Internet Engineering Task Force (IETF)
Request for Comments: 7344
Category: Informational
ISSN: 2070-1721

W. Kumari
Google
O. Gudmundsson
OGUD Consulting
G. Barwood

September 2014

Automating DNSSEC Delegation Trust Maintenance

Abstract

This document describes a method to allow DNS Operators to more easily update DNSSEC Key Signing Keys using the DNS as a communication channel. The technique described is aimed at delegations in which it is currently hard to move information from the Child to Parent.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7344.

Table of Contents

1. Introduction

The first time a DNS Operator signs a zone, they need to communicate the keying material to their Parent through some out-of-band method to complete the chain of trust. Depending on the desires of the Parent, the Child might send their DNSKEY record, a DS record, or both.

Each time the Child changes the key that is represented in the Parent, the updated and/or deleted key information has to be communicated to the Parent and published in the Parent's zone. How this information is sent to the Parent depends on the relationship the Child has with the Parent. In many cases this is a manual process -- and not an easy one. For each key change, there may be up to two interactions with the Parent. Any manual process is susceptible to mistakes and/or errors. In addition, due to the annoyance factor of the process, Operators may avoid changing keys or skip needed steps to publish the new DS at the Parent.

DNSSEC provides data integrity to information published in DNS; thus, DNS publication can be used to automate maintenance of delegation information. This document describes a method to automate publication of subsequent DS records after the initial one has been published.

Readers are expected to be familiar with DNSSEC, including [RFC4033], [RFC4034], [RFC4035], [RFC5011], and [RFC6781].

This document outlines a technique in which the Parent periodically (or upon request) polls its signed Children and automatically publishes new DS records. To a large extent, the procedures this document follows are as described in [RFC6781], Section 4.1.2.

This technique is designed to be friendly both to fully automated tools and humans. Fully automated tools can perform all the actions needed without human intervention and thus can monitor when it is safe to move to the next step.

The solution described in this document only allows transferring information about DNSSEC keys (DS and DNSKEY) from the Child to the Parental Agent. It lists exactly what the Parent should publish and allows for publication of standby keys. A different protocol, [CPSYNC-DNS], can be used to maintain other important delegation information, such as NS and glue records. These two protocols have been kept as separate solutions because the problems are fundamentally different and a combined solution is overly complex.

This document describes a method for automating maintenance of the delegation trust information and proposes a polled/periodic trigger for simplicity. Some users may prefer a different trigger, for example, a button on a web page, a REST interface, or a DNS NOTIFY. These alternate additional triggers are not discussed in this document.

This proposal does not include all operations needed for the maintenance of DNSSEC key material, specifically the initial introduction or complete removal of all keys. Because of this, alternate communications mechanisms must always exist, potentially introducing more complexity.

1.1. Terminology

The terminology we use is defined in this section. The highlighted roles are as follows:

- Child: The entity on record that has the delegation of the domain from the Parent.
- Parent: The domain in which the Child is registered.
- Child DNS Operator: The entity that maintains and publishes the zone information for the Child DNS.
- Parental Agent: The entity that the Child has a relationship with to change its delegation information.
- Provisioning System: A system that the Operator of the master DNS server operates to maintain the information published in the DNS. This includes the systems that sign the DNS data.
- CDS/CDNSKEY: This notation refers to CDS and/or CDNSKEY, i.e., one or both.

1.2. Requirements Notation

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

2. Background

2.1. DNS Delegations

DNS operation consists of delegations of authority. For each delegation, there are (most of the time) two parties: the Parent and the Child.

The Parent publishes information about the delegations to the Child; for the name servers, it publishes an NS [RFC1035] Resource Record Set (RRset) that lists a hint for name servers that are authoritative for the Child. The Child also publishes an NS RRset, and this set is the authoritative list of name servers to the Child zone.

The second RRset the Parent sometimes publishes is the DS [RFC4034] set. The DS RRset provides information about the DNSKEY(s) that the Child has told the Parent it will use to sign its DNSKEY RRset. In DNSSEC, a trust relationship between zones is provided by the following chain:

Parent DNSKEY --> DS --> Child DNSKEY.

