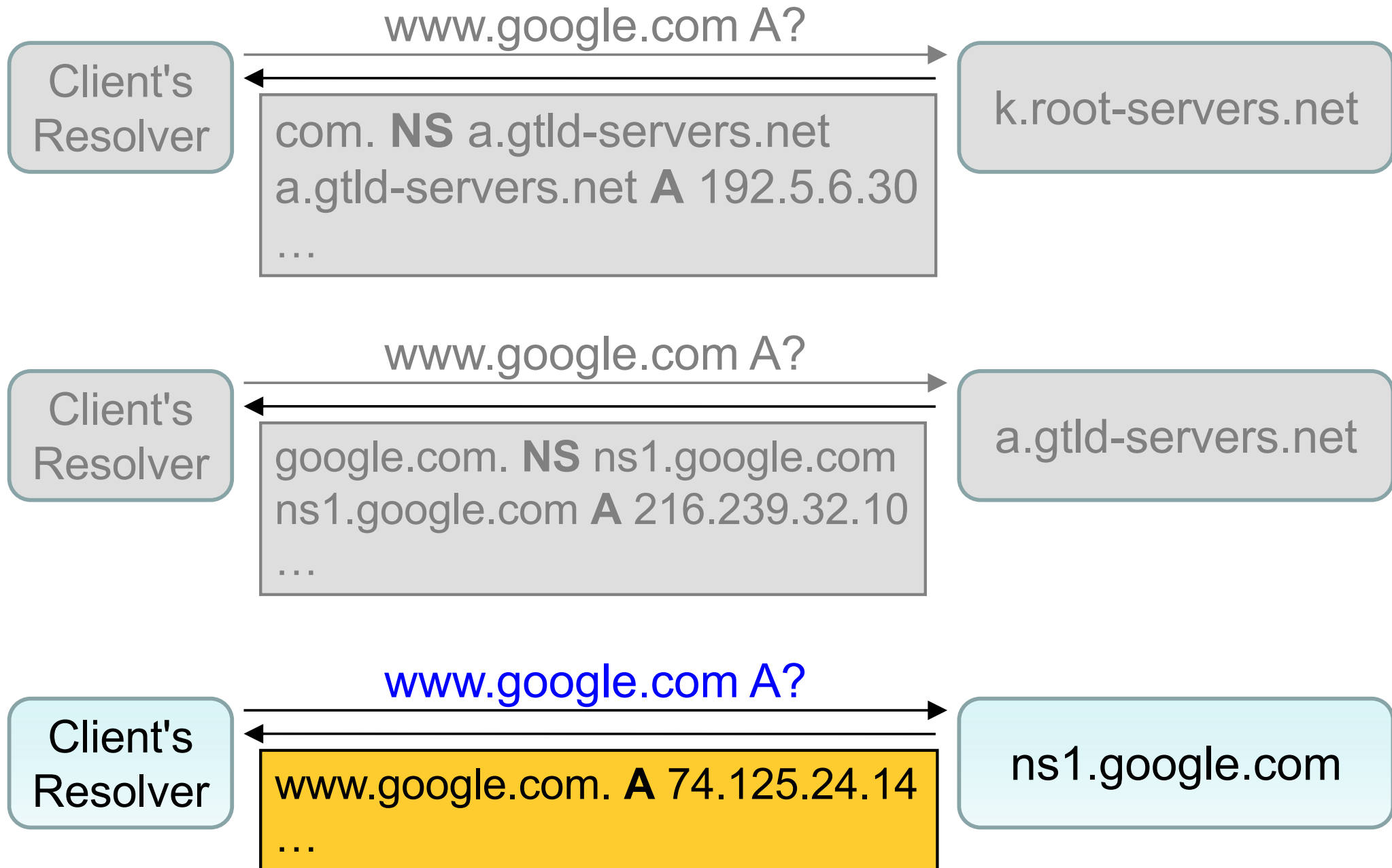
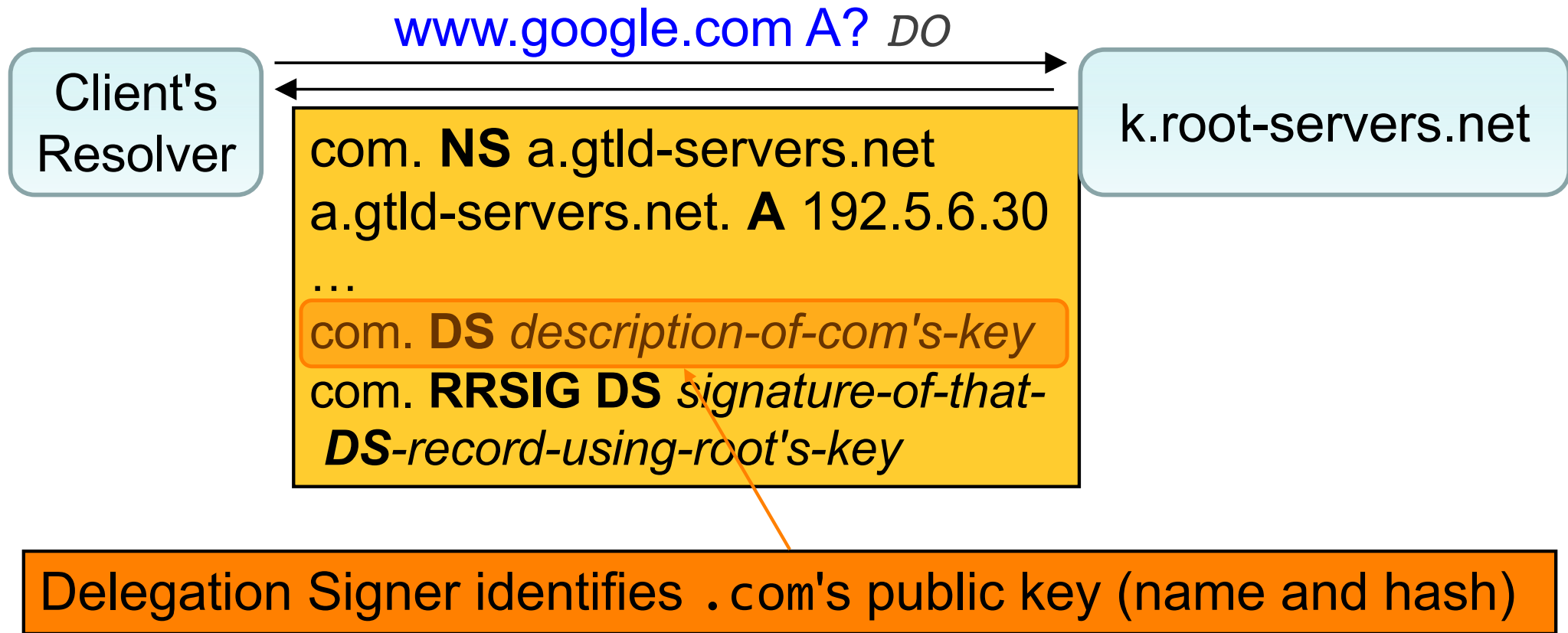


