Internet Engineering Task Force (IETF)
Request for Comments: 9526
Category: Experimental
ISSN: 2070-1721

D. Migault
Ericsson
R. Weber
Nominum
M. Richardson
Sandelman Software Works
R. Hunter
Globis Consulting BV

January 2024

Simple Provisioning of Public Names for Residential Networks

Abstract

Home network owners may have devices or services hosted on their home network that they wish to access from the Internet (i.e., from a network outside of the home network). Home networks are increasingly numbered using IPv6 addresses, which in principle makes this access simpler, but accessing home networks from the Internet requires the names and IP addresses of these devices and services to be made available in the public DNS.

This document describes how a Home Naming Authority (NHA) instructs the outsourced infrastructure to publish these pieces of information in the public DNS. The names and IP addresses of the home network are set in the Public Homenet Zone by the Homenet Naming Authority (HNA), which in turn instructs an outsourced infrastructure to publish the zone on behalf of the home network owner.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9526.

Table of Contents

1. Introduction

Home network owners may have devices or services hosted on their home network that they wish to access from the Internet (i.e., from a network outside of the home network). The use of IPv6 addresses in the home makes, in principle, the actual network access simpler, while on the other hand, the addresses are much harder to remember and are subject to regular renumbering. To make this situation simpler for typical home owners to manage, there needs to be an easy way for the names and IP addresses of these devices and services to be published in the public DNS.

As depicted in Figure 1, the names and IP address of the home network are made available in the Public Homenet Zone by the Homenet Naming Authority (HNA), which in turn instructs the DNS Outsourcing Infrastructure (DOI) to publish the zone on behalf of the HNA. This

document describes how an HNA can instruct a DOI to publish a Public Homenet Zone on its behalf.

This document introduces the Synchronization Channel and the Control Channel between the HNA and the Distribution Manager (DM), which is the main interface to the DOI.

The Synchronization Channel (see Section 7) is used to synchronize the Public Homenet Zone.

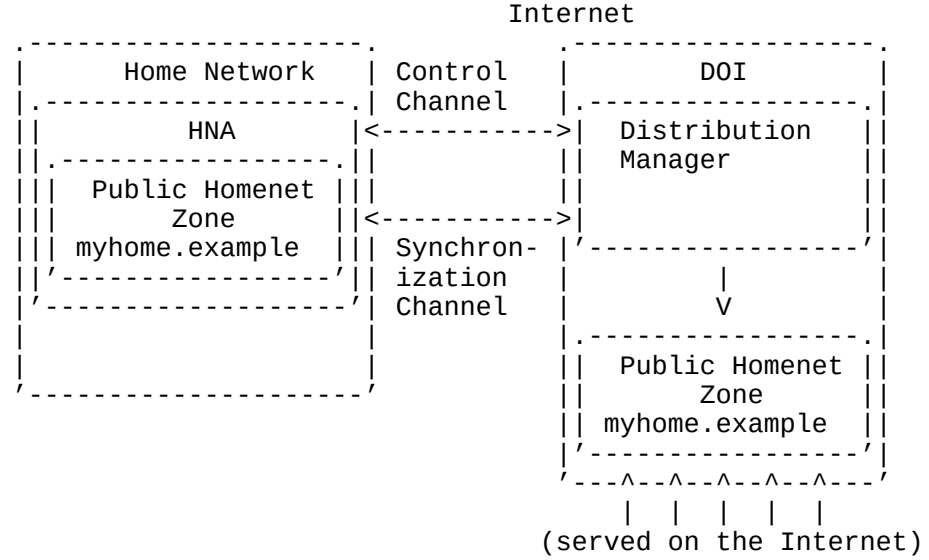


Figure 1: High-Level Architecture Overview of Outsourcing the Public Homenet Zone

The Synchronization Channel is a zone transfer, with the HNA configured as a primary server and the Distribution Manager configured as a secondary server. Some operators refer to this kind of configuration as a "hidden primary", but that term is not used in this document as it is not precisely defined anywhere, but it has many slightly different meanings to many.

The Control Channel (see Section 6) is used to set up the Synchronization Channel. This channel is in the form of a dynamic DNS update process, authenticated by TLS.

For example, to build the Public Homenet Zone, the HNA needs the authoritative servers (and associated IP addresses) of the DOI's servers (the visible primaries) that are actually serving the zone. Similarly, the DOI needs to know the IP address of the (hidden) primary (HNA) as well as potentially the hash of the Key Signing Key (KSK) in the DS RRset to secure the DNSSEC delegation with the parent zone.

The remainder of the document is as follows.

Section 2 defines the terminology. Section 3 presents the general problem of publishing names and IP addresses. Section 4 briefly describes some potential envisioned deployment scenarios. And Section 5 provides an architectural view of the HNA, DM, and DOI as well as their different communication channels (Control Channel, Synchronization Channel, and DM Distribution Channel) described in Sections 6, 7, and 8, respectively.

Then, Sections 6 and 7 deal with the two channels that interface to the home. Section 8 provides a set of requirements and expectations on how the distribution system works. This section is non-normative and not subject to standardization but reflects how many scalable DNS

distribution systems operate.

Sections 9 and 11 respectively detail HNA security policies as well as DNSSEC compliance within the home network.

Section 12 discusses how renumbering should be handled.

Finally, Sections 13 and 14 respectively discuss privacy and security considerations when outsourcing the Public Homenet Zone.

The appendices discuss the following aspects: management (see Section 10), provisioning (see Section 10), configurations (see Appendix B), and deployment (see Section 4 and Appendix C).

2. Terminology

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

Customer Premises Equipment (CPE): A router providing connectivity to the home network.

Homenet Zone: The DNS zone for use within the boundaries of the home network: "home.arpa" (see [RFC8375]). This zone is not considered public and is out of scope for this document.

Registered Homenet Domain: The domain name that is associated with the home network. A given home network may have multiple Registered Homenet Domains.

Public Homenet Zone: Contains the names in the home network that are expected to be publicly resolvable on the Internet. A home network can have multiple Public Homenet Zones.

Homenet Naming Authority (HNA): A function responsible for managing the Public Homenet Zone. This includes populating the Public Homenet Zone, signing the zone for DNSSEC, as well as managing the distribution of that Homenet Zone to the DOI.

DNS Outsourcing Infrastructure (DOI): The infrastructure responsible for receiving the Public Homenet Zone and publishing it on the Internet. It is mainly composed of a Distribution Manager and Public Authoritative Servers.

Public Authoritative Servers: The authoritative name servers for the Public Homenet Zone. Name resolution requests for the Registered Homenet Domain are sent to these servers. Some DNS operators refer to these as public secondaries, and higher resiliency networks are often implemented in an anycast fashion.

Homenet Authoritative Servers: The authoritative name servers for the Homenet Zone within the Homenet network itself. These are sometimes called "hidden primary servers".

Distribution Manager (DM): The server (or set of servers) that the HNA synchronizes the Public Homenet Zone to and that then distributes the relevant information to the Public Authoritative Servers. This server has been historically known as the Distribution Master.

Public Homenet Reverse Zone: The reverse zone file associated with the Public Homenet Zone.

Reverse Public Authoritative Servers: These are equivalent to Public Authoritative Servers, specifically for reverse resolution.

Reverse Distribution Manager: This is equivalent to the Distribution Manager, specifically for reverse resolution.

DNS Resolver: A resolver that performs a DNS resolution on the Internet for the Public Homenet Zone. The resolution is performed by requesting the Public Authoritative Servers. While the resolver does not necessarily perform DNSSEC resolutions, it is RECOMMENDED that DNSSEC is enabled.

Note that when "DNS Resolver" is used in this document, it refers to "DNS or DNSSEC Resolver".

Homenet DNS Resolver: A resolver that performs a DNS or DNSSEC resolution on the home network for the Public Homenet Zone. The resolution is performed by requesting the Homenet Authoritative Servers.

3. Selecting Names and Addresses to Publish

While this document does not create any normative mechanism to select the names to publish, it does anticipate that the home network administrator (a human being) will be presented with a list of current names and addresses either directly on the HNA or via another device such as a smartphone.

The administrator will mark which devices and services (by name) are to be published. The HNA will then collect the IP address(es) associated with that device or service and put the name into the Public Homenet Zone. The address of the device or service can be collected from a number of places: Multicast DNS (mDNS) [RFC6762], DHCP [RFC8415], Universal Plug and Play (UPnP), the Port Control Protocol (PCP) [RFC6887], or manual configuration.

A device or service SHOULD have Global Unicast Addresses (GUAs) (IPv6 [RFC3587] or IPv4) but MAY also have IPv6 Unique Local Addresses (ULAs) [RFC4193], IPv6 Link-Local Addresses (LLAs) [RFC4291] [RFC7404], IPv4 LLAs [RFC3927], and private IPv4 addresses [RFC1918].