A prior proposal [AUTO-CPSYNC] suggested that the Child send an "update" to the Parent via a mechanism similar to DNS UPDATE. The main issue became: how does the Child find the actual Parental Agent/ server to send the update to? While that could have been solved via technical means, it failed to reach consensus. There is also a similar proposal in [PARENT-ZONES].

As the DS record can only be present at the Parent [RFC4034], some other method is needed to automate which DNSKEYs are picked to be represented in the Parent zone’s DS records. One possibility is to use flags in the DNSKEY record. If the Secure Entry Point (SEP) bit is set, this indicates that the DNSKEY is intended for use as a secure entry point. This DNSKEY signs the DNSKEY RRset, and the Parental Agent can calculate DS records based on that. But this fails to meet some operating needs, including the Child having no influence on what DS digest algorithms are used and DS records that can only be published for keys that are in the DNSKEY RRset; thus, this technique would not be compatible with Double-DS rollover [RFC6781].

2.2. Relationship between Parent and Child DNS Operators

In practical application, there are many different relationships between the Parent and Child DNS Operators. The type of relationship affects how the Child DNS Operator communicates with the Parent.

This section will highlight some of the different situations but is by no means a complete list.

Different communication paths:

- Direct/API: The Child can change the delegation information via automated/scripted means. The Extensible Provisioning Protocol (EPP) [RFC5730], used by many Top-Level Domains (TLDs), is an example of this. Other examples are web-based programmatic interfaces that Registrars make available to their Resellers.

- User Interface: The Child uses a web site set up by the Parental Agent for updating delegation information.

- Indirect: The communication has to be transmitted via an out-of-band mechanism between two parties, such as by email or telephone. This is common when the Child DNS Operator is neither the Child itself nor the Registrar for the domain, but a third party.

- Multi-step Combinations: The information flows through an intermediary. It is possible, but unlikely, that all the steps are automated via APIs and there are no humans involved.

A domain name holder (Child) may operate its own DNS servers or outsource the operation. While we use the word "Parent" as singular, a Parent can consist of a single entity or a composite of many discrete parts that have rules and roles. We refer to the entity that the Child corresponds with as the Parent.

An organization (such as an enterprise) may delegate parts of its name-space to be operated by a group that is not the same as that which operates the organization’s DNS servers. In some of these cases, the flow of information is handled either in an ad hoc manner or via some corporate mechanism; this can range from email to a fully automated operation.

2.2.1. Solution Space

This document is aimed at the cases in which there is a separation between the Child and Parent.

A further complication is when the Child DNS Operator is not the Child. There are two common cases of this:

a) The Parental Agent (e.g., Registrar) handles the DNS operation.

b) A third party takes care of the DNS operation.

If the Parental Agent is the DNS Operator, life is much easier; the Parental Agent can inject any delegation changes directly into the Parent's provisioning system. The techniques described below are not needed in the case when the Parental Agent is the DNS Operator.

In the case of a third-party DNS Operator, the Child either needs to relay changes in DNS delegation or give the Child DNS Operator access to its delegation/registration account.

Some Parents want the Child to express their DNSKEYs in the form of DS records, while others want to receive the DNSKEY records and calculate the DS records themselves. There is no consensus on which method is better; both have good reasons to exist. This solution is DS vs. DNSKEY agnostic and allows operation with either.

2.2.2. DNSSEC Key Change Process

After a Child DNS Operator first signs the zone, there is a need to interact with the Parent, for example, via a delegation account interface to upload or paste in the zone's DS information. This action of logging in through the delegation account user interface authenticates that the user is authorized to change delegation information for the Child published in the Parent zone. In the case where the Child DNS Operator does not have access to the registration account, the Child needs to perform the action.

At a later date, the Child DNS Operator may want to publish a new DS record in the Parent, either because they are changing keys or because they want to publish a standby key. This involves performing the same process as before. Furthermore, when this is a manual process with cut and paste, operational mistakes will happen -- or worse, the update action will not be performed at all.

The Child DNS Operator may also introduce new keys and can do so when old keys exist and can be used. The Child may also remove old keys, but this document does not support removing all keys. This is to avoid making signed zones unsigned. The Child may not enroll the initial key or introduce a new key when there are no old keys that can be used (without some additional out-of-band validation of the keys) because there is no way to validate the information.

