HOMENET
Internet-Draft
Intended status: Standards Track
Expires: April 23, 2014

D. Migault (Ed)
Orange

October 20, 2013

IPv6 Home Network Naming Delegation
draft-mglt-homenet-dnssec-validator-dhc-options-00.txt

Abstract

DNSSEC provides data integrity and authentication for DNSSEC validators. However, without valid trust anchor(s) and an acceptable value for the current time. DNSSEC validation cannot be performed. This leads to multiple exceptions where DNSSEC validation MUST NOT be performed. This list of exception is expected to become larger if DNSSEC is deployed this way. All conditions where DNSSEC is disable adds complexity to the implementation and increases the vectors that disables security.

This document assumes that DNSSEC adoption by end devices requires that end devices can have DNSSEC always set today and in the future.

This document describes DHCP Options to provision the DHCP Client with valid trust anchors and time so DNSSEC validation can be performed.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 23, 2014.

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

DNSSEC [RFC4033], [RFC4034], [RFC4035] adds data authentication and integrity checks to DNS [RFC1034], [RFC1035]. For signature validation, DNSSEC requires a trusted anchor such as the Key Signing Key (KSK) of the Root Zone or any other zone. Without a trust anchor, DNSSEC validation cannot be performed. In addition KSKs and signatures are valid for a given period of time. As a result, DNSSEC validation cannot be performed if time shifting is to large.

This document considers DHCP DNSSEC Trust Anchor Option and DHCP Time Option to provision a device with trusted KSKs and current time. Although our priority is to provide the Root Zone KSK, we also consider the case other trusted KSK MAY be provided, for example if some Zone does not provides secure delegation, or to mitigate badly configured DNSSEC zones (like TLDs zones).

The main motivation for these DHCP Options is to enable a DHCP enabled device to have DNSSEC validation always set, and prevent the device from performing DNS resolution without DNSSEC validation. In fact, enabling DNS with no validation possible within a device represent a potential way to remove security and MAY be used by attackers. Similarly, DNSSEC configuration implemented in the end users device, MAY not consider future cases and introduce vulnerabilities. DHCP Options prevents this as long as the relationship between DHCP Client and DHCP Server is trusted.

In this document, we assume that the channel between the DHCP Client and the DHCP Server is trusted and secured with DHCP mechanisms described in [RFC3315], or IPsec [RFC4301].

3. Threat Model

This document addresses the case where a device is configured with DNSSEC validation set is plugged in, get connectivity using DHCP for example, but fails DNSSEC resolutions because its trust anchor KSK is not valid anymore or its local time is not valid.

This treat mainly address devices that can be switched off for a long period of time or devices that MAY be off-selves for a long time before being plugged in. CPE as well as any homenet device is concerned by this use case.

This treat also addresses DNSSEC emergency key roll over operations. Devices that have cached the out-of-date KSK will not be able to check the signatures until the TTL has expired on all cache.

This document proposes DHCP Options that provides the necessary parameters to perform DNSSEC validation. These Options MUST be used on a trusted network over a trusted channel between the DHCP Client

and the DHCP Server. These options MAY be used in conjunction of additional mechanisms.

3.1. Motivations for providing DNSSEC Trust Anchor

The first motivation for providing trusted KSKs is to provide automatic configuration of devices to enable DNSSEC validation. This avoids validator initial KSK provisioning issue as well as KSK roll over issues.

A validator MAY not be able to perform signature check with an authenticated KSK because:

- 1) It does not have a trust anchor (like the Root Zone KSK)

- 2) The KSK MAY have been authenticated, stored or cached with an expiration date valid but is not valid anymore. This MAY happen in the case of an emergency key roll over, if the device has been offline during the key roll over, or if the key roll over is not performed as described in [DPS-KSK], [RFC5011].

- 3) The chain of trust MAY have been broken. This can happen to non Root Zone KSK only and MAY not involve the responsibility of the owner of the zone. The deeper the Zone is in the hierarchy, the more likely this happens.

- 4) A DNSSEC zone MAY have been badly signed or a KSK MAY have been badly generated. The DNSSEC MAY be correct, but DNSSEC validator MAY keep for a long time the badly generated KSK, ZSK...

The goal of the DHCP DNSSEC Trust Anchor Option is to provide these validator trusted anchors like the Root Zone KSK, as well as other KSKs (TLDs...) so the validator has the proper KSKs to perform DNSSEC validation.

