dnsop D. Migault
Internet-Draft Ericsson
Intended status: Informational E. Lewis
Expires: June 1, 2019 ICANN
D. York
ISOC
November 28, 2018

DNSSEC Validator Requirements
draft-mglt-dnsop-dnssec-validator-requirements-07

Abstract

The DNS Security Extensions define a process for validating received data and assert them authentic and complete as opposed to forged.

This document describes what is needed in implementations to make the validation process manageable Considerations for accurate time as well as management of the trust anchor store.

Table of Contents

1. Requirements Notation

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Introduction

The act of DNSSEC validation [RFC4033][RFC4035] can be broken into two part:

o Signature Validation: which consists in checking the cryptographic signature of a Resource Record Set (RRset). The signature validation involves among other parameters a DNSKEY Resource Record (RR) and RRSIG RR and the RRset itself. The signature

validation process results in assertion that the owner of the private part of the public key contained in the DNSKEY RR has effectively published the RRset. The binding between the private key and the RRset is provided by the trust in the cryptographic algorithm.

- Trust: Signature Validation results in asserting a RRset is accurately validated if there is sufficient trust that the owner of the private key associated to the DNSKEY RR is the owner of the RRset - i.e. that is to say is the legitimate owner. Such trust is provided by a Trust Anchor (TA), and the chain of trust established between the TA and the DNSKEY RR. The chain of trust is obtained by recursively validating the DNSKEY RRs. As a result, such trust results from the trust placed in the TA as well as the delegation mechanism provided by DNSSEC and the Signature Validation. As TAs need to be managed over time, the trust also concerns the management procedure of the TA. This is the main concern of this document.

Once accurately validated the RRset is assumed to be accurately validated and trusted trusted during the time indicated by its TTL.

A threat associated to the Signature Validation could consist in a RRSet maliciously forged to be validated by a trusted DNSKEY RR. Such threat mostly rely on the use of weak cryptography by the authoritative server, and the DNSSEC validator has little means to prevent such threats.

The document considers instead the threat associated to the establishment of the trust where a DNSKEY RR is maliciously established. This may be through a weakness in the authentication of changes to the zone administration database, allowing a malicious key to be added and then signed according to the DNSSEC process. Once this is discovered to have happened, other data validated via such a key should be called into question.

This document is focused on the necessary mechanisms that DNSSEC validators should implement in order to implement sufficient Trust that makes DNSSEC validation output accurate. The mechanisms described in this document include, provisioning mechanisms as well as monitoring and management mechanisms that enables an administrator to validate the validity of the DNSSEC validation output.

The mechanisms provided are designed in accordance of the DNSSEC trust model as to meet the current operations of DNSSEC. Such trust model is briefly recapped in Section 4 so operators understand the limits and motivations for such mechanisms.

3. Terminology

This document uses the following terminology:

DNSSEC validator the entity that performs DNSSEC resolution and performs signature validation.

Accurate validation validation that avoids false positives and catches true negatives.

Trust Anchor Data Store a module (of code) implementing functions related to the trust anchors used by the validator. This is essentially a database allowing access, monitoring of, and changes to trust anchors.

4. DNSSEC Validator Description

This is a conceptual block diagram of the elements involved with DNSSEC validation. This is not meant to be an architecture for code, this is meant to be a framework for discussion and explanation.

```
+-------------+  +---------------+
|             |  |               |
| Time Source |  | Cryptographic |
|             |  |   Libraries   |
|             |  |               |
+-------------+  +---------------+
       |                 |
       v                 v
+---------------------------------+   +--------------+
|                                 |   |              |
|                                 |<--| Trust Anchor |
|    DNSSEC Validation Engine     |   |   Manager &  |
|                                 |-->|   Storage    |
|                                 |   |              |
+---------------------------------+   +--------------+
      ^ |                ^                   |
      | v                |                   |
+-------------+  +---------------+           |
|             |  |               |           |
| DNS Caches  |  | DNS Messages  |<----------+
|             |  |               |
+-------------+  +---------------+
```

Figure 1: DNSSEC Validator Description

Time Source The wall clock time provides the DNSSEC Validation Engine the current time. Time is among other used to validate the

RRSIG Signature and Inception Fields to provide some protection against replay attacks.