Of these, the LLAs are almost never useful for the Public Zone and should be omitted.

The IPv6 ULA and private IPv4 addresses may be useful to publish, if the home network environment features a VPN that would allow the home owner to reach the network. [RFC1918] addresses in public zones are generally filtered out by many DNS servers as they are considered rebind attacks [REBIND].

In general, one expects the GUA to be the default address to be published. A direct advantage of enabling local communication is to enable communications even in case of Internet disruption. Since communications are established with names that remain a global identifier, the communication can be protected (at the very least with integrity protection) by TLS the same way it is protected on the global Internet -- by using certificates.

4. Envisioned Deployment Scenarios

A number of deployment scenarios have been envisioned; this section aims at providing a brief description. The use cases are not limitations, and this section is not normative.

The main difference between the various deployments concerns the provisioning of the HNA -- that is, how it is configured to outsource

the Public Homenet Zone to the DOI -- as well as how the Public Homenet Zone is being provisioned before being outsourced. In both cases, these configuration aspects are out of the scope of this document.

Provisioning the configuration related to the DOI is expected to be automated as much as possible and require interaction with the end user as little as possible. Zero configuration can only be achieved under some circumstances, and [RFC9527] provides one such example under the assumption that the ISP provides the DOI. Section 4.1 describes another variant where the Customer Premises Equipment (CPE) is provided preconfigured with the DOI. Section 4.2 describes how an agnostic CPE may be configured by the home network administrator. Of course even in this case, the configuration can leverage mechanisms to prevent the end user from manually entering all information.

On the other hand, provisioning the Public Homenet Zone needs to combine the ability to closely reflect what the end user wishes to publish on the Internet while easing such interaction. The HNA may implement such interactions using web-based GUIs or specific mobile applications.

With the CPE configured with the DOI, the HNA contacts the DOI to build a template for the Public Homenet Zone and then provisions the Public Homenet Zone. Once the Public Homenet Zone is built, the HNA starts synchronizing it with the DOI on the Synchronization Channel.

4.1. CPE Vendor

A specific vendor that has specific relations with a registrar or a registry may sell a CPE that is provisioned with a domain name. Such a domain name is probably not human friendly and may consist of some kind of serial number associated with the device being sold.

One possible scenario is that the vendor provisions the HNA with a private key with an associated certificate used for the mutual TLS authentication. Note that these keys are not expected to be used for DNSSEC signing.

Instead, these keys are solely used by the HNA for the authentication to the DM. Normally, the keys are necessary and sufficient to proceed to the authentication.

When the home network owner plugs in the CPE at home, the relation between the HNA and DM is expected to work out of the box.

4.2. Agnostic CPE

A CPE that is not preconfigured may also use the protocol defined in this document, but some configuration steps will be needed.

1. The owner of the home network buys a domain name from a registrar and, as such, creates an account on that registrar.

2. The registrar may provide the outsourcing infrastructure, or the home network may need to create a specific account on the outsourcing infrastructure.

* If the DOI is the DNS Registrar, it has by design a proof of ownership of the domain name by the Homenet owner. In this case, it is expected that the DOI provides the necessary parameters to the home network owner to configure the HNA. One potential mechanism to provide the parameters would be to provide the user with a JSON object that they can copy and paste into the CPE, such as described in Appendix B. But what matters to the infrastructure is that the HNA is able to authenticate itself to

the DOI.

* If the DOI is not the DNS Registrar, then the proof of ownership needs to be established using some other protocol. Automatic Certificate Management Environment (ACME) [RFC8555] is one protocol that would allow an owner of an existing domain name to prove their ownership (but it requires that they have DNS already set up!). There are other ways to establish proof such as providing a DOI-generated TXT record, or web site contents, as championed by entities like Google's Sitemaster and Postmaster protocols. [DOMAIN-VALIDATION] describes a few ways ownership or control of a domain can be achieved.

5. Architecture Description

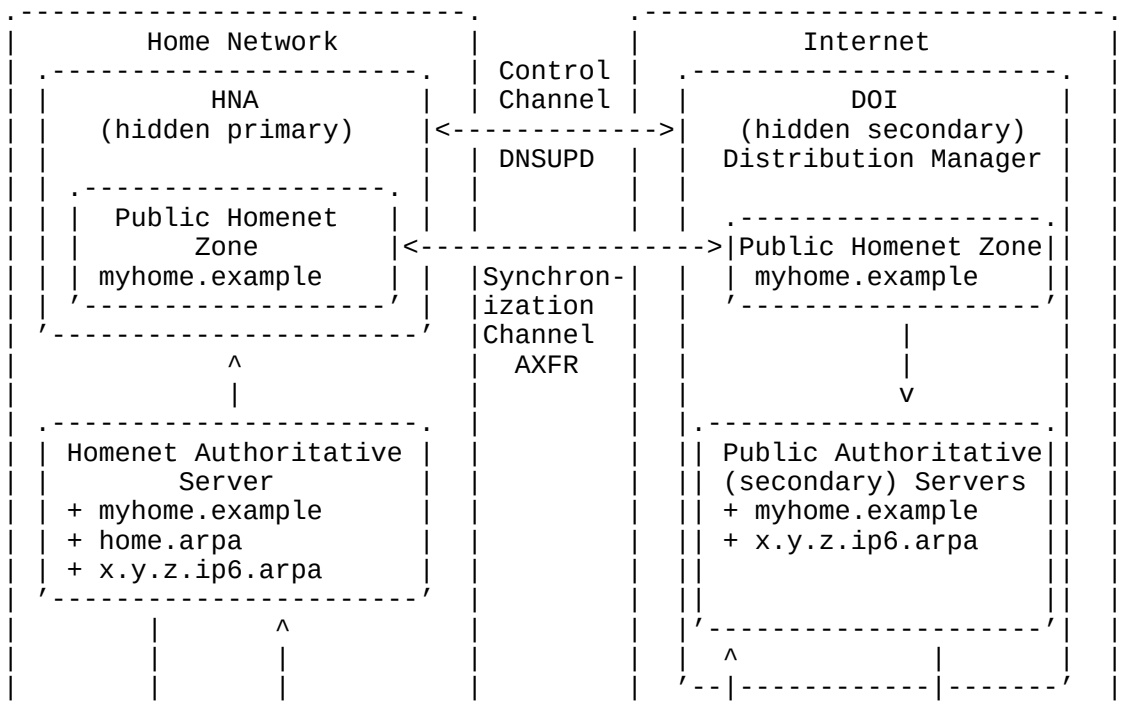
This section provides an overview of the architecture for outsourcing the authoritative naming service from the HNA to the DOI. As a consequence, this prevents HNA from handling the DNS traffic from the Internet that is associated with the resolution of the Homenet Zone.

The device-assigned zone or user-configurable zone that is used as the domain to publicly serve hostnames in the home network is called the Public Homenet Zone. In this document, "myhome.example" is used as the example for an end-user-owned domain configured as a Public Homenet Zone.

More specifically, DNS resolution for the Public Homenet Zone (here "myhome.example") from Internet DNSSEC resolvers is handled by the DOI as opposed to the HNA. The DOI benefits from a cloud infrastructure while the HNA is dimensioned for a home network and, as such, is likely unable to support any load. In the case where the HNA is a CPE, outsourcing to the DOI reduces the attack surface of the home network to DDoS, for example. Of course, the DOI needs to be informed dynamically about the content of myhome.example. The description of such a synchronization mechanism is the purpose of this document.

Note that Appendix B shows the necessary parameters to configure the HNA.

5.1. Architecture Overview



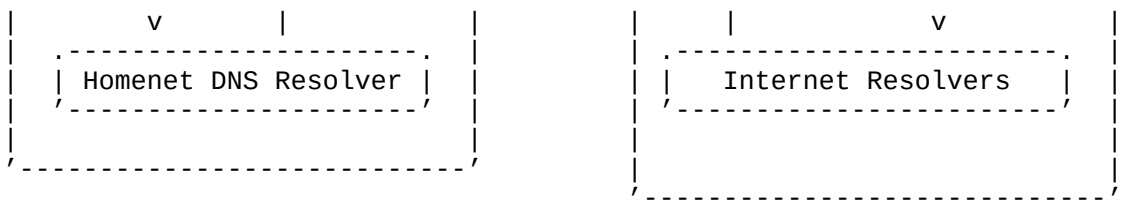


Figure 2: Homenet Naming Architecture

Figure 2 illustrates the architecture where the HNA outsources the publication of the Public Homenet Zone to the DOI. The DOI will serve every DNS request of the Public Homenet Zone coming from outside the home network. When the request is coming from within the home network, the resolution is expected to be handled by the Homenet DNS Resolver as further detailed below.

