HOMENET   D. Migault (Ed)
Internet-Draft   Orange
Intended status: Standards Track   W. Cloetens
Expires: March 22, 2015   SoftAtHome
                                                        C. Griffiths
                                                                 Dyn
                                                            R. Weber
                                                             Nominum
                                                  September 18, 2014

                Outsourcing Home Network Authoritative Naming Service
                draft-ietf-homenet-front-end-naming-delegation-00.txt

Abstract

   CPEs are designed to provide IP connectivity to home networks. Most
   CPEs assign IP addresses to the nodes of the home network which makes
   it a good candidate for hosting the naming service. With IPv6, the
   naming service makes nodes reachable from the home network as well as
   from the Internet.

   However, CPEs have not been designed to host such a naming service
   exposed on the Internet. This may expose the CPEs to resource
   exhaustion which would make the home network unreachable, and most
   probably would also affect the home network inner communications.

   In addition, DNSSEC management and configuration may not be well
   understood or mastered by regular end users. Misconfiguration may
   also results in naming service disruption, thus these end users may
   prefer to rely on third party naming providers.

   This document describes a homenet naming architecture where the CPEs
   manage the DNS zone associates to its home network, and outsources
   the naming service and eventually the DNSSEC management on the
   Internet to a third party designated as the Public Authoritative
   Servers.

Status of This Memo

   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 March 22, 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](). Introduction

   IPv6 provides global end to end IP reachability. To access services
   hosted in the home network with IPv6 addresses, end users prefer to
   use names instead of long and complex IPv6 addresses.

   CPEs are already providing IPv6 connectivity to the home network and
   generally provide IPv6 addresses or prefixes to the nodes of the home
   network. This makes the CPEs a good candidate to manage binding
   between names and IP addresses of the nodes. In addition,
   [[I-D.ietf-homenet-arch]()] recommends that home networks be resilient to
   connectivity disruption from the ISP. This requires that a dedicate
   device inside the home network manage bindings between names and IP
   addresses of the nodes and builds the DNS Homenet Zone. All this
   makes the CPE the natural candidate for setting the DNS(SEC) zone
   file of the home network.

   CPEs are usually low powered devices designed for the home network,
   but not for heavy traffic. As a result, hosting the an authoritative
   DNS service on the Internet may expose the home network to resource
   exhaustion, which may isolate the home network from the Internet and
   affect the services hosted by the CPEs, thus affecting the overall
   home network communications.

   In order to avoid resource exhaustion, this document describes an
   architecture that outsources the authoritative naming service of the
   home network. More specifically, the DNS(SEC) Homenet Zone built by

the CPE is outsourced to Public Authoritative Servers. These servers
publish the corresponding DN(SEC) Public Zone on the Internet.
Section 4.1 describes the architecture. In order to keep the
DNS(SEC) Public Zone up-to-date Section 5 describes how the DNS(SEC)
Homenet Zone and the DN(SEC) Public Zone can be synchronized. The
proposed architecture aims at deploying DNSSEC and the DNS(SEC)
Public Zone is expected to be signed with a secure delegation. The
zone signing and secure delegation can be performed either by the CPE
or by the Public Authoritative Servers. Section 6 discusses these
two alternatives. Section 7 discusses the impact of multiple views
and Section 8 discusses the case of the reverse zone.

3. 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 MAY also hosts
        services such as DHCPv6. This device MAY be provided by the
        ISP.

   - 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 MAY use specific servers for the
        synchronization of the DNS Homenet Zone: the Public
        Authoritative Name Server Set as public available name servers
        for the Registered Homenet Domain.

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

   - Public Authoritative Server: performs DNSSEC management

operations as well as provides the authoritative service for
the zone. In this document, the Public Authoritative Server
synchronizes the DNS Homenet Zone with the CPE via a hidden
master / slave architecture. The Public Authoritative Server
acts as a slave and MAY use specific servers called Public
Authoritative Name Server Set. Once the Public Authoritative
Server synchronizes the DNS Homenet Zone, it signs the zone and
generates the DNSSEC Public Zone. Then the Public
Authoritative Server hosts the zone as an authoritative server
on the Public Authoritative Master(s).

- DNSSEC Public Zone: corresponds to the signed version of the DNS
     Homenet Zone. It is hosted by the Public Authoritative Server,
     which is authoritative for this zone, and is reachable on the
     Public Authoritative Master(s).

- Public Authoritative Master(s):   are the visible name server
     hosting the DNSSEC Public 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.

