Options. In this section, for the sake of simplicity, we consider that the DHCP Server is able to communicate to the various DNS servers and provide them them the public key associated to the CPE. Once each server got the credentials, the CPE can proceed to updates in a authenticated and secure way.

This scenario has been chosen as it is believed to be the most popular scenario. This document does not ignore that scenarios where the DHCP Server does not have privilege relations with the Public Authoritative Name Server Set must be considered. These cases are discussed latter in Appendix A. Such scenario does not necessarily require configuration for the end user and can also be Zero Config.

The scenario is represented in Figure 1.

- 1:   The CPE provides its Public Key to the DHCP Server using a DHCP Public Key Option (OPTION_PUBLIC_KEY) and sends a DHCP Option Request Option (ORO) for the DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE), the DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET) and the DHCP Reverse

          Public Authoritative Name Server Set Option
          (OPTION_REVERSE_NAME_SERVER_SET).

  - 2:   The DHCP Server makes the Public Key available to the DNS
          servers, so the CPE can secure its DNS transactions. Note that
          the Public Key alone is not sufficient to perform the
          authentication and the key should be, for example, associated
          with an identifier, or the concerned domain name. How the
          binding is performed is out of scope of the document. It can
          be a centralized database or various bindings may be sent to
          the different servers. Figure 1 represents the specific case
          were the DHCP Server forwards the set (Public Key, Zone
          Template FQDN) to the DNS Template Server, the set (Public Key,
          IPv6 subnet) to the Reverse Public Authoritative Name Server
          Set and the set (Public Key, Registered Homenet Domain) to the
          Public Authoritative Name Server Set.

  - 3.:   The DHCP Server responds to the CPE with the requested DHCP
          Options, i.e. the DHCP Public Key Option (OPTION_PUBLIC_KEY),
          DHCP Zone Template Option OPTION_DNS_ZONE_TEMPLATE, DHCP Public
          Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET),
          DHCP Reverse Public Authoritative Name Server Set Option
          (OPTION_REVERSE_NAME_SERVER_SET).

  - 4.:   Upon receiving the DHCP Zone Template Option
          (OPTION_DNS_ZONE_TEMPLATE), the CPE performs an AXFR DNS query
          for the Zone Template FQDN. The exchange is secured according
          to the security protocols defined in the Security field of the
          DHCP option. Once the CPE has retrieved the DNS Zone Template,
          the CPE can build the DNS Homenet Zone and the DNS Homenet
          Reverse Zone. Eventually the CPE signs these zones.

  - 5.:   Once the DNS(SEC) Homenet Reverse Zone has been set, the CPE
          uploads the zone to the Reverse Public Authoritative Name
          Server Set. The DHCP Reverse Public Authoritative Name Server
          Set Option (OPTION_REVERSE_NAME_SERVER_SET) provides the
          Reverse Public Authoritative Name Server Set FQDN as well as
          the upload method, and the security protocol to secure the
          upload.