Cryptograhic Libraries The code performing mathematical functions provides the DNSSEC Validation Engine the ability to check the Signature Field that contains the cryptographic signature covering the RRSIG RDATA.

DNS Message DNS responses are used to carry the information from the DNS system. The receiver of the DNS message can be any kind of application including DNS-related application such as in the case of automated Trust Anchor update performed by the Trust Anchor Manager & Storage. The DNSSEC Validator Engine accurately validates the DNS responses before caching them in the DNS Cache and forwarding them to the DNS receiver. In case of validation failure, an error is returned and the information may be negatively cached.

DNS Caches Include positive and negative caches. The DNSSEC Validation Engine fills DNS Caches with the results of a validation (positive data, negative failures). The DNSSEC trust model considers that once a RRset has been accurately validated by the DNSSEC Validator Engine, the RRset is considered trusted (or untrusted) for its associated TTL. DNS Caches contain RRsets that may contain information requested by the application (RRset of type AAAA for example) as well as RRset necessary to accurately validate the RRsets (RRsets of type DNSKET or RRSIG for example). It also worth noticing that RRset validated with DNSSEC or RRset that are not validated with DNSSEC fill the DNS Cache with the same level of trust.

Trust Anchor Manager The database of trust anchors associated to database management processes. This function provides the DNSSEC Validation Engine Trust Anchor information when needed. When TA needs to be updated, the Trust Anchor Manager is also responsible to handle the updating procedure. This includes sending DNS Messages as well as treating appropriately the DNS responses that have been accurately validated by the DNSSEC Validator Engine. This will end up in the DNSSEC Validator Engine pushing new TAs.

DNSSEC Validation Engine follows local policy to approve data. The approved data is returned to the requesting application as well as in the DNS Caches. While the cryptographic computation of the RRSIG signature may be the most visible step, the RRSIG record also contains other information intended to help the validator perform its work, in some cases "sane value" checks are performed. For instance, the original TTL (needed to prepare the RR set for validation) ought to be equal to or higher than the received TTL.

Not shown - Name Server Process Management interfaces to elements, handling of Checking Disabled request, responses, as well as all API requests made of the name server.

5. Time deviation and absence of Real Time Clock

With M2M communication some devices are not expecting to embed Real Time Clock (Raspberry Pi is one example of such devices). When these devices are re-plugged the initial time is set to January 1 1970. Other devices that have clocks that may suffer from time deviation. These devices cannot rely on their time estimation to perform DNSSEC validation.

REQ1 A DNSSEC validator MUST be provided means to update the time without relying on DNSSEC.

Note that updating time in order to be able to perform DNSSEC validation may become a form of a chicken-and-egg problem when the NTP server is designated by its FQDN. The update mechanisms must consider the DNSSEC validator may not able to validate the DNSSEC queries. In other words, the mechanisms may have to update the time over an unsecure DNSSEC resolution.

6. Trust Anchor

6.1. Trust Anchor Bootstrapping

A validator needs to have trust anchors or it will never be able to construct a chain of trust. Trust anchors are defined by DNSSEC to be keys that are inherently trusted, configured by authorized parties, in the validator. The configuration can be via an automated process, such as Automated Updates of DNSSEC Trust Anchors [RFC5011], [I-D.ietf-dnsop-rfc5011-security-considerations], or via manual process.

An implementation of a validator needs to allow an operator to choose any automated process supported by the validator. (No requirements are stated about what processes to support, only one is standardized to date.) An implementation needs to also afford the operator the ability to override or manage via a purely manual process, the storage of managed keys. This includes adding, deleting, changing and inspecting.

Beyond the scope of these requirements are the decision processes of authorized parties in placing trust in keys.

