DNSSEC Revisited

Hoda Rohani *Anastasios Poulidis*

Supervisor: Jeroen Scheerder

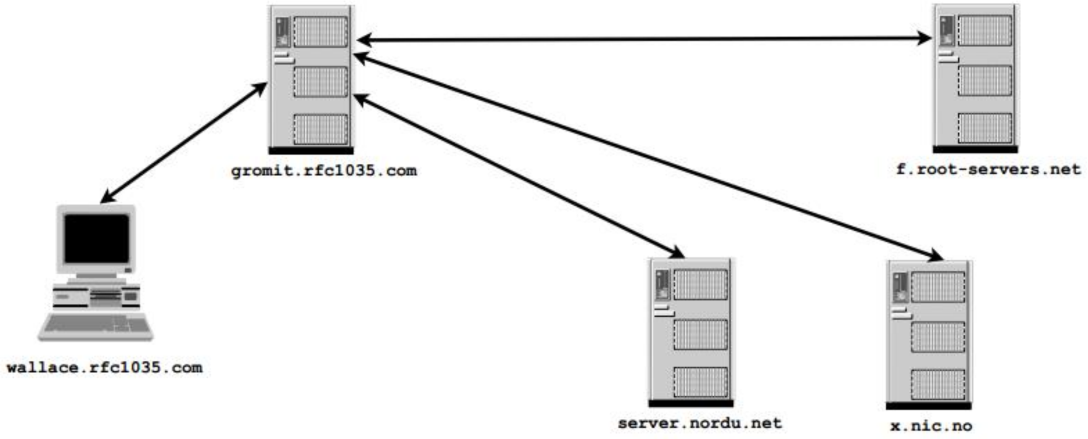
System and Network Engineering

July 2014

DNS Main Components

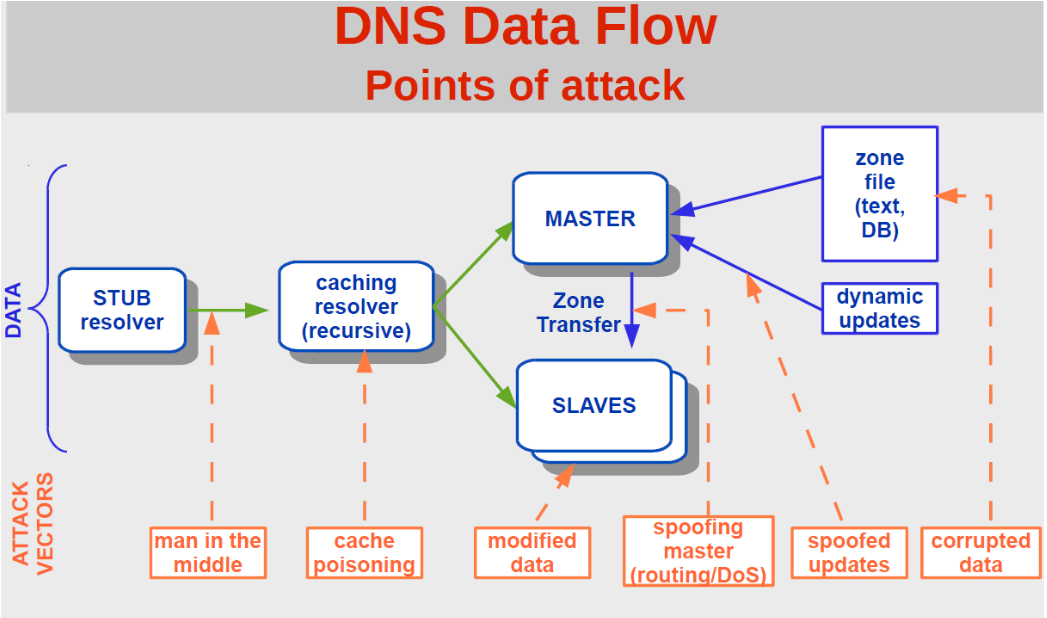
- Server Side:
  - Authoritative Servers
  - Resolvers (Recursive Resolvers, cache)
- Client Side:
  - Stub resolvers (usually on DNS client machines)

- No authentication at all!
- A client cannot be sure
  - Where an answer really came from
  - If the server replied is telling the truth or not
  - If it received exactly what the server sent



DNS Vulnerabilities

- Fill client or resolving server with forged answer
- Intercept a response packet and modify it
- Set up a fake name server for some zone
- Take control of name servers for some zone (false data)
- Inject bogus data into caches (DNS cache poisoning)
- Response to Non-Existent domains
- Compromise the registry: gain unauthorized access to registrar account and change the victim zone’s delegation to point at bogus name servers

