Network Working Group
Request for Comments: 4986
Category: Informational

H. Eland
Afilias Limited
R. Mundy
SPARTA, Inc.
S. Crocker
Shinkuro Inc.
S. Krishnaswamy
SPARTA, Inc.
August 2007

# Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover

## Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

## Abstract

Every DNS security-aware resolver must have at least one Trust Anchor to use as the basis for validating responses from DNS signed zones. For various reasons, most DNS security-aware resolvers are expected to have several Trust Anchors. For some operations, manual monitoring and updating of Trust Anchors may be feasible, but many operations will require automated methods for updating Trust Anchors in their security-aware resolvers. This document identifies the requirements that must be met by an automated DNS Trust Anchor rollover solution for security-aware DNS resolvers.

Table of Contents

## 1. Introduction

The Domain Name System Security Extensions (DNSSEC), as described in [2], [3], and [4], define new records and protocol modifications to DNS that permit security-aware resolvers to validate DNS Resource Records (RRs) from one or more Trust Anchors held by such security-aware resolvers.

Security-aware resolvers will have to initially obtain their Trust Anchors in a trustworthy manner to ensure the Trust Anchors are correct and valid. There are a number of ways that this initial step can be accomplished; however, details of this step are beyond the scope of this document. Once an operator has obtained Trust Anchors, initially entering the Trust Anchors into their security-aware resolvers will in many instances be a manual operation.

For some operational environments, manual management of Trust Anchors might be a viable approach. However, many operational environments will require a more automated, specification-based method for updating and managing Trust Anchors. This document provides a list of requirements that can be used to measure the effectiveness of any proposed automated Trust Anchor rollover mechanism in a consistent manner.

## 2. Terminology

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 RFC 2119 [1].

The use of RFC 2119 words in the requirements is intended to unambiguously describe a requirement. If a tradeoff is to be made between conflicting requirements when choosing a solution, the requirement with MUST language will have higher preference than requirements with SHOULD, MAY, or RECOMMENDED language. It is understood that a tradeoff may need to be made between requirements that both contain RFC 2119 language.

## 3. Background

DNS resolvers need to have one or more starting points to use in obtaining DNS answers. The starting points for stub resolvers are normally the IP addresses for one or more recursive name servers. The starting points for recursive name servers are normally IP addresses for DNS Root name servers. Similarly, security-aware resolvers must have one or more starting points to use for building the authenticated chain to validate a signed DNS response. Instead of IP addresses, DNSSEC requires that each resolver trust one or more

DNSKEY RRs or DS RRs as their starting point. Each of these starting points is called a Trust Anchor.

It should be noted that DNSKEY RRs and DS RRs are not Trust Anchors when they are created by the signed zone operator nor are they Trust Anchors because the records are published in the signed zone. A DNSKEY RR or DS RR becomes a Trust Anchor when an operator of a security-aware resolver determines that the public key or hash will be used as a Trust Anchor. Thus, the signed zone operator that created and/or published these RRs may not know if any of the DNSKEY RRs or DS RRs associated with their zone are being used as Trust Anchors by security-aware resolvers. The obvious exceptions are the DNSKEY RRs for the Root Zone, which will be used as Trust Anchors by many security-aware resolvers. For various reasons, DNSKEY RRs or DS RRs from zones other than Root can be used by operators of security-aware resolvers as Trust Anchors. It follows that responsibility lies with the operator of the security-aware resolver to ensure that the DNSKEY and/or DS RRs they have chosen to use as Trust Anchors are valid at the time they are used by the security-aware resolver as the starting point for building the authentication chain to validate a signed DNS response.

When operators of security-aware resolvers choose one or more Trust Anchors, they must also determine the method(s) they will use to ensure that they are using valid RRs and that they are able to determine when RRs being used as Trust Anchors should be replaced or removed. Early adopters of DNS signed zones have published information about the processes and methods they will use when their DNSKEY and/or DS RRs change so that operators of security-aware resolvers can manually change the Trust Anchors at the appropriate time. This manual approach will not scale and, therefore, drives the need for an automated specification-based approach for rollover of Trust Anchors for security-aware resolvers.