In this example, the Public Homenet Zone is identified by the Registered Homenet Domain name "myhome.example". This diagram also shows a reverse IPv6 map being hosted.

".local" and ".home.arpa" are explicitly not considered Public Homenet Zones; therefore, they are represented as a Homenet Zone in Figure 2. They are resolved locally but are not published because they are considered local content.

It is RECOMMENDED that the HNA implements DNSSEC, in which case the HNA MUST sign the Public Homenet Zone with DNSSEC.

The HNA handles all operations and keying material required for DNSSEC, so there is no provision made in this architecture for transferring private DNSSEC-related keying material between the HNA and the DM.

Once the Public Homenet Zone has been built, the HNA communicates and synchronizes it with the DOI using a primary/secondary setting as depicted in Figure 2. The HNA acts as a stealth server (see [RFC8499]) while the DM behaves as a hidden secondary. It is responsible for distributing the Public Homenet Zone to the multiple Public Authoritative Server instances that DOI is responsible for. The DM has three communication channels:

* DM Control Channel (Section 6) to configure the HNA and the DOI. This includes necessary parameters to configure the primary/secondary relation as well as some information provided by the DOI that needs to be included by the HNA in the Public Homenet Zone.

* DM Synchronization Channel (Section 7) to synchronize the Public Homenet Zone on the HNA and on the DM with the appropriately configured primary/secondary. This is a zone transfer over mutually authenticated TLS.

* One or more Distribution Channels (Section 8) that distribute the Public Homenet Zone from the DM to the Public Authoritative Servers serving the Public Homenet Zone on the Internet.

There might be multiple DMs and multiple servers per the DM. This document assumes a single DM server for simplicity, but there is no reason why each channel needs to be implemented on the same server or use the same code base.

It is important to note that while the HNA is configured as an authoritative server, it is not expected to answer DNS requests from the _public_ Internet for the Public Homenet Zone. More specifically, the addresses associated with the HNA SHOULD NOT be mentioned in the NS records of the Public Homenet Zone, unless

additional security provisions necessary to protect the HNA from external attack have been taken.

The DOI is also responsible for ensuring the DS record has been updated in the parent zone.

Resolution is performed by DNS Resolvers. When the resolution is performed outside the home network, the DNS Resolver resolves the DS record on the Global DNS and the name associated with the Public Homenet Zone (myhome.example) on the Public Authoritative Servers.

In order to provide resilience to the Public Homenet Zone in case of WAN connectivity disruption, the Homenet DNS Resolver MUST be able to perform the resolution on the Homenet Authoritative Servers. Note that the use of the Homenet DNS Resolver enhances privacy since the user on the home network would no longer be leaking interactions with internal services to an external DNS provider and to an on-path observer. These servers are not expected to be mentioned in the Public Homenet Zone nor to be accessible from the Internet. As such, their information as well as the corresponding signed DS record MAY be provided by the HNA to the Homenet DNS Resolvers, e.g., by using the Home Networking Control Protocol (HNCP) [RFC7788] or by configuring a trust anchor [DRO-RECS]. Such configuration is outside the scope of this document. Since the scope of the Homenet Authoritative Servers is limited to the home network, these servers are expected to serve the Homenet Zone as represented in Figure 2.

5.2. Distribution Manager (DM) Communication Channels

This section details the DM channels: the Control Channel, Synchronization Channel, and Distribution Channel.

The Control Channel and the Synchronization Channel are the interfaces used between the HNA and the DOI. The entity within the DOI responsible for handling these communications is the DM. Communications between the HNA and the DM MUST be protected and mutually authenticated. The different protocols that can be used for security are discussed in more depth in Section 6.6.

The information exchanged between the HNA and the DM uses DNS messages protected by DNS over TLS (DoT) [RFC7858]. This is configured identically to that described in [RFC9103], Section 9.3.3.

It is worth noting that both the DM and HNA need to agree on a common configuration in order to set up the Synchronization Channel and build and serve a coherent Public Homenet Zone. As previously noted, the visible NS records of the Public Homenet Zone (built by the HNA) remain pointing at the IP address of the DOI's Public Authoritative Servers. Unless the HNA is able to support the traffic load, the HNA SHOULD NOT appear as a visible NS record of the Public Homenet Zone. In addition, and depending on the configuration of the DOI, the DM also needs to update the parent zone's NS, DS, and associated A or AAAA glue records. Refer to Section 6.2 for more details.

This specification assumes:

* The DM serves both the Control Channel and Synchronization Channel on a single IP address, on a single port, and by using a single transport protocol.

* By default, the HNA uses a single IP address for both the Control and Synchronization channels; however, the HNA MAY use distinct IP addresses for the Control Channel and the Synchronization Channel -- see Sections 7 and 6.3 for more details.

The Distribution Channel is internal to the DOI and, as such, is not

normatively defined by this specification.

6. Control Channel

The DM Control Channel is used by the HNA and the DOI to exchange information related to the configuration of the delegation, which includes information to build the Public Homenet Zone (Section 6.1), to build the DNSSEC chain of trust (Section 6.2), and to set the Synchronization Channel (Section 6.3).

Some information is carried from the DOI to the HNA, as described in the next section. The HNA updates the DOI with the IP address on which the zone is to be transferred using the Synchronization Channel. The HNA is always initiating the exchange in both directions.

As such, the HNA has a prior knowledge of the DM identity (via an X.509 certificate), the IP address and port number to use, and the protocol to establish a secure session. The DM acquires knowledge of the identity of the HNA (X.509 certificate) as well as the Registered Homenet Domain. For more detail on how this can be achieved, please see Appendix A.1.

6.1. Building the Public Homenet Zone

The HNA builds the Public Homenet Zone based on a template that is returned by the DM to the HNA. Section 6.5 explains how this leverages the Authoritative Transfer (AXFR) mechanism.

In order to build its zone completely, the HNA needs the names (and possibly IP addresses) of the Public Authoritative Name Servers. These are used to populate the NS records for the zone. All the content of the zone MUST be created by the HNA because the zone is DNSSEC signed.

In addition, the HNA needs to know what to put into the MNAME of the SOA, and only the DOI knows what to put there. The DM MUST also provide useful operational parameters such as other fields of the SOA (SERIAL, RNAME, REFRESH, RETRY, EXPIRE, and MINIMUM); however, the HNA is free to override these values based upon local configuration. For instance, an HNA might want to change these values if it thinks that a renumbering event is approaching.

Because the information associated with the DM is necessary for the HNA to proceed, this information exchange is mandatory.

The HNA then performs a DNS Update operation to the DOI, updating the DOI with an NS, a DS, and A and AAAA records. These indicate where its Synchronization Channel is. The DOI does not publish this NS record but uses it to perform zone transfers.

6.2. Building the DNSSEC Chain of Trust

The HNA MUST provide the hash of the KSK via the DS RRset so that the DOI can provide this value to the parent zone. A common deployment use case is that the DOI is the registrar of the Registered Homenet Domain; therefore, its relationship with the registry of the parent zone enables it to update the parent zone. When such relation exists, the HNA should be able to request the DOI to update the DS RRset in the parent zone. A direct update is especially necessary to initialize the chain of trust.

Though the HNA may also directly update the values of the DS via the Control Channel at a later time, it is RECOMMENDED to use other mechanisms such as CDS and CDNSKEY [RFC7344] for transparent updates during key rollovers.

As some deployments may not provide a DOI that will be able to update the DS in the parent zone, this information exchange is OPTIONAL.

By accepting the DS RR, the DM commits to advertise the DS to the parent zone. On the other hand, if the DM does not have the capacity to advertise the DS to the parent zone, it indicates this by refusing the update to the DS RR.

6.3. Setting Up the Synchronization Channel

The HNA works as a hidden primary authoritative DNS server while the DM works like a secondary one. As a result, the HNA needs to provide the IP address that the DM should use to reach the HNA.

If the HNA detects that it has been renumbered, then it MUST use the Control Channel to update the DOI with the new IPv6 address it has been assigned.

The Synchronization Channel will be set between the new IPv6 (and IPv4) address and the IP address of the DM. By default, the IP address used by the HNA in the Control Channel is considered by the DM, and the explicit specification of the IP by the HNA is only OPTIONAL. The transport channel (including the port number) is the same as the one used between the HNA and the DM for the Control Channel.

6.4. Deleting the Delegation

The purpose of the previous sections is to exchange information in order to set a delegation. The HNA MUST also be able to delete a delegation with a specific DM.

Section 6.5.4 explains how a DNS Update operation on the Control Channel is used.

