Université Grenoble Alpes

Extended DNS Errors: Unlocking the Full Potential of DNS Troubleshooting

Yevheniya Nosyk, Maciej Korczyński, Andrzej Duda
Université Grenoble Alpes (Grenoble, France)

RIPE 89, DNS WG (Prague, Czechia)
October 30, 2024

RCODEs

RCODE	Name	RCODE	Name	RCODE	Name
0	NoError	9	NotAuth	19	BADMODE
1	FormErr	9	NotAuth	20	BADNAME
2	ServFail	10	NotZone	21	BADALG
3	NXDomain	11	DSOTYPENI	22	BADTRUNC
4	NotImp	12-15	Unassigned	23	BADCOOKIE
5	Refused	16	BADVERS	24-3840	Unassigned
6	YXDomain	16	BADSIG	3841-4095	Reserved for Private Use
7	YXRRSet	17	BADKEY	4096-65534	Unassigned
8	NXRRSet	18	BADTIME	65535	Reserved, can be allocated by Standards Action

RCODEs

RCODE	Name	RCODE	Name	RCODE	Name
0	NoError	9	NotAuth	19	BADMODE
1	FormErr	9	NotAuth	20	BADNAME
2	ServFail	10	NotZone	21	BADALG
3	NXDomain	11	DSOTYPENI	22	BADTRUNC
4	NotImp	12-15	Unassigned	23	BADCOOKIE
5	Refused	16	BADVERS	24-3840	Unassigned
6	YXDomain	16	BADSIG	3841-4095	Reserved for Private Use
7	YXRRSet	17	BADKEY	4096-65534	Unassigned
8	NXRRSet	18	BADTIME	65535	Reserved, can be allocated by Standards Action

RCODEs

RCODE	Name	RCODE	Name	RCODE	Name
0	NoError	9	NotAuth	19	BADMODE
1	FormErr	9	NotAuth	20	BADNAME
2	ServFail	10	NotZone	21	BADALG
3	NXDomain	11	DSOTYPENI	22	BADTRUNC
4	NotImp	12-15	Unassigned	23	BADCOOKIE
5	Refused	16	BADVERS	24-3840	Unassigned
6	YXDomain	16	BADSIG	3841-4095	Reserved for Private Use
7	YXRRSet	17	BADKEY	4096-65534	Unassigned
8	NXRRSet	18	BADTIME	65535	Reserved, can be allocated by Standards Action

RCODEs

RCODE	Name	RCODE	Name	RCODE	Name
0	NoError	9	NotAuth	19	BADMODE
1	FormErr	9	NotAuth	20	BADNAME
2	ServFail	10	NotZone	21	BADALG
3	NXDomain	11	DSOTYPENI	22	BADTRUNC
4	NotImp	12-15	Unassigned	23	BADCOOKIE
5	Refused	16	BADVERS	24-3840	Unassigned
6	YXDomain	16	BADSIG	3841-4095	Reserved for Private Use
7	YXRRSet	17	BADKEY	4096-65534	Unassigned
8	NXRRSet	18	BADTIME	65535	Reserved, can be allocated by Standards Action