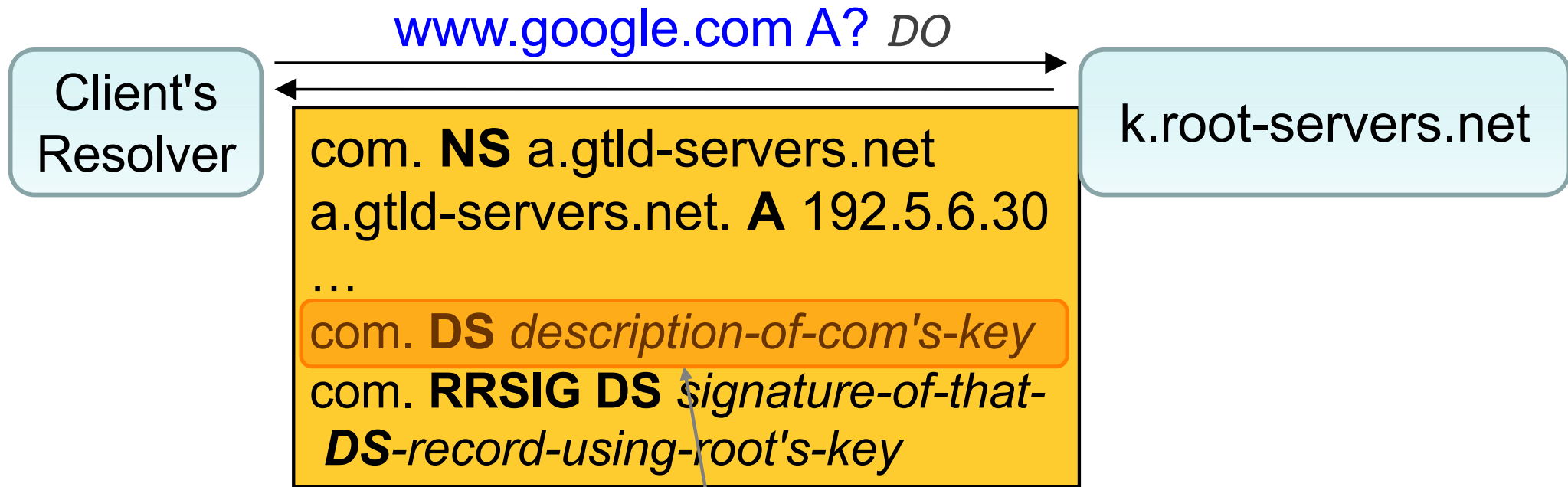
Ordinary DNS:



DNSSEC (with simplifications):

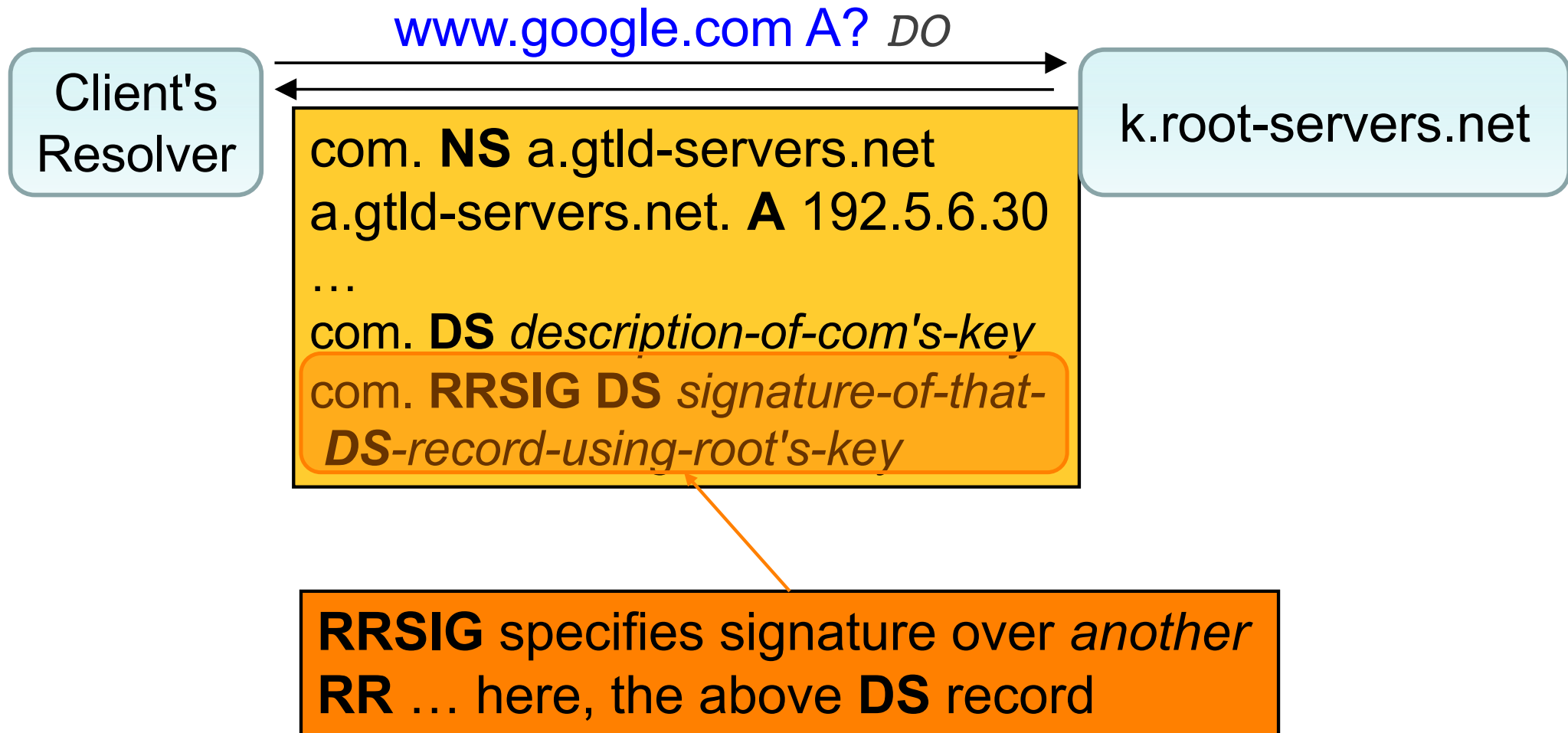


DNSSEC (with simplifications):