3. CDS (Child DS) and CDNSKEY (Child DNSKEY) Record Definitions

This document specifies two new DNS resource records, CDS and CDNSKEY. These records are used to convey, from one zone to its Parent, the desired contents of the zone's DS resource record set residing in the Parent zone.

The CDS and CDNSKEY resource records are published in the Child zone and give the Child control of what is published for it in the parental zone. The Child can publish these manually, or they can be automatically maintained by DNS provisioning tools. The CDS/CDNSKEY RRset expresses what the Child would like the DS RRset to look like after the change; it is a "replace" operation, and it is up to the software that consumes the records to translate that into the appropriate add/delete operations in the provisioning systems (and in the case of CDNSKEY, to generate the DS from the DNSKEY). If neither CDS nor CDNSKEY RRset is present in the Child, this means that no change is needed.

3.1. CDS Resource Record Format

The wire and presentation format of the Child DS (CDS) resource record is identical to the DS record [RFC4034]. IANA has allocated RR code 59 for the CDS resource record via Expert Review [DNS-TRANSPORT]. The CDS RR uses the same registries as DS for its fields.

No special processing is performed by authoritative servers or by resolvers, when serving or resolving. For all practical purposes, CDS is a regular RR type.

3.2. CDNSKEY Resource Record Format

The wire and presentation format of the CDNSKEY ("Child DNSKEY") resource record is identical to the DNSKEY record. IANA has allocated RR code 60 for the CDNSKEY resource record via Expert Review. The CDNSKEY RR uses the same registries as DNSKEY for its fields.

No special processing is performed by authoritative servers or by resolvers, when serving or resolving. For all practical purposes, CDNSKEY is a regular RR type.

4. Automating DS Maintenance with CDS/CDNSKEY Records

CDS/CDNSKEY resource records are intended to be "consumed" by delegation trust maintainers. The use of CDS/CDNSKEY is OPTIONAL.

If the Child publishes either the CDS or the CDNSKEY resource record, it SHOULD publish both. If the Child knows which the Parent consumes, it MAY choose to only publish that record type (for example, some Children wish the Parent to publish a DS, but they wish to keep the DNSKEY "hidden" until needed). If the Child publishes both, the two RRsets MUST match in content.

4.1. CDS and CDNSKEY Processing Rules

If there is neither CDS nor CDNSKEY RRset in the Child, this signals that no change should be made to the current DS set. This means that, once the Child and Parent are in sync, the Child DNS Operator MAY remove all CDS and CDNSKEY resource records from the zone. The Child DNS Operator may choose to do this to decrease the size of the zone or to decrease the workload for the Parent (if the Parent receives no CDS/CDNSKEY records, it can go back to sleep). If it does receive a CDS or CDNSKEY RRset, it needs to check them against what is currently published (see Section 5).

The following acceptance rules are placed on the CDS and CDNSKEY resource records as follows:

- Location: MUST be at the Child zone apex.
- Signer: MUST be signed with a key that is represented in both the current DNSKEY and DS RRsets, unless the Parent uses the CDS or CDNSKEY RRset for initial enrollment; in that case, the Parent validates the CDS/CDNSKEY through some other means (see Section 6.1 and the Security Considerations).
- Continuity: MUST NOT break the current delegation if applied to DS RRset.

If any these conditions fail, the CDS or CDNSKEY resource record MUST be ignored, and this error SHOULD be logged.

5. CDS/CDNSKEY Publication

The Child DNS Operator publishes CDS/CDNSKEY RRset(s). In order to be valid, the CDS/CDNSKEY RRset(s) MUST be compliant with the rules in Section 4.1. When the Parent DS is in sync with the CDS/CDNSKEY RRset(s), the Child DNS Operator MAY delete the CDS/CDNSKEY RRset(s); the Child can determine if this is the case by querying for DS records in the Parent.

6. Parent-Side CDS/CDNSKEY Consumption

The CDS/CDNSKEY RRset(s) SHOULD be used by the Parental Agent to update the DS RRset in the Parent zone. The Parental Agent for this uses a tool that understands the CDS/CDNSKEY signing rules in Section 4.1, so it might not be able to use a standard validator.

