Internet Engineering Task Force (IETF)
Request for Comments: 9975
Updates: 7344, 7477
Category: Standards Track
ISSN: 2070-1721
P. Thomassen
SSE
May 2026

Clarifications on CDS/CDNSKEY and CSYNC Consistency

Abstract

Maintenance of DNS delegations requires occasional changes of the DS and NS record sets on the parent side of the delegation. For the case of DS records, "Automating DNSSEC Delegation Trust Maintenance" (RFC 7344) provides automation by allowing the child to publish CDS and/or CDNSKEY records holding the prospective DS parameters that the parent can ingest. Similarly, "Child-to-Parent Synchronization in DNS" (RFC 7477) specifies CSYNC records to indicate a desired update of the delegation’s NS (and glue) records. Parent-side entities (e.g., Registries and Registrars) can query these records from the child and, after validation, use them to update the parent-side Resource Record Sets (RRsets) of the delegation.

This document specifies under which conditions the target states expressed via CDS/CDNSKEY and CSYNC records are considered "consistent". Parent-side entities accepting such records from the child have to ensure that update requests retrieved from different authoritative nameservers satisfy these consistency requirements before taking any action based on them.

This document updates RFCs 7344 and 7477.

Status of This Memo

This is an Internet Standards Track document.

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). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9975.

Copyright Notice

Table of Contents

1. Introduction

[RFC7344] automates DNS Security Extensions (DNSSEC) delegation trust maintenance by having the child publish CDS and/or CDNSKEY records that describe the prospective DS parameters. Similarly, [RFC7477] specifies CSYNC records indicating a desired update of the delegation's NS and associated glue records. Parent-side entities (e.g., Registries and Registrars) can use these records to update the corresponding records of the delegation.

For ingesting CSYNC records, Section 3.1 of [RFC7477] advocates that Parental Agents limit queries to a single authoritative nameserver (as done in normal resolution). [RFC7344] (on CDS/CDNSKEY) has a corresponding section (Section 6.1 of [RFC7344]) that contains no provision for how specifically queries for these records should be done.

Retrieving records from just one authoritative server (e.g., by directing queries towards a trusted validating resolver) works well under ideal operating scenarios. However, problems may arise if CDS/CDNSKEY/CSYNC record sets are inconsistent across authoritative nameserver either because they are out of sync (e.g., during a Key Signing Key (KSK) rollover) or because they are not controlled by the same entity (e.g., in a multi-signer setup [RFC8901]).

In such cases, if CDS/CDNSKEY/CSYNC records are retrieved from one nameserver only ("naively", without a consistency check), each nameserver can unilaterally trigger an update of the delegation's DS or NS record set.

For example, a single provider in a multi-signer setup may (accidentally or maliciously) cause another provider's trust anchors and/or nameservers to be removed from the delegation. This can occur both when the multi-signer configuration is temporary (e.g., during a provider change) and when it is permanent (e.g., for redundancy). In any case, a single provider should not be in the position to remove any other provider's records from the delegation.

Similar breakage can occur when the delegation has lame nameservers, where an attacker may illegitimately initialize a DS record set and then manipulate the delegation's NS record set at will. More detailed examples are given in Appendix A.

For a CDS/CDNSKEY/CSYNC consumer, it is generally impossible to estimate the impact of a requested delegation update unless all of the child's authoritative nameservers are inspected. At the same time, applying an automated delegation update "MUST NOT break the current delegation" (per [RFC7344], Section 4.1), i.e., it must not hamper availability or validatability of the Child's resolution. As part of a more holistic treatment of the problem space, [DS-AUTOMATION] provides more-specific guidance on such safety checks.

Therefore, this document specifies that parent-side entities need to ensure that the updates indicated by CDS/CDNSKEY and CSYNC record sets are plausibly consistent across the child's nameservers before taking any action based on these records.

Readers are expected to be familiar with DNSSEC [RFC9364], in particular, [RFC4033], [RFC4034], [RFC4035], [RFC7344], and [RFC7477]. For an overview of related operational practices, refer to [RFC6781] and [RFC8901].

1.1. 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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

Multi-provider setup: A constellation where several providers independently operate authoritative DNS service for a domain, usually for purposes of redundancy. This includes setups both with and without DNSSEC.