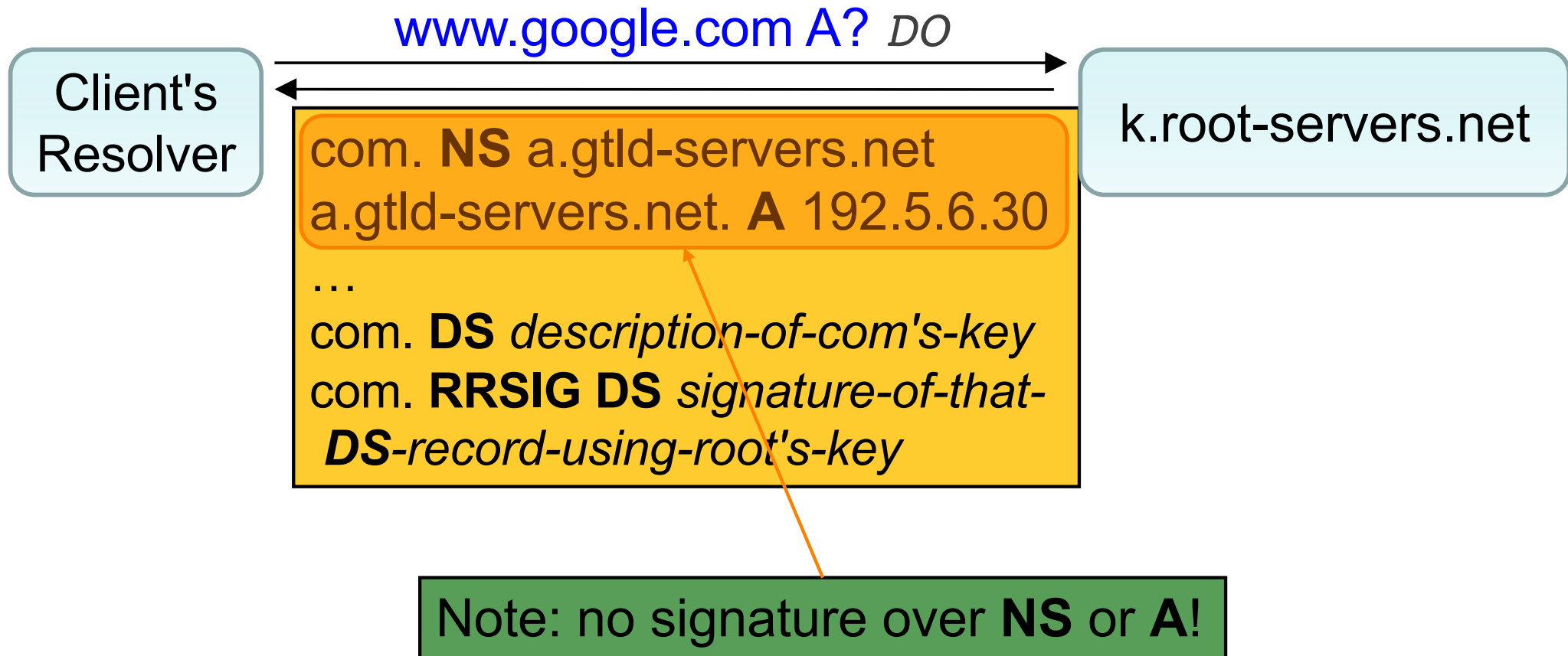


Retrieving .com's public key is complicated (actually involves multiple keys) ...

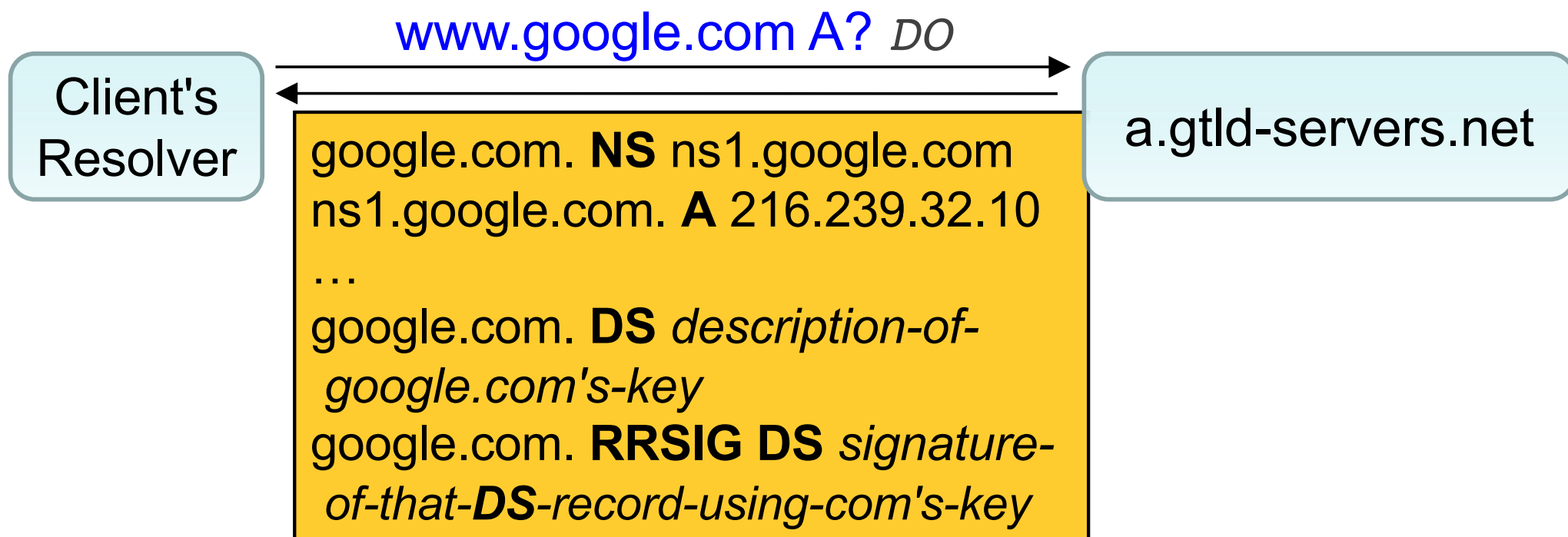
DNSSEC (with simplifications):