REQ2 A DNSSEC validator MUST check the validity of its Trust Anchors. When a Trust Anchor cannot be verified, the DNSSEC

validator MUST send a warning and SHOULD NOT start validating traffic without manual validation.

REQ3 A DNSSEC validator SHOULD be able to retrieve a Trust Anchor with bootstrapping mechanism. Such mechanism' security MUST NOT be based on DNSSEC, but could instead include downloading a XML file from a trusted URL, or a PKIX certificate.

Although some bootstrapping mechanisms to securely retrieve publish [RFC7958] and retrieve [UNBOUND-ANCHOR] the Root Zone Trust Anchor have been defined, it is believed these mechanisms should be extended to other KSKs or Trust Anchors. In fact it is not always possible to build a trusted delegation between the Root Zone and any sub zone. This may happen for example if one of the upper zones does not handle the secure delegation or improperly implement it. A DS RRset may not be properly filled or its associated signature cannot be validated. As the chain of trust between a zone and the root zone may not be validated, the DNSSEC validation for the zone requires a Trust Anchor. Such DNS(SEC) resolutions may be critical for infrastructure management. A company "Example" may, for example, address all its devices under the domain example.com and may not want disruption to happen if the .com delegation cannot be validated for any reason. Such companies may provision there DNSSEC validator with the Trust Anchor KSK for the zone example.com in addition to the regular DNSSEC delegation. Similarly some some domains may present different views such as a "private" view and a "public view". These zones may have some different content, and may use a different KSK for each view.

6.1.1. The IANA managed root zone KSK

The IANA managed root zone KSK is an operationally significant trust point in the global public Internet. Attention to the trust anchor for this point is paramount. Trust anchor management ought to recognize that the majority of operators deploying DNSSEC validators will need to explicitly or implicitly rely on this trust anchor. Trust anchor management needs to recognize that there may be other trust anchors of interest to operators. Besides deployments in networks other than the global public Internet (hence a different root), operators may want to configure other trust points.

The IANA managed root zone KSK is managed and published as described in "DNSSEC Trust Anchor Publication for the Root Zone" [RFC7598]. That document is written as specific to that trust point. Other trust points may adopt the technique describe (or may use other approaches).

This represents a consideration for implementations. On one hand, operators will place special emphasis on how the root zone DNSSEC KSK

is managed. On the other hand, implementations ought to accommodate trust anchors in a general manner, despite the odds that other trust anchors will not be configured in a specific deployment.

Because of this, it is recommended that implementations make the root zone trust anchor obvious to the operator while still enabling configuration of general trust points.

6.2. Trust Anchor Data Store

When DNSSEC validator are running and a Trust Anchor KSK roll over is ongoing, a network administrator or any trust party may be willing to check whether the new published keys are being stored in a Trust Anchor Data Store with an appropriated status. Such inspection aims at detecting an non successful Trust Anchor roll over before traffic is being rejected. When a new Trust Anchor has not been considered by the DNSSEC validator, a trusted party may be able to provision the DNSSEC validator with the new Trust Anchor, and eventually may remove the revoked Trust Anchor.

While using a Trust Anchor that has been removed results in the DNSSEC validator rejecting multiple legitimate responses, the consequences associated to accepting a rogue Trust Anchor as a legitimate Trust Anchor are even worst. Such attacks would result in an attacker taking control of the entire naming space behind the Trust Anchor. In the case of the Root Zone KSK, for example, almost all name space would be under the control of the attacker. In addition, to the name space, once the rogue Trust Anchor is configured, there is little hope the DNSSEC validator be re-configured with the legitimate Trust Anchor without manual intervention. As a result, it is crucial to cautiously handle operations related to the Trust Anchor provisioning. Means must be provided so network administrator can clearly diagnose the reason a Trust Anchor is not valid to avoid accepting a rogue Trust Anchor inadvertently.