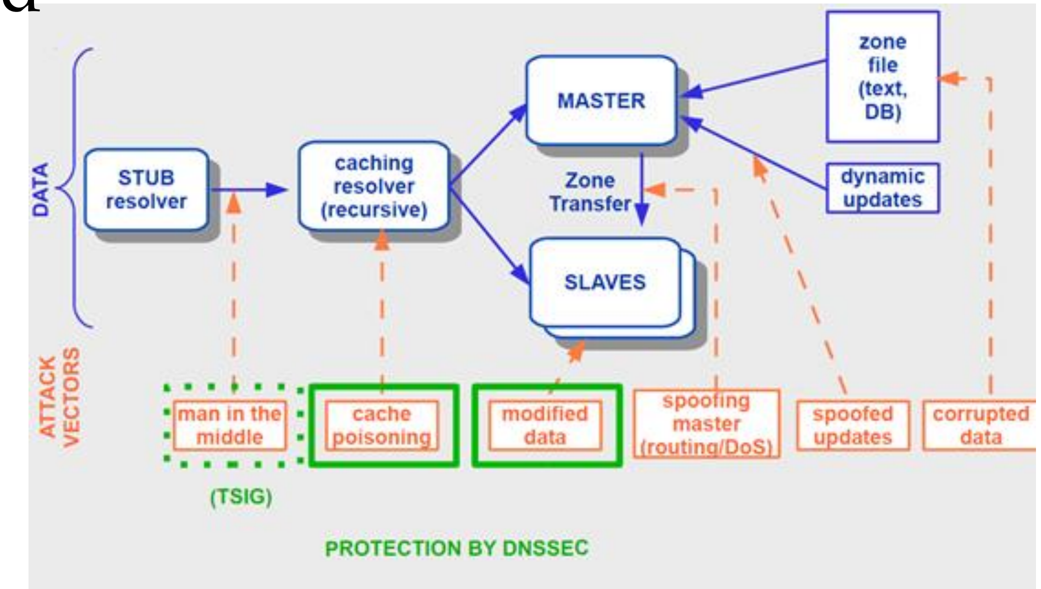


DNS Data Flow

Points of attack

What Does DNSSEC Protect

- DNSEC uses public key cryptography and digital signatures to provide:
  - Data origin authentication, Name server authenticity
  - Data integrity
  - Authenticated denial of existence



DNSSEC offers protection against spoofing of DNS data (TSIG)

General DNSSEC Caveats

- Increase Memory and CPU usage and also cost
  - Zone size increases significantly when signed
  - DNSSEC answers are larger
  - Server side & query side impacts
  - Interference by firewalls, proxies

- Increase bandwidth
  - DNSSEc added a lot to DNS packets. Resolvers and name servers need to send and receive these large DNS packets

- Administrative burden: Key Management (generating, publishing and rollover), interaction with parent

Key Rollover

- Not easy and expensive task
- Two methods
  - Pre-publish: ZSK
  - Double signature: KSK

ZSK Rollover: Pre-publish Policy

- Generate new ZSK, add key to zone (remember to increase the serial number)
- Re-sign zone with using old key and KSK
- Time passes … TTL

```
dnsops.gov   SOA
          RRSIG (new-zsk)

          DNSKEY   old-zsk
          DNSKEY   new-zsk
          DNSKEY   KSK
          RRSIG (old-zsk)
          RRSIG (KSK)
```

- Re-sign with the new key but leave the old zsk published in the zone

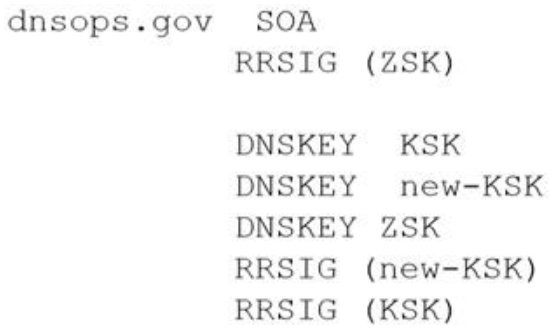
```
dnsops.gov   SOA
          RRSIG (new-zsk)

          DNSKEY   old-zsk
          DNSKEY   new-zsk
          DNSKEY   KSK
          RRSIG (new-zsk)
          RRSIG (KSK)
```

- After all records signed with the old private key have expired (wait zone propagation time + largest TTL of all records in the zone), remove old key
- Resign one last time

```
dnsops.gov   SOA
          RRSIG (new-zsk)

          DNSKEY   new-zsk
          DNSKEY   KSK
          RRSIG (new-zsk)
          RRSIG (KSK)
```

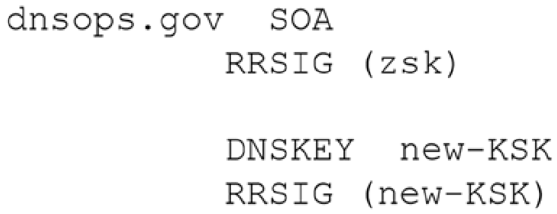
KSK Rollover: Double Signature Policy

- Generate new KSK, add new KSK to the zone and sign the DNSKEY RRset with both keys
- Wait TTL of the zone



```
dnsops.gov   SOA
           RRSIG (ZSK)

           DNSKEY   KSK
           DNSKEY   new-KSK
           DNSKEY  ZSK
           RRSIG  (new-KSK)
           RRSIG  (KSK)
```

- Upload new DS to the parent zone
- When new DS RR appears in the zone, wait TTL of the old DS record
- Remove the old KSK and resign zone
- Remove old DS record from parent

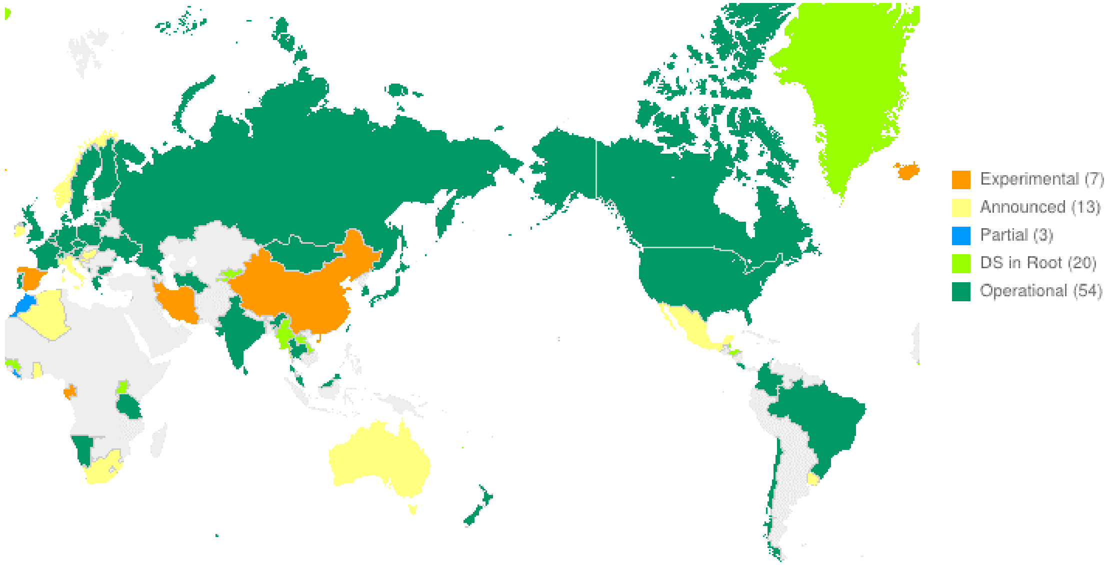


```
dnsops.gov   SOA
           RRSIG (zsk)

           DNSKEY   new-KSK
           RRSIG  (new-KSK)
```