## 4. Definitions

This document uses the definitions contained in RFC 4033, section 2, plus the following additional definitions:

Trust Anchor: From RFC 4033, "A configured DNSKEY RR or DS RR hash of a DNSKEY RR. A validating security-aware resolver uses this public key or hash as a starting point for building the authentication chain to a signed DNS response." Additionally, a DNSKEY RR or DS RR is associated with precisely one point in the DNS hierarchy, i.e., one DNS zone. Multiple Trust Anchors MAY be associated with each DNS zone and MAY be held by any number of security-aware resolvers. Security-aware resolvers MAY have Trust Anchors from multiple DNS zones. Those responsible for the

operation of security-aware resolvers are responsible for determining the set of RRs that will be used as Trust Anchors by that resolver.

Initial Trust Relationship: Operators of security-aware resolvers must ensure that they initially obtain any Trust Anchors in a trustworthy manner. For example, the correctness of the Root Zone DNSKEY RR(s) could be verified by comparing what the operator believes to be the Root Trust Anchor(s) with several 'well-known' sources such as the IANA web site, the DNS published Root Zone and the publication of the public key in well-known hard-copy forms. For other Trust Anchors, the operator must ensure the accuracy and validity of the DNSKEY and/or DS RRs before designating them Trust Anchors. This might be accomplished through a combination of technical, procedural, and contractual relationships, or use other existing trust relationships outside the current DNS protocol.

Trust Anchor Distribution: The method or methods used to convey the DNSKEY and/or DS RR(s) between the signed zone operator and the security-aware resolver operator. The method or methods MUST be deemed sufficiently trustworthy by the operator of the security-aware resolver to ensure source authenticity and integrity of the new RRs to maintain the Initial Trust Relationship required to designate those RRs as Trust Anchors.

Trust Anchor Maintenance: Any change in a validating security-aware resolver to add a new Trust Anchor, delete an existing Trust Anchor, or replace an existing Trust Anchor with another. This change might be accomplished manually or in some automated manner. Those responsible for the operation of the security-aware resolver are responsible for establishing policies and procedures to ensure that a sufficient Initial Trust Relationship is in place before adding Trust Anchors for a particular DNS zone to their security-aware resolver configuration.

Trust Anchor Revocation and Removal: The invalidation of a particular Trust Anchor that results when the operator of the signed zone revokes or removes a DNSKEY RR or DS RR that is being used as a Trust Anchor by any security-aware resolver. It is possible that a zone administrator may invalidate more than one RR at one point in time; therefore, it MUST be clear to both the zone administrator and the security-aware resolver the exact RR(s) that have been revoked or removed so the proper Trust Anchor or Trust Anchors are removed.

Trust Anchor Rollover: The method or methods necessary for the secure replacement of one or multiple Trust Anchors held by security-aware resolvers. Trust Anchor Rollover should be considered a subset of Trust Anchor Maintenance.

Normal or Pre-Scheduled Trust Anchor Rollover: The operator of a DNSSEC signed zone has issued a new DNSKEY and/or DS RR(s) as a part of an operational routine.

Emergency or Non-Scheduled Trust Anchor Rollover: The operator of a signed zone has issued a new DNSKEY and/or DS RR(s) as part of an exceptional event.

Emergency Trust Anchor Revocation: The operator of a signed zone wishes to indicate that the current DNSKEY and/or DS RR(s) are no longer valid as part of an exceptional event.

## 5. Requirements

Following are the requirements for DNSSEC automated specification-based Trust Anchor Rollover:

### 5.1. Scalability

The automated Trust Anchor Rollover solution MUST be capable of scaling to Internet-wide usage. The probable largest number of instances of security-aware resolvers needing to rollover a Trust Anchor will be those that use the public key(s) for the Root Zone as Trust Anchor(s). This number could be extremely large if a number of applications have embedded security-aware resolvers.

The automated Trust Anchor Rollover solution MUST be able to support Trust Anchors for multiple zones and multiple Trust Anchors for each DNS zone. The number of Trust Anchors that might be configured into any one validating security-aware resolver is not known with certainty at this time; in most cases it will be less than 20 but it may even be as high as one thousand.

### 5.2. No Known Intellectual Property Encumbrance

Because trust anchor rollover is likely to be "mandatory-to-implement", section 8 of [5] requires that the technical solution chosen must not be known to be encumbered or must be available under royalty-free terms.

For this purpose, "royalty-free" is defined as follows: worldwide, irrevocable, perpetual right to use, without fee, in commerce or otherwise, where "use" includes descriptions of algorithms,

distribution and/or use of hardware implementations, distribution and/or use of software systems in source and/or binary form, in all DNS or DNSSEC applications including registry, registrar, domain name service including authority, recursion, caching, forwarding, stub resolver, or similar.