4. Architecture Description

   This section describes the architecture for outsourcing the
   authoritative naming service from the CPE to the Public Authoritative

Master(s). [Section 4.1](#) describes the architecture, [Section 4.2](#) and
[Section 4.3](#) illustrate this architecture and shows how the DNS(SEC)
Homenet Zone should be built by the CPE, as well as lists the
necessary parameters the CPE needs to outsource the authoritative
naming service. These two section are informational and non
normative.

[4.1](#). Architecture Overview

Figure 1 provides an overview of the architecture.

The home network is designated by the Registered Homenet Domain Name
-- example.com in Figure 1. The CPE builds the DNS(SEC) Homenet Zone
associated to the home network. The content of the DNS(SEC) Homenet
Zone is out of the scope of this document. The CPE may host and
involve multiple services like a web GUI, DHCP [[RFC6644](#)] or mDNS
[[RFC6762](#)]. These services may coexist and may be used to populate
the DNS Homenet Zone. This document assumes the DNS(SEC) Homenet
Zone has been populated with domain names that are intended to be
publicly published and that are publicly reachable. More
specifically, names associated to services or devices that are not
expected to be reachable from outside the home network or names bound
to non globally reachable IP addresses MUST NOT be part of the
DNS(SEC) Homenet Zone.

Once the DNS(SEC) Homenet Zone has been built, the CPE does not host
the authoritative naming service for it, but instead outsources it to
the Public Authoritative Servers. The Public Authoritative Servers
take the DNS(SEC) Homenet as an input and publishes the DNS(SEC)
Public Zone. In fact the DNS(SEC) Homenet Zone and the DNS(SEC)
Public Zone have different names as they may be different. If the
CPE does not sign the DNS Homenet Zone, for example, the Public
Authoritative Servers may instead sign it on behalf of the CPE.
Figure 1 provides a more detailed description of the Public
Authoritative Servers, but overall, it is expected that the CPE
provides the DNS(SEC) Homenet Zone, the DNS(SEC) Public Zone is
derived from the DNS(SEC) Homenet Zone and published on the Internet.

As a result, DNS(SEC) queries from the DNS(SEC) Resolvers on the
Internet are answered by the Public Authoritative Server and do not

reach the CPE. Figure 1 illustrates the case of the resolution of
        node1.example.com.

```
home network +------------------+ Internet
             |                  |
             |        CPE       |
             |                  |                +---------------------+
+-------+    |+----------------+|                | Public Authoritative |
|       |    || DNS(SEC) Homenet||               | Servers              |
| node1 |    || Zone           ||                |+-------------------+|
|       |    ||                ||                ||DNS(SEC) Public Zone||
+-------+    || Homenet Domain ||========||       ||                   ||
             || Name           ||    ^    ||       ||   (example.com)   ||
node1.\      || (example.com)  ||    |    ||       |+-------------------+|
example.com  |+----------------+|    |    |       +---------------------+
             +------------------+    |              ^    |
                          Synchronization          |    |
                                                   |    |
        DNSSEC resolution for node1.example.com    |    v
                                              +---------------------+
                                              |                     |
                                              |   DNSSEC Resolver   |
                                              |                     |
                                              +---------------------+
```
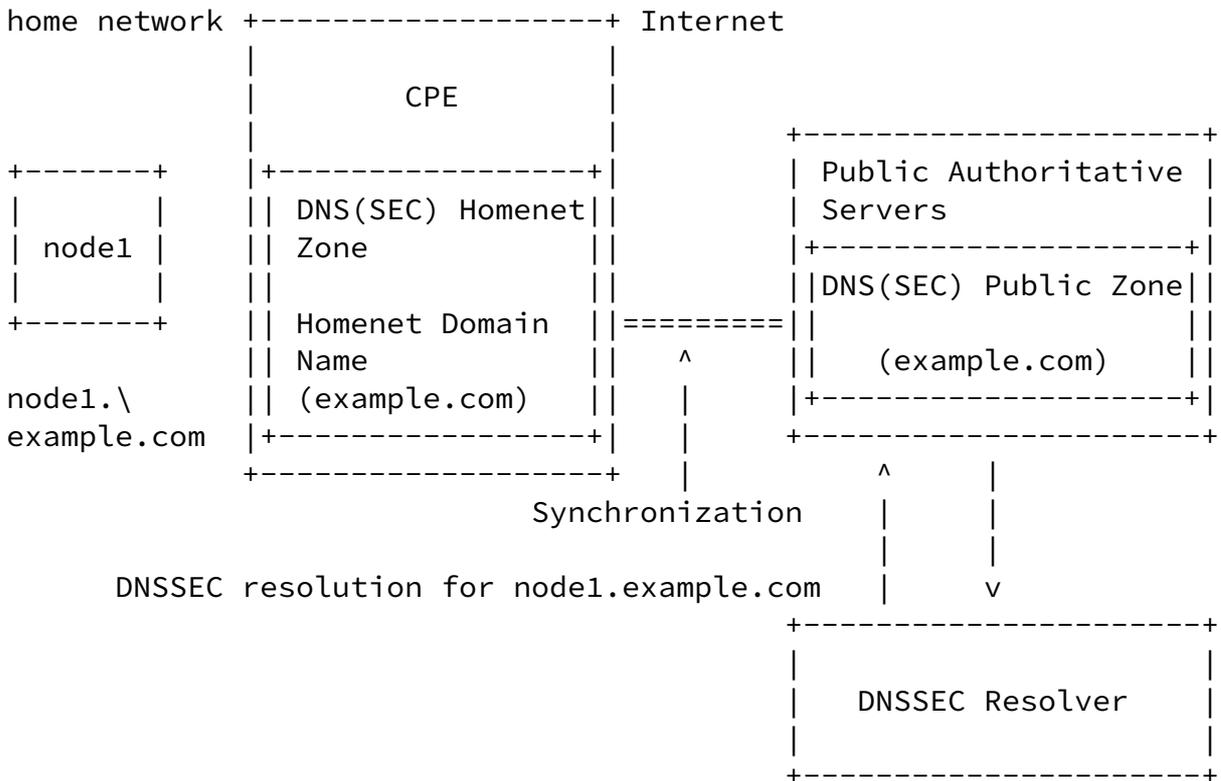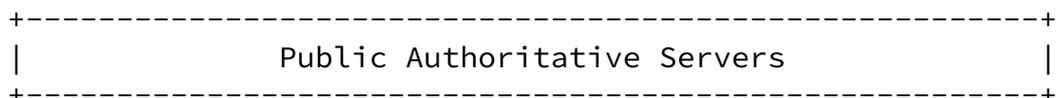
             Figure 1: Homenet Naming Architecture Description