Deployment Status

- Root signed (July 2010), most TLD signed (July 2014 status)
  - TLDS signed: 445 out of 630 (70%) in the root zone in total
  - 435 TLDs have trust anchors published as DS records in the root zone
  - 5 TLDs have trust anchors published in the ISC DLV Repository

ccTLD DNSSEC Status on 2013-07-01



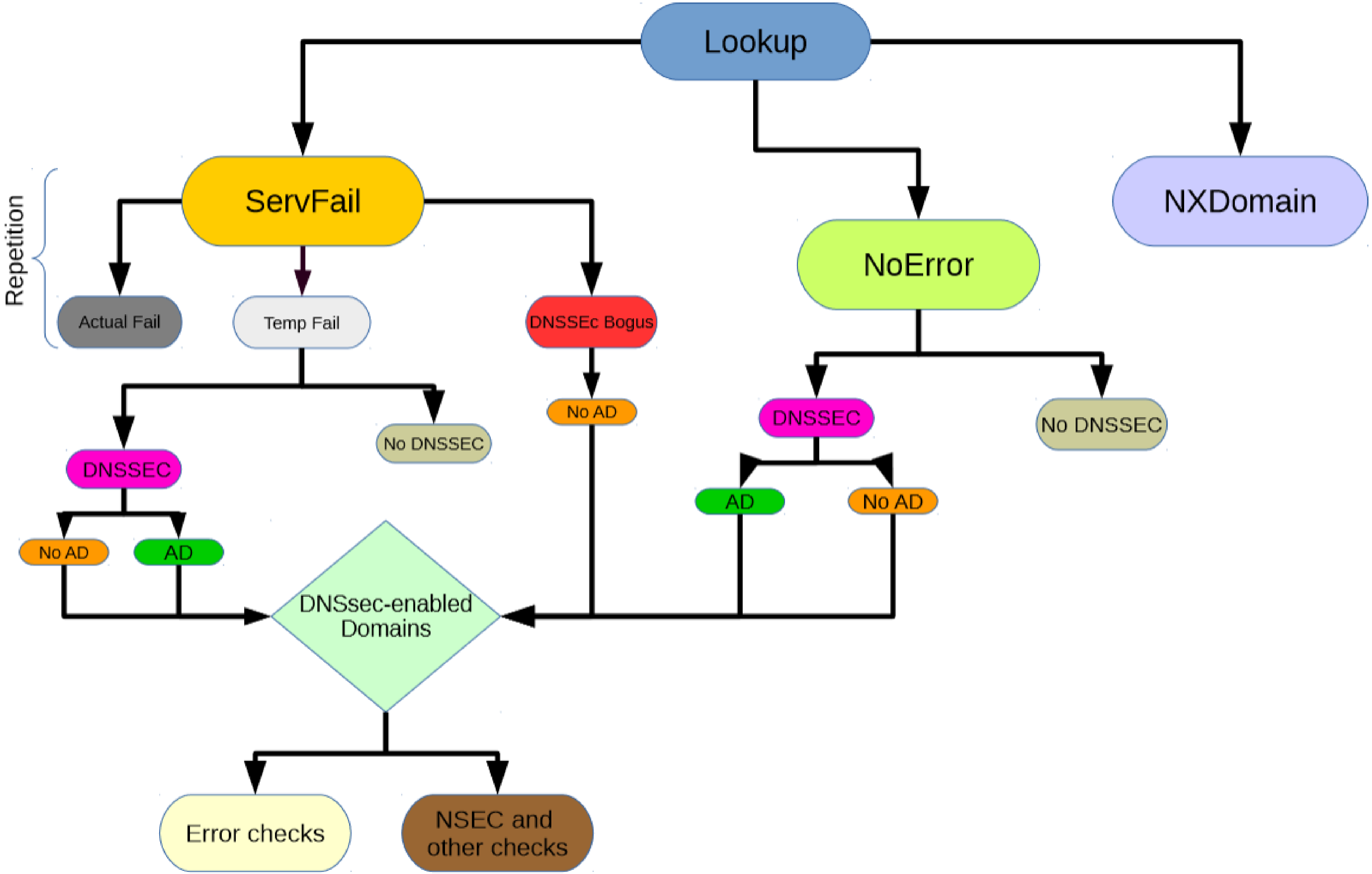
Research Questions & Related work

- What is the DNSsec adoption rate among the most popular domains?
- If the DNSsec is deployed in the zone, is it managed and operated properly?
  - What are the causes of bogus DNSsec enabled zone

- Many websites keep statistics of DNSsec deployment
  - But most of them are restricted to the number of checked domains and TLDs
  - They also lack information about maintenance