  - 6.:   Once the DNS(SEC) Homenet Zone has been set, the CPE uploads
          the zone to the Public Authoritative Name Server Set. The DHCP
          Public Authoritative Name Server Set Option
          (OPTION_NAME_SERVER_SET) provides the Public Authoritative Name
          Server Set FQDN as well as the upload method and the security
          protocol to secure the upload.

```
        +----------------------+
        |     DHCP Server      |
        +----------------------+
             ^    ^         ^
             |    |        |2.
           1.|   |3.       |
             v   v         |
           +------+        |    +--------------------------------+
           |      | 4.   +--->|  DNS Template Server            |
           |      |<---------->|                                |
           |      |      |    +--------------------------------+
           | CPE  |      |
           |      |      |    +--------------------------------+
           |      | 5.   +--->|  Reverse Public Authoritative  |
           |      |<---------->|  Name Server Set               |
           |      |      |    +--------------------------------+
        -------|      |-------|--------------------------------------
           |      |      |    +--------------------------------+
           +------+      +--->|  Public Authoritative          |
                              |  Name Server Set               |
                              +--------------------------------+
```
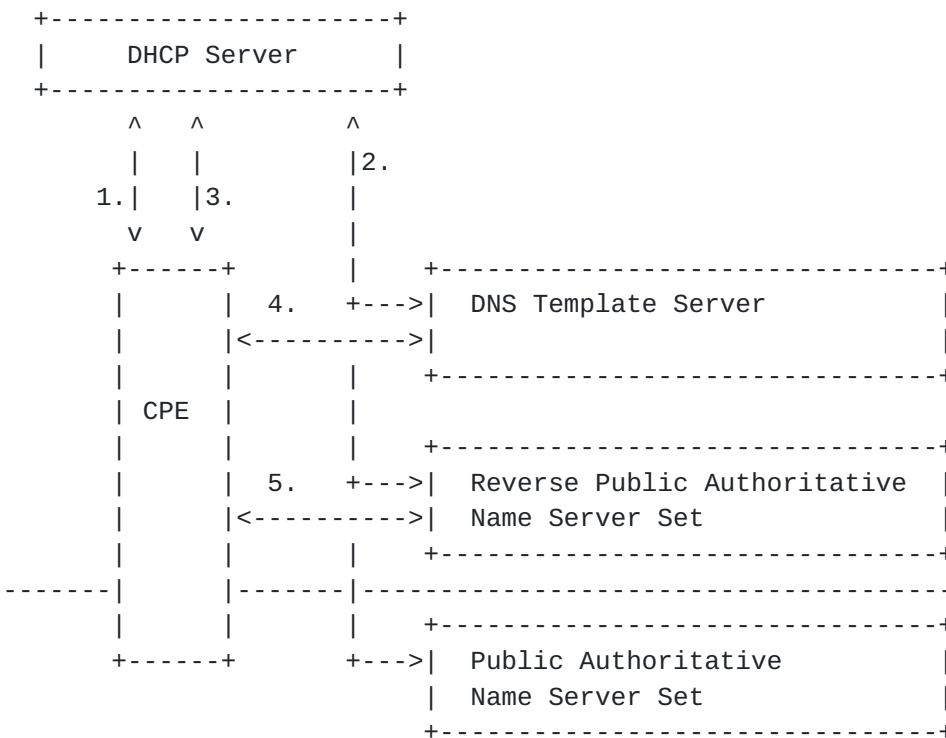
Figure 1: Protocol Overview

5. Securing the exchanges

Multiple protocols like IPsec [RFC4301] or TLS / DTLS [RFC5246] /
[RFC6347] may be used to secure DNS transactions between the CPE and
the DNS servers. This document restricts the scope of security
protocols to those that have been designed specifically for DNS.
This includes DNSSEC [RFC4033], [RFC4034], [RFC4035] that
authenticates and provides integrity protection of DNS data, TSIG
[RFC2845], [RFC2930] that use a shared secret to secure a transaction
between two end points and SIG(0) [RFC2931] authenticates the DNS
packet exchanged.

The key issue with TSIG is that a shared secret must be negotiated
between the CPE and the server. On the other end, TSIG performs
symmetric cryptography which is light in comparison with asymmetric
cryptography used by SIG(0). As a result, over large zone transfer,
TSIG may be preferred to SIG(0).

This document does not provides means to distribute shared secret for
example using a specific DHCP Option. The only assumption made is
that the CPE generates or is assigned a public key.

As a result, when the document specifies the transaction is secured
with TSIG, it means that either the CPE and the DNS Server have been

manually configured with a shared secret, or the shared secret has
been negotiated using TKEY [RFC2930], and the TKEY exchanged are
secured with SIG(0).

Exchange with the DNS Template Server to retrieve the DNS Homenet
Zone Template may be protected by SIG(0), TSIG or DNSSEC. When
DNSSEC is used, it means the DNS Template Server only provides
integrity protection, and does not necessarily prevents someone else
to query the DNS Homenet Zone Template. In addition, DNSSEC is only
a way to protect the communication of AXFR queries, in other words,
DNSSEC cannot be used to secure updates. If DNSSEC is used to
provide integrity protection for the AXFR response, the CPE should
proceed to the DNSSEC signature checks. If signature check fails, it
MUST reject the response. If the signature check succeeds, the CPE
removes all DNSSEC related RRsets (DNSKEY, RRSIG, NSEC* ...) before
building the DNS Homenet Zone. In fact, these DNSSEC related fields
as associated to the DNS Homenet Zone Template and not the DNS
Homenet Zone.

Any update exchange should use SIG(0) or TSIG to authenticate the
exchange.

6. DNS Zones Update Mechanisms

6.1. Data subjected to update

The CPE is likely to update various DNS contents:

- DNS Homenet Zone Template: may be updated by the CPE if the
     configuration of the zone may be changed. This can include
     additional Public Authoritative Master(s), a different
     Registered Homenet Domain as the one initially proposed, or a
     redirection to another domain.

- DNS Homenet Reverse Zone: may be updated every time a new device
     is connected or dis-connected.

- DNS Homenet Zone: may be updated every time a new device is
     connected, dis-connected.

6.2. Master / Slave Synchronization versus DNS Update

As updates only concern DNS zones, this document only considers DNS
update mechanisms such as DNS update [RFC2136] [RFC3007] or a master
/ slave synchronization.