Most document currently concerns the Root Zone KSK for which recommendation and alternative mechanisms have been described. [I-D.jabley-dnsop-validator-bootstrap] provides guide lines on how to retrieve and select DNSSEC Trust Anchors. Section 5.3 and [I-D.jabley-dnssec-trust-anchor] describes mechanisms to retrieve securely the Root Zone KSK relying on TLS security. It suggests to use insecure DNS resolution to set HTTPS connections. Using HTTPS requires downloading the keyDigest id (key-label) from https://data.iana.org/root-anchors/root-anchors.xml, followed by an HTTPS request at https://data.iana.org/root-anchors/key-label.crt to get the whole certificate.

The key advantages of the DHCP DNSSEC Trust Anchor Option described in this document are that we extend the mechanism to any KSK, and validator can set DNSSEC validation on for all DNS queries. However, we do not see any contradiction between recommendations provided by [I-D.jabley-dnsop-validator-bootstrap] and [I-D.jabley-dnssec-trust-anchor] and believe the principle described in these documents SHOULD be applied by the validator. Note also that DHCP DNSSEC Trust Anchor Option only benefit to validators that are configured via DHCP.

To recover from a DNSSEC failure and remove a particular data from cache, [I-D.jabley-dnsop-dns-flush] suggests to use a NOTIFY message between Authoritative Servers and Resolvers. This mechanisms is set between Recursive Server and Authoritative Servers with a specific trusted relationship. This is probably a selection of TLDs. This document, does not address the DNSSEC failure over Recursive Servers, but addresses more specifically DHCP configured devices. These are typically CPEs or End Users. We believe that configuring and restarting DNSSEC validator with DHCP Option, is an easier way to cope with this issue. First the trust relation between DHCP Server already exists, we do not need additional trusted channel between Authoritative Servers or eventually the Recursive Server. Then basic implementations of stub resolvers, in CPE or desktops may not address NOTIFY message.

3.2. Motivations for providing Time

KSKs and signatures are always associated to an expiration time. As a result, DNSSEC validation requires that the validator knows the current time.

A number of mechanisms exists like [TLSDATE] or [RFC5905] for setting the time of the device. In addition, [RFC5908] provides a Network Time Protocol (NTP) Server Option for DHCP. The DHCP Time Option describes in this document differs from [RFC5908] as it provides an estimation of the current time, instead of providing the NTP servers location information. The time value provided by the DHCP Time Option should be used only if previously mentioned mechanisms are either not implemented on the device or are unavailable. One of the reason MAY be that you MAY need valid DNS(SEC) resolution to use these protocols. The time provided by the DHCP Time Option does not have the accuracy of NTP and SHOULD be considered as a best effort value. [I-D.jabley-dnsop-validator-bootstrap] also recommend that when time has not been verified by the validator, the signature validation SHOULD be done with time off.

The key advantage of the DHCP Time Option is that it makes possible to have DNSSEC validation always set. It limits the possible DNSSEC

validation variants which potentially expose the device to disable DNSSEC validations. Note also that DHCP Time Option only benefit to validators that are configured via DHCP.

4. Terminology

5. DHCP DNSSEC Trust Anchor Options

This section describes two options:

- DHCP DNSSEC KSK Trust Anchor Options: carries the KSK RRset as described in [RFC1035] with a DNSKEY RDATA as described in [RFC4033]. This data is not integrity protected, nor it can be authenticated. Such data SHOULD be trusted over a trusted DHCP channel.

- DHCP DNSSEC CERT Trust Anchor Options: Carries a certificate encoded as described in [RFC4398]. The advantage of the Certificate is that is enables authentication of the received information by a trusted party. For example, CPE providers MAY provide a trusted certification authority. Unlike DNSSEC key roll over, the CPE provider controls the key roll over of the certification authority it provides.

5.1. DHCP DNSSEC KSK RR Trust Anchor Options

The DHCP DNSSEC KSK Trust Anchor Option provides the RRset as mentioned in the DNS(SEC) Zone. In other words, it carries the RR as defined in Section 3.2. of [RFC1035] and a RDATA DNSKEY as defined in Section 2.1 of [RFC4033]. As the RR has a variable length, the DHCP DNSSEC KSK Trust Anchor Options follows the recommendation format of Section 5.9 of [I-D.ietf-dhc-option-guidelines].