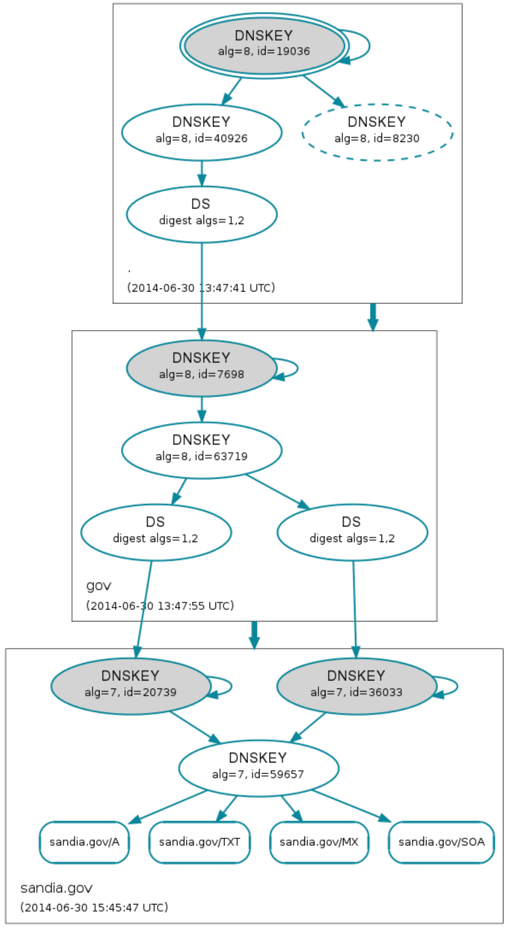
Methodology

- Gather data: get top one million ranked websites by Alexa
  - Extract their domains
  - Find authoritative servers of domains and ask for data of domain
    - Note their serial number and (in)consistency of their answers
    - Look for RRSIG RRs
    - Check for (no)validated answers
    - Ensure that the zone issues a secure denial of existence for names that do not exist
  - Validating Resolvers
    - Our servers and Google public DNS
    - Check to see if those signatures correspond to DNSKEYs served by the zone are valid or not
- Analysis to find out possible errors on the deployment of DNSsec

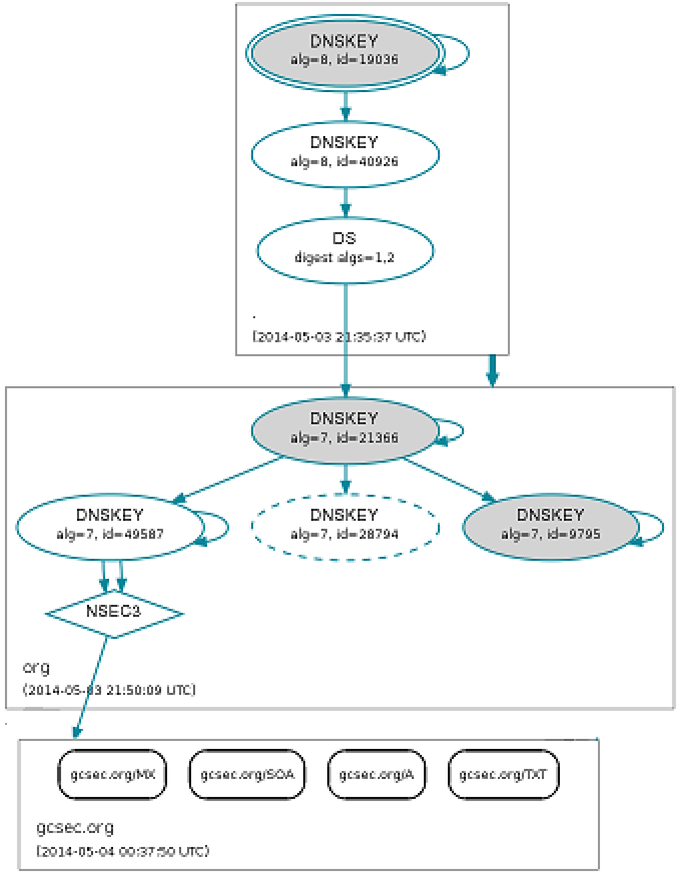

Lookup
ServFail
NoError
NXDomain
Repetition
Actual Fail
Temp Fail
DNSSEc Bogus
No AD
DNSSEC
No DNSSEC
DNSSEC
No DNSSEC
AD
No AD
No AD
AD
DNSsec-enabled Domains
Error checks
NSEC and other checks

DNSSEC Validation Status

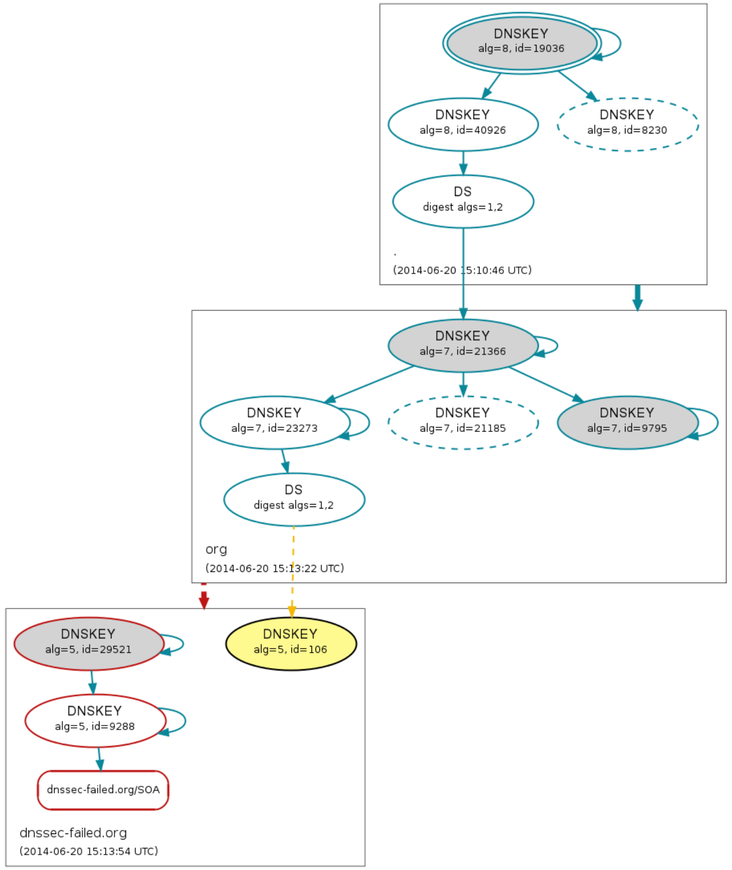
Secure: Unbroken chain from anchor to RRset



