# The ISP Column

*A column on various things Internet*

|  |
| --- |
| September 2025 |

Geoff Huston

# That's a "No!"

The IETF has just published RFC 9824 – Compact Denial of Existence, and while the concept is not exactly recent, it highlights a couple of aspects of today's DNS that I would like to look at in this article.

The DNS Security Extensions (DNSSEC) introduced a means where a receiver of a DNS response could check a response for its authenticity and currency. In other words, is the DNS answer that's I've received in response to my query the genuine response? In the original DNSSEC framework it was assumed that generating digital signatures for entries in a DNS zone file was computationally expensive and there was a single zone signing key used to generate the digital signatures that were attached to each record in the zone. The chosen solution was to pre-compute a new zone file which included these digital signatures and then pass this signed zone file to the authoritative servers for the zone as would be done for any other zone file. That allowed



### Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.



### Author

*Geoff Huston* AM, M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

[*www.potaroo.net*](http://www.potaroo.net)