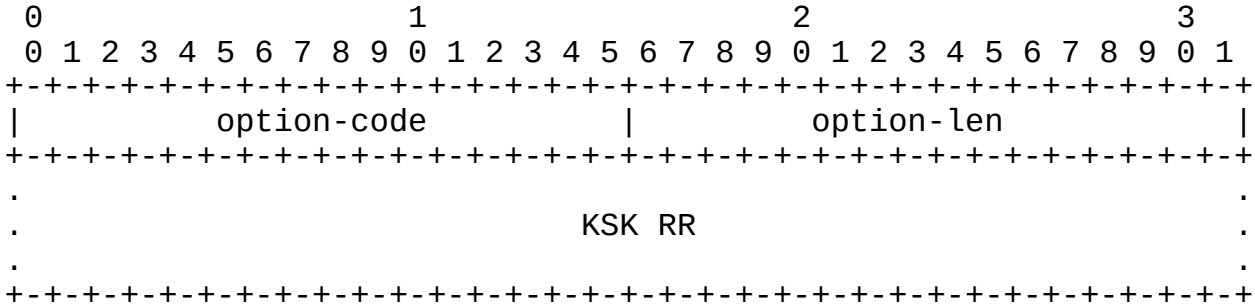

Figure 1: DHCP DNSSEC KSK Trust Anchor Options Payload Description

- option-code: OPTION_DNSSEC_KSK_RR_TRUST_ANCHOR

- option-len: An unsigned integer giving the length of the KSK RR field in this option in octets

5.2. DHCP DNSSEC KSK CERT Trust Anchor Options

The DHCP DNSSEC CERT Trust Anchor Option provides a certificate. The CERT RR is described in [RFC4398]. Note that only the RDATA associated to the CERT is present in the DHCP Option. As the RR has a variable length, the DHCP DNSSEC KSK Trust Anchor Options follows the recommendation format of Section 5.9 of [I-D.ietf-dhc-option-guidelines].

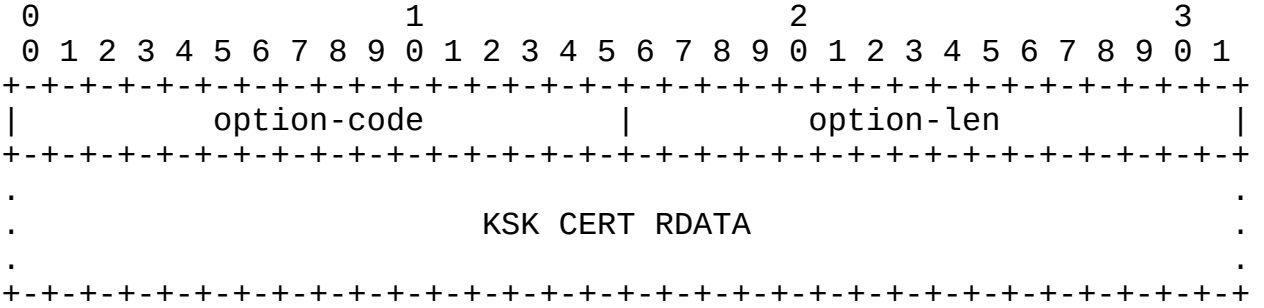

Figure 2: DHCP DNSSEC CERT Trust Anchor Options Payload Description

- option-code: OPTION_DNSSEC_CERT_TRUST_ANCHOR

- option-len: An unsigned integer giving the length of the KSK RR field in this option in octets

The X.509 [RFC5280] certificate MUST have a keyUsage set to digitalSignature (0) and nonRepudiation (1). Subject Alternative Name DNS name indicates the name of the zone.

In order to be compliant with the certificate of the Root Zone described [I-D.jabley-dnssec-trust-anchor]. The CERT for a KSK SHOULD have a Common Name (CN) with the string "'Zone-FQDN' Zone KSK" followed by the time and date of key generation in the format specified in [RFC3339]. 'Zone-FQDN' is the name of the zone and SHOULD be the same as the one mentioned in Subject Alternative Name. The resourceRecord Attribute SHOULD be set with the DS RRset.