   The Public Authoritative Servers are described in Figure 2. The
   Public Authoritative Name Server Set receives the DNS(SEC) Homenet
   Zone as an input. The received zone may be transformed to output the
   DNS(SEC) Public Zone. Various operations may be performed here,
   however the one this document considers here is zone signing when the

   CPE outsources this operation. Implications of such policy are
   detailed in Section 6 and Section 7.

```
                                Internet


        +----------------------------------------------------------+
        |              Public Authoritative Servers                |
        +----------------------------------------------------------+
```

```
            +--------------------+         +---------------------+
            |                    |         |                     |
            | Public Authoritative|        | Public Authoritative|
            | Name Server Set    |         | Masters             |
            |                    |         |                     |
            | +----------------+ |    X    | +-----------------+ |
            | | DNS(SEC) Homenet | |   ^     | | DNS(SEC) Public | |
     ========>| | Zone           | |   |     | | Zone            | |
        ^   | |                | |    |    | |                 | |
            | | (example.com)  | |    |    | | (example.com)   | |
            | | +------------+ | |    |    | | +-------------+ | |
            | +----------------+ |    |    | +-----------------+ |
            | +--------------------+   |    +---------------------+
            |                  Homenet to Public Zone
         Synchronization           transformation
         from the CPE
```
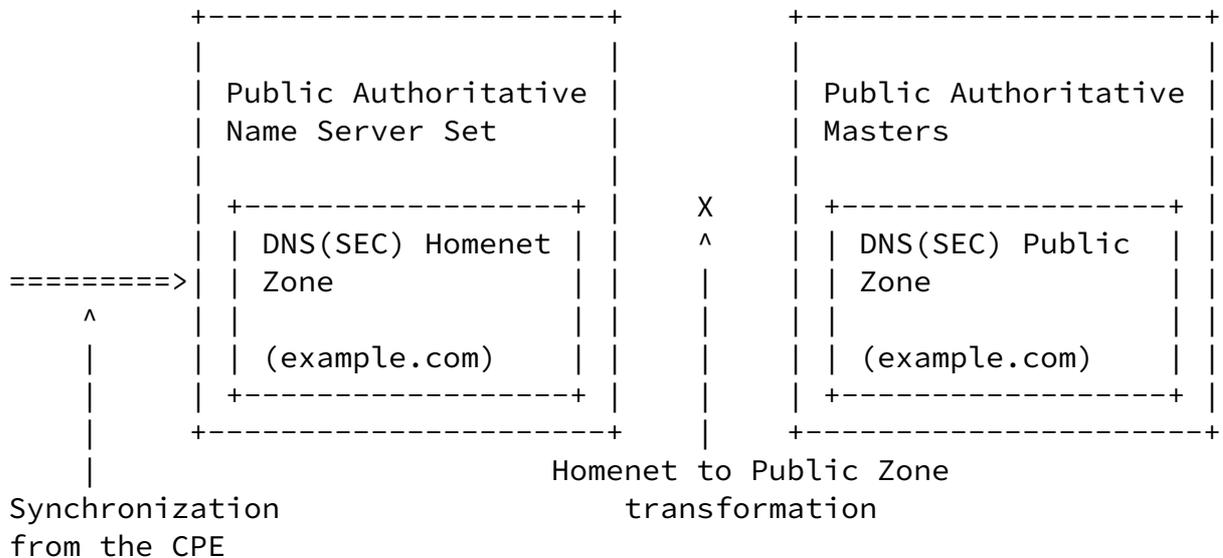
                Figure 2: Public Authoritative Servers Description