The DNS Homenet Zone Template can only be updated with DNS update. The reason is that the DNS Homenet Zone Template contains static configuration data that is not expected to evolve over time.

The DNS Homenet Reverse Zone and the DNS Homenet Zone can be updated either with DNS update or using a master / slave synchronization. As these zones may be large, with frequent updates, we recommend to use the master / slave architecture as described in [I-D.mglt-homenet-front-end-naming-delegation]. The master / slave mechanism is preferred as it better scales and avoids DoS attacks: First the master notifies the slave the zone must be updated, and leaves the slave to proceed to the update when possible. Then, the NOTIFY message sent by the master is a small packet that is less likely to load the slave. At last, the AXFR query performed by the slave is a small packet sent over TCP (section 4.2 [RFC5936]) which makes unlikely the slave to perform reflection attacks with a forged NOTIFY. On the other hand, DNS updates can use UDP, packets require more processing then a NOTIFY, and they do not provide the server the opportunity to post-pone the update.

6.3. Setting Master / Slave Synchronization

The master / slave architecture is described in [I-D.mglt-homenet-front-end-naming-delegation]. The CPE is configured as a master whereas the DNS Server is configured as a slave. The DNS Server represents the Public Authoritative Name Server Set or the Reverse Public Authoritative Name Server Set.

When the CPE is plugged its IP address may be unknown to the slave. The section details how the CPE or master communicate the necessary information to set up the slave.

In order to set the master / slave configuration, both master and slaves must agree on 1) the zone to be synchronized, 2) the IP address used by both master and slave. In this document we assume that synchronization is performed on both side on port 53.

[QUESTION Do we have to consider different port of port 53 is fine. I guess it is fine.]

6.4. Master / Slave Synchronization: CPE / Public Authoritative Name Server Set

The CPE knows the zone to be synchronized by reading the Registered Homenet Domain in the DNS Homenet Zone Template provided by the DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE). The IP address of the slave is provided by the DHCP Public Authoritative Name Server Set Option (OPTION_NAME_SERVER_SET).

The Public Authoritative Name Server Set has been configured with the
Registered Homenet Domain and the Public Key that identifies the CPE.
The only thing missing is the IP address of the CPE. This IP address
is provided by the CPE by sending a NOTIFY [RFC1996].

When the CPE has built its DNS Homenet Zone, it sends a NOTIFY
message to the Public Authoritative Name Server Sets. Upon receiving
the NOTIFY message, the slave reads the Registered Homenet Domain and
checks the NOTIFY is sent by the authorized master. This can be done
using the shared secret (TSIG) or the public key (SIG(0)). Once the
NOTIFY has been authenticated, the Public Authoritative Name Server
Sets might consider the source IP address of the NOTIFY query to
configure the masters attributes.

6.5. Master / Slave Synchronization: CPE / Reverse Public Authoritative Name Server Set

The CPE knows the zone to be synchronized by looking at its assigned
prefix. The IP address of the slave is provided by the DHCP Reverse
Public Authoritative Name Server Set Option
(OPTION_REVERSE_NAME_SERVER_SET).

Configuration of the slave is performed as illustrated in
Section 6.4.

7. DNS Zone Update Data

7.1. DNS Homenet Zone Template

The DNS Homenet Zone Template contains at least the related fields of
the Public Authoritative Master(s) as well as the Homenet Registered
Domain, that is SOA, and NS fields. This template might be generated
automatically by the owner of the DHCP Server. For example, an ISP
might provide a default Homenet Registered Domain as well as default
Public Authoritative Master(s). This default settings should provide
the CPE the necessary pieces of information to set the homenet naming
architecture.

If the DNS Homenet Zone Template is not subject to modifications or
updates, the owner of the template might only use DNSSEC to enable
integrity check.

The DNS Homenet Zone Template might be subject to modification by the
CPE. The advantage of using the standard DNS zone format is that
standard DNS update mechanism can be used to perform updates. These
updates might be accepted or rejected by the owner of the DNS Homenet
Zone Template. Policies that defines what is accepted or rejected is
out of scope of this document. However, in this document we assume

the Registered Homenet Domain is used as an index by the Public
Authoritative Name Server Set, and SIG(0), TSIG are used to
authenticate the CPE. As a result, the Registered Homenet Domain
should not be modified unless the Public Authoritative Name Server
Set can handle with it.