Insecure: Chain that securely terminates in the parent

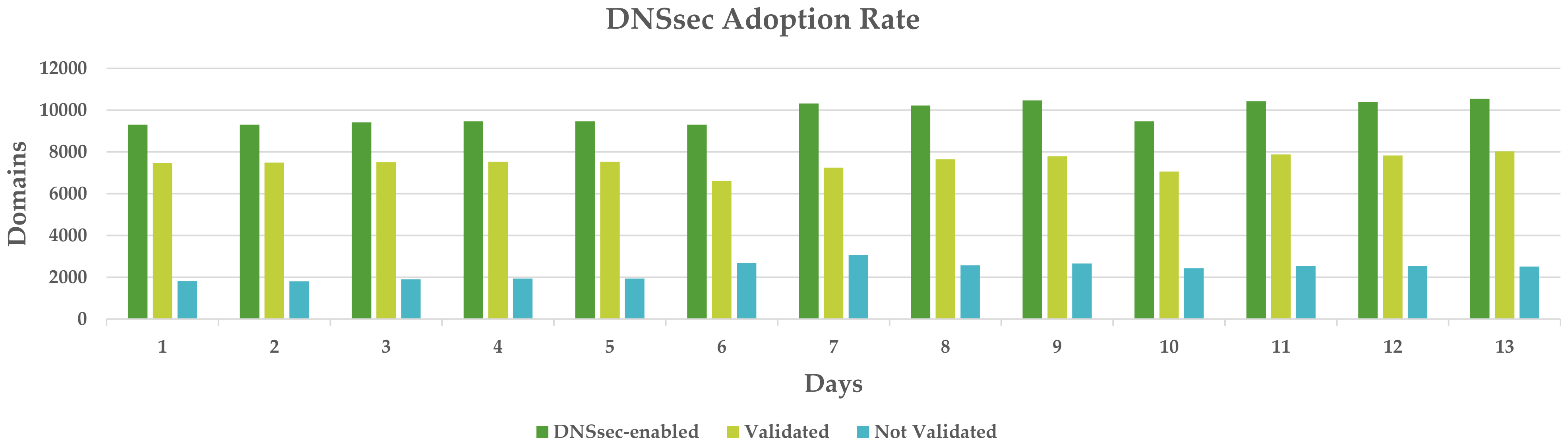


Bogus: Broken chain



How Many Domains are deploying DNSSEC

- On average 9916 signed domains out of a total of ~930000 (1.066%)
- With an average of 7562 (76%) Validated and 2355 (24%) Not Validated domains.



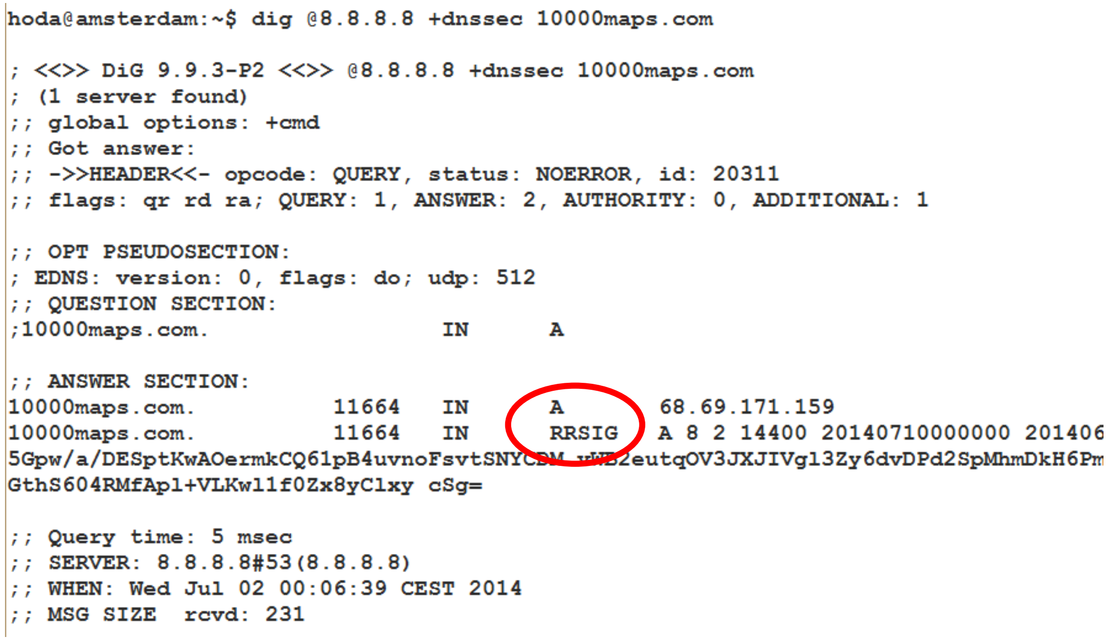
Domain Nameserver (in)consistencies

- On average each domain has 3.5 nameservers

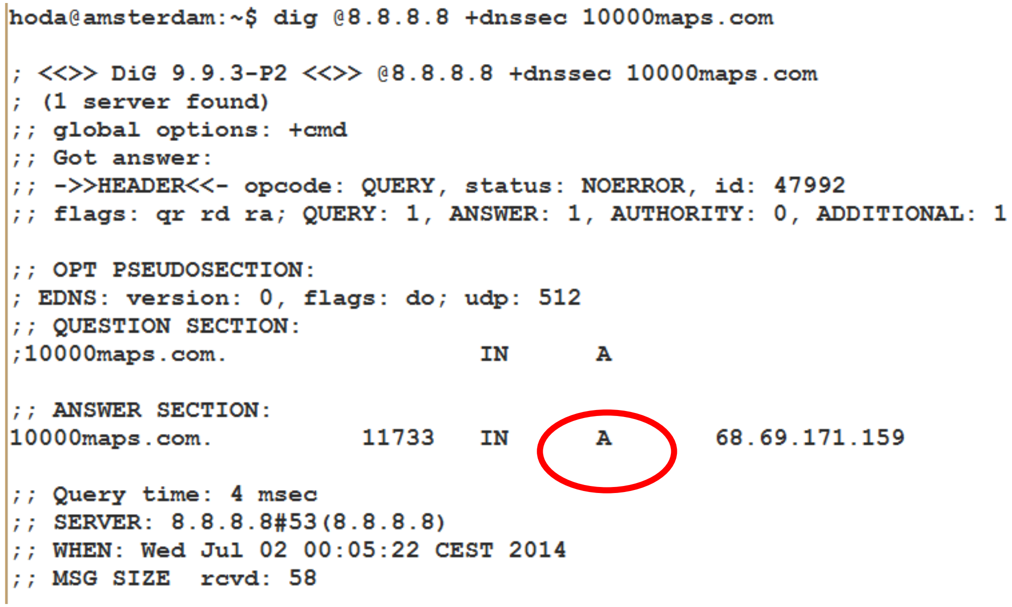
- ~84% of signed domains have multiple nameservers with the same data (8239)
- ~16% of signed domains have multiple nameservers with different data (1568)
  - Inconsistent data
  - Consistent data