4.2. Example: DNS(SEC) Homenet Zone

   This section is not normative and intends to illustrate how the CPE
   builds the DNS(SEC) Homenet Zone.

   As depicted in Figure 1 and Figure 2, the DNS(SEC) Public Zone is
   hosted on the Public Authoritative Masters, whereas the DNS(SEC)
   Homenet Zone is hosted on the CPE. Motivations for keeping these two
   zones identical are detailed in Section 7, and this section considers
   that the CPE builds the zone that will be effectively published on
   the Public Authoritative Masters. In other words "Homenet to Public
   Zone transformation" is the identity.

   In that case, the DNS Homenet Zone should configure its Name Server
   RRset (NS) and Start of Authority (SOA) with the ones associated to
   the Public Authoritative Masters. This is illustrated in Figure 3.
   public.masters.example.net is the FQDN of the Public Authoritative
   Masters, and IP1, IP2, IP3, IP4 are the associated IP addresses.
   Then the CPE should add the different new nodes that enter the home
   network, remove those that should be removed and sign the DNS Homenet
   Zone.

```
          $ORIGIN example.com
```

```
        $TTL 1h

        @  IN  SOA  public.masters.example.net
                    hostmaster.example.com. (
                 2013120710 ; serial number of this zone file
                 1d         ; slave refresh
                 2h         ; slave retry time in case of a problem
                 4w         ; slave expiration time
                 1h         ; maximum caching time in case of failed
                            ; lookups
                 )

        @   NS  public.authoritative.servers.example.net

        public.masters.example.net   A @IP1
        public.masters.example.net   A @IP2
        public.masters.example.net   AAAA @IP3
        public.masters.example.net   AAAA @IP4
```

                    Figure 3: DNS Homenet Zone

   The SOA RRset is defined in [RFC1033], [RFC1035]. This SOA is
   specific as it is used for the synchronization between the Hidden
   Master and the Public Authoritative Name Server Set and published on
   the DNS Public Authoritative Master.

   - MNAME: indicates the primary master. In our case the zone is
        published on the Public Authoritative Master, and its name MUST
        be mentioned. If multiple Public Authoritative Masters are
        involved, one of them MUST be chosen. More specifically, the
        CPE MUST NOT place the name of the Hidden Master.

   - RNAME: indicates the email address to reach the administrator.
        [RFC2142] recommends to use hostmaster@domain and replacing the
        '@' sign by '.'.

   - REFRESH and RETRY: indicate respectively in seconds how often
        slaves need to check the master and the time between two
        refresh when a refresh has failed. Default value indicated by
        [RFC1033] are 3600 (1 hour) for refresh and 600 (10 minutes)
        for retry. This value MAY be long for highly dynamic content.
        However, Public Authoritative Masters and the CPE are expected
        to implement NOTIFY [RFC1996]. Then short values MAY increase
        the bandwidth usage for slaves hosting large number of zones.
        As a result, default values looks fine.

   EXPIRE: is the upper limit data SHOULD be kept in absence of
        refresh. Default value indicated by [RFC1033] is 3600000 about
        42 days. In home network architectures, the CPE provides both
        the DNS synchronization and the access to the home network.
        This device MAY be plug / unplugged by the end user without
        notification, thus we recommend large period.

   MINIMUM: indicates the minimum TTL. Default value indicated by
        [RFC1033] is 86400 (1 day). For home network, this value MAY
        be reduced, and 3600 (1hour) seems more appropriated.

4.3. Example: CPE necessary parameters for outsourcing

   This section specifies the various parameters required by the CPE to
   configure the naming architecture of this document. This section is
   informational, and is intended to clarify the information handled by
   the CPE and the various settings to be done.

   Public Authoritative Name Server Set may be defined with the
   following parameters. These parameters are necessary to establish a
   secure channel between the CPE and the Public Authoritative Name
   Server Set:

   - Public Authoritative Name Server Set: The associated FQDNs or IP
        addresses of the Public Authoritative Server. IP addresses are
        optional and the FQDN is sufficient. To secure the binding
        name and IP addresses, a DNSSEC exchange is required.
        Otherwise, the IP addresses should be entered manually.