Upon receiving the instruction to delete the delegation, the DM MUST stop serving the Public Homenet Zone.

The decision to delete an inactive HNA by the DM is part of the commercial agreement between the DOI and HNA.

6.5. Message Exchange Description

Multiple ways were considered on how the control information could be exchanged between the HNA and the DM.

This specification defines a mechanism that reuses the DNS zone transfer format. Note that while information is provided using DNS exchanges, the exchanged information is not expected to be set in any zone file; instead, this information is used as commands between the HNA and the DM. This was found to be simpler on the home router side, as the HNA already has to have code to deal with all the DNS encodings/decodings. Inventing a new way to encode the DNS information in, for instance, JSON seemed to add complexity for no return on investment.

The Control Channel is not expected to be a long-term session. After a predefined timer (similar to those used for TCP), the Control Channel is expected to be terminated by closing the transport channel. The Control Channel MAY be reopened at any later time.

The use of TLS session tickets (see [RFC8446], Section 4.6.1) is RECOMMENDED.

The authentication of the channel MUST be based on certificates for

both the DM and each HNA. The DM may also create the initial configuration for the delegation zone in the parent zone during the provisioning process.

6.5.1. Retrieving Information for the Public Homenet Zone

The information provided by the DM to the HNA is retrieved by the HNA with an AXFR exchange [RFC1034]. AXFR enables the response to contain any type of RRsets.

To retrieve the necessary information to build the Public Homenet Zone, the HNA MUST send a DNS request of type AXFR associated with the Registered Homenet Domain.

The zone that is returned by the DM is used by the HNA as a template to build its own zone.

The zone template MUST contain an RRset of type SOA, one or multiple RRsets of type NS, and zero or more RRsets of type A or AAAA (if the NS is in-domain [RFC8499]). The zone template will include Time-To-Live (TTL) values for each RR, and the HNA SHOULD take these as suggested maximum values, but it MAY use lower values for operational reasons, such as for impending renumbering events.

* The SOA RR indicates the value of the MNAME of the Public Homenet Zone to the HNA.

* The NAME of the SOA RR MUST be the Registered Homenet Domain.

* The MNAME value of the SOA RDATA is the value provided by the DOI to the HNA.

* Other RDATA values (RNAME, REFRESH, RETRY, EXPIRE, and MINIMUM) are provided by the DOI as suggestions.

The NS RRsets carry the Public Authoritative Servers of the DOI. Their associated NAME MUST be the Registered Homenet Domain.

In addition to the considerations above about default TTL, the HNA SHOULD take care to not pick a TTL larger than the parent NS, based upon the resolver’s guidelines in [NS-REVALIDATION] and [DRO-RECS]. The RRsets of Type A and AAAA MUST have their NAME matching the NSDNAME of one of the NS RRsets.

Upon receiving the response, the HNA MUST validate the format and properties of the SOA, NS, and A or AAAA RRsets. If an error occurs, the HNA MUST stop proceeding and MUST log an error. Otherwise, the HNA builds the Public Homenet Zone by setting the MNAME value of the SOA as indicated by the SOA provided by the AXFR response. The HNA MUST NOT exceed the values of NAME, REFRESH, RETRY, EXPIRE, and MINIMUM of the SOA provided by the AXFR response. The HNA MUST insert the NS and corresponding A or AAAA RRsets in its Public Homenet Zone. The HNA MUST ignore other RRsets.

If an error message is returned by the DM, the HNA MUST proceed as a regular DNS resolution. Error messages SHOULD be logged for further analysis. If the resolution does not succeed, the outsourcing operation is aborted and the HNA MUST close the Control Channel.

6.5.2. Providing Information for the DNSSEC Chain of Trust

To provide the DS RRset to initialize the DNSSEC chain of trust, the HNA MAY send a DNS update [RFC3007] message.

The DNS update message is composed of a Header section, a Zone section, a Prerequisite section, an Update section, and an additional

section. The Zone section MUST set the ZNAME to the parent zone of the Registered Homenet Domain, which is where the DS records should be inserted. As described in [RFC2136], ZTYPE is set to SOA and ZCLASS is set to the zone's class. The Prerequisite section MUST be empty. The Update section is a DS RRset with its NAME set to the Registered Homenet Domain, and the associated RDATA corresponds to the value of the DS. The Additional Data section MUST be empty.

Though the Prerequisite section MAY be ignored by the DM, this value is fixed to remain coherent with a standard DNS update.

Upon receiving the DNS update request, the DM reads the DS RRset in the Update section. The DM checks that ZNAME corresponds to the parent zone. The DM MUST ignore the Prerequisite and Additional Data sections, if present. The DM MAY update the TTL value before updating the DS RRset in the parent zone. Upon a successful update, the DM should return a NOERROR response as a commitment to update the parent zone with the provided DS. An error indicates that the DM does not update the DS, and the HNA needs to act accordingly; otherwise, another method should be used by the HNA.

The regular DNS error message MUST be returned to the HNA when an error occurs. In particular, a FORMERR is returned when a format error is found, including when unexpected RRsets are added or when RRsets are missing. A SERVFAIL error is returned when an internal error is encountered. A NOTZONE error is returned when the Update and Zone sections are not coherent, and a NOTAUTH error is returned when the DM is not authoritative for the Zone section. A REFUSED error is returned when the DM refuses the configuration or performing the requested action.

6.5.3. Providing Information for the Synchronization Channel

The default IP address used by the HNA for the Synchronization Channel is the IP address of the Control Channel. To provide a different IP address, the HNA MAY send a DNS UPDATE message.

Similar to what is described in Section 6.5.2, the HNA MAY specify the IP address using a DNS update message. The Zone section sets its ZNAME to the parent zone of the Registered Homenet Domain, ZTYPE to SOA, and ZCLASS to the zone's type. Prerequisite is empty. The Update section is an RRset of type NS. The Additional Data section contains the RRsets of type A or AAAA that designate the IP addresses associated with the primary (or the HNA).

The reason to provide these IP addresses is to keep them unpublished and prevent them from being resolved. It is RECOMMENDED that the IP address of the HNA be randomly chosen to prevent it from being easily discovered as well.

Upon receiving the DNS update request, the DM reads the IP addresses and checks that the ZNAME corresponds to the parent zone. The DM MUST ignore a non-empty Prerequisite section. The DM configures the secondary with the IP addresses and returns a NOERROR response to indicate it is committed to serve as a secondary.

Similar to what is described in Section 6.5.2, DNS errors are used, and an error indicates the DM is not configured as a secondary.

6.5.4. Initiating Deletion of the Delegation

To initiate the deletion of the delegation, the HNA sends a DNS UPDATE Delete message.

The Zone section sets its ZNAME to the Registered Homenet Domain, the ZTYPE to SOA, and the ZCLASS to the zone's type. The Prerequisite

section is empty. The Update section is an RRset of type NS with the NAME set to the Registered Domain Name. As indicated by [RFC2136], Section 2.5.2, the delete instruction is initiated by setting TTL to 0, CLASS to ANY, and RDLENGTH to 0, and RDATA MUST be empty. The Additional Data section is empty.

Upon receiving the DNS update request, the DM checks the request and removes the delegation. The DM returns a NOERROR response to indicate the delegation has been deleted. Similar to what is described in Section 6.5.2, DNS errors are used, and an error indicates that the delegation has not been deleted.

6.6. Securing the Control Channel

TLS [RFC8446] MUST be used to secure the transactions between the DM and the HNA, and the DM and HNA MUST be mutually authenticated. The DNS exchanges are performed using DNS over TLS [RFC7858].

The HNA may be provisioned by the manufacturer or during some user-initiated onboarding process, for example, with a browser, by signing up to a service provider, and with a resulting OAuth 2.0 token to be provided to the HNA. Such a process may result in a passing of a settings from a registrar into the HNA through an http API interface. (This is not in scope for this document.)

When the HNA connects to the DM's Control Channel, TLS will be used, and the connection will be mutually authenticated. The DM will authenticate the HNA's certificate based upon having participated in some provisioning process that is not standardized by this document. The results of the provisioning process is a series of settings described in Appendix A.1.

The HNA will validate the DM's Control Channel certificate by performing a DNS-ID check on the name as described in [RFC9525].

In the future, other specifications may consider protecting DNS messages with other transport layers such as DNS over DTLS [RFC8094], DNS over HTTPS (DoH) [RFC8484], or DNS over QUIC [RFC9250].

7. Synchronization Channel

The DM Synchronization Channel is used for communication between the HNA and the DM for synchronizing the Public Homenet Zone. Note that the Control Channel and the Synchronization Channel are different channels by construction even though they may use the same IP address. Suppose the HNA and the DM are using a single IP address designated by XX, and YYYYY and ZZZZZ are the various ports involved in the communications.