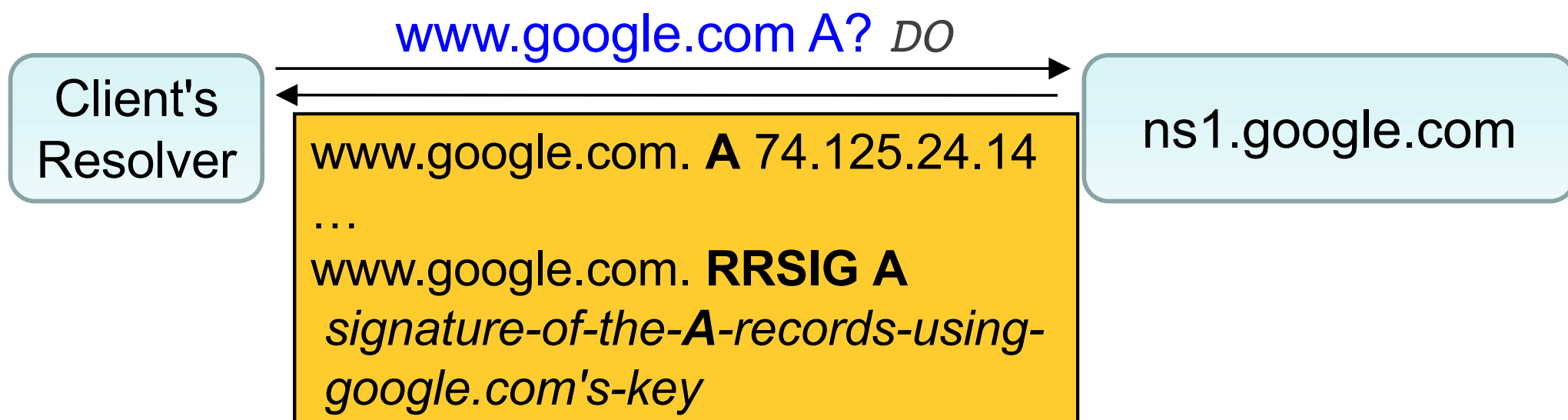
DNSSEC (with simplifications):