   - Authentication Method: How the CPE authenticates itself to the
        Public Server. This MAY depend on the implementation but we
        should consider at least IPsec, DTLS and TSIG

   - Authentication data: Associated Data. PSK only requires a single
        argument. If other authentication mechanisms based on
        certificates are used, then, files for the CPE private keys,
        certificates and certification authority should be specified.

   - Public Authoritative Master(s):   The FQDN or IP addresses of the
        Public Authoritative Master. It MAY correspond to the data
        that will be set in the NS RRsets and SOA of the DNS Homenet
        Zone. IP addresses are optional and the FQDN is sufficient.
        To secure the binding name and IP addresses, a DNSSEC exchange
        is required. Otherwise, the IP addresses should be entered
        manually.

    - Registered Homenet Domain: The domain name the Public
        Authoritative is configured for DNS slave, DNSSEC zone signing
        and DNSSEC zone hosting.

   Setting the DNS(SEC) Homenet Zone requires the following information.

    - Registered Homenet Domain: The Domain Name of the zone. Multiple
        Registered Homenet Domain may be provided. This will generate
        the creation of multiple DNS Homenet Zones.

    - Public Authoritative Server: The Public Authoritative Servers
        associated to the Registered Homenet Domain. Multiple Public
        Authoritative Server may be provided.

5. Synchronization between CPE and Public Authoritative Servers

   The DNS(SEC) Homenet Reverse Zone and the DNS Homenet Zone can be
   updated either with DNS update [RFC2136] or using a master / slave
   synchronization. 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.

   This document recommends the use of a master / slave mechanism
   instead of the use of nsupdates. This section details the master /
   slave mechanism.

5.1. Synchronization with a Hidden Master

   Uploading and dynamically updating the zone file on the Public
   Authoritative Name Server Set can be seen as zone provisioning
   between the CPE (Hidden Master) and the Public Authoritative Name

Server Set (Slave Server). This can be handled either in band or out
of band.

The Public Authoritative Name Server Set is configured as a slave for
the Homenet Domain Name. This slave configuration has been
previously agreed between the end user and the provider of the Public
Authoritative Servers. In order to set the master/ slave
architecture, the CPE acts as a Hidden Master Server, which is a
regular Authoritative DNS(SEC) Server listening on the WAN interface.

The Hidden Master Server is expected to accept SOA [RFC1033], AXFR
[RFC1034], and IXFR [RFC1995] queries from its configured slave DNS
servers. The Hidden Master Server SHOULD send NOTIFY messages
[RFC1996] in order to update Public DNS server zones as updates
occur. Because, DNS Homenet Zones are likely to be small, CPE MUST
implement AXFR and SHOULD implement IXFR.

Hidden Master Server differs from a regular authoritative server for
the home network by:

- Interface Binding: the Hidden Master Server listens on the WAN
     Interface, whereas a regular authoritative server for the home
     network would listen on the home network interface.

- Limited exchanges: the purpose of the Hidden Master Server is to
     synchronizes with the Public Authoritative Name Server Set, not
     to serve zone. As a result, exchanges are performed with
     specific nodes (the Public Authoritative Servers). Then
     exchange types are limited. The only legitimate exchanges are:
     NOTIFY initiated by the Hidden Master and IXFR or AXFR
     exchanges initiated by the Public Authoritative Name Server
     Set. On the other hand regular authoritative servers would
     respond any hosts on the home network, and any DNS(SEC) query
     would be considered. The CPE SHOULD filter IXFR/AXFR traffic
     and drop traffic not initiated by the Public Authoritative
     Server. The CPE MUST listen for DNS on TCP and UDP and at
     least allow SOA lookups to the DNS Homenet Zone.

5.2. Securing Synchronization

Exchange between the Public Servers and the CPE MUST be secured, at
least for integrity protection and for authentication. This is the

case whatever mechanism is used between the CPE and the Public
Authoritative Name Server Set.

TSIG [RFC2845] or SIG(0) [RFC2931] can be used to secure the DNS
communications between the CPE and the Public DNS(SEC) Servers. TSIG
uses a symmetric key which can be managed by TKEY [RFC2930].
Management of the key involved in SIG(0) is performed through zone
updates. How to roll the keys with SIG(0) is out-of-scope of this
document. The advantage of these mechanisms is that they are only
associated with the DNS application. Not relying on shared libraries
ease testing and integration. On the other hand, using TSIG, TKEY or
SIG(0) requires that these mechanisms to be implemented on the
DNS(SEC) Server's implementation running on the CPE, which adds
codes. Another disadvantage is that TKEY does not provides
authentication mechanism.