DNSSEC may also be used in some private environment. Corporate networks and home networks, for example, may want to take advantage of DNSSEC for a local scope network. Typically, a corporate network may use a local scope Trust Anchor to validate DNS RRsets provided by authoritative DNSSEC server in the corporate network. This use case is also known as the "split-view" use case. These RRsets within the corporate network may differ from those hosted on the public DNS infrastructure. Note that using different Trust Anchor for a given zone may expose a zone to signature invalidation. This is especially the case for DNSSEC validators that are expected to flip-flop between local and public scope. How validators have to handle the various provisioned Trust Anchors is out of scope of the document.

Home network may use DNSSEC with TLDs or associated domain names that are of local scope and not even registered in the public DNS infrastructure. This requires the ability to manage the Trust Anchor as well.

The necessity to interact with the Trust Anchors lead to the following requirements:

REQ4 A DNSSEC validator MUST store its Trust Anchors in a dedicated Trust Anchor Data Store. Such database MUST store information associated to each Trust Anchor status as well as the time the status has been noticed by the DNSSEC validator. Such database MUST be resilient to DNSSEC validator reboot.

REQ5 Trust Anchor states SHOULD at least consider those described in [RFC5011] (Start, AddPend, Valid, Missing, Revoked, Removed). Additional states SHOULD also be able to indicate additional motivations for revoking the Trust Anchor such as a Trust Anchor known to be corrupted, a Trust anchor miss published, or part of a regular roll over procedure.

REQ6 A DNSSEC validator MUST provide access to the Trust Anchor Data Base to authorized user only. Access control is expected to be based on a least privileged principles.

REQ7 A trusted party MUST be able to add, remove a Trust Anchor in the Trust Anchor Data Store.

6.3. Interactions with the cached RRsets

In addition when a Trust Anchor is revoked, the DNSSEC validator may behave differently if the revocation is motivated by a regular roll over operation or instead by revoking a Trust Anchor that is known as being corrupted. In the case the roll over procedure, is motivated by revoking a Trust Anchor that is known to be corrupted, the DNSSEC validator may be willing to flush all RRsets that depends on the Trust Anchor.

REQ8 A DNSSEC validator MUST be able to flush the cached RRsets that rely on a Trust Anchor.

7. ZSK / KSK

KSK / ZSK are not part of the DNSSEC validator configuration. Their values in the DNS Caches may not reflect those published by the authoritative servers or may be incoherent with the RRset in the DNS Cache they are validating. However, such incoherence primary results from error in the management of the authoritative servers. As a

result, it is not expected that the DNSSEC validator provides complex management facilities to address these issues as this will modify the DNS architecture and add complexity that is not proved to be beneficial.

7.1. KSK/ZSK Data Store

A number of reasons may result in inconsistencies between the RRsets stored in the cache and those published by the authoritative server.

An emergency KSK / ZSK rollover may result in a new KSK / ZSK with associated new RRSIG published in the authoritative zone, while DNSSEC validator may still cache the old value of the ZSK / KSK. For a RRset not cached, the DNSSEC validator performs a DNSSEC query to the authoritative server that returns the RRset signed with the new KSK / ZSK. The DNSSEC validator may not be able to retrieve the new KSK / ZSK while being unable to validate the signature with the old KSK / ZSK. This either result in a bogus resolution or in an invalid signature check. Note that by comparing the Key Tag Fields, the DNSSEC validator is able to notice the new KSK / ZSK used for signing differs from the one used to generate the received generated signature. However, the DNSSEC validator is not expected to retrieve the new ZSK / KSK, as such behavior could be used by an attacker. Instead, ZSK / ZSK key roll over procedure are expected to avoid such inconsistencies.