Multi-signer setup: A multi-provider setup for a DNSSEC-enabled domain with multiple independent signing entities [RFC8901]. Such a setup may be permanent (for redundancy) or temporary (for continuity of DNSSEC operation while changing the provider of a domain that normally uses a single one).

Otherwise, the terminology in this document is as defined in [RFC7344].

2. Updates to RFCs 7344 and 7477

Section 4.1 of [RFC7344] lists acceptance rules for CDS/CDNSKEY records. This list is extended with the consistency requirements defined in this document. This document does not modify any other part of [RFC7344].

Sections 3.1 and 4.2 of [RFC7477] have logic for deciding from which nameserver to query CSYNC information. This logic is replaced with the CSYNC consistency requirements defined in this document.

3. Processing Requirements

Consistency requirements that apply equally to CDS/CDNSKEY and CSYNC are listed first; type-specific consistency criteria are described in separate subsections.

In order to determine plausible consistency of CDS/CDNSKEY or CSYNC RRsets across the child's nameservers, the Parental Agent MUST fetch all IP addresses for each nameserver hostname as listed in the Child's delegation from the Parent using a validating resolver, including any available glue records. Before acting on any CDS/

CDNSKEY or CSYNC record for the child, the Parental Agent MUST have established plausible consistency by querying all of these IP addresses for the record set(s) in question, as per the guidelines spelled out in the following subsections.

In all cases, consistency is REQUIRED across received responses only. (A NODATA response (see [RFC9499]) is a received response.)

When a response cannot be obtained from a given nameserver, the Parental Agent SHOULD attempt to obtain it at a later time, before concluding that the nameserver is permanently unreachable and removing it from consideration. A configurable retry schedule is RECOMMENDED to increase the likelihood of collecting data from all nameservers. An exponential back-off schedule (e.g., 5, 10, 20, 40, ... minutes) provides a balance between faster task completion while accommodating transient unreachability. To sidestep localized routing issues, the Parental Agent MAY also attempt contacting the nameserver from another network vantage point.

If an inconsistent state is encountered, the Parental Agent MUST abort the operation. Specifically, it MUST NOT delete or alter any existing RRset that would have been deleted or altered, and it MUST NOT create any RRsets that would have been created had the nameservers given consistent responses.

To accommodate transient inconsistencies (e.g., replication delays), implementations MAY be configurable to undertake a retry of the full process, repeating all queries (suggested default: enabled with exponential back-off).

Any pending queries can immediately be dequeued when encountering a response that confirms the status quo, either implicitly (NODATA) or explicitly (via a response that matches the current delegation state). This is because any subsequent responses could only confirm that nothing needs to happen or give an inconsistent result in which case nothing needs to happen. The parent may apply local policy in determining whether the requested update is consistent or not with the status quo, as illustrated in the type-specific sections below. In any case, queries may be continued across all nameservers for reporting purposes.

Existing requirements for ensuring integrity remain in effect. In particular, DNSSEC signatures MUST be requested and validated for all queries unless otherwise noted.

3.1. CDS and CDNSKEY

When retrieving a Child’s CDS/CDNSKEY RRset for DNSSEC delegation trust maintenance, the Parental Agent, knowing both the Child zone name and its NS hostnames, MUST ascertain that queries are made against all nameservers listed in the Child’s delegation from the Parent. The Parental Agent MUST also ensure that each key referenced in any of the received answers is also referenced in all other received responses (subject to the CDS digest type considerations below) or that responses consistently indicate a request for removal of the entire DS RRset ([RFC8078], Section 6).

In other words, CDS/CDNSKEY records at the Child zone apex must be fetched directly from each reachable authoritative server as determined by the delegation’s NS record set. When a key is referenced in an eligible CDS record set but not the CDNSKEY record set (or vice versa), or returned by one nameserver but is missing from at least one other nameserver’s answer, the CDS/CDNSKEY state MUST be considered inconsistent. Similarly, the state MUST be considered inconsistent if there is a CDS or CDNSKEY response that indicates a removal request for the DS RRset whereas another response indicates no change (NODATA) or a DS update.

CDS records MUST be considered for consistency only when their digest type field is designated as "MUST" in the "Implement for DNSSEC Delegation" column of the "Digest Algorithms" registry [DS-IANA]). Consistency of records with other digest types need not be verified, especially when the digest type is unsupported; such records can be ignored.