Protocols like TLS [RFC5246] / DTLS [RFC6347] can be used to secure
the transactions between the Public Authoritative Servers and the
CPE. The advantage of TLS/DTLS is that this technology is widely
deployed, and most of the boxes already embeds a TLS/DTLS libraries,
eventually taking advantage of hardware acceleration. Then TLS/DTLS
provides authentication facilities and can use certificates to
authenticate the Public Authoritative Server and the CPE. On the
other hand, using TLS/DTLS requires to integrate DNS exchange over
TLS/DTLS, as well as a new service port. This is why we do not
recommend this option.

IPsec [RFC4301] IKEv2 [RFC5996] can also be used to secure the
transactions between the CPE and the Public Authoritative Servers.
Similarly to TLS/DTLS, most CPE already embeds a IPsec stack, and
IKEv2 provides multiple authentications possibilities with its EAP
framework. In addition, IPsec can be used to protect the DNS
exchanges between the CPE and the Public Authoritative Servers
without any modifications of the DNS Servers or client. DNS
integration over IPsec only requires an additional security policy in
the Security Policy Database. One disadvantage of IPsec is that it
hardly goes through NATs and firewalls. However, in our case, the
CPE is connected to the Internet, and IPsec communication between the
CPE and Public Authoritative Server SHOULD NOT be impacted by middle
boxes.

As mentioned above, TSIG, IPsec and TLS/DTLS may be used to secure
transactions between the CPE and the Public Authentication Servers.
The CPE and Public Authoritative Server SHOULD implement TSIG and
IPsec.

How the PSK can be used by any of the TSIG, TLS/DTLS or IPsec
protocols. Authentication based on certificates implies a mutual
authentication and thus requires the CPE to manage a private key, a
public key or certificates as well as Certificate Authorities. This
adds complexity to the configuration especially on the CPE side. For
this reason, we recommend that CPE MAY use PSK or certificate base
authentication and that Public Authentication Servers MUST support
PSK and certificate based authentication.

5.3. CPE Security Policies

   This section details security policies related to the Hidden Master /
   Slave synchronization.

   The Hidden Master, as described in this document SHOULD drop any
   queries from the home network. This can be performed with port
   binding and/or firewall rules.

   The Hidden Master SHOULD drop on the WAN interface any DNS queries
   that is not issued from the Public Authoritative Server Name Server
   Set.

   The Hidden Master SHOULD drop any outgoing packets other than DNS
   NOTIFY query, SOA response, IXFR response or AXFR responses.

   The Hidden Master SHOULD drop any incoming packets other than DNS
   NOTIFY response, SOA query, IXFR query or AXFR query.

   The Hidden Master SHOULD drop any non protected IXFR or AXFR
   exchange. This depends how the synchronization is secured.

6. DNSSEC compliant Homenet Architecture

   [I-D.ietf-homenet-arch] in Section 3.7.3 recommends DNSSEC to be
   deployed on the both the authoritative server and the resolver. The
   resolver side is out of scope of this document, and only the

authoritative part is considered.

Deploying DNSSEC requires signing the zone and configuring a secure
delegation. As described in Section 4.1, signing can be performed by
the CPE or by the Public Authoritative Servers. Section 6.1 details
the implications of these two alternatives. Similarly, the secure
delegation can be performed by the CPE or by the Public Authoritative
Servers. Section 6.2 discusses these two alternatives.

6.1. Zone Signing

This section discusses the pros and cons when zone signing is
performed by the CPE or by the Public Authoritative Servers. It is
recommended to sign the zone by the CPE unless there is a strong
argument against it, like a CPE that is not able to sign the zone.
In that case zone signing may be performed by the Public
Authoritative Servers on behalf of the CPE.

Reasons for signing the zone by the CPE are:

- 1: Keeping the Homenet Zone and the Public Zone equals. This
      aspect is discussed in detail in Section 7. More specifically,
      if the CPE signs the DNS Homenet Zone, then, the CPE has the
      ability to host the authoritative naming service of the homenet
      for DNSSEC queries coming from within the network. As a
      result, a query will be resolved the same way whether it is
      sent from the home network or from the Internet. On the other
      hand, if the CPE does not sign the DNS Homenet Zone, either it
      acts as an authoritative server for the home network or not.
      If the CPE is an authoritative server for queries initiated

      from within the home network, then nodes connected to both
      networks-- the home network and the Internet -- do not have a
      unique resolution. Devices that may be impacted are mobile
      phones with Radio Access Network interfaces and WLAN
      interfaces. Alternatively if the CPE does not act as an
      authoritative server, it goes against the principles
      connectivity disruption independence exposed in
      [I-D.ietf-homenet-arch] section 4.4.1 and 3.7.5. In case of
      connectivity disruption, naming resolution for nodes inside the
      home network for nodes in the home network are not possible.