Similarly, a KSK / ZSK roll over may be performed normally, that is as described in [RFC6781] and [RFC7583]. While the KSK / ZSK roll over is performed, there is no obligation to flush the RRsets in the cache that have been associated with the old key. In fact, these RRset may still be considered as trusted and be removed from the cache as their TTL timeout. With very long TTL, these RRset may remain in the cache while the ZSK / KSK with a shorter TTL is no longer published nor in the cache. In such situations, the purpose of the KSK / ZSK is to validate the data is considered trusted at the time it enters the cache, and such trust may remain after the KSK / ZSK is being rolled over. Note also that even though the data may not be associated to the KSK / ZSK that has been used to validate the data, the link between the KSK / ZSK and the data is still stored in the cache using the RRSIG. Note also that inconsistencies between the ZSK / KSK stored in the cache and those published on the authoritative server, may lead to inconsistencies to downstream DNSSEC validators that rely on multiple cache over time. Typically, a request for the KSK / ZSK may have been provided by a cache that is storing the new published value, while the data and associated signatures may be associated to the old KSK / ZSK.

Incoherence between RRsets and DNSKEYs may be limited by configuring the DNSSEC validator with generic rules that applies to the validation process. Typically, the TTL associate to the DNSKEY is an engagement from the authoritative server that the DNSKEY will remain valid over this period. As this engagement supersedes the validation of any RRSIG and by extension to any RRset in the zone, this TTL value may be used as the maximum value for the TTL associated to FQDNs in the zone. This would at least reduce inconsistencies during regular KSK roll over. In addition, the DNSSEC validator should also be able to provide a maximum values for TTLs.

REQ DNSSEC Validator MUST be able to enforce TTL policies of RRsets based on the TTL of the KSK/ZSK. RRsets TTL SHOULD NOT exceed the KSK / ZSK initial TTL value.

The detection of a misbehaving KSK / ZSK mostly results from publication misconfigurations or an attack at the publication level. As a result, a primary focus is put on DNSSEC Validators monitoring KSK / ZSK with sufficient care to enable the network administrator to take the appropriated actions. Such actions could include out-of-band exchanges as well as specific actions details in section Section 7.2 and section Section 7.3. The monitoring requirements on KSK / ZSK are as follows:

REQ9 A DNSSEC validator MUST log its KSK/ZSK in a dedicated KSK/ ZSK Data Base. Such database MUST store information associated to each KSK/ZSK status as well as the time the status has been noticed by the DNSSEC validator. Such database SHOULD be resilient to DNSSEC validator reboot, that is the information stored in the Data Base MUST NOT be used to populate the cache, while it MAY be used as second factor verification, or audit for example.

REQ10 KSK/ZSK status and information SHOULD be monitored continuously and associated with their respective state as well as verified time. These states and time SHOULD be resilient to reboot.

REQ11 KSK/ZSK states SHOULD at least consider those described in section 3.1 of [RFC7583] (Generated, Published, Ready, Active, Retired, Dead, Removed, Revoked). Additional states SHOULD also be able to indicate additional motivations for revoking the KSK/ ZSK such as a KSK/ZSK known to be corrupted, a KSK/ZSK miss published, or part of a regular roll over procedure.

7.2. KSK ZSK Data Store and Trust Anchor Data Store

A zone may have been badly signed, which means that the KSK or ZSK cannot validate the RRSIG associated to the RRsets. This may not be due to a key roll over, but to an incompatibility between the keys (KSK or ZSK) and the signatures.

When such situation occurs, there is only a choice between not validating the RRsets or invalidating their signature. This is a policy design that needs to be taken by the network administrator. In other ways, flushing the RRset are not expected to address this issue. Such KSK/ZSK are known as Negative Trust Anchors [RFC7646].

With Negative Trust Anchor, the zone for a given time will be known as "known insecure". The DNSSEC Validator is not expected to perform signature validation for this zone. It is expected that this information is associated to a Time To Live (TTL). Note that, this information may be used as an attack vector to impersonate a zone, and must be provided in a trusted way, by a trusted party.

If a zone has been badly signed, the administrator of the authoritative DNS server may resign the zone with the same keys or proceed to an emergency key rollover. If the signature is performed with the same keys, the DNSSEC Validator may notice by itself that RRSIG can be validated. On the other hand if a key rollover is performed, the newly received RRSIG will carry a new key id. Upon receiving a new key id in the RRSIG, the DNSSEC Validator is expected to retrieve the new ZSK/KSK. If the RRSIG can be validated, the DNSSEC validator is expected to remove the "known insecure" flag.