7.2. DNS Homenet Zone

The DNS Homenet Zone might be generated from the DNS Homenet Zone
Template. How the DNS Homenet Zone is generated is out of scope of
this document. In some cases, the DNS Homenet Zone might be the
exact copy of the DNS Homenet Zone Template. In other cases, it
might be generated from the DNS Homenet Zone Template with additional
RRsets. In some other cases, the DNS Homenet Zone might be generated
without considering the DNS Homenet Zone Template, but only
considering specific configuration rules.

In the current document the CPE only sets a single zone that is
associated with one single Homenet Registered Domain. The domain
might be assigned by the owner of the DNS Homenet Zone Template.
This constrain does not prevent the CPE to use multiple domain names.
How additional domains are considered is out of scope of this
document. One way to handle these additional zones is to configure
static redirections to the DNS Homenet Zone using CNAME [RFC2181],
[RFC1034], DNAME [RFC6672] or CNAME+DNAME
[I-D.sury-dnsext-cname-dname].

8. Payload Description

8.1. Security Field

The Security Field of the DHCP Option is represented in Figure 2. It
indicates the security mechanism supported by the DNS Server. One of
these mechanism MUST be chosen by the CPE in order to perform a
transaction with the DNS server. See Section 5 for more details.

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Security           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
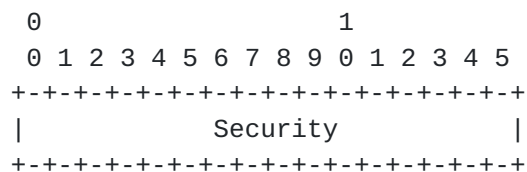
                    Figure 2: Security Field

- DNS (Bit 0):   indicates, when set to 1, that DNS without any
     security extension is supported.

   - DNSSEC (Bit 1):   indicates, when set to 1, that DNSSEC provides
        integrity protection. This can only be used for read
        operations like retrieving the DNS Homenet Zone Template.

   - SIG(0) (Bit 2):   indicates, when set to 1, that transaction
        protected by SIG(0) are supported.

   - TSIG (Bit 3):   indicates, when set to 1, that transaction using
        TSIG is supported. Note that if a shared secret has not been
        previously negotiated between the two party, it should be
        negotiated using TKEY. The TKEY exchanges MUST be protected
        with SIG(0) even though SIG(0) is not supported.

   - Remaining Bits (Bit 4-15):   MUST be set to 0 by the DHCP Server
        and ignored by the DHCP Client.

   A Security field with all bits set to zero indicates the operation is
   not permitted. The Security field may be set to zero when updates
   operations are not permitted for the DNS Homenet Template. In any
   other case this is an error.

8.2. Update Field

   The Update Field of the DHCP Option is represented in Figure 3. It
   indicates the update mechanism supported by the DNS server. See
   Section 6 for more details.

```
 0
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|    Update     |
+-+-+-+-+-+-+-+-+
```

                       Figure 3: Update Field

   - Master / Slave (Bit 0):   indicates, when set to 1, that DNS Server
        supports data synchronization using a Master / Slave mechanism.

   - DNS Update (Bit 1):   indicates, when set to 1, that DNS Server
        supports data synchronization using DNS Updates.

   - Remaining Bits (Bit 2-7):   MUST be set to 0 by the DHCP Server and
        ignored by the DHCP Client.

8.3. DHCP Public Key Option

   The DHCP Public Key Option (OPTION_PUBLIC_KEY) indicates the Public
   Key that is used to authenticate the CPE.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       OPTION_PUBLIC_KEY        |          option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                      Public Key Data                          /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
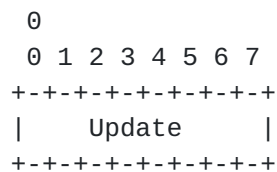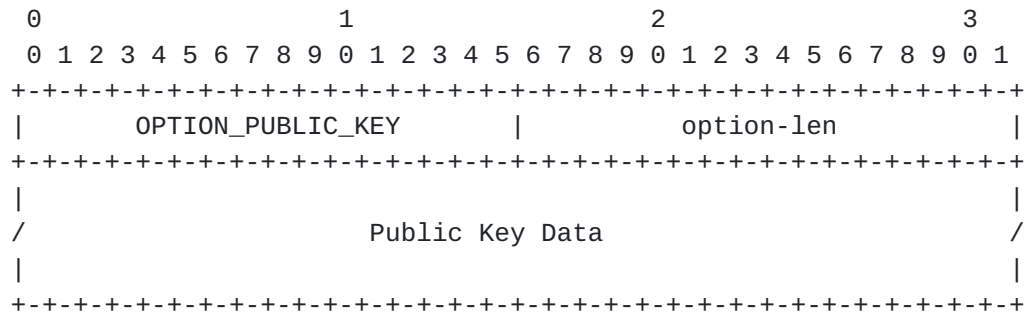
                    Figure 4: DHCP Public Key Option

   - OPTION_PUBLIC_KEY (variable): the option code for the DHCP Public
        Key Option.