The Parent MUST choose to use either CDNSKEY or CDS resource records as its default updating mechanism. The Parent MAY only accept either CDNSKEY or CDS, but it MAY also accept both so it can use the other in the absence of the default updating mechanism; it MUST NOT expect there to be both.

6.1. Detecting a Changed CDS/CDNSKEY

How the Parental Agent gets the CDS/CDNSKEY RRset may differ. Below are two examples of how this can take place.

Polling: The Parental Agent operates a tool that periodically checks each of the Children that has a DS record to see if there is a CDS or CDNSKEY RRset.

Pushing: The delegation user interface has a button {Fetch DS} that, when pushed, performs the CDS/CDNSKEY processing. If the Parent zone does not contain DS for this delegation, then the "push" SHOULD be ignored. If the Parental Agent displays the contents of the CDS/CDNSKEY to the user and gets confirmation that this represents their key, the Parental Agent MAY use this for initial enrollment (when the Parent zone does not contain the DS for this delegation).

In either case, the Parental Agent MAY apply additional rules that defer the acceptance of a CDS/CDNSKEY change. These rules may include a condition that the CDS/CDNSKEY remains in place and valid for some time period before it is accepted. It may be appropriate in the "Pushing" case to assume that the Child is ready and thus accept changes without delay.

6.1.1. CDS/CDNSKEY Polling

This is the only defined use of CDS/CDNSKEY resource records in this document. There are limits to the scalability of polling techniques; thus, some other mechanism is likely to be specified later that addresses CDS/CDNSKEY resource record usage in the situation where polling runs into scaling issues. Having said that, polling will work in many important cases such as enterprises, universities, and smaller TLDs. In many regulatory environments, the Registry is prohibited from talking to the Registrant. In most of these cases, the Registrant has a business relationship with the Registrar, so the Registrar can offer this as a service.

If the CDS/CDNSKEY RRset(s) do not exist, the Parental Agent MUST take no action. Specifically, it MUST NOT delete or alter the existing DS RRset.

6.1.2. Polling Triggers

It is assumed that other mechanisms will be implemented to trigger the Parent to look for an updated CDS/CDNSKEY RRset. As the CDS/CDNSKEY resource records are validated with DNSSEC, these mechanisms can be unauthenticated. As an example, a Child could telephone its Parent and request that it process the new CDS or CDNSKEY resource records, or an unauthenticated POST could be made to a web server (with rate-limiting).

Other documents can specify the trigger conditions.

6.2. Using the New CDS/CDNSKEY Records

Regardless of how the Parental Agent detected changes to a CDS/CDNSKEY RRset, the Parental Agent SHOULD use a DNSSEC validator to obtain a validated CDS/CDNSKEY RRset from the Child zone. A NOT RECOMMENDED exception to this is if the Parent performs some additional validation on the data to confirm that it is the "correct" key.

The Parental Agent MUST ensure that previous versions of the CDS/CDNSKEY RRset do not overwrite more recent versions. This MAY be accomplished by checking that the signature inception in the Resource Record Signature (RRSIG) for CDS/CDNSKEY RRset is later and/or that the serial number on the Child’s Start of Authority (SOA) is greater. This may require the Parental Agent to maintain some state information.

The Parental Agent MAY take extra security measures. For example, to mitigate the possibility that a Child’s Key Signing Key (KSK) has been compromised, the Parental Agent may inform (by email or other methods) the Child DNS Operator of the change. However, the precise out-of-band measures that a Parent zone takes are outside the scope of this document.

Once the Parental Agent has obtained a valid CDS/CDNSKEY RRset it MUST check the publication rules from Section 4.1. In particular, the Parental Agent MUST check the Continuity rule and do its best not to invalidate the Child zone. Once checked, if the information in the CDS/CDNSKEY and DS differ, it may apply the changes to the Parent zone. If the Parent consumes CDNSKEY, the Parent should calculate the DS before doing this comparison.

6.2.1. Parent Calculates DS

There are cases where the Parent wants to calculate the DS record due to policy reasons. In this case, the Child publishes CDNSKEY records, and the Parent calculates the DS records on behalf of the Children.