The Control Channel is between

* the HNA working as a client using port number YYYYY (an ephemeral also commonly designated as a high range port) and

* a service provided by the DM at port 853, when using DoT.

On the other hand, the Synchronization Channel is between

* the DM working as a client using port ZZZZZ (another ephemeral port) and

* a service provided by the HNA at port 853.

As a result, even though the same pair of IP addresses may be involved, the Control Channel and the Synchronization Channel are always distinct channels.

Uploading and dynamically updating the zone file on the DM can be seen as zone provisioning between the HNA (hidden primary server) and the DM (secondary server). This is handled using the normal zone transfer mechanism involving the AXFR and Incremental Zone Transfer (IXFR).

Part of the process to update the zone involves the owner of the zone (the hidden primary server, the HNA) sending a DNS Notify to the secondaries. In this situation, the only destination that is known by the HNA is the DM's Control Channel, so DNS Notifies are sent over the Control Channel, secured by a mutually authenticated TLS.

Please note that DNS Notifies are not critical to normal operation, as the DM will be checking the zone regularly based upon SOA record comments. DNS Notifies do speed things up as they cause the DM to use the Synchronization Channel to immediately do an SOA query to detect any updates. If there are any changes, then the DM immediately transfers the zone updates.

This specification standardizes the use of a primary/secondary mechanism [RFC1996] rather than an extended series of DNS update messages. The primary/secondary mechanism was selected as it scales better and avoids DoS attacks. Because this AXFR runs over a TCP channel secured by a mutually authenticated TLS, the DNS update is more complicated.

Note that this document provides no standard way to distribute a DNS primary between multiple devices. As a result, if multiple devices are candidates for hosting the hidden primary server, some specific mechanisms should be designed so the home network only selects a single HNA for the hidden primary server. Selection mechanisms based on HNCP [RFC7788] are good candidates for future work.

7.1. Securing the Synchronization Channel

The Synchronization Channel uses mutually authenticated TLS, as described by [RFC9103].

There is a TLS client certificate used by the DM to authenticate itself. The DM uses the same certificate that was configured into the HNA for authenticating the Control Channel, but as a client certificate rather than a server certificate.

[RFC9103] makes no requirements or recommendations on any extended key usage flags for zone transfers, and this document adopts the view that none should be required. Note that once an update to [RFC9103] is published, this document's normative reference to [RFC9103] will be considered updated as well.

For the TLS server certificate, the HNA uses the same certificate that it uses to authenticate itself to the DM for the Control Channel.

The HNA MAY use this certificate as the authorization for the zone transfer, or the HNA MAY have been configured with an Access Control List (ACL) that will determine if the zone transfer can proceed. This is a local configuration option as it is premature to determine which will be operationally simpler.

When the HNA expects to do zone transfer authorization by certificate only, the HNA MAY still apply an ACL on inbound connection requests to avoid load. In this case, the HNA MUST regularly check (via a DNS resolution) the validity of the address(es) of the DM in the filter.

8. DM Distribution Channel

The DM Distribution Channel is used for communication between the DM and the Public Authoritative Servers. The architecture and communication used for the DM Distribution Channels are outside the scope of this document, but there are many existing solutions available, e.g., rsync, DNS AXFR, REST, and DB copy.

9. HNA Security Policies

The HNA, as the hidden primary server, processes only limited message exchanges on its Internet-facing interface. This should be enforced using security policies to allow only a subset of DNS requests to be received by HNA.

The hidden primary server on the HNA differs from the regular authoritative server for the home network due to the following:

Interface Binding: The hidden primary server will almost certainly listen on the WAN Interface, whereas a regular Homenet Authoritative Server will listen on the internal home network interface.

Limited Exchanges: The purpose of the hidden primary server is to synchronize with the DM, not to serve any zones to end users or the public Internet. This results in a limited number of possible exchanges (AXFR/IXFR) with a small number of IP addresses, and an implementation MUST enable filtering policies: it should only respond to queries that are required to do zone transfers. That list includes SOA queries and AXFR/IXFR queries.

10. Public Homenet Reverse Zone

The Public Homenet Reverse Zone works similarly to the Public Homenet Zone. The main difference is that the ISP that provides the IPv6 connectivity is likely to also be the owner of the corresponding IPv6 reverse zone who administrates the Reverse Public Authoritative Servers. The configuration and the setting of the Synchronization Channel and Control Channel can largely be automated using DHCPv6 messages that are a part of the IPv6 prefix delegation process.

The Public Homenet Zone is associated with a Registered Homenet Domain, and the ownership of that domain requires a specific registration from the end user as well as the HNA being provisioned with some authentication credentials. Such steps are mandatory unless the DOI has some other means to authenticate the HNA. Such situation may occur, for example, when the ISP provides the Homenet Domain as well as the DOI.

In this case, the HNA may be authenticated by the physical link layer, in which case the authentication of the HNA may be performed without additional provisioning of the HNA. While this may not be so common for the Public Homenet Zone, this situation is expected to be quite common for the Reverse Homenet Zone as the ISP owns the IP address or IP prefix.

More specifically, a common case is that the upstream ISP provides the IPv6 prefix to the Homenet with an identity association for a prefix delegation (IA_PD) option [RFC8415] and manages the DOI of the associated reverse zone.

This leaves a place for setting up the relation between the HNA and DOI automatically as described in [RFC9527].

In the case of the reverse zone, the DOI authenticates the source of the updates by IPv6 ACLs, and the ISP knows exactly what addresses have been delegated. Therefore, the HNA SHOULD always originate

Synchronization Channel updates from an IP address within the zone that is being updated. Exceptionally, the Synchronization Channel might be from a different zone delegated to the HNA (if there were multiple zones or renumbering events were in progress).

For example, if the ISP has assigned 2001:db8:f00d:1234::/64 to the WAN interface (by DHCPv6 or PPP with Router Advertisement (RA)), then the HNA should originate Synchronization Channel updates from, for example, 2001:db8:f00d:1234::2.

If an ISP has delegated 2001:db8:aeae::/56 to the HNA via DHCPv6-PD, then the HNA should originate Synchronization Channel updates to an IP address within that subnet, such as 2001:db8:aeae:1::2.

With this relation automatically configured, the synchronization between the Home network and the DOI happens in a similar way to the synchronization of the Public Homenet Zone described earlier in this document.

Note that for home networks connected to multiple ISPs, each ISP provides only the DOI of the reverse zones associated with the delegated prefix. It is also likely that the DNS exchanges will need to be performed on dedicated interfaces to be accepted by the ISP. More specifically, the reverse zone update associated with prefix 1 cannot be performed by the HNA using an IP address that belongs to prefix 2. Such constraints do not raise major concerns for hot standby or load-sharing configuration.

With IPv6, the reverse domain space for IP addresses associated with a subnet such as ::/64 is so large that the reverse zone may be confronted with scalability issues. How the reverse zone is generated is out of scope of this document. [RFC8501] provides guidance on how to address scalability issues.

11. DNSSEC-Compliant Homenet Architecture

Section 3.7.3 of [RFC7368] recommends that DNSSEC be deployed on both the authoritative server and the resolver.

The resolver side is out of scope of this document, and only the authoritative part of the server is considered. Other documents such as [RFC5011] deal with the continuous update of trust anchors required for operation of a DNSSEC Resolver.

The Public Homenet Zone and the Public Reverse Zone MUST be DNSSEC signed by the HNA.

Secure delegation is achieved only if the DS RRset is properly set in the parent zone. Secure delegation can be performed by the HNA or the DOIs, and the choice highly depends on which entity is authorized to perform such updates. Typically, the DS RRset is updated manually through a registrar interface and can be maintained with mechanisms such as CDS [RFC7344].

When the operator of the DOI is also the registrar for the domain, then it is a trivial matter for the DOI to initialize the relevant DS records in the parent zone. In other cases, some other initialization will be required, and that will be specific to the infrastructure involved. It is beyond the scope of this document.

There may be some situations where the HNA is unable to arrange for secure delegation of the zones, but the HNA MUST still sign the zones.

12. Renumbering

During a renumbering of the home network, the HNA IP address may be changed and the Public Homenet Zone will be updated by the HNA with new AAAA records.

The HNA will then advertise to the DM via a NOTIFY on the Control Channel. The DM will need to note the new originating IP for the connection, and it will need to update its internal database of Synchronization Channels. A new zone transfer will occur with the new records for the resources that the HNA wishes to publish.

The remainder of the section provides recommendations regarding the provisioning of the Public Homenet Zone, especially the IP addresses.