However, if the KSK/ZSK are rolled over and RRSIG cannot be validated, it remains hard for the DNSSEC validator to determine whether the RRSIG cannot be validated or that RRSIG are invalid. As a result:

REQ14 A trusted party MUST be able to indicate a DNSSEC validator that a KSK or a ZSK as Negative Trust Anchor. Such Trust Anchors MUST NOT be used for RRSIG validation and MUST be moved to the Trust Anchor Data Store, so the information become resilient to reboot.

REQ15 A trusted party MUST be able to indicate a DNSSEC validator that a KSK/ZSK is known "back to secure".

7.3. Interactions with cached RRsets

The key roll over procedure intends to ensure that the published RRsets can be validated with the KSK / ZSK stored in the various cache of the DNSSEC validators. As a consequence, the key roll over enables trusted data to be cached. However, the key roll over does not necessarily prevents that cached be always validated with the currently published key. In fact, a cached data may have been validated by the former key and remain in the cache while the former key has been rolled out. Such inconsistencies may be acceptable and correspond to the following trust model: the KSK / ZSK validate the cached data can be trusted at time T. There is no specific information that leads to considers that trust at time T is subject to doubts at current time, so the cached data remain trusted.

While such inconsistencies may have little impact on end host DNSSEC validators, it may be different for large resolving platforms with downstream DNSSEC validators, and a DNSSEC validator may be willing to maintain its cached data consistent with the published KSK / ZSK. A trusted third party may willing to remove all cached RRsets that have been validated by the KSK/ZSK upon some specific states (revoked, or Removed for example), of after some time after the state is noticed. In this later case, only the RRset whose TTL has not expired yet would be flushed.

On the other hand, when a KSK / ZSK is known to be corrupted, this state may affect the trust that has been established at time T. In such case, the DNSSEC validator may be willing to flush all cached data that has been validated by the currently known corrupted KSK / ZSK, including the KSK / ZSK itself.

As a result, the following requirements are expected:

REQ16 A DNSSEC validator MUST be able to flush the cached KSK/ZSK.

REQ17 A DNSSEC validator SHOULD be able to flush the cached RRsets associated to a KSK/ZSK.

8. Cryptography Deprecation

As mentioned in [RFC8247] and [RFC8221] cryptography used one day is expected over the time to be replaced by new and more robust cryptographic mechanisms. In the case of DNSSEC signature protocols are likely to be updated over time. In order to anticipate the sunset of one of the signature scheme, a DNSSEC validator may willing to estimate the impact of deprecating one signature scheme.

Currently [RFC6975] provides the ability for a DNSSEC validator to announce an authoritative server the supported signature schemes. However, a DNSSEC validator is not able to determine other than by trying whether a signature scheme is supported by the authoritative server.

In order for a DNSSEC validator to safely deprecate one signature scheme the following requirement should be fulfilled.

REQ18 A DNSSEC validator SHOULD be able to request the signature scheme supported by an authoritative server.

9. Reporting

A DNSSEC validator receiving a DNS response cannot make the difference between receiving an non-secure response versus an attack. Dropping DNSSEC fields by a misconfigured middle boxes, such as DS, RRRSIG is considered as an attack. A DNSSEC validator is expected to perform secure DNS resolution and as such protect its stub client. An invalid response may be the result of an attack or a misconfiguration, and the DNSSEC validator may play an important role in sharing this information.

REQ19 A DNSSEC validation SHOULD be able to report the unavailability of the DNSSEC service.

REQ20 A DNSSEC validator SHOULD be able to report a invalid DNSSEC validation.

10. IANA Considerations

There are no IANA consideration for this document.

11. Security Considerations

The requirements listed in this document aim at providing the DNSSEC validator appropriated information so DNSSEC validation can be performed. On the other hand, providing inappropriate information can lead to misconfiguring the DNSSEC validator, and thus disrupting the DNSSEC resolution service. As a result, enabling the setting of configuration parameters by a third party may open a wide surface of attacks.