6. DHCP Time Option

The DHCP DNSSEC Time Option is used by the DHCP Server to indicate the Time to the DHCP Client. The Time is provided in a string format as specified in [RFC3339] and in [I-D.ietf-dhc-option-guidelines] Section 5.8.

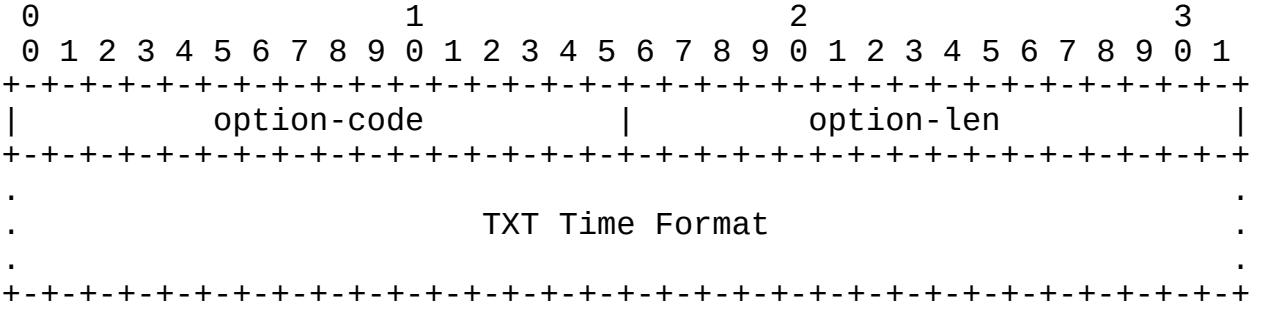

Figure 2: DHCP Time Options Payload Description

- option-code: OPTION_TIME

- option-len: A string representing the Time

7. DHCP Client Behavior

DHCP DNSSEC KSK Trust Anchor Option, DHCP DNSSEC CERT Trust Anchor Option or DHCP Time Option described in this document are intended for DNSSEC validation. If a connected device is not performing DNSSEC validation, it MUST NOT send a DHCP an Option Request DHCP Option (ORO) [RFC3315] for any of these options, and MUST ignore all these options if provided by the DHCP Server.

The DHCP sends a DHCP ORO for one or multiple options described in the document. Motivations for sending this Option Request DHCP Option is out of scope of the document. It could be a device switched off for a long time, a device that cannot validate the DNSSEC responses.

A channel is considered trusted if 1) the DHCP Server is trusted and authenticated and 2) exchanged data between the DHCP Client and the DHCP Server is integrity protected. IPsec [RFC4301], for example, MAY be used to establish a secure channel.

Over a trusted channel, the DHCP Client that performs DNSSEC validation MAY send an ORO for any of the DHCP DNSSEC KSK Trust Anchor Option, the DHCP DNSSEC CERT Trust Anchor Option or the DHCP Time Option to a DHCP Server.

Over a trusted channel, the DHCP Client that performs DNSSEC validation SHOULD consider the DHCP DNSSEC KSK Trust Anchor Option, the DHCP DNSSEC CERT Trust Anchor Option or the DHCP Time Option sent by the DHCP Server.

Over a non trusted channel, the DHCP Client MAY only send ORO for a DHCP DNSSEC CERT Trust Anchor Option. This option is the only one that MAY be considered by the DHCP Client if sent by the DHCP Server. If the DHCP Client does not trust the signer of the certificate, the option MUST be ignored.

When a DHCP DNSSEC KSK Trust Anchor Option or a DHCP DNSSEC CERT Trust Anchor Option is accepted by the DHCP Client, it MUST remove overwrite old values for the KSK with the new one.

When a DHCP Time Option is accepted by the DHCP Client, it MUST check the difference between its clock and the time provided by the Option. It SHOULD overwrite its clock value only if the difference is too large.

In any other case, ORO requests MUST NOT be sent by the DHCP Client, and options received by the DHCP Server MUST NOT be considered by the DHCP Client. The remaining of the section details when the options MUST NOT be requested by the DHCP Client and MUST be ignored by the DHCP Client when received by the DHCP Server.

The DHCP Client MUST NOT send an ORO for a DHCP DNSSEC KSK Trust Anchor Option, a DHCP DNSSEC CERT Trust Anchor Option or a DHCP Time Option to a DHCP Server that is either not trusted or not authenticated.