Solution:
Extended DNS Errors

RFC 8914

Status:	Proposed Standard
More info:	Datatracker | IPR | Info page

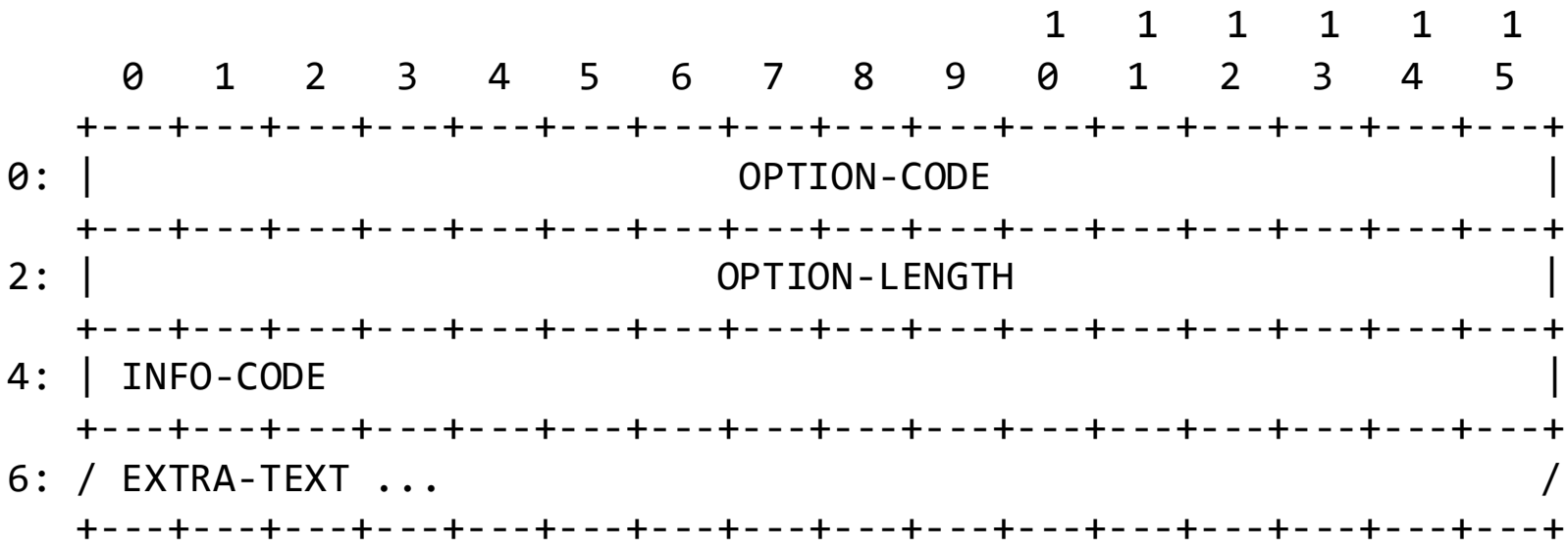
Stream:	Internet Engineering Task Force (IETF)
RFC:	8914
Category:	Standards Track
Published:	October 2020
ISSN:	2070-1721

Authors:	W. Kumari	E. Hunt	R. Arends	W. Hardaker	D. Lawrence
	Google	*ISC*	*ICANN*	*USC/ISI*	*Salesforce*

RFC 8914
Extended DNS Errors

Source: https://www.rfc-editor.org/rfc/rfc8914.html

RFC 8914: Format



Source: https://www.rfc-editor.org/rfc/rfc8914.html

Before: SERVFAIL

```
$ dig rrsig-exp-all.extended-dns-errors.com

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> @64.6.64.6 rrsig-exp-all.extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4244
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;rrsig-exp-all.extended-dns-errors.com. IN A
```

After: SERVFAIL + EDE 7

```
$ dig rrsig-exp-all.extended-dns-errors.com

; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> @1.1.1.1 rrsig-exp-all.extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 37882
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1


;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; EDE: 7 (Signature Expired): (for DNSKEY rrsig-exp-all.extended-dns-errors.com., id = 11245: RRSIG
rrsig-exp-all.extended-dns-errors.com., expiration = 1728310744)
;; QUESTION SECTION:
;rrsig-exp-all.extended-dns-errors.com. IN A
```

Extended DNS Error Codes

Code	Purpose	Code	Purpose	Code	Purpose
0	Other Error	11	No Zone Key Bit Set	22	No Reachable Authority
1	Unsupported DNSKEY Algorithm	12	NSEC Missing	23	Network Error
2	Unsupported DS Digest Type	13	Cached Error	24	Invalid Data
3	Stale Answer	14	Not Ready	25	Signature Expired before Valid
4	Forged Answer	15	Blocked	26	Too Early
5	DNSSEC Indeterminate	16	Censored	27	Unsupported NSEC3 Iterations Value
6	DNSSEC Bogus	17	Filtered	28	Unable to conform to policy
7	Signature Expired	18	Prohibited	29	Synthesized
8	Signature Not Yet Valid	19	Stale NXDomain Answer	30	Invalid Query Type
9	DNSKEY Missing	20	Not Authoritative	31-49151	Unassigned
10	RRSIGs Missing	21	Not Supported	49152-65535	Reserved for Private Use

DNS Resolver Recommendations

RIPE-823
Publication date: 01 May 2024
State: Published

Author
Shane Kerr

Working Group
DNS Resolver Best Common Practice Task Force

File(s)
PDF (415.4 KB)

Extended DNS Errors

Extended DNS errors should be enabled.

For: All DNS resolver operators.