As an appropriate time value is necessary to perform signature check, an attacker may provide rogue time value to prevent the DNSSEC validator to check signatures.

An attacker may also affect the resolution service by regularly asking the DNSSEC validator to flush the KSK/ZSK from its cache. All associated data will also be flushed. This generates additional DNSSEC resolution and additional validations, as RRSet that were cached require a DNSSEC resolution over the Internet. This affects the resolution service by slowing down responses, and increases the load on the DNSSEC validator.

An attacker may ask the DNSSEC validator to consider a rogue KSK/ZSK, thus hijacking the DNS zone. Similarly, an attacker may inform the DNSSEC validator not to trust a given KSK in order to prevent DNSSEC validation to be performed.

An attacker (cf. Section 7) can advertise a "known insecure" KSK or ZSK is "back to secure" to prevent signature check to be performed correctly.

As a result, information considered by the DNSSEC validator should be from a trusted party. This trust party should have been authenticated, and the channel used to exchange the information should also be protected and authenticated.

12. Acknowledgment

The need to address DNSSEC issues on the resolver side started in the Home Networks mailing list and during the IETF87 in Berlin. Among others, people involved in the discussion were Ted Lemon, Ralph Weber, Normen Kowalewski, and Mikael Abrahamsson. People involved in the email discussion initiated by Jim Gettys were, with among others, Paul Wouters, Joe Abley and Michael Richardson.

The current document has been initiated after a discussion with Paul Wouter and Evan Hunt.

13. References

13.1. Normative References

[I-D.ietf-dnsop-rfc5011-security-considerations]
Hardaker, W. and W. Kumari, "Security Considerations for RFC5011 Publishers", draft-ietf-dnsop-rfc5011-security-considerations-13 (work in progress), July 2018.

[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>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[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>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/info/rfc6781>.

[RFC6975] Crocker, S. and S. Rose, "Signaling Cryptographic Algorithm Understanding in DNS Security Extensions (DNSSEC)", RFC 6975, DOI 10.17487/RFC6975, July 2013, <https://www.rfc-editor.org/info/rfc6975>.

[RFC7583] Morris, S., Ihren, J., Dickinson, J., and W. Mekking, "DNSSEC Key Rollover Timing Considerations", RFC 7583, DOI 10.17487/RFC7583, October 2015, <https://www.rfc-editor.org/info/rfc7583>.

[RFC7646] Ebersman, P., Kumari, W., Griffiths, C., Livingood, J., and R. Weber, "Definition and Use of DNSSEC Negative Trust Anchors", RFC 7646, DOI 10.17487/RFC7646, September 2015, <https://www.rfc-editor.org/info/rfc7646>.

[RFC7958] Abley, J., Schlyter, J., Bailey, G., and P. Hoffman, "DNSSEC Trust Anchor Publication for the Root Zone", RFC 7958, DOI 10.17487/RFC7958, August 2016, <https://www.rfc-editor.org/info/rfc7958>.

[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>.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221>.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017, <https://www.rfc-editor.org/info/rfc8247>.

13.2. Informative References

[RFC7598] Mrugalski, T., Troan, O., Farrer, I., Perreault, S., Dec, W., Bao, C., Yeh, L., and X. Deng, "DHCPv6 Options for Configuration of Softwire Address and Port-Mapped Clients", RFC 7598, DOI 10.17487/RFC7598, July 2015, <https://www.rfc-editor.org/info/rfc7598>.

[UNBOUND-ANCHOR] "unbound-anchor - Unbound anchor utility", n.d., <https://nlnetlabs.nl/documentation/unbound/unbound-anchor/>.

Authors' Addresses

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

EMail: daniel.migault@ericsson.com

Edward Lewis
ICANN

EMail: edward.lewis@icann.org

Dan York
ISOC

EMail: york@isoc.org