All DHCP DNSSEC KSK Trust Anchor Option, a DHCP DNSSEC CERT Trust Anchor Option or a DHCP Time Option received from DHCP Server that is not authenticated or that is not trusted MUST be ignored by the DHCP Client.

The DHCP Client MUST NOT send an ORO for a DHCP DNSSEC KSK Trust Anchor Option or a DHCP Time Option to a trusted DHCP Server over an untrusted channel. A DHCP DNSSEC CERT Trust Anchor Option MAY be requested over an untrusted channel since the certificate is signed and thus can be authenticated. A DHCP DNSSEC CERT Trust Anchor Option signed by an untrusted authority MUST be ignored by the DHCP Client.

All DHCP DNSSEC KSK Trust Anchor Option or a DHCP Time Option received from DHCP Server over a channel that is not trusted MUST be ignored by the DHCP Client.

8. DHCP Server Behavior

The DHCP Server SHOULD properly answer with the requested options in the ORO, even if the DHCP Server does not consider the channel with DHCP Client as trusted.

The DHCP Server MAY also provide DHCP DNSSEC KSK Trust Anchor Option, DHCP DNSSEC CERT Trust Anchor Option or DHCP Time Option without being requested by the DHCP Client. This could for example prevent failures not detected by the DHCP Client.

9. DHCP Relay Agent Behavior

The DHCP Options described in the document do not impact the Relay Agent.

10. IANA Considerations

The DHCP options detailed in this document is:

- OPTION_DNSSEC_KSK_RR_TRUST_ANCHOR: TBD

- OPTION_DNSSEC_KSK_CERT_TRUST_ANCHOR: TBD

- OPTION_TIME: TBD

11. Security Considerations

Security has been discussed in the "DHCP Client Behavior Section". As information contained in the payloads are use to enable signature validation, these pieces of information MUST be considered only when issued by a trusted party, and when integrity protection is provided.

12. Acknowledgment

Bringing DNSSEC in Home Networks discussion has started during the IETF87 in Berlin with Ted Lemon, Ralph Weber, Normen Kowalewski, and Mikael Abrahamsson. An email discussion has also been initiated by Jim Gettys with among others, helpful remarks from Paul Wouters, Joe Abley, Michael Ridchardson.

13. References

13.1. 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.

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

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

[RFC3339] Klyne, G., Ed. and C. Newman, "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

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

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

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

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

[RFC4398] Josefsson, S., "Storing Certificates in the Domain Name System (DNS)", RFC 4398, March 2006.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, September 2007.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5905] Mills, D., Martin, J., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[RFC5908] Gayraud, R. and B. Lourdelet, "Network Time Protocol (NTP) Server Option for DHCPv6", RFC 5908, June 2010.

13.2. Informational References

[DPS-KSK] Ljunggren, F., Okubo, T., Lamb, R., and J. Schlyter, "DNSSEC Practice Statement for the Root Zone KSK Operation", Root DNSSEC Design Team, URL: http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt, 2010.

[I-D.ietf-dhc-option-guidelines] Hankins, D., Mrugalski, T., Siodelski, M., Jiang, S., and S. Krishnan, "Guidelines for Creating New DHCPv6 Options", draft-ietf-dhc-option-guidelines-14 (work in progress), September 2013.

[I-D.jabley-dnsop-dns-flush] Abley, J., "A Mechanism for Remote-Triggered DNS Cache Flushes (DNS FLUSH)", draft-jabley-dnsop-dns-flush-00 (work in progress), June 2013.

[I-D.jabley-dnsop-validator-bootstrap] Abley, J. and D. Knight, "Establishing an Appropriate Root Zone DNSSEC Trust Anchor at Startup", draft-jabley-dnsop-validator-bootstrap-00 (work in progress), January 2011.

[I-D.jabley-dnssec-trust-anchor] Abley, J., Schlyter, J., and G. Bailey, "DNSSEC Trust Anchor Publication for the Root Zone", draft-jabley-dnssec-trust-anchor-07 (work in progress), June 2013.

[TLSDATE] error, IO., "tlsdate: secure parasitic rdate replacement", URL: https://github.com/ioerror/tlsdate, 2013.

Appendix A. Document Change Log

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

-00: First version published.

Author’s Address

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

Phone: +33 1 45 29 60 52
Email: mglt.ietf@gmail.com