Inconsistency: Different Data in Nameservers

- 235 signed domains have some nameservers with RRSIG data while others don't have RRSIG



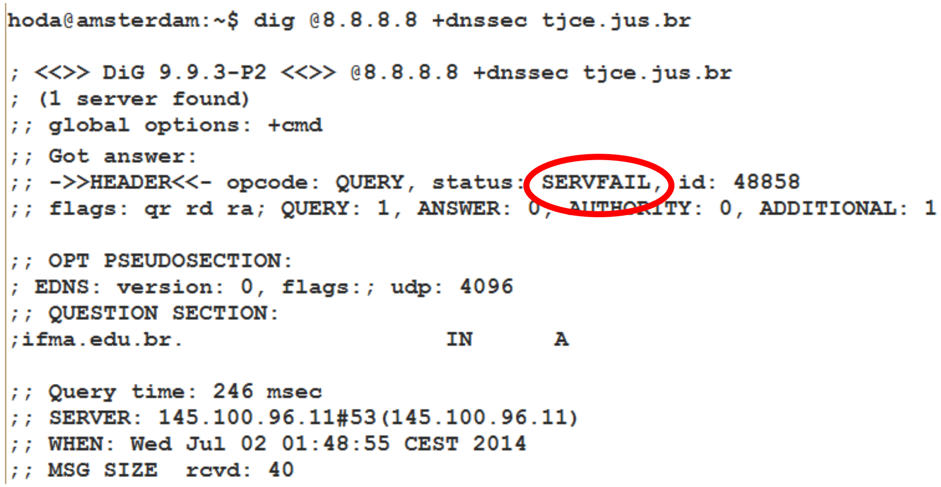
```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec 10000maps.com

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec 10000maps.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20311
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;10000maps.com.                 IN      A

;; ANSWER SECTION:
10000maps.com.          11664   IN      A       68.69.171.159
10000maps.com.          11664   IN      RRSIG   A 8 2 14400 20140710000000 201406
5Gpw/a/DESptKwAOermkCQ61pB4uvnoFsvtSNYCDM vWB2eutqOV3JXJIVgl3Zy6dvDPd2SpMhmDkH6Pm
GthS604RMfApl+VLKwl1f0Zx8yClxy cSg=

;; Query time: 5 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jul 02 00:06:39 CEST 2014
;; MSG SIZE  rcvd: 231
```



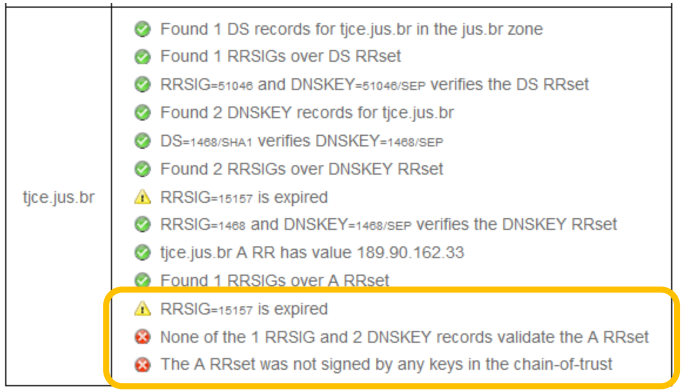
```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec 10000maps.com

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec 10000maps.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47992
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;10000maps.com.                 IN      A

;; ANSWER SECTION:
10000maps.com.          11733   IN      A       68.69.171.159

;; Query time: 4 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Jul 02 00:05:22 CEST 2014
;; MSG SIZE  rcvd: 58
```

The returned answer depends on which nameserver is selected by the resolver

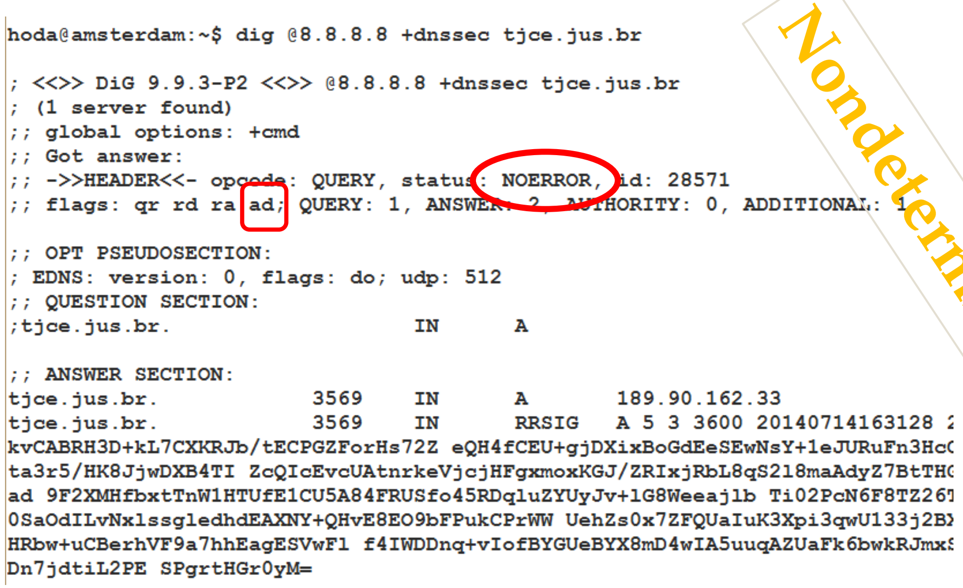
Inconsistency: Different Data in Nameservers



```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec tjce.jus.br

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec tjce.jus.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 48858
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

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

;; Query time: 246 msec
;; SERVER: 145.100.96.11#53(145.100.96.11)
;; WHEN: Wed Jul 02 01:48:55 CEST 2014
;; MSG SIZE  rcvd: 40
```