DNS traditionally provides very broad error reporting, SERVFAIL being the most common. This makes diagnosing and fixing problems difficult. Extended DNS errors provide extra information about failures, for example expired DNSSEC signatures. They also allow resolver operators to report administrative reasons for DNS failures, such as blocks due to legal requirements.

RFC8914 defines extended DNS errors.

Source: https://www.ripe.net/publications/docs/ripe-823/

Is the RFC-8914 implemented in software and public resolvers?

Tested Systems

Software:

- BIND 9.19.23
- Unbound 1.20.0
- PowerDNS Recursor 5.0.4
- Knot Resolver 5.7.3

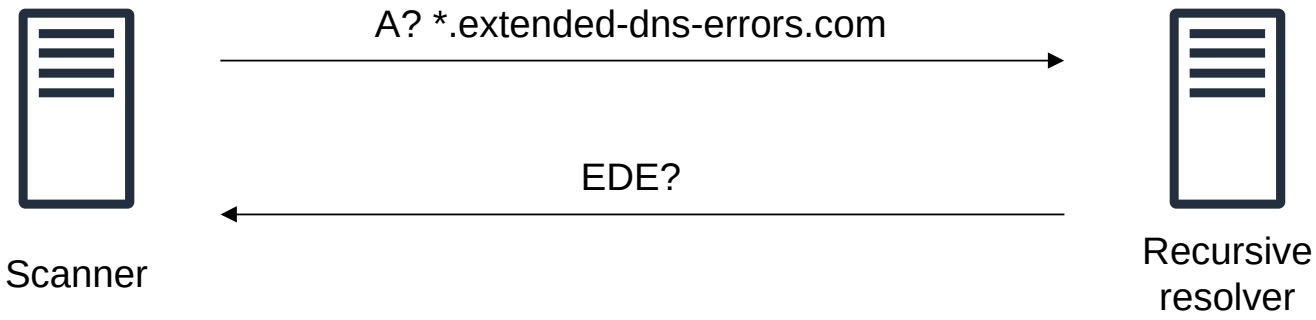
Public resolvers:

- Cloudflare (1.1.1.1)
- Google (8.8.8.8)
- Quad9 (9.9.9.9)
- DNS4ALL (194.0.5.3)
- OpenDNS (208.67.222.222)

extended-dns-errors.com

Subdomain	Configuration
`valid`	The correctly configured control domain
`unsigned`	The domain name is not signed with DNSSEC
`allow-query-none`	Nameserver does not accept queries for the subdomain
`allow-query-localhost`	Nameserver only accepts queries from the localhost
`no-ds`	The subdomain is correctly signed but no `DS` record was published at the parent zone
`ds-bad-tag`	The key tag field of the `DS` record at the parent zone does not correspond to the `KSK DNSKEY` ID at the child zone
`ds-bad-key-algo`	The algorithm field of the `DS` record at the parent zone does not correspond to the `KSK DNSKEY` algorithm at the child zone
`ds-unassigned-key-algo`	The algorithm value of the `DS` record at the parent zone is unassigned (`100`)
`ds-reserved-key-algo`	The algorithm value of the `DS` record at the parent zone is reserved (`200`)
`ds-unassigned-digest-algo`	The digest algorithm value of the `DS` record at the parent zone is unassigned (`100`)

Methodology



OpenDNS Censored?

```
$ dig @208.67.222.222 extended-dns-errors.com

; <<>> DiG 9.16.48-Debian <<>> @208.67.222.222 extended-dns-errors.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 16690
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1410
; EDE: 16 (Censored)
;; QUESTION SECTION:
;extended-dns-errors.com.       IN      A

;; ADDITIONAL SECTION:

extended-dns-errors.com. 0      IN      TXT     "The OpenDNS service is currently unavailable in France and some
French territories due to a court order under Article L.333-10 of the French Sport Code. See
https://support.opendns.com/hc/en-us"
```

Results

	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid	None	None	None	None	None	None	None	None	None
no-ds	None	None	None	None	None	None	None	None	None
ds-bad-tag	9	9	6	6	6	None	6	9	6
ds-bad-key-algo	9	9	6	6	6	None	6	9	None
rrsig-no-a	10	10	10	None	10	None	10	10	None
ds-unassigned-key-algo	9	None	None	6	None	None	None	None	None
ed448	1	None	None	None	None	None	None	None	None
nsec3-iter-151	6,27	5	None	12	None	None	None	None	None
allow-query-none	9,18,22	18,22,23	22	18	3	None	None	22	None

