How DNSSEC Works

The domain name system (DNS) is the phone book of the Internet: it tells computers where to send and retrieve information. Unfortunately, it also accepts any address given to it, no questions asked.

Email servers use DNS to route their messages, which means they're vulnerable to security issues in the DNS infrastructure. In September 2014, just one year ago, researchers at CMU found email supposed to be sent through Yahoo!, Hotmail, and Gmail servers routing instead through rogue mail servers. Attackers were exploiting a decades-old vulnerability in the Domain Name System (DNS)—it doesn't check for credentials before accepting an answer.

CLOUDFLARE

A Gentle Introduction to DNSSEC

DNSSEC creates a secure domain name system by adding cryptographic signatures to existing DNS records. These digital signatures are stored in DNS name servers alongside common record types like A, AAAA, MX, CNAME, etc. By checking its associated signature, you can verify that a requested DNS record comes from its authoritative name server and wasn't altered en-route, opposed to a fake record injected in a man-in-the-middle attack.

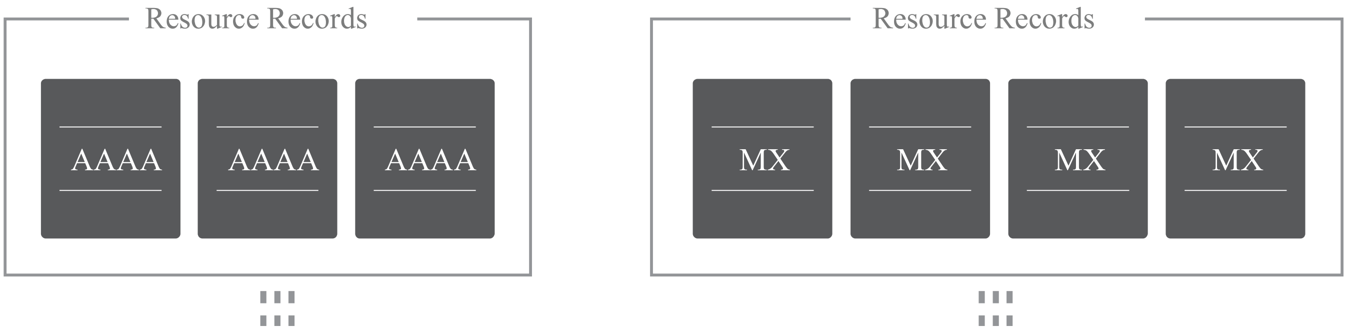
To facilitate signature validation, DNSSEC adds a few new DNS record types:

- RRSIG - Contains a cryptographic signature
- DNSKEY - Contains a public signing key
- DS - Contains the hash of a DNSKEY record
- NSEC and NSEC3 - For explicit denial-of-existence of a DNS record
- CDNSKEY and CDS - For a child zone requesting updates to DS record(s) in the parent zone.

The interaction between RRSIG, DNSKEY, and DS records, as well as how they add a layer of trust on top of DNS, is what we'll be talking about in this article.

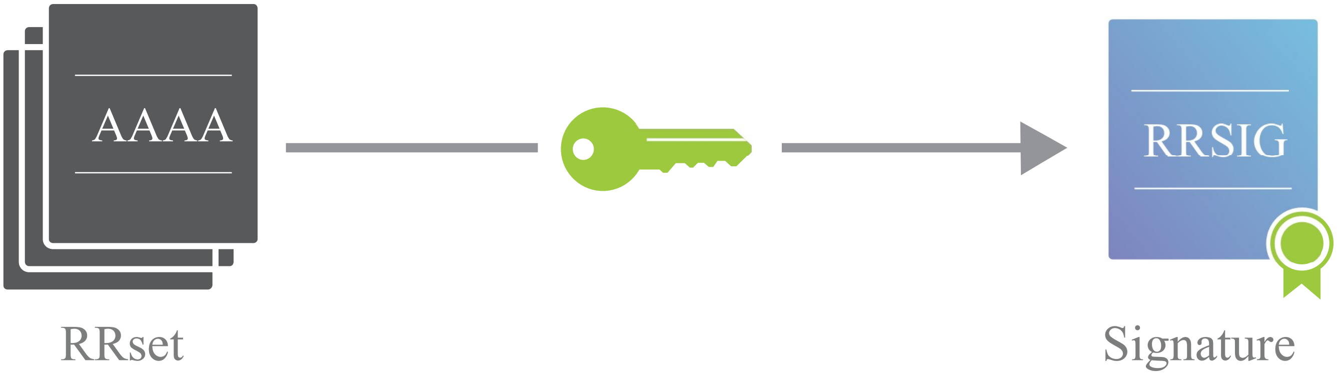
RRsets

The first step towards securing a zone with DNSSEC is to group all the records with the same type into a resource record set (RRset). For example, if you have three AAAA records in your zone on the same label (i.e. label.example.com), they would all be bundled into a single AAAA RRset.