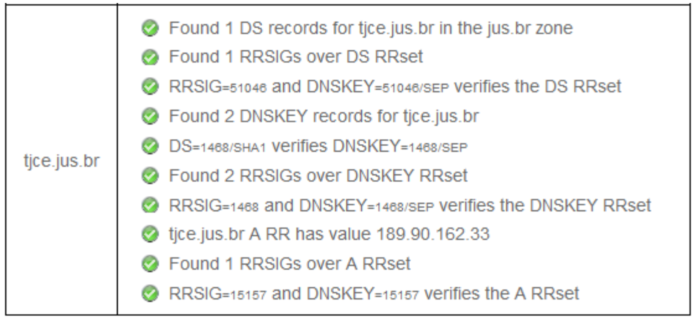


tjce.jus.br	✓ Found 1 DS records for tjce.jus.br in the jus.br zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=51046 and DNSKEY=51046/SEP verifies the DS RRset ✓ Found 2 DNSKEY records for tjce.jus.br ✓ DS=1468/SHA1 verifies DNSKEY=1468/SEP ✓ Found 2 RRSIGs over DNSKEY RRset ⚠ RRSIG=15157 is expired ✓ RRSIG=1468 and DNSKEY=1468/SEP verifies the DNSKEY RRset ✓ tjce.jus.br A RR has value 189.90.162.33 ✓ Found 1 RRSIGs over A RRset ⚠ RRSIG=15157 is expired ☒ None of the 1 RRSIG and 2 DNSKEY records validate the A RRset ☒ The A RRset was not signed by any keys in the chain-of-trust



```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec tjce.jus.br

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec tjce.jus.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28571
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;tjce.jus.br.                   IN      A

;; ANSWER SECTION:
tjce.jus.br.            3569    IN      A       189.90.162.33
tjce.jus.br.            3569    IN      RRSIG   A 5 3 3600 20140714163128
kvCABRH3D+kL7CXKRJb/tECPGZForHs72Z eQH4fCEU+gjDXixBoGdEeSEwNsY+1eJURuFn3Hc
ta3r5/HK8JjwDXB4TI ZcQIcEvcUAtnrkeVjcjHFgxmoxKGJ/ZRIxjRbL8qS218maAdyZ7BtTH
ad 9F2XMHfbxtTnW1HTUfE1CU5A84FRUSfo45RDqluZYUyJv+1G8Weeajlb Ti02PcN6F8TZ26
0SaOdILvNxlssgledhdEAXNY+QHvE8EO9bFPukCPrWW UehZs0x7ZFQUaIuK3Xpi3qwU133j2B
HRbw+uCBerhVF9a7hhEagESVwFl f4IWDDnq+vIofBYGUeBYX8mD4wIA5uuqAZUaFk6bwkRJmx
Dn7jdtiL2PE SPgrtHGr0yM=
```