Renumbering has been extensively described in [RFC4192] and analyzed in [RFC7010], and the reader is expected to be familiar with them before reading this section. In the make-before-break renumbering scenario, the new prefix is advertised, and the network is configured to prepare the transition to the new prefix. During a period of time, the two prefixes (old and new) coexist before the old prefix is completely removed. New resource records containing the new prefix SHOULD be published, while the old resource records with the old prefixes SHOULD be withdrawn. If the HNA anticipates that the period of overlap will be long (perhaps due to the knowledge of router and DHCPv6 lifetimes), it MAY publish the old prefixes with a significantly lower TTL.

In break-before-make renumbering scenarios, including flash renumbering scenarios [RFC8978], the old prefix becomes unusable before the new prefix is known or advertised. As explained in [RFC8978], some flash renumberings occur due to power cycling of the HNA, where ISPs do not properly remember what prefixes have been assigned to which user.

An HNA that boots up MUST immediately use the Control Channel to update the location for the Synchronization Channel. This is a reasonable thing to do on every boot, as the HNA has no idea how long it has been offline or if the (DNSSEC) zone has perhaps expired during the time the HNA was powered off.

The HNA will have a list of names that should be published, but it might not yet have IP addresses for those devices. This could be because at the time of power on, the other devices were not yet online. If the HNA is sure that the prefix has not changed, then it should use the previously known addresses, with a very low TTL.

Although the new and old IP addresses may be stored in the Public Homenet Zone, it is RECOMMENDED that only the newly reachable IP addresses be published.

Regarding the Public Homenet Reverse Zone, the new Public Homenet Reverse Zone has to be populated as soon as possible, and the old Public Homenet Reverse Zone will be deleted by the owner of the zone (and the owner of the old prefix, which is usually the ISP) once the prefix is no longer assigned to the HNA. The ISP MUST ensure that the DNS cache has expired before reassigning the prefix to a new home network. This may be enforced by controlling the TTL values.

To avoid reachability disruption, IP connectivity information provided by the DNS MUST be coherent with the IP in use. In our case, this means the old IP address MUST NOT be provided via the DNS when it is not reachable anymore.

In the make-before-break scenario, it is possible to make the transition seamless. Let T be the TTL associated with an RRset of the Public Homenet Zone; Time_NEW be the time the new IP address replaces the old IP address in the Homenet Zone; and

Time_OLD_UNREACHABLE be the time the old IP will not be reachable anymore.

In the case of the make-before-break scenario, seamless reachability is provided as long as Time_OLD_UNREACHABLE - T_NEW > (2 * T). If this is not satisfied, then devices associated with the old IP address in the home network may become unreachable for 2 * T - (Time_OLD_UNREACHABLE - Time_NEW).

In the case of a break-before-make scenario, Time_OLD_UNREACHABLE = Time_NEW, and the device may become unreachable up to 2 * T. Of course, if Time_NEW >= Time_OLD_UNREACHABLE, then the outage is not seamless.

13. Privacy Considerations

Outsourcing the DNS Authoritative service from the HNA to a third party raises a few privacy-related concerns.

The Public Homenet Zone lists the names of services hosted in the home network. Combined with blocking of AXFR queries, the use of NSEC3 [RFC5155] (vs. NSEC [RFC4034]) prevents an attacker from being able to walk the zone to discover all the names. However, recent work [GPUNSEC3] [ZONEENUM] has shown that the protection provided by NSEC3 against dictionary attacks should be considered cautiously, and [RFC9276] provides guidelines to configure NSEC3 properly. In addition, the attacker may be able to walk the reverse DNS zone or use other reconnaissance techniques to learn this information as described in [RFC7707].

The zone may be also exposed during the synchronization between the primary and the secondary. The casual risk of this occurring is low, and the use of [RFC9103] significantly reduces this. Even if DNS zone transfer over TLS [RFC9103] is used by the DOI, it may still leak the existence of the zone through Notifies. The protocol described in this document does not increase that risk, as all Notifies use the encrypted Control Channel.

In general, a home network owner is expected to publish only names for which there is some need to reference them externally. Publication of the name does not imply that the service is necessarily reachable from any or all parts of the Internet. [RFC7084] mandates that the outgoing-only policy [RFC6092] be available, and in many cases, it is configured by default. A well-designed user interface would combine a policy for making a service public by a name with a policy on who may access it.

In many cases, and for privacy reasons, the home network owner has wanted to publish names only for services that they will be able to access. The access control may consist of an IP source address range, or access may be restricted via some VPN functionality. The main advantages of publishing the names are that the service may be accessed by the same name both within and outside the home, and the DNS resolution can be handled similarly both within and outside the home. This considerably eases the ability to use VPNs where the VPN can be chosen according to the IP address of the service. Typically, a user may configure its device to reach its Homenet devices via a VPN while the remaining traffic is accessed directly.

Enterprise networks have generally adopted another strategy designated as split-horizon-DNS. While such strategy might appear as providing more privacy at first sight, its implementation remains challenging and the privacy advantages need to be considered carefully. In split-horizon-DNS, names are designated with internal names that can only be resolved within the corporate network. When such strategy is applied to the homenet, VPNs need to be configured

with naming resolution policies and routing policies. Such an approach might be reasonable with a single VPN, but maintaining a coherent DNS space and IP space among various VPNs comes with serious complexities. Firstly, if multiple homenets are using the same domain name -- like home.arpa -- it becomes difficult to determine on which network the resolution should be performed. As a result, homenets should at least be differentiated by a domain name. Secondly, the use of split-horizon-DNS requires each VPN to be associated with a resolver and specific resolutions to be performed by the dedicated resolver. Such policies can easily raise some conflicts (with significant privacy issues) while remaining hard to be implemented.

In addition to the Public Homenet Zone, pervasive DNS monitoring can also monitor the traffic associated with the Public Homenet Zone. This traffic may provide an indication of the services an end user accesses, plus how and when they use these services. Although, caching may obfuscate this information inside the home network, it is likely that this information will not be cached outside the home network.

14. Security Considerations

The HNA never answers DNS requests from the Internet. These requests are instead served by the DOI.

While this limits the level of exposure of the HNA, the HNA still has some exposure to attacks from the Internet. This section analyses the attack surface associated with these communications, the data published by the DOI, as well as operational considerations.

14.1. Registered Homenet Domain

The DOI MUST NOT serve any Public Homenet Zone when it is not confident that the HNA owns the Registered Homenet Domain. Proof of ownership is outside the scope of this document, and it is assumed that such a phase has preceded the outsourcing of the zone.

14.2. HNA DM Channels

The channels between HNA and DM are mutually authenticated and encrypted with TLS [RFC8446], and its associated security considerations apply.

To ensure that the multiple TLS sessions are continuously authenticating the same entity, TLS may take advantage of second-factor authentication as described in [RFC8672] for the TLS server certificate for the Control Channel. The HNA should also cache the TLS server certificate used by the DM, in order to authenticate the DM during the setup of the Synchronization Channel. (Alternatively, the HNA is configured with an ACL from which Synchronization Channel connections will originate.)

The Control Channel and Synchronization Channel follow the guidelines in [RFC7858] and [RFC9103], respectively.

The DNS protocol is subject to reflection attacks; however, these attacks are largely applicable when DNS is carried over UDP. The interfaces between the HNA and DM are using TLS over TCP, which prevents such reflection attacks. Note that Public Authoritative servers hosted by the DOI are subject to such attacks, but that is out of scope of this document.

Note that in the case of the Reverse Homenet Zone, the data is less subject to attacks than in the Public Homenet Zone. In addition, the DM and Reverse Distribution Manager (RDM) may be provided by the ISP

-- as described in [RFC9527], in which case DM and RDM might be less exposed to attacks -- as communications within a network.

14.3. Names Are Less Secure than IP Addresses

This document describes how an end user can make their services and devices from their home network reachable on the Internet by using names rather than IP addresses. This exposes the home network to attackers because names are expected to include less entropy than IP addresses. IPv4 addresses are 4-bytes long leading to 2^32 possibilities. With IPv6 addresses, the Interface Identifier is 64-bits long leading to up to 2^64 possibilities for a given subnetwork. This is not to mention that the subnet prefix is also 64-bits long, thus providing up to 2^64 possibilities. On the other hand, names used for either the home network domain or the devices present less entropy (livebox, router, printer, nicolas, jennifer, ...) and thus potentially expose the devices to dictionary attacks.

14.4. 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 a time-invariant prefix by ISPs. In addition, IPv6 enables temporary addresses that makes them even more volatile [RFC8981]. As a result, observing IP addresses only 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 than logging IP addresses, especially to profile an 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, PTR DNS queries MAY be configured to return with NXDOMAIN instead.

14.5. Deployment Considerations

The HNA is expected to sign the DNSSEC zone and, as such, hold the private KSK and Zone Signing Key (ZSK).