When a Parent operates in "calculate DS" mode, it can operate in one of two sub-modes:

full: The Parent only publishes DS records it calculates from DNSKEY records.

augment: The Parent will make sure there are DS records for the digest algorithm(s) it requires(s).

In the case where the Parent fetches the CDNSKEY RRset and calculates the DS, the resulting DS can differ from the CDS published by the Child. It is expected that the differences are only due to the different set of digest algorithms used.

7. IANA Considerations

IANA has assigned RR Type code 59 for the CDS resource record. This was done for a draft version whose content was later incorporated into this document [DNS-TRANSPORT]. This document is the reference for CDS RRtype.

IANA has assigned an RR Type for the CDNSKEY as described below:

Type: CDNSKEY

Value: 60

Meaning: DNSKEY(s) the Child wants reflected in DS

Reference: This document

8. Privacy Considerations

All of the information handled or transmitted by this protocol is public information published in the DNS.

9. Security Considerations

This work is for the normal case; when things go wrong there is only so much that automation can fix.

If the Child breaks DNSSEC validation by removing all the DNSKEYs that are represented in the DS set, its only repair actions are to contact the Parent or restore the DNSKEYs in the DS set.

In the event of a compromise of the server or system generating signatures for a zone, an attacker might be able to generate and publish new CDS/CDNSKEY resource records. The modified CDS/CDNSKEY records will be picked up by this technique and may allow the attacker to extend the effective time of his attack. If there is a delay in accepting changes to DS, as in [RFC5011], then the attacker needs to hope his activity is not detected before the DS in the Parent is changed. If this type of change takes place, the Child needs to contact the Parent (possibly via a Registrar web interface) and remove any compromised DS keys.

A compromise of the account with the Parent (e.g., Registrar) will not be mitigated by this technique, as the "new Registrant" can delete or modify the DS records at will.

While it may be tempting, the techniques specified in this document SHOULD NOT be used for initial enrollment of keys since there is no way to ensure that the initial key is the correct one. If it is used, strict rules for inclusion of keys -- such as hold-down times, challenge data inclusion, or similar -- MUST be used along with some kind of challenge mechanism. A Child cannot use this mechanism to go from signed to unsigned (publishing an empty CDS/CDNSKEY RRset means no change should be made in the Parent).

The CDS RR type should allow for enhanced security by simplifying the process. Since key change is automated, updating a DS RRset by other means may be regarded as unusual and subject to extra security checks.

As this introduces a new mechanism to update information in the Parent, it MUST be clear who is fetching the records and creating the appropriate records in the Parent zone. Specifically, some operations may use mechanisms other than what is described here. For example, a Registrar may assume that it is maintaining the DNSSEC key information in the Registry and may have this cached. If the Registry is fetching the CDS/CDNSKEY RRset, then the Registry and Registrar may have different views of the DNSSEC key material; the

result of such a situation is unclear. Therefore, this mechanism SHOULD NOT be used to bypass intermediaries that might cache information and, because of that, get the wrong state.

If there is a failure in applying changes in the Child zone to all DNS servers listed in either Parent or Child NS set, it is possible that the Parental Agent may get confused either because it gets different answers on different checks or CDS RR validation fails. In the worst case, the Parental Agent performs an action reversing a prior action after the Child signing system decides to take the next step in the key change process, resulting in a broken delegation.

DNS is a loosely coherent distributed database with local caching; therefore, it is important to allow old information to expire from caches before deleting DS or DNSKEY records. Similarly, it is important to allow new records to propagate through the DNS before use (see [RFC6781]).

It is common practice for users to outsource their DNS hosting to a third-party DNS provider. In order for that provider to be able to maintain the DNSSEC information, some users give the provider their Registrar login credentials (which obviously has negative security implications). Deploying the solution described in this document allows third-party DNS providers to maintain the DNSSEC information without Registrants giving their Registrar credentials, thereby improving security.

By automating the maintenance of the DNSSEC key information (and removing humans from the process), we expect to decrease the number of DNSSEC related outages, which should increase DNSSEC deployment.