   - option-len (16 bits): length in octets of the option-data field as
        described in [RFC3315].

   - Public Key Data: contains the Public Key. The format is the DNSKEY
        RDATA format as defined in [RFC4034].

8.4. DHCP Zone Template Option

   The DHCP Zone Template Option (OPTION_DNS_ZONE_TEMPLATE) Option
   indicates the CPE how to retrieve the DNS Homenet Zone Template. It
   provides a FQDN the CPE SHOULD query with a DNS query of type AXFR.
   The option also specifies which security protocols are available on
   the authoritative server. DNS Homenet Zone Template update, if
   permitted MUST use the DNS Update mechanism.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    OPTION_DNS_ZONE_TEMPLATE    |          option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Security (axfr)         |           Security            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
/                     Zone Template FQDN                        /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                  Figure 5: DHCP Zone Template Option
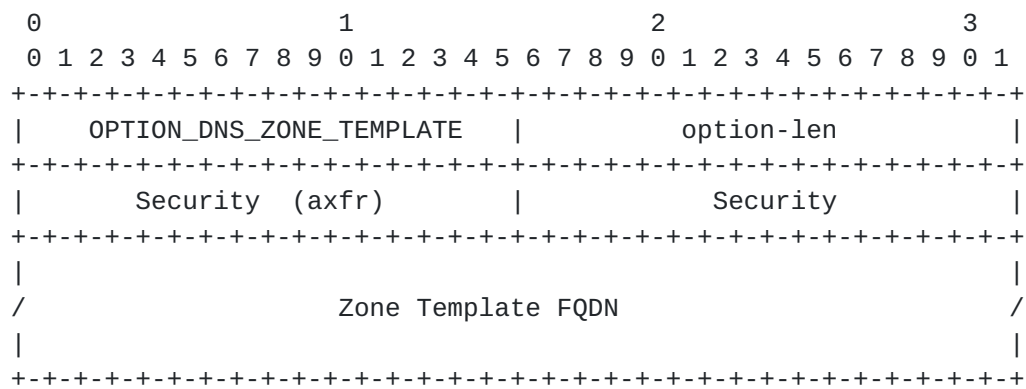
- OPTION_DNS_ZONE_TEMPLATE (variable): the option code for the DHCP
     Zone Template Option.

- option-len (16 bits): length in octets of the option-data field as
     described in [RFC3315].

- Security (axfr) (16 bits): defines which security protocols are
     supported by the DNS server. This field concerns the AXFR and
     consultation queries, not the update queries. See Section 8.1
     for more details.

- Security (16 bits): defines which security protocols are supported
     by the DNS server. This field concerns the update. See
     Section 8.1 for more details.

- Zone Template FQDN FQDN (variable): the FQDN of the DNS server
     hosting the DNS Homenet Zone Template.

8.5. DHCP Public Authoritative Name Server Set Option

The DHCP Public Authoritative Name Server Set Option
(OPTION_NAME_SERVER_SET) provides information so the CPE can upload
the DNS Homenet Zone to the Public Authoritative Name Server Set.
Finally, the option provides the security mechanisms that are
available to perform the upload. The upload is performed via a DNS
master / slave architecture or DNS updates.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     OPTION_NAME_SERVER_SET     |           option-len          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Security            |    Update   |                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                |
|                                                               |
/          Public Authoritative Name Server Set FQDN            /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
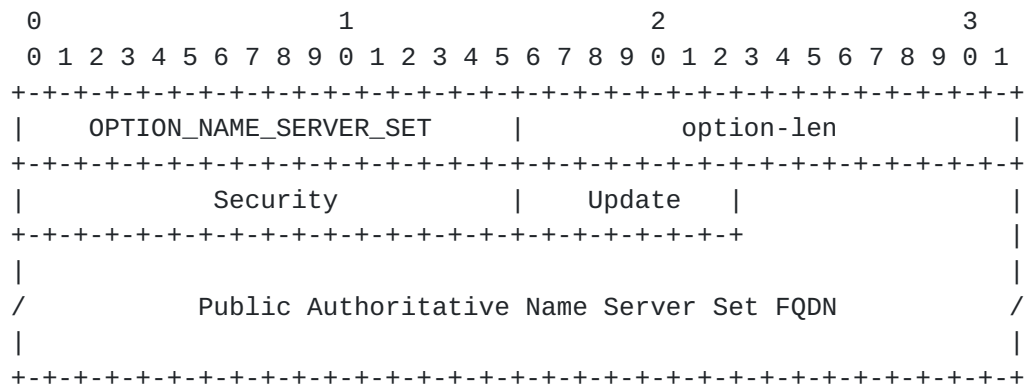
        Figure 6: DHCP Public Authoritative Name Server Set Option

- OPTION_NAME_SERVER_SET (16 bits): the option code for the DHCP
     Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as
     described in [RFC3315].