In this case, there is no strong justification to use a separate KSK and ZSK. If an attacker can get access to one of them, it is likely that they will access both of them. If the HNA is run in a home router with a secure element (SE) or trusted platform module (TPM), storing the private keys in the secure element would be a useful precaution. The DNSSEC keys are generally needed on an hourly to weekly basis, but not more often.

While there is some risk that the DNSSEC keys might be disclosed by malicious parties, the bigger risk is that they will simply be lost if the home router is factory reset or just thrown out / replaced with a newer model.

Generating new DNSSEC keys is relatively easy; they can be deployed using the Control Channel to the DM. The key that is used to authenticate that connection is the critical key that needs protection and should ideally be backed up to offline storage (such as a USB key).

14.6. Operational Considerations

Homenet technologies make it easier to expose devices and services to the Internet. This imposes broader operational considerations for the operator and the Internet as follows:

* The home network operator must carefully assess whether a device

or service previously fielded only on a home network is robust enough to be exposed to the Internet.

* The home network operator will need to increase the diligence to regularly managing these exposed devices due to their increased risk posture of being exposed to the Internet.

* Depending on the operational practices of the home network operators, there is an increased risk to the Internet through the possible introduction of additional Internet-exposed systems that are poorly managed and likely to be compromised.

15. IANA Considerations

This document has no IANA actions.

16. References

16.1. 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>.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, DOI 10.17487/RFC1918, February 1996, <https://www.rfc-editor.org/info/rfc1918>.

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, DOI 10.17487/RFC1996, August 1996, <https://www.rfc-editor.org/info/rfc1996>.

[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>.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, DOI 10.17487/RFC3007, November 2000, <https://www.rfc-editor.org/info/rfc3007>.

[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>.

[RFC5155] Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, DOI 10.17487/RFC5155, March 2008, <https://www.rfc-editor.org/info/rfc5155>.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, DOI 10.17487/RFC7344, September 2014, <https://www.rfc-editor.org/info/rfc7344>.

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

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8375] Pfister, P. and T. Lemon, "Special-Use Domain 'home.arpa.'", RFC 8375, DOI 10.17487/RFC8375, May 2018, <https://www.rfc-editor.org/info/rfc8375>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8499] Hoffman, P., Sullivan, A., and K. Fujiwara, "DNS Terminology", BCP 219, RFC 8499, DOI 10.17487/RFC8499, January 2019, <https://www.rfc-editor.org/info/rfc8499>.

[RFC9103] Toorop, W., Dickinson, S., Sahib, S., Aras, P., and A. Mankin, "DNS Zone Transfer over TLS", RFC 9103, DOI 10.17487/RFC9103, August 2021, <https://www.rfc-editor.org/info/rfc9103>.

[RFC9525] Saint-Andre, P. and R. Salz, "Service Identity in TLS", RFC 9525, DOI 10.17487/RFC9525, November 2023, <https://www.rfc-editor.org/info/rfc9525>.

16.2. Informative References

[DOMAIN-VALIDATION] Sahib, S., Huque, S., Wouters, P., and E. Nygren, "Domain Control Validation using DNS", Work in Progress, Internet-Draft, draft-ietf-dnsop-domain-verification-techniques-03, 17 October 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-domain-verification-techniques-03>.

[DRO-RECS] Migault, D., Lewis, E., and D. York, "Recommendations for DNSSEC Resolvers Operators", Work in Progress, Internet-Draft, draft-ietf-dnsop-dnssec-validator-requirements-07, 13 November 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-dnssec-validator-requirements-07>.

[GPUNSEC3] Wander, M., Schwittmann, L., Boelmann, C., and T. Weis, "GPU-Based NSEC3 Hash Breaking", DOI 10.1109/NCA.2014.27, August 2014, <https://doi.org/10.1109/NCA.2014.27>.

[HOMEROUTER-PROVISION] Richardson, M., "Provisioning Initial Device Identifiers into Home Routers", Work in Progress, Internet-Draft, draft-richardson-homerouter-provisioning-02, 14 November 2021, <https://datatracker.ietf.org/doc/html/draft-richardson-homerouter-provisioning-02>.

[NS-REVALIDATION] Huque, S., Vixie, P., and R. Dolmans, "Delegation Revalidation by DNS Resolvers", Work in Progress, Internet-Draft, draft-ietf-dnsop-ns-revalidation-04, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-ns-revalidation-04>.

[REBIND] Wikipedia, "DNS rebinding", September 2023, <https://en.wikipedia.org/w/index.php?title=DNS_rebinding&oldid=1173433859>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, DOI 10.17487/RFC3587, August 2003, <https://www.rfc-editor.org/info/rfc3587>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <https://www.rfc-editor.org/info/rfc3927>.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, DOI 10.17487/RFC4192, September 2005, <https://www.rfc-editor.org/info/rfc4192>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, DOI 10.17487/RFC5011, September 2007, <https://www.rfc-editor.org/info/rfc5011>.

[RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011, <https://www.rfc-editor.org/info/rfc6092>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6887] Wing, D., Ed., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, DOI 10.17487/RFC6887, April 2013, <https://www.rfc-editor.org/info/rfc6887>.

[RFC7010] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W. George, "IPv6 Site Renumbering Gap Analysis", RFC 7010, DOI 10.17487/RFC7010, September 2013, <https://www.rfc-editor.org/info/rfc7010>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[RFC7368] Chown, T., Ed., Arkko, J., Brandt, A., Troan, O., and J. Weil, "IPv6 Home Networking Architecture Principles", RFC 7368, DOI 10.17487/RFC7368, October 2014, <https://www.rfc-editor.org/info/rfc7368>.

[RFC7404] Behringer, M. and E. Vyncke, "Using Only Link-Local Addressing inside an IPv6 Network", RFC 7404, DOI 10.17487/RFC7404, November 2014, <https://www.rfc-editor.org/info/rfc7404>.

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016, <https://www.rfc-editor.org/info/rfc7707>.

[RFC7788] Stenberg, M., Barth, S., and P. Pfister, "Home Networking Control Protocol", RFC 7788, DOI 10.17487/RFC7788, April 2016, <https://www.rfc-editor.org/info/rfc7788>.

[RFC8094] Reddy, T., Wing, D., and P. Patil, "DNS over Datagram Transport Layer Security (DTLS)", RFC 8094, DOI 10.17487/RFC8094, February 2017, <https://www.rfc-editor.org/info/rfc8094>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

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

[RFC8501] Howard, L., "Reverse DNS in IPv6 for Internet Service Providers", RFC 8501, DOI 10.17487/RFC8501, November 2018, <https://www.rfc-editor.org/info/rfc8501>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8672] Sheffer, Y. and D. Migault, "TLS Server Identity Pinning with Tickets", RFC 8672, DOI 10.17487/RFC8672, October 2019, <https://www.rfc-editor.org/info/rfc8672>.

[RFC8978] Gont, F., or, J., and R. Patterson, "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events", RFC 8978, DOI 10.17487/RFC8978, March 2021, <https://www.rfc-editor.org/info/rfc8978>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

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

[RFC9276] Hardaker, W. and V. Dukhovni, "Guidance for NSEC3 Parameter Settings", BCP 236, RFC 9276, DOI 10.17487/RFC9276, August 2022, <https://www.rfc-editor.org/info/rfc9276>.

[RFC9527] Migault, D., Weber, R., and T. Mrugalski, "DHCPv6 Options for the Homenet Naming Authority", RFC 9527, DOI 10.17487/RFC9527, January 2024, <https://www.rfc-editor.org/info/rfc9527>.

[ZONEENUM] Wang, Z., Xiao, L., and R. Wang, "An efficient DNSSEC zone enumeration algorithm", DOI 10.2495/MIIT130591, April

2014, <https://doi.org/10.2495/MIIT130591>.

Appendix A. HNA Channel Configurations

A.1. Public Homenet Zone

This document does not deal with how the HNA is provisioned with a trusted relationship to the Distribution Manager for the forward zone.

This section details what needs to be provisioned into the HNA and serves as a requirements statement for mechanisms.

The HNA needs to be provisioned with:

* the Registered Domain (e.g., myhome.example);

* the contact information for the DM, including the DNS name (the fully qualified domain name (FQDN)), possibly the IP literal, and a certificate (or anchor) to be used to authenticate the service;

* the DM transport protocol and port (the default is DNS over TLS, on port 853); and

* the HNA credentials used by the DM for its authentication.

The HNA will need to select an IP address for communication for the Synchronization Channel. This is typically the WAN address of the CPE, but it could be an IPv6 LAN address in the case of a home with multiple ISPs (and multiple border routers). This is detailed in Section 6.5.3 when the NS and A or AAAA RRsets are communicated.