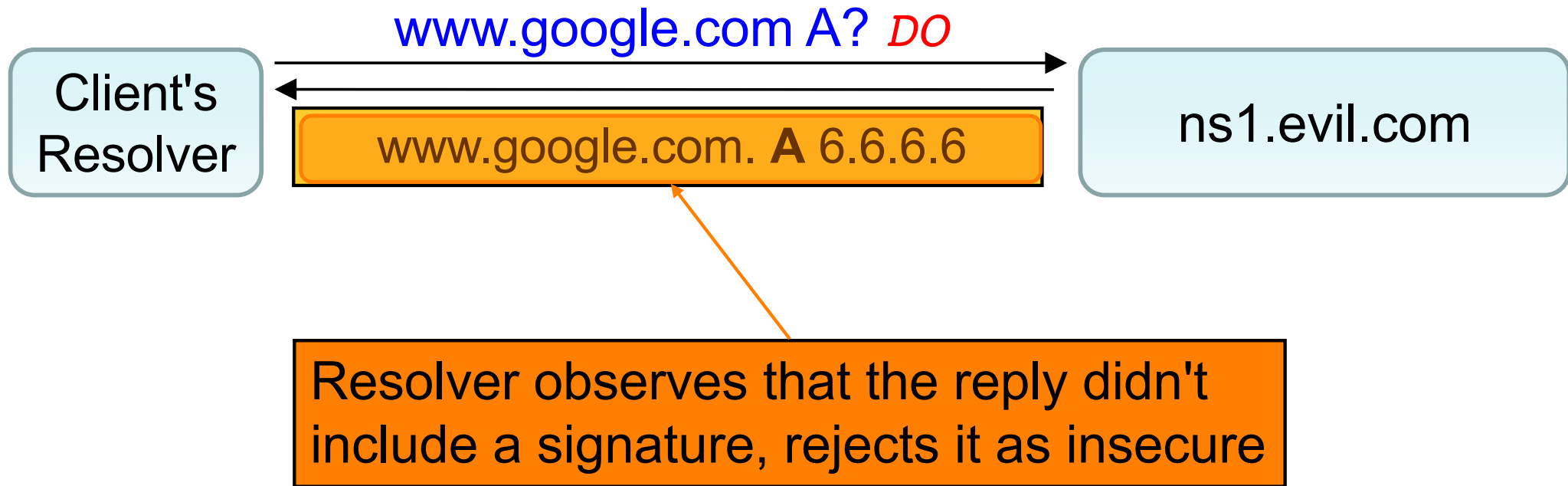
DNSSEC (with simplifications):



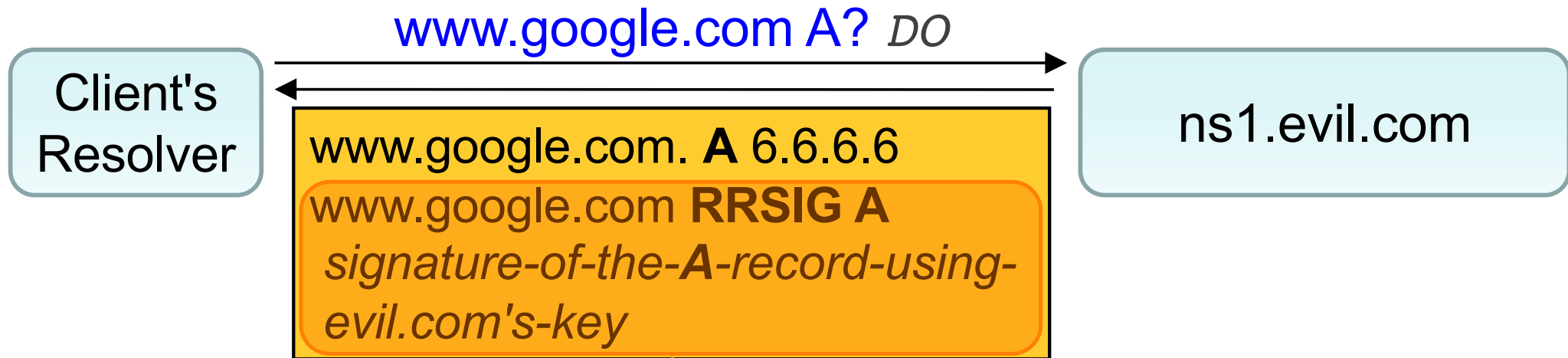
DNSSEC (with simplifications):



DNSSEC - Mallory attacks!

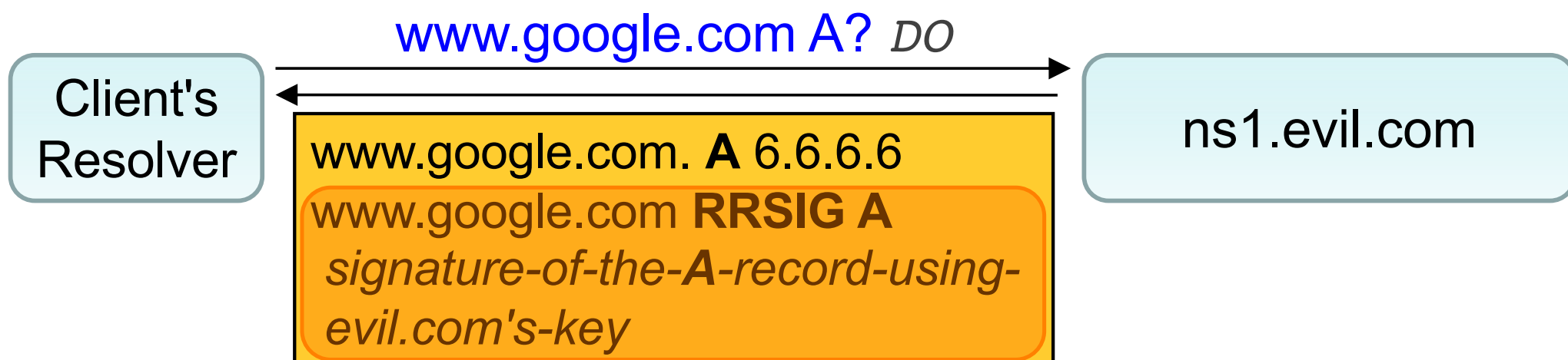


DNSSEC - Mallory attacks!



