DNS Extensions
Internet-Draft
Expires: June 17, 2004

O. Kolkman
RIPE NCC
J. Schlyter

E. Lewis
ARIN

December 18, 2003

DNSKEY RR Secure Entry Point Flag
draft-ietf-dnsext-keyrr-key-signing-flag-12

Status of this Memo

Copyright Notice

Abstract

With the Delegation Signer (DS) resource record the concept of a public key acting as a secure entry point has been introduced. During exchanges of public keys with the parent there is a need to differentiate secure entry point keys from other public keys in the DNSKEY resource record (RR) set. A flag bit in the DNSKEY RR is defined to indicate that DNSKEY is to be used as a secure entry point. The flag bit is intended to assist in operational procedures to correctly generate DS resource records, or to indicate what DNSKEYs are intended for static configuration. The flag bit is not to

be used in the DNS verification protocol. This document updates RFC 2535 and RFC 3445.

Table of Contents

1. Introduction

"All keys are equal but some keys are more equal than others" [6]

With the definition of the Delegation Signer Resource Record (DS RR) [5] it has become important to differentiate between the keys in the DNSKEY RR set that are (to be) pointed to by parental DS RRs and the other keys in the DNSKEY RR set. We refer to these public keys as Secure Entry Point (SEP) keys. A SEP key either used to generate a DS RR or is distributed to resolvers that use the key as the root of a trusted subtree[3].

In early deployment tests, the use of two (kinds of) key pairs for each zone has been prevalent. For one kind of key pair the private key is used to sign just the zone's DNSKEY resource record (RR) set. Its public key is intended to be referenced by a DS RR at the parent or configured statically in a resolver. The private key of the other kind of key pair is used to sign the rest of the zone's data sets. The former key pair is called a key-signing key (KSK) and the latter is called a zone-signing key (ZSK). In practice there have been usually one of each kind of key pair, but there will be multiples of each at times.

It should be noted that division of keys pairs into KSK's and ZSK's is not mandatory in any definition of DNSSEC, not even with the introduction of the DS RR. But, in testing, this distinction has been helpful when designing key roll over (key super-cession) schemes. Given that the distinction has proven helpful, the labels KSK and ZSK have begun to stick.

There is a need to differentiate the public keys for the key pairs that are used for key signing from keys that are not used key signing (KSKs vs ZSKs). This need is driven by knowing which DNSKEYs are to be sent for generating DS RRs, which DNSKEYs are to be distributed to resolvers, and which keys are fed to the signer application at the

appropriate time.

In other words, the SEP bit provides an in-band method to communicate a DNSKEY RR's intended use to third parties. As an example we present 3 use cases in which the bit is useful:

> The parent is a registry, the parent and the child use secured DNS queries and responses, with a preexisting trust-relation, or plain DNS over a secured channel to exchange the child's DNSKEY RR sets. Since a DNSKEY RR set will contain a complete DNSKEY RRset the SEP bit can be used to isolate the DNSKEYs for which a DS RR needs to be created.

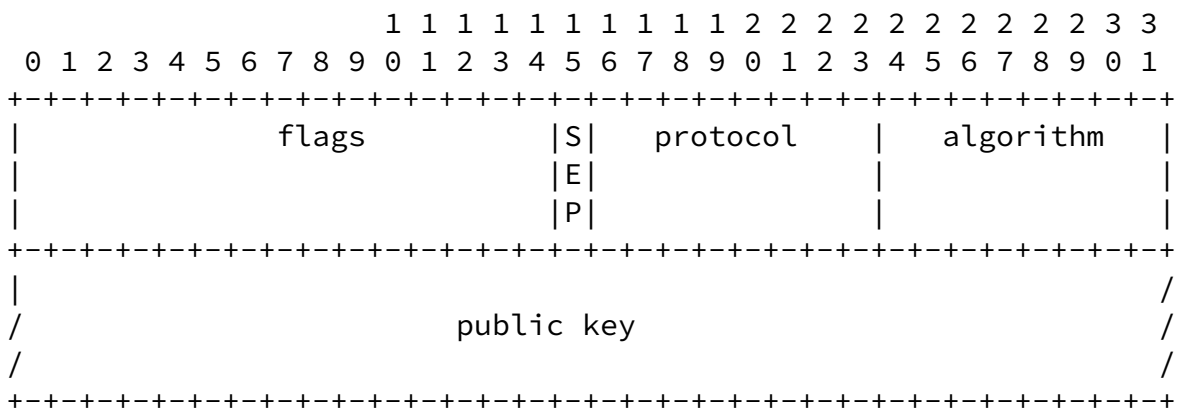
> An administrator has configured a DNSKEY as root for a trusted subtree into security aware resolver. Using a special purpose tool that queries for the KEY RRs from that domain's apex, the administrator will be able to notice the roll over of the trusted anchor by a change of the subset of KEY RRs with the DS flag set.
>
> A signer might use the SEP bit on the public key to determine which private key to use to exclusively sign the DNSKEY RRset and which private key to use to sign the other RRsets in the zone.

As demonstrated in the above examples it is important to be able to differentiate the SEP keys from the other keys in a DNSKEY RR set in the flow between signer and (parental) key-collector and in the flow between the signer and the resolver configuration. The SEP flag is to be of no interest to the flow between the verifier and the authoritative data store.

The reason for the term "SEP" is a result of the observation that the distinction between KSK and ZSK key pairs is made by the signer, a key pair could be used as both a KSK and a ZSK at the same time. To be clear, the term SEP was coined to lessen the confusion caused by the overlap. (Once this label was applied, it had the side effect of removing the temptation to have both a KSK flag bit and a ZSK flag bit.)