In summary, no implementor, distributor, or operator of the technology chosen for trust anchor management shall be expected or required to pay any fee to any IPR holder for the right to implement, distribute, or operate a system which includes the chosen mandatory-to-implement solution.

### 5.3. General Applicability

The solution MUST provide the capability to maintain Trust Anchors in security-aware resolvers for any and all DNS zones.

### 5.4. Support Private Networks

The solution MUST support private networks with their own DNS hierarchy.

### 5.5. Detection of Stale Trust Anchors

The Trust Anchor Rollover solution MUST allow a validating security-aware resolver to be able to detect if the DNSKEY and/or DS RR(s) can no longer be updated given the current set of actual trust-anchors. In these cases, the resolver should inform the operator of the need to reestablish initial trust.

### 5.6. Manual Operations Permitted

The operator of a security-aware resolver may choose manual or automated rollover, but the rollover protocol must allow the implementation to support both automated and manual Trust Anchor Maintenance operations. Implementation of the rollover protocol is likely to be mandatory, but that’s out of scope for this requirements document.

### 5.7. Planned and Unplanned Rollovers

The solution MUST permit both planned (pre-scheduled) and unplanned (non-scheduled) rollover of Trust Anchors. Support for providing an Initial Trust Relationship is OPTIONAL.

### 5.8. Timeliness

Resource Records used as Trust Anchors SHOULD be able to be distributed to security-aware resolvers in a timely manner.

Security-aware resolvers need to acquire new and remove revoked DNSKEY and/or DS RRs that are being used as Trust Anchors for a zone such that no old RR is used as a Trust Anchor for long after the zone issues new or revokes existing RRs.

### 5.9. High Availability

Information about the zone administrator's view of the state of Resource Records used as Trust Anchors SHOULD be available in a trustworthy manner at all times to security-aware resolvers. Information about Resource Records that a zone administrator has invalidated and that are known to be used as Trust Anchors should be available in a trustworthy manner for a reasonable length of time.

### 5.10. New RR Types

If a Trust Anchor Rollover solution requires new RR types or protocol modifications, this should be considered in the evaluation of solutions. The working group needs to determine whether such changes are a good thing or a bad thing or something else.

### 5.11. Support for Trust Anchor Maintenance Operations

The Trust Anchor Rollover solution MUST support operations that allow a validating security-aware resolver to add a new Trust Anchor, delete an existing Trust Anchor, or replace an existing Trust Anchor with another.

### 5.12. Recovery from Compromise

The Trust Anchor Rollover solution MUST allow a security-aware resolver to be able to recover from the compromise of any of its configured Trust Anchors for a zone so long as at least one other key, which is known to have not been compromised, is configured as a Trust Anchor for that same zone at that resolver.

### 5.13. Non-Degrading Trust

The Trust Anchor Rollover solution MUST provide sufficient means to ensure authenticity and integrity so that the existing trust relation does not degrade by performing the rollover.

## 6. Security Considerations

This document defines overall requirements for an automated specification-based Trust Anchor Rollover solution for security-aware resolvers but specifically does not define the security mechanisms needed to meet these requirements.

## 7. Acknowledgements

This document reflects the majority opinion of the DNSEXT Working Group members on the topic of requirements related to DNSSEC trust anchor rollover. The contributions made by various members of the working group to improve the readability and style of this document are graciously acknowledged.

## 8. Normative References

[1] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

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

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

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

[5] Bradner, S., "Intellectual Property Rights in IETF Technology", RFC 3979, March 2005.

## Authors' Addresses

Howard Eland
Afilias Limited
300 Welsh Road
Building 3, Suite 105
Horsham, PA 19044
USA

EMail: heland@afilias.info

Russ Mundy
SPARTA, Inc.
7110 Samuel Morse Dr.
Columbia, MD 21046
USA

EMail: mundy@sparta.com

Steve Crocker
Shinkuro Inc.
1025 Vermont Ave, Suite 820
Washington, DC 20005
USA

EMail: steve@shinkuro.com

Suresh Krishnaswamy
SPARTA, Inc.
7110 Samuel Morse Dr.
Columbia, MD 21046
USA

EMail: suresh@sparta.com

## Full Copyright Statement



## Intellectual Property