Domain Name System Operations Working Group G. Barwood
Internet-Draft
Intended status: Standards Track 22 May 2010

DNS Transport
draft-barwood-dnsop-ds-publish-00

Abstract

This document describes a new resource record type that allows a child zone to publish the DS RRset.

Status of this Memo

Copyright Notice

1. Introduction

This document defines a new resource record that may be used to publish the DS RRset [RFC4034] in the child zone. A new resource record type is needed, because the DS RR appears only on the upper (parental) side of a delegation.

The mnenomic for the new resource record type is "CDS", which is intended to stand for "Child DS".

The DNSSEC DS RRset for a zone is defined by the child zone but stored in the parent zone. After creating a new key signing key, the child zone needs to update the parent zone.

There is currently no DNS protocol mechanism for accomplishing this. It is assumed that the DS RRset is transferred by some out-of-band mechanism.

In particular the CDS RR MAY be used to securely automate the rollover of the key signing key for a zone.

2. Definitions

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].

3. Resource Record Format

The wire and presentation format is identical to the DS record.

However no special processing is performed by servers or clients when serving or resolving.

The CDS record MUST be signed with a Key Signing Key, that is a key for which there is a DS record.

3. Usage

The CDS RRset MAY be used by the parent zone to create or update the DS RRset. The parent zone MAY periodically check the child zone to see if the CDS RRset has changed. No notification mechanism is defined in this document, although a notification mechanism might be useful.

The parent zone SHOULD authenticate [RFC4033] the CDS RRset if possible, using the current DS RRset. If the authentication succeeds, or yields Insecure, extra security checks MAY be performed. If the authentication fails (the result is Bogus), extra security checks MUST be performed. This corresponds to a situation where the child zone has lost the secret key(s) for the zone, and needs to reset the parent DS

RRset.

If the CDS RRset does not exist, the parent MUST take no action. Specifically it MUST NOT delete the existing DS RRset, unless stringent out-of-band security checks confirm that this is required.

To mitigate situations where a key signing key has been compromised, the parent zone MAY take extra security measures, for example informing (by email) the zone administrator of the change, and delaying the acceptance of the new DS RRset for some period of time. However the precise out-of-band measures that a parent zone SHOULD take are outside the scope of this document.

4. IANA Considerations

IANA is requested to assign the DNS Resource Record Type code for the CDS record.

5. Security considerations

This document is entirely concerned with security considerations.

6. Acknowledgements

This document was created following discussion on automation of KSK rollover on the DNS Extensions Working Group mailing list.

The restriction on the signing key is due to Olafur Gudmundsson.

7. Normative References

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

[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.

Author's Address

George Barwood
33 Sandpiper Close
Gloucester
GL2 4LZ
United Kingdom

EMail: george.barwood@blueyonder.co.uk