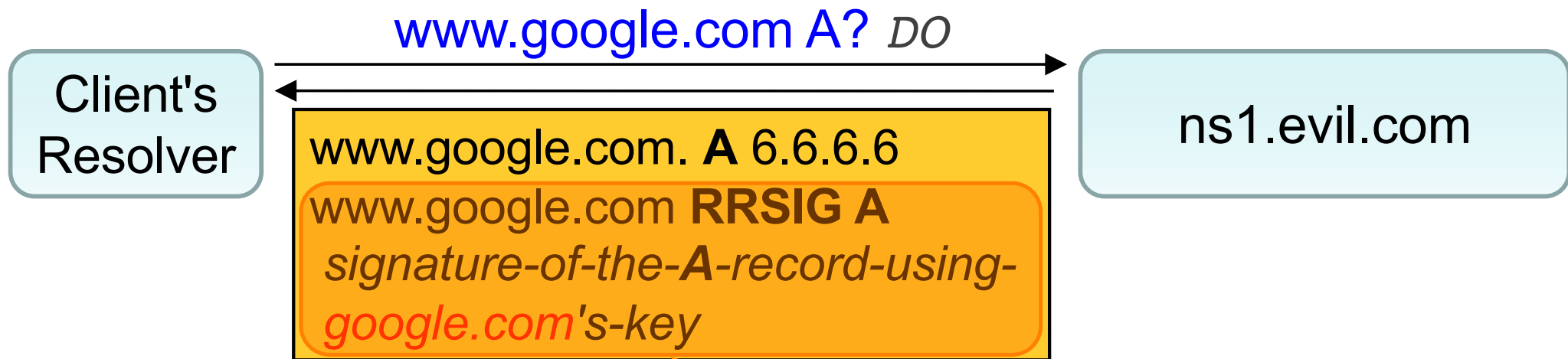
(1) If resolver didn't receive a signature from .com for evil.com's key, then it can't validate this signature & ignores reply since it's not properly signed ...

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!



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

... but no such signature should exist unless either:
(1) google.com's private key was compromised, or
(2) google.com *intended* to sign the RR

```
% dig +dnssec berkeley.edu
```

69-byte query

% dig +dnssec berkeley.edu

; <<> DiG 9.8.3-P1 <<> +dnssec berkeley.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60422
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 8, ADDITIONAL: 27

3419-byte reply

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;berkeley.edu. IN A

;; ANSWER SECTION:
berkeley.edu. 198 IN A 128.32.203.137
berkeley.edu. 198 IN RRSIG A 10 2 300 20160906161321 20160902155734 20552 berkeley.edu. C6rreK8RPffJjJbMuoAj3jQP5Koez6nEPjumLRzT0cPY08bXHVmNrSf5 R/Q1/hf0uk9B
berkeley.edu. 198 IN RRSIG A 10 2 300 20160906161321 20160902155734 55763 berkeley.edu. E2C1U8B1vWNLXTLK5Wx47VatSKqrXQbW2396REcJ0M4bndqwkHTJrrHS Qr9VI64G+Gj6

;; AUTHORITY SECTION:
berkeley.edu. 10536 IN NS sns-pb.isc.org.
berkeley.edu. 10536 IN NS aodns1.berkeley.edu.
berkeley.edu. 10536 IN NS phloem.uoregon.edu.
berkeley.edu. 10536 IN NS adns1.berkeley.edu.
berkeley.edu. 10536 IN NS aodns2.berkeley.edu.
berkeley.edu. 10536 IN NS adns2.berkeley.edu.
berkeley.edu. 10012 IN RRSIG NS 10 2 10800 20160906161321 20160902155734 20552 berkeley.edu. ghIrnq0rISbm8RWxJcF/pR9zCa3QXrpPJftcdSYpTk/I6LFYjKK5B10F 0wVyK3Nu
berkeley.edu. 10012 IN RRSIG NS 10 2 10800 20160906161321 20160902155734 55763 berkeley.edu. rL2T1w4RWVZpu/zUIhigwT7sSSwJZp8gnbY4uLZnCLr73a3ue3XBjGrf x2xDkt/AP