10. Acknowledgements

We would like to thank a large number of folk, including Mark Andrews, Joe Abley, Jaap Akkerhuis, Roy Arends, Doug Barton, Brian Dickson, Paul Ebersman, Tony Finch, Jim Galvin, Paul Hoffman, Samir Hussain, Tatuya Jinmei, Olaf Kolkman, Stephan Lagerholm, Cricket Liu, Matt Larson, Marco Sanz, Antoin Verschuren, Suzanne Woolf, Paul Wouters, John Dickinson, Timothe Litt, and Edward Lewis.

Special thanks to Wes Hardaker for contributing significant text and creating the complementary (CSYNC) solution, and to Patrik Faltstrom, Paul Hoffman, Matthijs Mekking, Mukund Sivaraman, and Jeremy C. Reed for text and in-depth review. Brian Carpenter provided a good Gen-ART review.

There were a number of other folk with whom we discussed this document; apologies for not remembering everyone.

11. References

11.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[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.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", STD 74, RFC 5011, September 2007.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, December 2012.

11.2. Informative References

[AUTO-CPSYNC]
Mekking, W., "Automated (DNSSEC) Child Parent Synchronization using DNS UPDATE", Work in Progress, December 2010.

[CPSYNC-DNS]
Hardaker, W., "Child To Parent Synchronization in DNS", Work in Progress, July 2014.

[DNS-TRANSPORT]
Barwood, G., "DNS Transport", Work in Progress, June 2011.

[PARENT-ZONES]
Andrews, M., "Updating Parent Zones", Work in Progress, November 2013.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, August 2009.

[RFC5910] Gould, J. and S. Hollenbeck, "Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)", RFC 5910, May 2010.

Appendix A. RRR Background

RRR is our shorthand for the Registry/Registrar/Registrant model of Parent-Child relationships.

In the RRR world, the different parties are frequently from different organizations. In the single enterprise world, there are also organizational, geographical, and cultural separations that affect how information flows from a Child to the Parent.

Due to the complexity of the different roles and interconnections, automation of delegation information has not yet occurred. There have been proposals to automate this, in order to improve the reliability of the DNS. These proposals have not gained enough traction to become standards.

For example, in many of the TLD cases, there is the RRR model (Registry/Registrar/Registrant). The Registry operates DNS for the TLD, and the Registrars accept registrations and place information into the Registry's database. The Registrant only communicates with the Registrar; frequently, the Registry is not allowed to communicate with the Registrant. In that case, as far as the Registrant is concerned, the Registrar is the same entity as the Parent.

In many RRR cases, the Registrar and Registry communicate via EPP [RFC5730] and use the EPP DNSSEC extension [RFC5910]. In a number of Country Code TLDs (ccTLDs), there are other mechanisms in use as well as EPP, but in general, there seems to be a movement towards EPP usage when DNSSEC is enabled in the TLD.

Appendix B. CDS Key Rollover Example

This section shows an example on how CDS is used when performing a KSK rollover. This example will demonstrate the Double-DS rollover method from Section 4.1.2 of [RFC6781]. Other rollovers using CDNSKEY and double KSK are left as an exercise to the reader. The table below does not reflect the Zone Signing Keys (ZSKs) as they do not matter during KSK rollovers. The wait steps highlight what RRset needs to expire from caches before progressing to the next step.

Step	State	Parent DS	Child KSK	DNSKEY and CDS signer	Child CDS
	Beginning	A	A	A	
1	Add CDS	A	A	A	AB
Wait	for DS change	A	A	A	AB
2	Updated DS	AB	A	A	AB
Wait	> DS TTL	AB	A	A	AB
3	Actual	AB	B	B	AB
	Rollover				
Wait	> DNSKEY TTL	AB	B	B	AB
4	Child Cleanup	AB	B	B	B
5	Parent cleans	B	B	B	B
6	Optional CDS	B	B	B	
	delete				

Table 1: States

Authors' Addresses

Warren Kumari
Google
1600 Amphitheatre Parkway
Mountain View, CA 94043
US

EMail: warren@kumari.net

Olafur Gudmundsson
OGUD Consulting
3821 Village Park Dr.
Chevy Chase, MD 20815
US

EMail: ogud@ogud.com

George Barwood
33 Sandpiper Close
Gloucester GL2 4LZ
United Kingdom

EMail: george.barwood@blueyonder.co.uk