Zone-Signing Keys

Each zone in DNSSEC has a zone-signing key pair (ZSK): the private portion of the key digitally signs each RRset in the zone, while the public portion verifies the signature. To enable DNSSEC, a zone operator creates digital signatures for each RRset using the private ZSK and stores them in their name server as RRSIG records. This is like saying, “These are my DNS records, they come from my server, and they should look like this.”

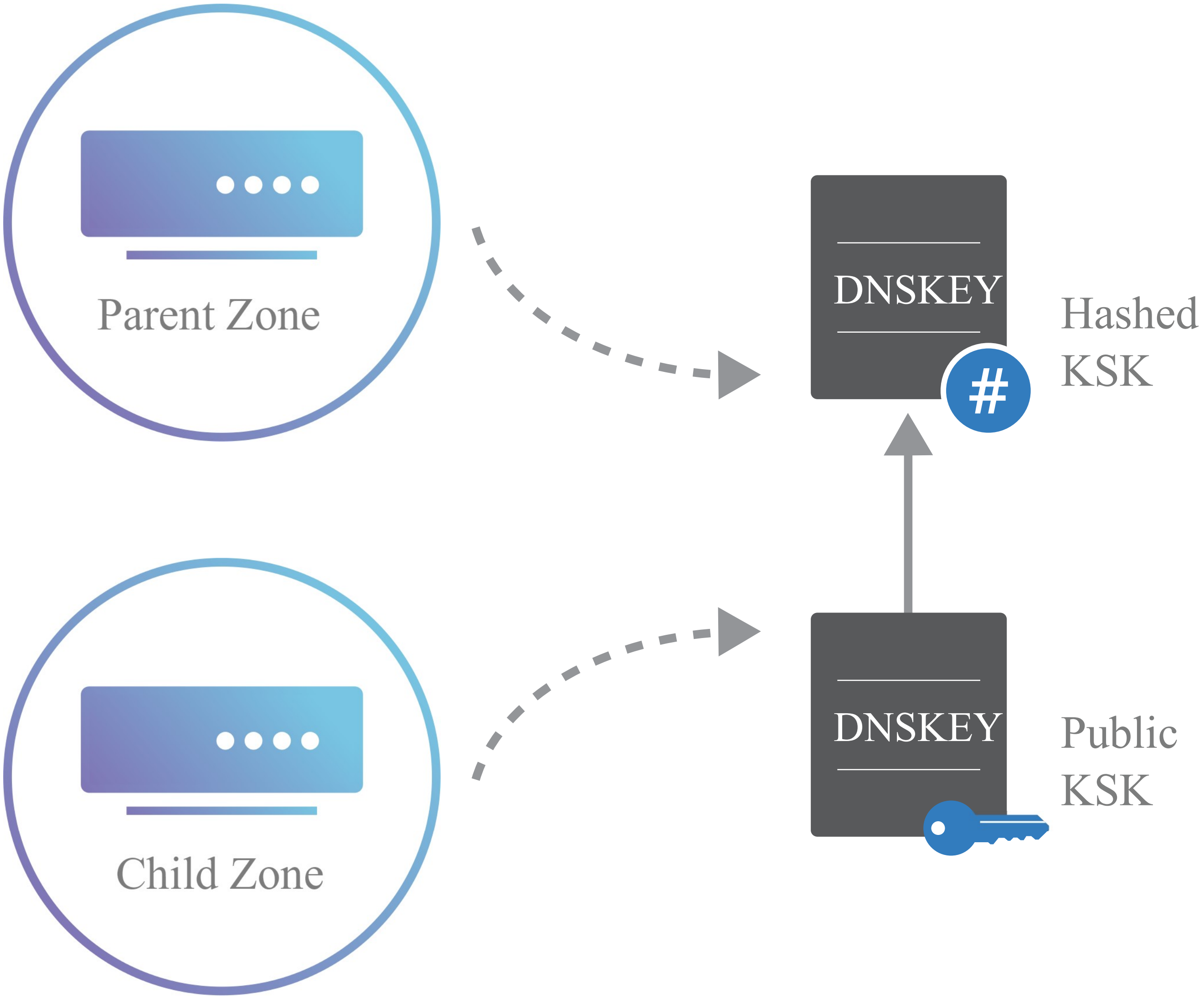


However, these RRSIG records are useless unless DNS resolvers have a way of verifying the signatures. The zone operator also needs to make their public ZSK available by adding it to their name server in a DNSKEY record.

When a DNSSEC resolver requests a particular record type (e.g., AAAA), the name server also returns the corresponding RRSIG. The resolver can then pull the DNSKEY record containing the public ZSK from the name server. Together, the RRset, RRSIG, and public ZSK can validate the response.

Delegation Signer Records

DNSSEC introduces a delegation signer (DS) record to allow the transfer of trust from a parent zone to a child zone. A zone operator hashes the DNSKEY record containing the public KSK and gives it to the parent zone to publish as a DS record.