- 2: Privacy and Integrity of the DNS Zone are better guaranteed.
         When the Zone is signed by the CPE, it makes modification of
         the DNS data -- for example for flow redirection -- not
         possible. As a result, signing the Homenet Zone by the CPE
         provides better protection for the end user privacy.

   Reasons for signing the zone by the Public Authoritative Servers are:

   - 1: The CPE is not able to sign the zone, most likely because its
         firmware does not make it possible. However the reason is
         expected to be less and less valid over time.

   - 2: Outsourcing DNSSEC management operations. Management
         operations involve key-roll over which can be done
         automatically by the CPE and transparently for the end user.
         As result avoiding DNSSEC management is mostly motivated by bad
         software implementations.

   - 3: Reducing the impact of CPE replacement on the Public Zone.
         Unless the CPE private keys are backuped, CPE replacement
         results in a emergency key roll over. This can be mitigated
         also by using relatively small TTLs.

   - 4: Reducing configuration impacts on the end user. Unless there
         are some zero configuration mechanisms to provide credentials
         between the new CPE and the Public Authoritative Name Server
         Sets. Authentications to Public Authoritative Name Server Set
         should be re-configured. As CPE replacement is not expected to
         happen regularly, end users may not be at ease with such
         configuration settings. However, mechanisms as described in
         [I-D.mglt-homenet-naming-architecture-dhc-options] use DHCP
         Options to outsource the configuration and avoid this issue.

   - 5: Public Authoritative Servers are more likely to handle securely
         private keys than the CPE. However, having all private
         information at one place may also balance that risk.

6.2. Secure Delegation

   The secure delegation is set if the DS RRset is properly set in the
   parent zone. Secure delegation can be performed by the CPE or the

Public Authoritative Servers.

The DS RRset can be updated manually by the CPE or the Public
Authoritative Servers. This can be used then with nsupdate for
example bu requires the CPE or the Public Authoritative Server to be
authenticated by the Parent Zone Server. Such a trust channel
between the CPE and the Parent Zone server may be hard to maintain,
and thus may be easier to establish with the Public Authoritative
Server. On the other hand,
[I-D.ietf-dnsop-delegation-trust-maintainance] may mitigate such
issues.

7. Handling Different Views

The issue raised by handling different views of the DNS Homenet Zone
or a DNS Homenet Zone that differs from the Public Zone is that a
given DNS query may lead to different responses. The responses may
be different values for the queried RRsets or different RCODE or
different RRsets types in the responses for DNS/DNSSEC responses.

The document does not recommend the CPE manages different views,
since devices may be connected to different networks at the same time
or may flip / flop from one network to the other.

8. Reverse Zone

Most of the description considered the DNS Homenet Zone as the non-
Reverse Zone. This section is focused on the Reverse Zone.

First, all considerations for the DNS Homenet Zone apply to the
Reverse Homenet Zone. The main difference between the Reverse DNS
Homenet Zone and the DNS Homenet Zone is that the parent zone of the
Reverse Homenet Zone is most likely managed by the ISP. As the ISP
also provides the IP prefix to the CPE, it may be able to
authenticate the CPE. If the Reverse Public Authoritative Name
Server Set is managed by the ISP, credentials to authenticate the CPE
for the zone synchronization may be set automatically and
transparently to the end user.
[I-D.mglt-homenet-naming-architecture-dhc-options] describes how
automatic configuration may be performed.

9. Security Considerations

   The Homenet Naming Architecture described in this document solves
   exposing the CPE's DNS service as a DoS attack vector.

9.1. Names are less secure than IP addresses

   This document describes how an End User can make his services and
   devices from his home network reachable on the Internet with Names
   rather than IP addresses. This exposes the home network to attackers
   since names are expected to provide less randomness than IP
   addresses. The naming delegation protects the End User's privacy by
   not providing the complete zone of the home network to the ISP.
   However, using the DNS with names for the home network exposes the
   home network and its components to dictionary attacks. In fact, with
   IP addresses, the Interface Identifier is 64 bit length leading to
   2^64 possibilities for a given subnetwork. This is not to mention
   that the subnet prefix is also of 64 bit length, thus providing
   another 2^64 possibilities. On the other hand, names used either for
   the home network domain or for the devices present less randomness
   (livebox, router, printer, nicolas, jennifer, ...) and thus exposes
   the devices to dictionary attacks.

