Domain Name System Operations Working Group
Internet-Draft
Intended status: Standards Track

G. Barwood

03 July 2010

DNS Transport
draft-barwood-dnsop-ds-publish-01

Abstract

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

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 3, 2011.

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.

A new resource record type is preferred to using flags in the DNSKEY RRset. It allows the DS to be published without revealing the public key, delaying the time at which an attacker can start cryptanalysis; the size of the DNSKEY RRset is not changed, which avoids potential transport problems with large responses; and it allows arbitrary DS records to be published which may have no corresponding DNSKEY, which might be useful in future for defining transport parameters.

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 that has the Secure Entry Point flag set.

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. The child zone MAY send a NOTIFY message

[RFC1996] to a name server for the parent zone to expidite the process.

The parent zone SHOULD attempt to authenticate [RFC4033] the CDS RRset. If the authentication succeeds or yields Insecure, extra security checks are not normally necessary, but MAY be performed according to the parent zone policy. If the authentication fails (the result is Bogus), no action is taken, other than appropriate alerts to inform operators or administrators that there is a problem.

The parent zone SHOULD check that the signing key(s) have the Secure Entry Point flag set.

The parent zone SHOULD ensure that old versions of the CDS RRset do not overwrite newer versions, which can occur if there is a delay updating secondary name servers for the child zone. This MAY be accomplished by checking that the signature inception in the RRSIG has increased.

If the CDS RRset does not exist, the parent MUST take no action. Specifically it MUST NOT delete the existing DS RRset.

If the child zone loses the secret key(s) for the zone, and needs to reset the parent DS RRset, this must be accomplished by an out-of-band mechanism not defined here.

To mitigate situations where a key signing key has been compromised, the parent zone MAY take extra security measures, for example informing (by email or other methods) 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 Operations Working Group mailing list.

Thanks to the people who provided review and suggestions:
Mark Andrews, Richard Doty, Olafur Gudmundsson, Shane Kerr,
Stephan Lagerholm, Chris Thompson.

7. Normative References

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

[RFC1996] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY)", RFC 1996, August 1996.

[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