Results: EDE consistency

	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid	None	None	None	None	None	None	None	None	None
no-ds	None	None	None	None	None	None	None	None	None
ds-bad-tag	9	9	6	6	6	None	6	9	6
ds-bad-key-algo	9	9	6	6	6	None	6	9	None
rrsig-no-a	10	10	10	None	10	None	10	10	None
ds-unassigned-key-algo	9	None	None	6	None	None	None	None	None
ed448	1	None	None	None	None	None	None	None	None
nsec3-iter-151	6,27	5	None	12	None	None	None	None	None
allow-query-none	9,18,22	18,22,23	22	18	3	None	None	22	None

Results: resolver configurations

	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid	None	None	None	None	None	None	None	None	None
no-ds	None	None	None	None	None	None	None	None	None
ds-bad-tag	9	9	6	6	6	None	6	9	6
ds-bad-key-algo	9	9	6	6	6	None	6	9	None
rrsig-no-a	10	10	10	None	10	None	10	10	None
ds-unassigned-key-algo	9	None	None	6	None	None	None	None	None
ed448	1	None	None	None	None	None	None	None	None
nsec3-iter-151	6,27	5	None	12	None	None	None	None	None
allow-query-none	9,18,22	18,22,23	22	18	3	None	None	22	None

Results: resolver configurations

```
$ dig @1.1.1.1 foo.nsec3-iter-151.extended-dns-errors.com
…
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 7907
…
; EDE: 6 (DNSSEC Bogus): (proof of non-existence of foo.nsec3-iter-151.extended-dns-errors.com. A)
; EDE: 27: (NSEC3 iterations limit exceeded)
```

```
$ dig @8.8.8.8 foo.nsec3-iter-151.extended-dns-errors.com
…
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 15632
…
; EDE: 5 (DNSSEC Indeterminate): (NSEC3 iteration count 151 is too high (RFC9276) at foo.nsec3-iter-
151.extended-dns-errors.com/a)
```

```
$ dig @208.67.222.222 foo.nsec3-iter-151.extended-dns-errors.co
…
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 4004
…
; EDE: 12 (NSEC Missing)
```

Results: resolver capabilities

	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid	None	None	None	None	None	None	None	None	None
no-ds	None	None	None	None	None	None	None	None	None
ds-bad-tag	9	9	6	6	6	None	6	9	6
ds-bad-key-algo	9	9	6	6	6	None	6	9	None
rrsig-no-a	10	10	10	None	10	None	10	10	None
ds-unassigned-key-algo	9	None	None	6	None	None	None	None	None
ed448	1	None	None	None	None	None	None	None	None
nsec3-iter-151	6,27	5	None	12	None	None	None	None	None
allow-query-none	9,18,22	18,22,23	22	18	3	None	None	22	None

Results: EDE-6 (DNSSEC Bogus)

	Cloudflare	Google	Quad9	OpenDNS	DNS4ALL	bind9-9.19.23	unbound-1.20.0	pdns-recursor-5.0.4	knot-resolver-5.7.3
valid	None	None	None	None	None	None	None	None	None
no-ds	None	None	None	None	None	None	None	None	None
ds-bad-tag	9	9	6	6	6	None	6	9	6
ds-bad-key-algo	9	9	6	6	6	None	6	9	None
rrsig-no-a	10	10	10	None	10	None	10	10	None
ds-unassigned-key-algo	9	None	None	6	None	None	None	None	None
ed448	1	None	None	None	None	None	None	None	None
nsec3-iter-151	6,27	5	None	12	None	None	None	None	None
allow-query-none	9,18,22	18,22,23	22	18	3	None	None	22	None

Why important?