The key words "MAY","MAY NOT", "MUST", "MUST NOT", "REQUIRED", "RECOMMENDED", "SHOULD", and "SHOULD NOT" in this document are to be interpreted as described in RFC2119 [1].

2. The Secure Entry Point (SEP) Flag



DNSKEY RR Format

This document assigns the 15'th bit in the flags field as the secure entry point (SEP) bit. If the the bit is set to 1 the key is intended to be used as secure entry point key. One SHOULD NOT assign special meaning to the key if the bit is set to 0. Operators can recognize the secure entry point key by the even or odd-ness of the decimal representation of the flag field.

3. DNSSEC Protocol Changes

The bit MUST NOT be used during the resolving and verification process. The SEP flag is only used to provide a hint about the different administrative properties of the key and therefore the use of the SEP flag does not change the DNS resolution protocol or the resolution process.

4. Operational Guidelines

The SEP bit is set by the key-pair-generator and MAY be used by the zone signer to decide whether the public part of the key pair is to be prepared for input to a DS RR generation function. The SEP bit is recommended to be set (to 1) whenever the public key of the key pair

will be distributed to the parent zone to build the authentication chain or if the public key is to be distributed for static configuration in verifiers.

When a key pair is created, the operator needs to indicate whether the SEP bit is to be set in the DNSKEY RR. As the SEP bit is within the data that is used to compute the 'key tag field' in the SIG RR, changing the SEP bit will change the identity of the key within DNS. In other words, once a key is used to generate signatures, the setting of the SEP bit is to remain constant. If not, a verifier will not be able to find the relevant KEY RR.

When signing a zone, it is intended that the key(s) with the SEP bit set (if such keys exist) are used to sign the KEY RR set of the zone. The same key can be used to sign the rest of the zone data too. It is conceivable that not all keys with a SEP bit set will sign the DNSKEY RR set, such keys might be pending retirement or not yet in use.

When verifying a RR set, the SEP bit is not intended to play a role. How the key is used by the verifier is not intended to be a consideration at key creation time.

Although the SEP flag provides a hint on which public key is to be used as trusted root, administrators can choose to ignore the fact that a DNSKEY has its SEP bit set or not when configuring a trusted root for their resolvers.

Using the SEP flag a key roll over can be automated. The parent can use an existing trust relation to verify DNSKEY RR sets in which a new DNSKEY RR with the SEP flag appears.

5. Security Considerations

As stated in Section 3 the flag is not to be used in the resolution protocol or to determine the security status of a key. The flag is to be used for administrative purposes only.

No trust in a key should be inferred from this flag - trust MUST be inferred from an existing chain of trust or an out-of-band exchange.

Since this flag might be used for automating public key exchanges, we

think the following consideration is in place.

Automated mechanisms for roll over of the DS RR might be vulnerable to a class of replay attacks. This might happen after a public key exchange where a DNSKEY RR set, containing two DNSKEY RRs with the SEP flag set, is sent to the parent. The parent verifies the DNSKEY RR set with the existing trust relation and creates the new DS RR from the DNSKEY RR that the current DS RR is not pointing to. This key exchange might be replayed. Parents are encouraged to implement a replay defense. A simple defense can be based on a registry of keys that have been used to generate DS RRs during the most recent roll over. These same considerations apply to entities that configure keys in resolvers.

6. IANA Considerations

The flag bits in the DNSKEY RR are assigned by IETF consensus and registered in the DNSKEY Flags registry (created by [4]). This document assigns the 15th bit in the DNSKEY RR as the Secure Entry Point (SEP) bit.

7. Internationalization Considerations

Although SEP is a popular acronym in many different languages, there are no internationalization considerations.

8. Acknowledgments

The ideas documented in this document are inspired by communications we had with numerous people and ideas published by other folk. Among others Mark Andrews, Rob Austein, Miek Gieben, Olafur Gudmundsson, Daniel Karrenberg, Dan Massey, Scott Rose, Marcos Sanz and Sam Weiler have contributed ideas and provided feedback.

This document saw the light during a workshop on DNSSEC operations hosted by USC/ISI in August 2002.

Normative References

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

[2] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[3] Lewis, E., "DNS Security Extension Clarification on Zone Status", RFC 3090, March 2001.

[4] Weiler, S., "Legacy Resolver Compatibility for Delegation Signer", draft-ietf-dnsext-dnssec-2535typecode-change-05 (work in progress), October 2003.

Informative References

[5] Gudmundsson, O., "Delegation Signer Resource Record", draft-ietf-dnsext-delegation-signer-15 (work in progress), June 2003.

[6] Orwell, G. and R. Steadman (illustrator), "Animal Farm; a Fairy Story", ISBN 0151002177 (50th anniversary edition), April 1996.

Authors' Addresses

Olaf M. Kolkman
RIPE NCC
Singel 256
Amsterdam 1016 AB
NL

Phone: +31 20 535 4444
EMail: olaf@ripe.net
URI: http://www.ripe.net/

Jakob Schlyter
Karl Gustavsgatan 15
Goteborg SE-411 25
Sweden

EMail: jakob@schlyter.se

Edward P. Lewis
ARIN
3635 Concorde Parkway Suite 200
Chantilly, VA 20151
US

Phone: +1 703 227 9854
EMail: edlewis@arin.net
URI: http://www.arin.net/

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.