;; ADDITIONAL SECTION:
aodns2.berkeley.edu. 6294 IN A 128.253.35.148
phloem.uoregon.edu. 75123 IN A 128.223.32.35
phloem.uoregon.edu. 13252 IN AAAA 2001:468:d01:20::80df:2023
adns2.berkeley.edu. 6294 IN A 128.32.136.14
adns2.berkeley.edu. 7474 IN AAAA 2607:f140:ffff:ffff::e
sns-pb.isc.org. 6524 IN A 192.5.4.1
sns-pb.isc.org. 46194 IN AAAA 2001:500:2e::1
aodns1.berkeley.edu. 6294 IN A 192.35.225.133
aodns1.berkeley.edu. 2523 IN AAAA 2607:f010:3f8:8000::ff:fe00:53
adns1.berkeley.edu. 1959 IN A 128.32.136.3
adns1.berkeley.edu. 7474 IN AAAA 2607:f140:ffff:ffff::3
aodns2.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906163122 20160902154100 20552 berkeley.edu. Lw8t2yxfTffwLThv0x/JZdAdCPk307Zr+rMVzG44fpLmn6SWH4/EG2IA sx2CjQEd3/
aodns2.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906163122 20160902154100 55763 berkeley.edu. eLe04M4BGzB0NYRtif8DpozUSSeQrucZoc6FpyGhLUHv8kfTncsXK3xw dWSGwhDzzq
adns2.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906155418 20160902145750 20552 berkeley.edu. WK0+3QLDd/6kujgkcJc3d5QJMyD9VWwQM2xGE9kYQ/IW51155c2zxG6X Q7XD2KfQR0
adns2.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906155418 20160902145750 55763 berkeley.edu. hET89n7x16PWr6QYD9YdDUDZWyHMKND9xSRnuIgeX+C37rnIncSolYj HlAdQKHCEj
adns2.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906154405 20160902150354 20552 berkeley.edu. jXP79E6IyKchNV3DxbvOntNC8HmgWKK5Ho0FgxHauDvkYiPEi66/6xNJ thY2v2a
adns2.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906154405 20160902150354 55763 berkeley.edu. bCCo55hQ/7NHVbSpjb/ZCit8G8gs15wL6lATL8ihILFDZrIMxQy5gkIG vUSnzKD
sns-pb.isc.org. 6524 IN RRSIG A 5 3 7200 20160928233609 20160829233609 13953 isc.org. duIqItz21MYE1962AAk2BT5cHeR2vd0HjePEE2S2ABY0JfQX/s+zDRai A/EKRiGDrj38iBp6o
aodns1.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906152003 20160902151259 20552 berkeley.edu. cMXajdGuQgk6tt6IiC1QAM1232yLT2zFxDwfm0EuW6cJ570LOVPbEzDq S6hhaKo70d
aodns1.berkeley.edu. 6294 IN RRSIG A 10 3 10800 20160906152003 20160902151259 55763 berkeley.edu. pHACF3XdiELFuLPe5kroahEMU0vgnNJ4+s0Q0Z286IPMaMgwrbrN511e M7FMQ0Tr14
aodns1.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906162655 20160902155822 20552 berkeley.edu. T+LsA9xpW82/HiZUitYPQeP3C59yKp4lfpafJdeoRBukJee2z0E+dldU AqY2ox5
aodns1.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906162655 20160902155822 55763 berkeley.edu. BMsWj9LiDhKW2CJUB6enhIQ91/csxb0f7IKyxyVZby11E/P5UDjGxyBY d8ZC0iU
adns1.berkeley.edu. 1959 IN RRSIG A 10 3 10800 20160905162046 20160901152849 20552 berkeley.edu. du5i0Lvc+8HfbEAs3f3qnRDwXgsQHEW8xgRoSHXfC/KBURr5+Lygkdni XA2fx1+t7m
adns1.berkeley.edu. 1959 IN RRSIG A 10 3 10800 20160905162046 20160901152849 55763 berkeley.edu. x6GHsd1KhAAiWQVRI1XJGafav+Xoz1YCK/z+XGARSjW0uW9pPTrTT/HL TXNYU201Rx
adns1.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906161659 20160902160412 20552 berkeley.edu. I22a0F87Tp22T3bcZx7sPUxzM9BrsoNvEzo7lqTE3PkP58UmdyL57Azj 2X7j9K5
adns1.berkeley.edu. 10229 IN RRSIG AAAA 10 3 10800 20160906161659 20160902160412 55763 berkeley.edu. ce5Eko5g9DctMWDYeCaqKibWlUmmXMT2N4A41MRtuyIHI+oxA9mtQhx Fuksjf0