Status:	Proposed Standard
More info:	Datatracker | IPR | Info page
Stream:	Internet Engineering Task Force (IETF)
RFC:	9567
Category:	Standards Track
Published:	April 2024
ISSN:	2070-1721
Authors:	R. Arends *ICANN*, M. Larson *ICANN*

RFC 9567
DNS Error Reporting

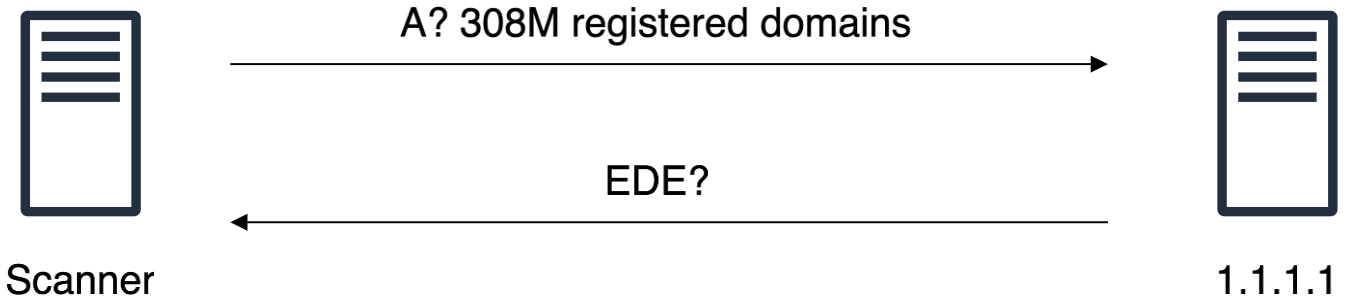
Abstract

DNS error reporting is a lightweight reporting mechanism that provides the operator of an authoritative server with reports on DNS resource records that fail to resolve or validate. A domain owner or DNS hosting organization can use these reports to improve domain hosting. The reports are based on extended DNS errors as described in RFC 8914.

Source: https://www.rfc-editor.org/rfc/rfc9567.html

What are the most common misconfigurations in the wild?

Methodology



Results

- 19.1M domains trigger EDEs
- 19 unique EDE codes
- 240 combinations of up to 5 individual EDEs

EDE 22 (No Reachable Authority)

The resolver could not reach any of the authoritative name servers (or they potentially refused to reply).

```
$ dig @1.1.1.1 example.com
…
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32496
…
; EDE: 22 (No Reachable Authority): (at delegation example.com.)
```

14.1 million domains

EDE 23 (Network Error)

An unrecoverable error occurred while communicating with another server.

```
$ dig @1.1.1.1 example.com
…
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32496
…
; EDE: 23 (Network Error): (X.X.X.X:53 rcode=REFUSED for example.com A)
```

10.2 million domains

EDE 22 + EDE 23

The most common combination of EDEs.

```
$ dig @1.1.1.1 example.com

…

;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 32496

…

; EDE: 22 (No Reachable Authority): (at delegation example.com.)
; EDE: 23 (Network Error): (X.X.X.X:53 timed out for example.com A)
```

8.6 million domains

EDE 20 (Not Authoritative)

An authoritative server that receives a query with the Recursion Desired (RD) bit clear, or when it is not configured for recursion for a domain for which it is not authoritative, SHOULD include this EDE code in the REFUSED response. A resolver that receives a query with the RD bit clear SHOULD include this EDE code in the REFUSED response.

```
$ dig @1.1.1.1 example.com
…
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 17365
…
; EDE: 20 (Not Authoritative): (zone not managed by server)
; EDE: 22 (No Reachable Authority): (at delegation example.com.)
```

2.2 million domains

EDE 18 (Prohibited)

An authoritative server or recursive resolver that receives a query from an "unauthorized" client can annotate its REFUSED message with this code. Examples of "unauthorized" clients are recursive queries from IP addresses outside the network, blocklisted IP addresses, local policy, etc.

```
$ dig @1.1.1.1 example.com

…
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17365
…

; EDE: 18 (Prohibited)
```

1.6 million domains

EDE 10 (RRSIGs Missing)

