Intended Status: Informational
Network Working Group
Internet-Draft
Expires: August 21, 2008

O. Gudmundsson
OGUD Consulting LLC
J. Ihren
AAB

February 18, 2008

Names of States in the life of a DNSKEY
draft-gudmundsson-life-of-dnskey-00

Status of this Memo

Copyright Notice

Abstract

This document recommends a specific terminology to use when expressing the state that a DNSKEY is in at particular time. This does not affect how the protocol operates in any way.

Table of Contents

1. Introduction

When the editors of this document where comparing their DNSSEC key management projects they discovered that they where discussing roughly the same thing but using different terminology.

This document presents a unified terminology to use when describing the current state of a DNSKEY.

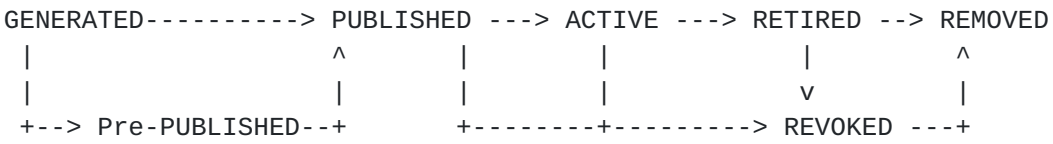
The DNSSEC standards documents ([1], [2] and [3]) do not address the required states for the key management of a DNSSEC key. The DNSSEC Operational Practices [4] document does propose that keys be published before use but uses inconsistent or confusing terms. This document assumes basic understanding of DNSSEC and key management.

The terms proposed in this document attempt to avoid any confusion and make the states of keys to be as clear as possible. The terms used in this document are intended as a operational supplement to the terms defined in Section 2 of [1].

To large extent this discussion is motivated by Trust anchor keys but the same terminology can be used for zone signing keys.

2. DNSKEY timeline

The model in this document is that keys progress through a state machine along a one-way path, keys never move to an earlier states.



DNSKEY time line.

There are few more states that are defined below but these apply only to the publisher of TA's and the consumer of TA's. Two of these are sub-sets of the Published state, the other two are error states.

3. Life stages of a DNSKEY

3.1. Generated

Once a key is generated it enters state Generated and stays there until the next state. While in this state only the owner of the key is aware of its existence and can prepare for its future use.

3.2. Published

Once the key is added to the DNSKEY set of a zone the key is there for the world to see, or published. The key needs to remain in this state for some time to propagate to all validators that have cached the prior version of the DNSKEY set. In the case of KSK the key should remain in this state for a longer time as documented in DNSSEC Timers RFC [5].

3.2.1. Pre-Publication

In certain circumstances a zone owner may want to give out a new Trust Anchor before exposing the actual public key. In this case the zone can publish a DS record of the key. This allows others to configure the trust anchor but will not be able to use the key until the key is published in the DNSKEY RRset.

3.2.2. Out-Of-Band Publication

In certain circumstances a domain may want to give out a new Trust Anchor outside DNS to give others a long lead time to configure the new key as trust anchor. The reason people may want to do this is to keep the size of the DNSKEY set smaller and only add new trust anchor just before the key goes into use. One likely use for this is the DNS "." root key as it does not have a parent that can publish a DS record for it. The publication mechanism does not matter it can be any one of web-site, advertisement in Financial Times and other international publication, e-mail to DNS related mailing lists, etc..

3.3. Active

The key is in ACTIVE state while it is actively signing data in the zone it resides in. It is one of the the keys that are signing the zone or parts of the zone.

3.4. Retired

When the key is no longer used for signing the zone it enters state Retired. In this state there may still be signatures by the key in cached data from the zone available at recursive servers, but the

authoritative servers for the zone do no longer carry any signatures generated by the key.

3.5. Removed

Once the key is removed from the DNSKEY RRset it enters the state Removed. At this point all signatures by the key that may still be temporarily valid will fail to verify once the validator refreshes the DNSKEY RRset in its memory.

Therefore "removal" of a key is typically not done until all the cached signatures have expired. Entering this state too early may cause number of validators to end up with STALE Trust Anchors.

3.5.1. Lame

A Trust Anchor is Lame if the parent continues to publish DS pointing to the key after it has been removed from the DNSKEY RRset. A Trust Anchor is arguably Lame if there are no signatures by a Retired KSK in the zone.

3.5.2. Stale

A Stale Trust Anchor is an old TA that remains in a validators list of active key(s) after the key has been removed from the zone's DNSKEY RRset.

3.6. Revoked

There are times when a zone wants to signal that a particular key should not be used at all. The mechanism to do this is to set the REVOKE bit [5]. Any key in any of the while the key is the DNSSKEY set can be exited to Revoked state. After some time in the Revoke state the key will be Removed.

4. Security considerations

TBD

5. IANA considerations

This document does not have any IANA actions.

6. References

6.1. Normative References

6.2. Informative References

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

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

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

[4] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

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

Authors' Addresses

Olafur Gudmundsson
OGUD Consulting LLC
3821 Village Park Drive
Chevy Chase, MD 20815
USA

Email: ogud@ogud.com

Johan Ihren
Automatica, AB
Bellmansgatan 30
Stockholm, SE-118 47
Sweden

Email: johani@automatica.se

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).