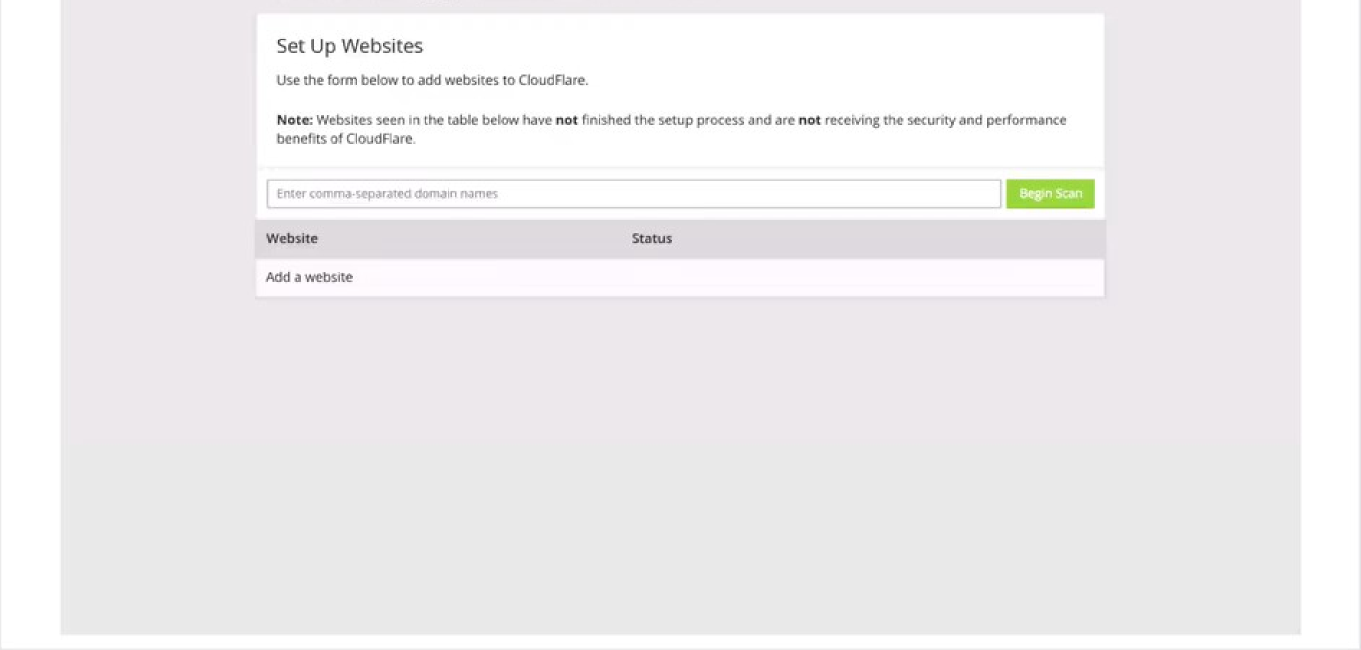
Every time a resolver is referred to a child zone, the parent zone also provides a DS record. This DS record is how resolvers know that the child zone is DNSSEC-enabled. To check the validity of the child zone's public KSK, the resolver hashes it and compares it to the DS record from the parent. If they match, the resolver can assume that the public KSK hasn't been tampered with, which means it can trust all of the records in the child zone. This is how a chain of trust is

Similar to HTTPS, DNSSEC adds a layer of security by enabling authenticated answers on top of an otherwise insecure protocol. Whereas HTTPS encrypts traffic so nobody on the wire can snoop on your Internet activities, DNSSEC merely signs responses so that forgeries are detectable. DNSSEC provides a solution to a real problem without the need to incorporate encryption.

Cloudflare's goal is to make it as easy as possible to enable DNSSEC. Right now, customers with Cloudflare paid plans can add DNSSEC to their web properties by flipping a switch to enable DNSSEC and uploading a DS record (which we'll generate automatically) to their registrar. Learn more about how to get DNSSEC.

We've also published an Internet Draft outlining an automated way for registries and registrars to upload DS records on behalf of our customers. This will enable Cloudflare to automatically enable DNSSEC for our entire community. Stay tuned for updates.

Setting Up Cloudflare Is Easy



Set Up Websites

Use the form below to add websites to CloudFlare.

Note: Websites seen in the table below have **not** finished the setup process and are **not** receiving the security and performance benefits of CloudFlare.

Website	Status
Add a website	

Set up a domain in less than 5 minutes. Keep your hosting provider. No code changes required.

Cloudflare Pricing

Everyone's Internet application can benefit from using Cloudflare.
Pick a plan that fits your needs.

Free $0 /month per website

SELECT

Expand to see more

PRO $20 /month per website

BUSINESS $200 /month per website

SELECT

Expand to see more

Enterprise contact us

SELECT

Expand to see more

Trusted By

Read some of our case studies ›

CLOUDFLARE

zendesk

mapbox

LogMeIn

DigitalOcean

okcupid

Montecito Bank & Trust

DISCORD

LIBRARY OF CONGRESS

UDACITY

CISCO

Contact Sales ▼

Sales:

+33 75 7 90 52 73

What We Do ▼

CLOUDFLARE

About ▼

CLOUDFLARE®