Independently of this, the parent may, as a matter of local policy, make its own choice regarding the hash digest types used when publishing a DS RRset (notwithstanding the requirements specified in [DS-IANA]). (The set of keys referenced in the DS RRset is not up to local policy. Only if all keys from the CDNSKEY RRset and eligible CDS records are included is the DS RRset considered consistent.)

During initial DS provisioning (DNSSEC bootstrapping), conventional DNSSEC validation for CDS/CDNSKEY responses is not (yet) available; in this case, authenticated bootstrapping [RFC9615] should be used.

3.2. CSYNC

A CSYNC-based workflow generally consists of:

1. querying the CSYNC (and possibly SOA) record to determine which data records shall be synchronized from child to parent, and

2. querying for these data records (e.g., NS) before placing them in the parent zone.

If the below conditions are not met during these steps, the CSYNC state MUST be considered inconsistent.

When querying the CSYNC record, the Parental Agent MUST ascertain that queries are made against all nameservers listed in the Child’s delegation from the Parent and ensure that the record’s immediate flag and type bitmap are equal across received responses.

The CSYNC record’s SOA serial field and soaminimum flag might legitimately differ across nameservers (such as in multi-provider setups); thus, equality is not required across responses. Instead, for a given response, processing of these values MUST occur with respect to the SOA record as obtained from the same nameserver. If the resulting per-nameserver assessments of whether the update is permissible do not all agree, the CSYNC state MUST be considered inconsistent.

Further, when retrieving the data record sets as indicated in the CSYNC record (such as NS or A/AAAA records), the Parental Agent MUST ascertain that all queries are made against all nameservers from which a CSYNC record was received and ensure that all of them return responses with equal rdata sets (including cases where all are empty).

As an example of local policy, the parent may choose to accept glue records only for in-domain or sibling NS hostnames [RFC9499].

Other CSYNC processing rules from Section 3 of [RFC7477] remain in place without modification. For example, when the NS type flag is present, associated NS processing has to occur before potential glue updates to ensure that glue addresses match the right set of nameservers. Also, when the type bitmap contains the A/AAAA flags, corresponding address queries are only to be sent for NS hostnames that are in bailiwick, while out-of-bailiwick NS records are ignored. Refer to Sections 3.2.2 and 4.3 of [RFC7477] for more details.

CSYNC-based updates may cause validation or even insecure resolution to break (e.g., by changing the delegation to a set of nameservers that do not serve required DNSKEY records or do not know the zone at all). Parental Agents SHOULD check that CSYNC-based updates, if applied, do not break the delegation.

4. IANA Considerations

This document has no IANA actions.

5. Security Considerations

The level of rigor mandated by this document is needed to prevent publication of half-baked DS or delegation NS RRsets (authorized only under an insufficient subset of authoritative nameservers), ensuring that a single operator cannot unilaterally modify the delegation (add or remove trust anchors or nameservers) when other operators are present. This applies both when the setup is intentional and when it is unintentional (such as in the case of lame-delegation hijacking).

As a consequence, the delegation’s records can only be modified when zones are synchronized across operators, unanimously reflecting the domain owner’s intentions. Both availability and integrity of the domain’s DNS service benefit from this policy.

In order to resolve situations in which consensus about child zone contents cannot be reached (e.g., because one of the nameserver operators is uncooperative), Parental Agents SHOULD continue to accept DS and NS/glue update requests from the domain owner via an authenticated out-of-band channel (such as Extensible Provisioning Protocol (EPP) [RFC5730]), irrespective of the adoption of automated delegation maintenance. Availability of such an interface also enables recovery from a situation where the private key is no longer available for signing the CDS/CDNSKEY or CSYNC records in the child zone.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005, <https://www.rfc-editor.org/info/rfc4034>.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005, <https://www.rfc-editor.org/info/rfc4035>.

[RFC5730] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, DOI 10.17487/RFC5730, August 2009, <https://www.rfc-editor.org/info/rfc5730>.

[RFC7344] Kumari, W., Gudmundsson, O., and G. Barwood, "Automating DNSSEC Delegation Trust Maintenance", RFC 7344, DOI 10.17487/RFC7344, September 2014, <https://www.rfc-editor.org/info/rfc7344>.