- Security (16 bits): defines which security protocols are supported
     by the DNS server. See Section 8.1 for more details.

- Update (8 bits): defines which update mechanisms are supported by
     the DNS server. See Section 6 for more details.

- Public Authoritative Name Server Set FQDN (variable): the FQDN of
     the Public Authoritative Name Server Set.

8.6. DHCP Reverse Public Authoritative Name Server Set Option

The DHCP Reverse Public Authoritative Name Server Set Option
(OPTION_REVERSE_NAME_SERVER_SET) provides information so the CPE can
upload the DNS Homenet Zone to the Public Authoritative Name Server
Set. The option provides the security mechanisms that are available
to perform the upload. The upload is performed via a DNS master /
slave architecture or DNS updates.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| OPTION_REVERSE_NAME_SERVER_SET|          option-len           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Security           |    Update   |                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                 |
|                                                               |
/      Reverse Public Authoritative Name Server Set FQDN        /
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
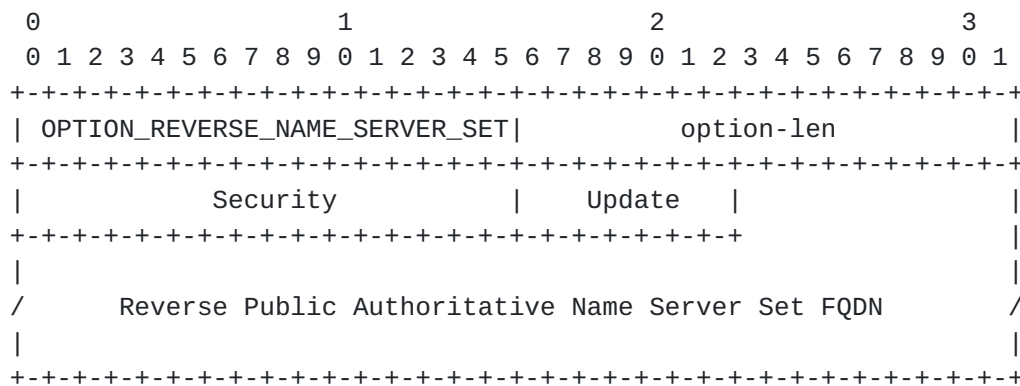
 Figure 7: DHCP Reverse Public Authoritative Name Server Set Option

- OPTION_REVERSE_NAME_SERVER_SET (16 bits): the option code for the
     DHCP Reverse Public Authoritative Name Server Set Option.

- option-len (16 bits): length in octets of the option-data field as
     described in [RFC3315].

- Security (16 bits): defines which security protocols are supported
     by the DNS server. See Section 8.1 for more details.

- Update (8 bits): defines which update mechanisms are supported by
     the DNS server. See Section 6 for more details.

- Reverse Public Authoritative Name Server Set FQDN (variable): The
     FQDN of the Reverse Public Authoritative Name Server Set.

9. DHCP Behavior

9.1. DHCPv6 Server Behavior

   The DHCP Server sends the DHCP Zone Template Option
   (OPTION_DNS_ZONE_TEMPLATE), DHCP Public Authoritative Name Server Set
   Option (OPTION_NAME_SERVER_SET), DHCP Reverse Public Authoritative
   Name Server Set Option (OPTION_REVERSE_NAME_SERVER_SET) upon request
   by the DHCP Client.

   The DHCP Server MAY receive a DHCP Public Key Option
   (OPTION_PUBLIC_KEY) from the CPE. Upon receipt of this DHCP Option,
   the DHCP Sever is expect to communicate this credential to the
   available DNS Servers like the DNS Template Server, the Public
   Authoritative Name Server Set and the Reverse Public Authoritative
   Name Server Set.

9.2. DHCPv6 Client Behavior

   The DHCP Client MAY send a DHCP Public Key Option (OPTION_PUBLIC_KEY)
   to the DHCP Server. This Public Key authenticates the CPE.

   The DHCP Client sends a DHCP Option Request Option (ORO) with the
   necessary DHCP options.

   A CPE SHOULD only send the an ORO request for DHCP Options it needs
   or for information that needs to be up-to-date.

   Upon receiving a DHCP option described in this document, the CPE
   SHOULD retrieve or update DNS zones using the associated security and
   update protocols.