The above parameters MUST be provisioned for ISP-specific reverse zones. One example of how to do this can be found in [RFC9527]. ISP-specific forward zones MAY also be provisioned using [RFC9527], but zones that are not related to a specific ISP zone (such as with a DNS provider) must be provisioned through other means.

Similarly, if the HNA is provided by a registrar, the HNA may be handed preconfigured to the end user.

In the absence of specific pre-established relations, these pieces of information may be entered manually by the end user. In order to ease the configuration from the end user, the following scheme may be implemented.

The HNA may present the end user with a web interface that provides the end user the ability to indicate the Registered Homenet Domain or the registrar with, for example, a preselected list. Once the registrar has been selected, the HNA redirects the end user to that registrar in order to receive an access token. The access token will enable the HNA to retrieve the DM parameters associated with the Registered Domain. These parameters will include the credentials used by the HNA to establish the Control and Synchronization Channels.

Such architecture limits the necessary steps to configure the HNA from the end user.

Appendix B. Information Model for Outsourced Information

This section specifies an optional format for the set of parameters required by the HNA to configure the naming architecture of this document.

In cases where a home router has not been provisioned by the

manufacturer (when forward zones are provided by the manufacturer) or by the ISP (when the ISP provides this service), then a home user/owner will need to configure these settings via an administrative interface.

By defining a standard format (in JSON) for this configuration information, the user/owner may be able to copy and paste a configuration blob from the service provider into the administrative interface of the HNA.

This format may also provide the basis for a future OAuth 2.0 [RFC6749] flow that could do the set up automatically.

The HNA needs to be configured with the following parameters as described by the Concise Data Definition Language (CDDL) [RFC8610]. These parameters are necessary to establish a secure channel between the HNA and the DM as well as to specify the DNS zone that is in the scope of the communication.

```
hna-configuration = {
  "registered_domain" : tstr,
  "dm"                : tstr,
  ? "dm_transport" : "DoT"
  ? "dm_port"        : uint,
  ? "dm_acl"         : hna-acl / [ +hna-acl ]
  ? "hna_auth_method": hna-auth-method
  ? "hna_certificate": tstr
}

hna-acl          = tstr
hna-auth-method  /= "certificate"
```

For example:

```
{
  "registered_domain" : "n8d234f.r.example.net",
  "dm"                : "2001:db8:1234:111:222::2",
  "dm_transport"      : "DoT",
  "dm_port"           : 4433,
  "dm_acl"            : "2001:db8:1f15:62e::/64"
                  or [ "2001:db8:1f15:62e::/64", ... ]
  "hna_auth_method"   : "certificate",
  "hna_certificate"   : "-----BEGIN CERTIFICATE-----\nMIIDTjCCFGy..",
}
```

Registered Homenet Domain (registered_domain): The Domain Name of the zone. Multiple Registered Homenet Domains may be provided. This will generate the creation of multiple Public Homenet Zones. This parameter is mandatory.

Distribution Manager notification address (dm): The associated FQDNs or IP addresses of the DM to which DNS Notifies should be sent. This parameter is mandatory. IP addresses are optional, and the FQDN is sufficient and preferred. If there are concerns about the security of the name to IP translation, then DNSSEC should be employed.

As the session between the HNA and the DM is authenticated with TLS, the use of names is easier.

As certificates are more commonly emitted for FQDN than for IP addresses, it is preferred to use names and authenticate the name of the DM during the TLS session establishment.

Supported Transport (dm_transport): The transport that carries the DNS exchanges between the HNA and the DM. The typical value is

"DoT", but it may be extended in the future with "DoH" or "DoQ", for example. This parameter is optional, and the HNA uses DoT by default.

Distribution Manager Port (dm_port): Indicates the port used by the DM. This parameter is optional, and the default value is provided by the Supported Transport. In the future, an additional transport may not have a default port, in which case either a default port needs to be defined or this parameter becomes mandatory.

Note that HNA does not define ports for the Synchronization Channel. In any case, this is not expected to be a part of the configuration but is instead negotiated through the Configuration Channel. Currently, the Configuration Channel does not provide this and limits its agility to a dedicated IP address. If such agility is needed in the future, additional exchanges will need to be defined.

Authentication Method ("hna_auth_method"): How the HNA authenticates itself to the DM within the TLS connection(s). The authentication method can typically be "certificate", "psk", or "none". This parameter is optional, and the Authentication Method is "certificate" by default.

Authentication data ("hna_certificate", "hna_key"): The certificate chain used to authenticate the HNA. This parameter is optional, and when not specified, a self-signed certificate is used.

Distribution Manager AXFR permission netmask (dm_acl): The subnet from which the CPE should accept SOA queries and AXFR requests. A subnet is used in the case where the DOI consists of a number of different systems. An array of addresses is permitted. This parameter is optional, and if unspecified, the CPE uses the IP addresses provided by the dm parameter either directly when the dm indicates the IP address(es) returned by the DNS or DNSSEC resolution when dm indicates an FQDN.

For forward zones, the relationship between the HNA and the forward zone provider may be the result of a number of transactions:

1. The forward zone outsourcing may be provided by the maker of the Homenet router. In this case, the identity and authorization could be built in the device at the manufacturer provisioning time. The device would need to be provisioned with a device-unique credential, and it is likely that the Registered Homenet Domain would be derived from a public attribute of the device, such as a serial number (see Appendix C or [HOMEROUTER-PROVISION] for more details).

2. The forward zone outsourcing may be provided by the ISP. In this case, the use of [RFC9527] to provide the credentials is appropriate.

3. The forward zone may be outsourced to a third party, such as a domain registrar. In this case, the use of the JSON-serialized YANG data model described in this section is appropriate, as it can easily be copy and pasted by the user or downloaded as part of a web transaction.

For reverse zones, the relationship is always with the upstream ISP (although there may be more than one), so [RFC9527] always applies.

The following is an abridged example of a set of data that represents the needed configuration parameters for outsourcing.

Appendix C. Example: A Manufacturer-Provisioned HNA Product Flow

This scenario is one where a Homenet router device manufacturer decides to offer DNS hosting as a value add.

[HOMEROUTER-PROVISION] describes a process for a home router credential provisioning system. The outline of it is that near the end of the manufacturing process, as part of the firmware loading, the manufacturer provisions a private key and certificate into the device.

In addition to having an asymmetric credential known to the manufacturer, the device also has been provisioned with an agreed-upon name. In the example in the above document, the name "n8d234f.r.example.net" has already been allocated and confirmed with the manufacturer.

The HNA can use the above domain for itself. It is not very pretty or personal, but if the owner would like to have a better name, they can arrange it.

The configuration would look like the following:

```
{
  "dm" : "2001:db8:1234:111:222::2",
  "dm_acl"    : "2001:db8:1234:111:222::/64",
  "dm_ctrl"   : "manufacturer.example.net",
  "dm_port"   : "4433",
  "ns_list"   : [ "ns1.publicdns.example", "ns2.publicdns.example"],
  "zone"      : "n8d234f.r.example.net",
  "auth_method" : "certificate",
  "hna_certificate":"-----BEGIN CERTIFICATE-----\nMIIDTjCCFGy....",
}
```

The dm_ctrl and dm_port values would be built into the firmware.

Acknowledgments

The authors wish to thank Philippe Lemordant for his contributions to the earlier draft versions of this document; 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 HNA 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, Stephen Farrell, and Ray Bellis for their feedback on handling different views as well as clarifying the impact of outsourcing the zone-signing operation outside the HNA; and Mark Andrew and Peter Koch for clarifying the renumbering.

The authors would like to thank Kiran Makhijani for her in-depth review that contributed to shaping the final version of this document.

The authors would also like to thank our Area Director ric Vyncke for his constant support and pushing the document through the IESG process and the many reviewers from various directorates including Anthony Somerset, Geoff Huston, Tim Chown, Tim Wicinski, Matt Brown, Darrel Miller, and Christer Holmberg.

Contributors

The coauthors would like to thank Chris Griffiths and Wouter Cloetens for providing significant contributions to the earlier draft versions

of this document.

Authors' Addresses

Daniel Migault
Ericsson
8275 Trans Canada Route
Saint Laurent QC 4S 0B6
Canada
Email: daniel.migault@ericsson.com

Ralf Weber
Nominum
2000 Seaport Blvd.
Redwood City, CA 94063
United States of America
Email: ralf.weber@nominum.com

Michael Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa ON K1Z 5V7
Canada
Email: mcr+ietf@sandelman.ca

Ray Hunter
Globis Consulting BV
Weegschaalstraat 3
5632CW Eindhoven
Netherlands
Email: v6ops@globis.net