[RFC7477] Hardaker, W., "Child-to-Parent Synchronization in DNS", RFC 7477, DOI 10.17487/RFC7477, March 2015, <https://www.rfc-editor.org/info/rfc7477>.

[RFC8078] Gudmundsson, O. and P. Wouters, "Managing DS Records from the Parent via CDS/CDNSKEY", RFC 8078, DOI 10.17487/RFC8078, March 2017, <https://www.rfc-editor.org/info/rfc8078>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC9364] Hoffman, P., "DNS Security Extensions (DNSSEC)", BCP 237, RFC 9364, DOI 10.17487/RFC9364, February 2023, <https://www.rfc-editor.org/info/rfc9364>.

[RFC9615] Thomassen, P. and N. Wisiol, "Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone’s Operator", RFC 9615, DOI 10.17487/RFC9615, July 2024, <https://www.rfc-editor.org/info/rfc9615>.

6.2. Informative References

[DS-AUTOMATION] Sheng, S. and P. Thomassen, "Operational Recommendations for DNSSEC Delegation Signer (DS) Automation", Work in Progress, Internet-Draft, draft-ietf-dnsop-ds-automation-09, 22 May 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-dnsop-ds-automation-09>.

[DS-IANA] IANA, "DNSSEC Delegation Signer (DS) Resource Record (RR) Type Digest Algorithms", <https://www.iana.org/assignments/ds-rr-types>.

[LAME1] Akiwate, G., Jonker, M., Sommese, R., Foster, I., Voelker, G. M., Savage, S., and K. Claffy, "Unresolved Issues: Prevalence, Persistence, and Perils of Lame Delegations", IMC ’20: Proceedings of the ACM Internet Measurement Conference, pp. 281-294, DOI 10.1145/3419394.3423623, 27 October 2020, <https://doi.org/10.1145/3419394.3423623>.

[LAME2] Akiwate, G., Savage, S., Voelker, G. M., and K. Claffy, "Risky BIZness: risks derived from registrar name management", IMC ’21: Proceedings of the 21st ACM Internet Measurement Conference, pp. 673-686, DOI 10.1145/3487552.3487816, 2 November 2021, <https://doi.org/10.1145/3487552.3487816>.

[RFC6781] Kolkman, O., Mekking, W., and R. Gieben, "DNSSEC Operational Practices, Version 2", RFC 6781, DOI 10.17487/RFC6781, December 2012, <https://www.rfc-editor.org/info/rfc6781>.

[RFC8901] Huque, S., Aras, P., Dickinson, J., Vcelak, J., and D. Blacka, "Multi-Signer DNSSEC Models", RFC 8901, DOI 10.17487/RFC8901, September 2020, <https://www.rfc-editor.org/info/rfc8901>.

[RFC9499] Hoffman, P. and K. Fujiwara, "DNS Terminology", BCP 219, RFC 9499, DOI 10.17487/RFC9499, March 2024, <https://www.rfc-editor.org/info/rfc9499>.

Appendix A. Failure Scenarios due to Inconsistencies

The following scenarios are informative examples of how things can go wrong when consistency is not enforced by the parent during CDS/CDNSKEY/CSYNC processing. Other scenarios that cause similar (or perhaps even more) harm may exist.

The common feature of these scenarios is that if one nameserver steps out of line and the parent is not careful, DNS resolution and/or validation will break down. When several DNS providers are involved, this undermines the very guarantees of operator independence that multi-provider configurations are intended to provide.

A.1. DS Breakage due to Replication Lag

If an authoritative nameserver is lagging behind during a key rollover, the parent may see different CDS/CDNSKEY RRsets depending on the nameserver contacted. This may cause old and new DS RRsets to be deployed in an alternating fashion and without the awareness of the zone maintainer, who may then inadvertently break the chain of trust by prematurely removing a DNSKEY still referenced by a (stale) CDS/CDNSKEY RRset.

While foreseen in Section 6.2 of [RFC7344], the solution specified there requires parents to keep state on CDS/CDNSKEY RRsets. This document achieves the same without this burden and, in case the parent reports consistency errors downstream, can also help detection of the child-side replication issue by the operator.

A.2. Escalation of Lame Delegation Takeover

A delegation may include a nonexistent NS hostname, for example, due to a typo or the nameserver’s domain registration having expired. (Re-)registering such a non-resolvable nameserver domain allows a third party to run authoritative DNS service for all domains delegated to that NS hostname, serving responses different from the legitimate ones.