9.3. DHCPv6 Relay Behavior

   DHCP Relay behavior are not modified by this document.

10. IANA Considerations

   The DHCP options detailed in this document is:

   - OPTION_DNS_ZONE_TEMPLATE: TBD

   - OPTION_NAME_SERVER_SET: TBD

   - OPTION_REVERSE_NAME_SERVER_SET: TBD

   - OPTION_PUBLIC_KEY: TBD

11. Security Considerations

11.1. DNSSEC is recommended to authenticate DNS hosted data

It is recommended that the (Reverse) DNS Homenet Zone is signed with
DNSSEC. The zone may be signed by the CPE or by a third party. We
recommend the zone to be signed by the CPE, and that the signed zone
is uploaded.

11.2. Channel between the CPE and ISP DHCP Server MUST be secured

The document considers that the channel between the CPE and the ISP
DHCP Server is trusted. More specifically, the CPE is authenticated
and the exchanged messages are protected. The current document does
not specify how to secure the channel. [RFC3315] proposes a DHCP
authentication and message exchange protection, [RFC4301], [RFC5996]
propose to secure the channel at the IP layer.

In fact, the channel MUST be secured because the CPE provides
authentication credentials. Unsecured channel may result in CPE
impersonation attacks.

11.3. CPEs are sensitive to DoS

CPE have not been designed for handling heavy load. The CPE are
exposed on the Internet, and their IP address is publicly published
on the Internet via the DNS. This makes the Home Network sensitive
to Deny of Service Attacks. The resulting outsourcing architecture
is described in [I-D.mglt-homenet-front-end-naming-delegation]. This
document shows how the outsourcing architecture can be automatically
set.

12. Acknowledgment

We would like to thank Tomasz Mrugalski, Marcin Siodelski and Bernie
Volz for their comments on the design of the DHCP 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.

13. References

13.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities",
           STD 13, RFC 1034, November 1987.

   [RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone
              Changes (DNS NOTIFY)", RFC 1996, August 1996.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound,
              "Dynamic Updates in the Domain Name System (DNS UPDATE)",
              RFC 2136, April 1997.

   [RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS
              Specification", RFC 2181, July 1997.

   [RFC2845] Vixie, P., Gudmundsson, O., Eastlake, D., and B.
              Wellington, "Secret Key Transaction Authentication for DNS
              (TSIG)", RFC 2845, May 2000.

   [RFC2930] Eastlake, D., "Secret Key Establishment for DNS (TKEY
              RR)", RFC 2930, September 2000.

   [RFC2931] Eastlake, D., "DNS Request and Transaction Signatures (
              SIG(0)s)", RFC 2931, September 2000.

   [RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic
              Update", RFC 3007, November 2000.

   [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
              and M. Carney, "Dynamic Host Configuration Protocol for
              IPv6 (DHCPv6)", RFC 3315, July 2003.

   [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "DNS Security Introduction and Requirements", RFC
              4033, March 2005.

   [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Resource Records for the DNS Security Extensions",
              RFC 4034, March 2005.

   [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S.
              Rose, "Protocol Modifications for the DNS Security
              Extensions", RFC 4035, March 2005.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
              Internet Protocol", RFC 4301, December 2005.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
              (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC5936] Lewis, E. and A. Hoenes, "DNS Zone Transfer Protocol
              (AXFR)", RFC 5936, June 2010.

   [RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen,
              "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC
              5996, September 2010.

   [RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer
              Security Version 1.2", RFC 6347, January 2012.

   [RFC6672] Rose, S. and W. Wijngaards, "DNAME Redirection in the
              DNS", RFC 6672, June 2012.

13.2. Informational 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.mglt-homenet-front-end-naming-delegation]
              Migault, D., Cloetens, W., Griffiths, C., and R. Weber,
              "IPv6 Home Network Naming Delegation", draft-mglt-homenet-
              front-end-naming-delegation-03 (work in progress), October
              2013.

   [I-D.sury-dnsext-cname-dname]
              Sury, O., "CNAME+DNAME Name Redirection", draft-sury-
              dnsext-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.

A.1. Base Scenario

   The base scenario is the one described in Section 4. It is typically
   the one of an ISP that manages the DHCP Server, and all DNS servers.

   The end user subscribes to the ISP (foo), and at subscription time
   registers for example.foo as its Registered Homenet Domain
   example.foo. Since the ISP knows the Registered Homenet Domain and
   the Public Authoritative Master(s) the ISP is able to build the DNS
   Homenet Zone Template.