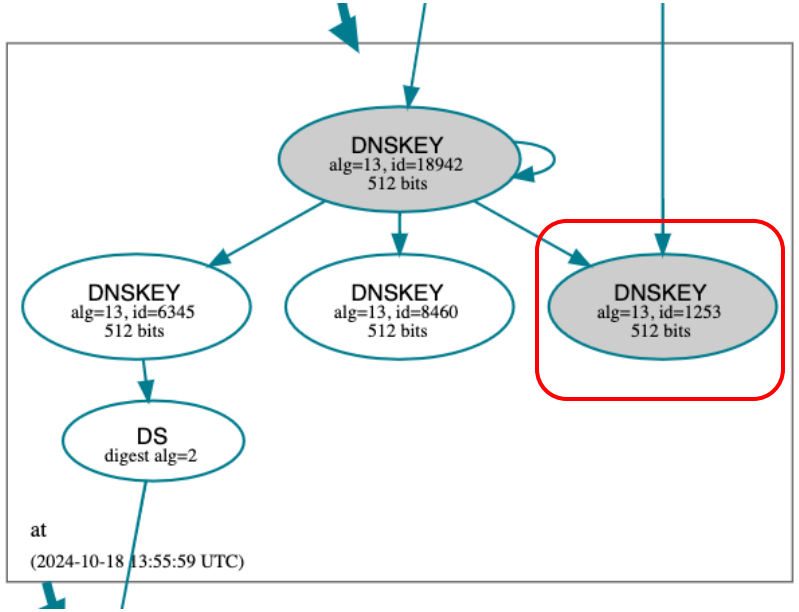
The resolver attempted to perform DNSSEC validation, but no RRSIGs could be found for at least one RRset where RRSIGs were expected.

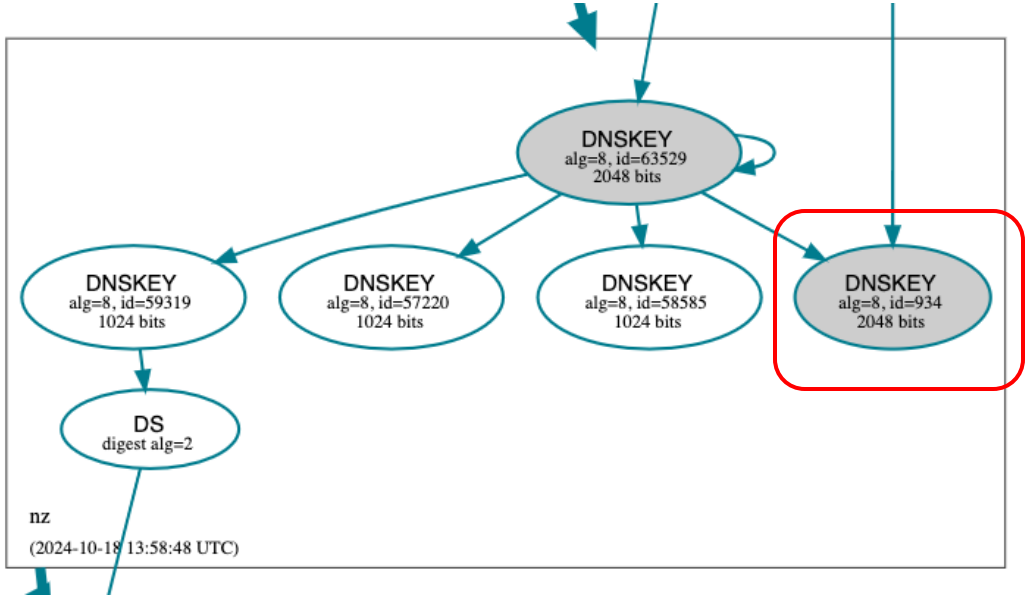
```
$ dig @1.1.1.1 nic.at
…
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6033
…
; EDE: 10 (RRSIGs Missing): (for DNSKEY at., id = 1253)
```

```
$ dig @1.1.1.1 internetnz.nz
…
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4234
…
; EDE: 10 (RRSIGs Missing): (for DNSKEY nz., id = 934)
```

2.2 million domains

EDE 10 (RRSIGs Missing)





Source: https://dnsviz.net/d/nic.at/dnssec/

EDE 10 (RRSIGs Missing)

10	RRSIGs Missing	`EDE: 10 (RRSIGs Missing): (for DNSKEY example.com., id = 12345)`	1.1.1.1 was unable to retrieve Resource Record Signatures (RRSigs) to verify the authenticity of the records. Check your DNS configuration and the response code. If the response code is not `SERVFAIL`, this error indicates that there is a non-operational key issue somewhere along the path, but the resolver found at least one successful path for validation. Examples of non-operational key issues include but are not limited to key rollover in-progress, stand-by key, and attacker stripping signatures made by a certain key.

Source: https://developers.cloudflare.com/1.1.1.1/infrastructure/extended-dns-error-codes/

Many more interesting cases to dig into …

Conclusions

- Supported by major DNS systems
- Identifies the root cause of problems
- Efficient at scale

Thanks!

yevheniya.nosyk@univ-grenoble-alpes.fr