This strategy for hijacking (at least part of the) DNS traffic and spoofing responses is not new but is surprisingly common [LAME1] [LAME2]. It is also known that DNSSEC reduces the impact of such an attack, as validating resolvers will reject illegitimate responses due to lack of signatures consistent with the delegation’s DS records.

On the other hand, if the delegation is not protected by DNSSEC, the rogue nameserver is not only able to serve unauthorized responses without detection: it is even possible for the attacker to escalate the nameserver takeover to a full domain takeover.

In particular, the rogue nameserver can publish CDS/CDNSKEY records. If those are processed by the parent without ensuring consistency with other authoritative nameservers, the delegation will, with some patience, get secured with the attacker’s DNSSEC keys. Of course, as the parent’s query (or sometimes queries) need to hit the attacker’s nameserver, this requires some statistical luck, but, eventually, it will succeed. As responses served by the remaining legitimate nameservers are not signed with these keys, validating resolvers will start rejecting them.

Once DNSSEC is established, the attacker can use CSYNC to remove other nameservers from the delegation at will (and potentially add new ones under their control) or change glue records to point to the attacker’s nameservers. This enables the attacker to position itself as the only party providing authoritative DNS service for the victim domain, significantly augmenting the attack’s impact.

A.3. Multi-Provider (Permanent Multi-Signer)

A.3.1. DS Breakage

While performing a key rollover and adjusting the corresponding CDS/CDNSKEY records, a provider could accidentally publish CDS/CDNSKEY records that only include its own keys.

When the parent happens to retrieve the records from a nameserver controlled by this provider, the other providers' DS records would be removed from the delegation. As a result, the zone is broken (at least for some queries).

A.3.2. NS Breakage

A similar scenario affects the CSYNC record, which is used to update the delegation's NS record set at the parent. For example, the issue occurs when a provider accidentally includes only their own set of hostnames in the local NS record set or publishes an otherwise flawed NS record set.

If the parent then observes a CSYNC signal and fetches the flawed NS record set without ensuring consistency across nameservers, the delegation may be updated in a way that breaks resolution or silently reduces the multi-provider setup to a single-provider setup.

A.4. Bogus Provider Change (Temporary Multi-Signer)

Transferring DNS service for a domain name from one (signing) DNS provider to another, without going insecure, necessitates a brief period during which the domain is operated in multi-signer mode. First, the providers include each other's signing keys as DNSKEY and CDS/CDNSKEY records in their own copy of the zone. Once the parent learns about the updated CDS/CDNSKEY record set at the old provider, the delegation's DS record set is updated. Then, after waiting for cache expiration, the new provider's NS hostnames can be added to the zone's NS record set so that queries start balancing across both providers. To conclude the handover, the old provider is removed by inverting these steps with swapped roles.

The multi-signer phase of this process breaks when the new provider, perhaps unaware of the situation and its intricacies, fails to include the old provider's keys in the DNSKEY (and CDS/CDNSKEY) record sets. One obvious consequence is that whenever the resolver happens to retrieve the DNSKEY record set from the new provider, the old provider's RRSIGs no longer validate, causing SERVFAIL to be returned.

However, an even worse consequence can occur when the parent performs their next CDS/CDNSKEY scan. The incorrect CDS/CDNSKEY record set is fetched from the new provider and used to update the delegation's DS record set. As a result, the old provider (who still appears in the delegation) is prematurely removed from the domain's DNSSEC chain of trust. The new DS record set authenticates the new provider's DNSKEYs only, and DNSSEC validation fails for all answers served by the old provider.

Acknowledgments

In order of first contribution or review: Viktor Dukhovni, Wes Hardaker, Libor Peltan, Oli Schacher, David Blacka, Charlie Kaufman, Michael Bauland, Patrick Mevzek, Joe Abley, Ondej Caletka, Ondej Sur, Mohamed Boucadair, Vijay Gurbani, Gorry Fairhurst, Paul Wouters, Andy Newton, Mike Bishop, and Warren Kumari.

Author's Address

Peter Thomassen
SSE - Secure Systems Engineering GmbH
Hauptstrae 3
10827 Berlin
Germany
Email: pth@systemsecurity.com