   The ISP manages the DNS Template Server, so it is able to load the
   DNS Homenet Zone Template on the DNS Template Server.

When the CPE is plugged (at least the first time), it provides its
Public Key to the DHCP Server. In this scenario, the DHCP Server and
the DNS Servers are managed by the ISP so the DHCP Server can provide
authentication credentials of the CPE to enable secure authenticated
transaction between the CPE and these DNS servers. More
specifically, credentials are provided to:

-       Public Authoritative Name Server Set

-       Reverse Public Authoritative Name Server Set

-       DNS Template Server

The CPE can update the zone using DNS update or a master / slave
configuration in a secure way.

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.

A.2. Third Party Registered Homenet Domain

This section considers the case when the end user wants its home
network to use example.com as a Registered Homenet Domain instead of
example.foo that has been assigned by the ISP. We also suppose that
example.com is not managed by the ISP.

This can also be achieved without any configuration. 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 CPE may be changed, the zone can be updated as in Appendix A.1
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 A.1. 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.

A.3. 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 Public Authoritative Name Server Set and Public Authoritative Master(s) to a third party. All other DNS Servers DNS Template Server, Reverse Public Authoritative Master(s) and Reverse Public Authoritative Name Server Set remain managed by the ISP. The reason we consider that Reverse Public Authoritative Masters(s) and Reverse Public Authoritative Name Server Set remains managed by the ISP are that the prefix is managed by the ISP, so outsourcing these resources requires some redirection agreement with the ISP. More specifically the ISP will need to configure the redirection on one of its Reverse DNS Servers. That said, outsourcing these resources is similar as outsourcing Public Authoritative Name Server Set and Public Authoritative Master(s) to a third party. Similarly, the DNS Template Server can be easily outsourced as detailed in this section

Outsourcing Public Authoritative Name Server Set and Public Authoritative Master(s) requires:

- 1) Updating the DNS Homenet Zone Template: this can be easily done as detailed in Section 6 as the DNS Template Server is still managed by the ISP. Such modification can be performed once by any CPE. Once this modification has been performed, the CPE can be changed, the Public Key of the CPE may be changed, this does not need to be done another time. One can imagine a GUI on the CPE asking the end user to fill the field with Registered Homenet Domain, optionally Public Authoritative Master(s), with a button "Configure DNS Homenet Zone Template".

- 2) Updating the DHCP Server Information. In fact the Reverse Public Authoritative Name Server Set returned by the ISP is modified. 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.

- 3) Upload the authentication credential of the CPE, that is the Public Key of the CPE, to the third party. Unless we use specific mechanisms, like communication between the DHCP Server

and the third party, or a specific token that is plugged into
the CPE, this operation is likely to be performed every time
the CPE is changed, and every time the Public Key generated by
the CPE is changed.

The main advantage of this scenario is that the DNS infrastructure is
completely outsourced to the third party. Most likely the Public Key
that authenticate the CPE need to be configured for every CPE.
Configuration is expected to be CPE live-long.

Appendix B. Document Change Log

[RFC Editor: This section is to be removed before publication]

-03: Working Version Major modifications are:

- Redesigning options/scope: according to feed backs received from
    the IETF89 presentation in the dhc WG.

- Redesigning architecture: according to feed backs received from
    the IETF89 presentation in the homenet WG, discussion with Mark
    and Lorenzo.

-02: Working Version Major modifications are:

- Redesigning options/scope: As suggested by Bernie Volz

-01: Working Version Major modifications are:

- Remove the DNS Zone file construction: As suggested by Bernie Volz

- DHCPv6 Client behavior: Following options guide lines

- DHCPv6 Server behavior: Following options guide lines

-00: version published in the homenet WG. Major modifications are:

- Reformatting of DHCP Options: Following options guide lines

- DHCPv6 Client behavior: Following options guide lines

- DHCPv6 Server behavior: Following options guide lines

-00: First version published in dhc WG.

Authors' Addresses

   Daniel Migault
   Orange
   38 rue du General Leclerc
   92794 Issy-les-Moulineaux Cedex 9
   France

   Phone: +33 1 45 29 60 52
   Email: daniel.migault@orange.com

   Wouter Cloetens
   SoftAtHome
   vaartdijk 3 701
   3018 Wijgmaal
   Belgium

   Email: wouter.cloetens@softathome.com

   Chris Griffiths
   Dyn
   150 Dow Street
   Manchester, NH 03101
   US

   Email: cgriffiths@dyn.com
   URI: http://dyn.com

   Ralf Weber
   Nominum
   2000 Seaport Blvd #400
   Redwood City, CA 94063
   US

   Email: ralf.weber@nominum.com
   URI: http://www.nominum.com