9.2. Names are less volatile than IP addresses

   IP addresses may be used to locate a device, a host or a Service.
   However, home networks are not expected to be assigned the same
   Prefix over time. As a result observing IP addresses provides some
   ephemeral information about who is accessing the service. On the
   other hand, Names are not expected to be as volatile as IP addresses.
   As a result, logging Names, over time, may be more valuable that
   logging IP addresses, especially to profile End User's
   characteristics.

   PTR provides a way to bind an IP address to a Name. In that sense
   responding to PTR DNS queries may affect the End User's Privacy. For
   that reason we recommend that End Users may choose to respond or not
   to PTR DNS queries and may return a NXDOMAIN response.

10. IANA Considerations

   This document has no actions for IANA.

11. Acknowledgment

   The authors wish to thank Philippe Lemordant for its contributions on
   the early versions of the draft, Ole Troan for pointing out issues

with the IPv6 routed home concept and placing the scope of this

document in a wider picture, Mark Townsley for encouragement and
injecting a healthy debate on the merits of the idea, Ulrik de Bie
for providing alternative solutions, Paul Mockapetris, Christian
Jacquenet, Francis Dupont and Ludovic Eschard for their remarks on
CPE and low power devices, Olafur Gudmundsson for clarifying DNSSEC
capabilities of small devices, Simon Kelley for its feedback as
dnsmasq implementer. Andrew Sullivan, Mark Andrew, Ted Lemon, Mikael
Abrahamson and Michael Richardson, Ray Bellis for their feed backs on
handling different views as well as clarifying the impact of
outsourcing the zone signing operation outside the CPE.

12. References

12.1. Normative References

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

   [RFC1035]   Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, November 1987.

   [RFC1995]   Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995,
               August 1996.

   [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.

   [RFC2142]   Crocker, D., "MAILBOX NAMES FOR COMMON SERVICES, ROLES AND
               FUNCTIONS", RFC 2142, May 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.

[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.

[RFC6644] Evans, D., Droms, R., and S. Jiang, "Rebind Capability in
           DHCPv6 Reconfigure Messages", RFC 6644, July 2012.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762,
           February 2013.

12.2. Informational References

[I-D.ietf-dnsop-delegation-trust-maintainance]
           Kumari, W., Gudmundsson, O., and G. Barwood, "Automating
           DNSSEC Delegation Trust Maintenance", draft-ietf-dnsop-
           delegation-trust-maintainance-14 (work in progress), June
           2014.

[I-D.ietf-homenet-arch]
           Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil,
           "IPv6 Home Networking Architecture Principles", draft-

ietf-homenet-arch-16 (work in progress), June 2014.

[I-D.mglt-homenet-naming-architecture-dhc-options]
Migault, D., Cloetens, W., Griffiths, C., and R. Weber,
"DHCP Options for Homenet Naming Architecture", draft-
mglt-homenet-naming-architecture-dhc-options-02 (work in
progress), July 2014.

[RFC1033] Lottor, M., "Domain administrators operations guide", RFC
1033, November 1987.

Appendix A.   Document Change Log

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

   -04:

   *Clarifications on zone signing

   *Rewording

   *Adding section on different views

   *architecture clarifications

   -03:

   *Simon's comments taken into consideration

   *Adding SOA, PTR considerations

   *Removing DNSSEC performance paragraphs on low power devices

   *Adding SIG(0) as a mechanism for authenticating the servers

   *Goals clarification: the architecture described in the document 1)
   does not describe new protocols, and 2) can be adapted to specific

cases for advance users.

-02:

*remove interfaces: "Public Authoritative Server Naming Interface" is replaced by "Public Authoritative Master(s)". "Public Authoritative Server Management Interface" is replaced by "Public Authoritative Name Server Set".

-01.3:

*remove the authoritative / resolver services of the CPE. Implementation dependent

*remove interactions with mdns and dhcp. Implementation dependent.

*remove considerations on low powered devices

*remove position toward homenet arch

*remove problem statement section

-01.2:

* add a CPE description to show that the architecture can fit CPEs

* specification of the architecture for very low powered devices.

* integrate mDNS and DHCP interactions with the Homenet Naming Architecture.

* Restructuring the draft. 1) We start from the homenet-arch draft to derive a Naming Architecture, then 2) we show why CPE need mechanisms that do not expose them to the Internet, 3) we describe the mechanisms.

* I remove the terminology and expose it in the figures A and B.

* remove the Front End Homenet Naming Architecture to Homenet Naming

-01:

* Added C. Griffiths as co-author.

   * Updated [section 5.4](#) and other sections of draft to update section
   on Hidden Master / Slave functions with CPE as Hidden Master/Homenet
   Server.

   * For next version, address functions of MDNS within Homenet Lan and
   publishing details northbound via Hidden Master.

   -00: First version published.

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