Ordinary DNS:

Client's Resolver → www.google.com A?

com. **NS** a.gtld-servers.net
a.gtld-servers.net **A** 192.5.6.30
...

→ k.root-servers.net
Ordinary DNS:

Client's Resolver → www.google.com A?
com. NS a.gtld-servers.net
a.gtld-servers.net A 192.5.6.30
...

k.root-servers.net

Client's Resolver ← www.google.com A?

google.com. NS ns1.google.com
ns1.google.com A 216.239.32.10
...

a.gtld-servers.net
Ordinary DNS:

Client's Resolver → www.google.com A?
com. NS a.gtld-servers.net
a.gtld-servers.net A 192.5.6.30
...

k.root-servers.net

Client's Resolver → www.google.com A?
google.com. NS ns1.google.com
ns1.google.com A 216.239.32.10
...

a.gtld-servers.net

Client's Resolver → www.google.com A?
...

ns1.google.com
DNSSEC (with simplifications):

Client's Resolver → www.google.com A? DO → k.root-servers.net

com. **NS** a.gtld-servers.net
a.gtld-servers.net. **A** 192.5.6.30
...
com. **DS** description-of-com's-key
com. **RRSIG DS** signature-of-that-DS-record-using-root's-key
DNSSEC (with simplifications):

Client's Resolver → www.google.com A? DO → k.root-servers.net

com. **NS** a.gtld-servers.net
a.gtld-servers.net. **A** 192.5.6.30
...
com. **DS** description-of-com's-key
com. **RRSIG DS** signature-of-that-DS-record-using-root's-key

Delegation Signer identifies .com's public key (name and hash)
DNSSEC (with simplifications):

Retrieving .com's public key is complicated (actually involves multiple keys) ...
DNSSEC (with simplifications):

Client's Resolver → www.google.com A? DO → k.root-servers.net

com. **NS** a.gtld-servers.net
a.gtld-servers.net. **A** 192.5.6.30
...
com. **DS** description-of-com's-key
com. **RRSIG** **DS** signature-of-that-DS-record-using-root's-key

Specifies signature over another **RR** ... here, the above **DS** record
DNSSEC (with simplifications):

www.google.com A? DO

Client's Resolver

com. **NS** a.gtld-servers.net
a.gtld-servers.net. A 192.5.6.30

... com. **DS** description-of-com's-key
com. **RRSIG DS** signature-of-that-DS-record-using-root's-key

k.root-servers.net

Note: no signature over **NS** or **A**!
DNSSEC (with simplifications):

Client's Resolver

www.google.com A? DO

google.com. **NS** ns1.google.com
sns1.google.com. **A** 216.239.32.10
...

google.com. **DS** description-of-
google.com's-key
google.com. **RRSIG DS** signature-of-that-**DS**-record-using-com's-key

a.gtld-servers.net
DNSSEC (with simplifications):

www.google.com A? DO

...
www.google.com. RRSIG A
signature-of-the-A-records-using-google.com's-key
DNSSEC - Mallory attacks!

Client's Resolver

www.google.com A? DO

www.google.com. A 6.6.6.6

ns1.evil.com
DNSSEC - Mallory attacks!

Client's Resolver

www.google.com A? \textit{DO}

www.google.com. A 6.6.6.6

ns1.evil.com

Resolver observes that the reply didn't include a signature, rejects it as insecure
DNSSEC - Mallory attacks!

Client's Resolver

www.google.com. A 6.6.6.6
www.google.com RRSIG A
signature-of-the-A-record-using-evil.com's-key

ns1.evil.com
DNSSEC - Mallory attacks!

(1) If resolver didn't receive a signature from .com for evil.com's key, then it can't validate this signature & ignores reply since it's not properly signed …
DNSSEC - Mallory attacks!

(2) If resolver *did* receive a signature from .com for evil.com's key, then it knows the key is for evil.com and not google.com ... and ignores it
DNSSEC - Mallory attacks!

www.google.com A? **DO**

Client's Resolver

www.google.com. **A** 6.6.6.6
www.google.com **RRSIG A**
signature-of-the-**A**-record-using-
google.com's-key

ns1.evil.com
DNSSEC - Mallory attacks!

If signature **actually** comes from google.com's key, resolver will believe it …

… but no such signature should exist unless either:

1. google.com *intended* to sign the RR, or
2. google.com's private key was compromised