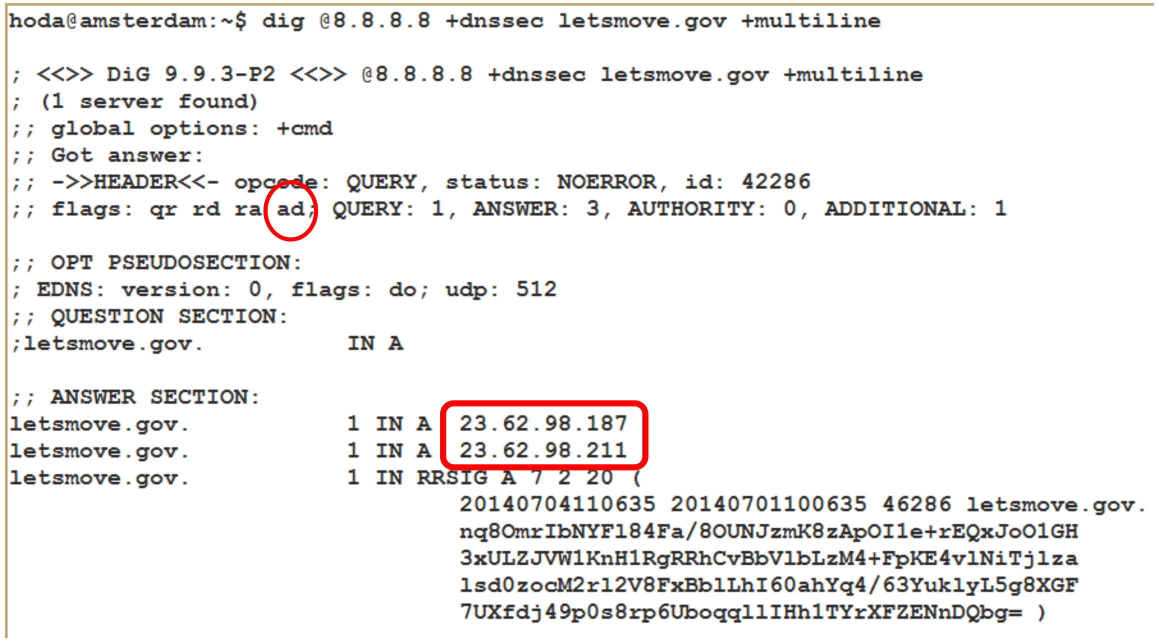
Nondeterministic behavior



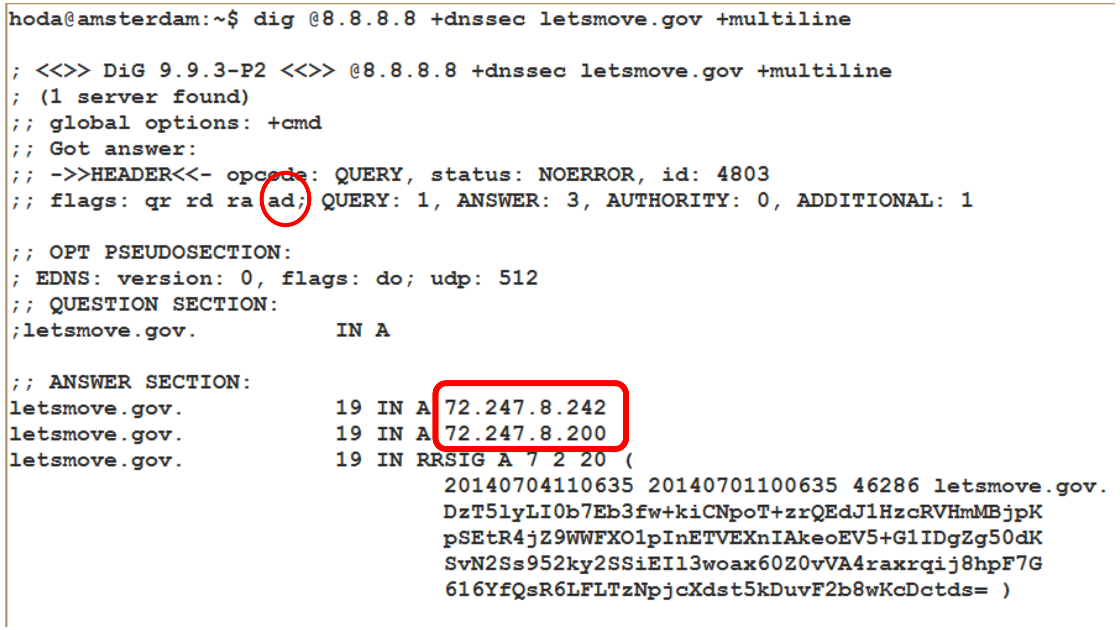
tjce.jus.br	✓ Found 1 DS records for tjce.jus.br in the jus.br zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=51046 and DNSKEY=51046/SEP verifies the DS RRset ✓ Found 2 DNSKEY records for tjce.jus.br ✓ DS=1468/SHA1 verifies DNSKEY=1468/SEP ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=1468 and DNSKEY=1468/SEP verifies the DNSKEY RRset ✓ tjce.jus.br A RR has value 189.90.162.33 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=15157 and DNSKEY=15157 verifies the A RRset

Consistency: Different Data in Nameservers

- Differences in A records



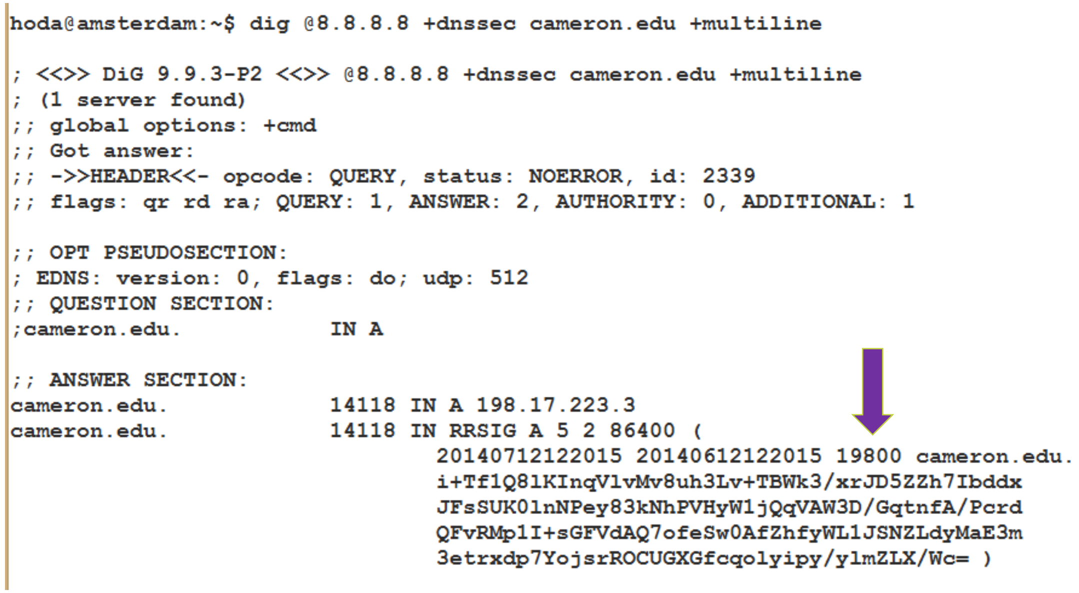
```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec letsmove.gov +multiline

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec letsmove.gov +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42286
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;letsmove.gov.           IN A

;; ANSWER SECTION:
letsmove.gov.            1 IN A  23.62.98.187
letsmove.gov.            1 IN A  23.62.98.211
letsmove.gov.            1 IN RRSIG A 7 2 20 (
                                 20140704110635 20140701100635 46286 letsmove.gov.
                                 nq8OmrIbNYF184Fa/8OUNJzmK8zApOI1e+rEQxJoO1GH
                                 3xULZJVW1KnH1RgRRhCvBbV1bLzM4+FpKE4vlNiTjlza
                                 1sd0zocM2rl2V8FxBblLhI60ahYq4/63YuklyL5g8XGF
                                 7UXfdj49p0s8rp6UboqqllIHh1TYrXFZENnDQbg= )
```



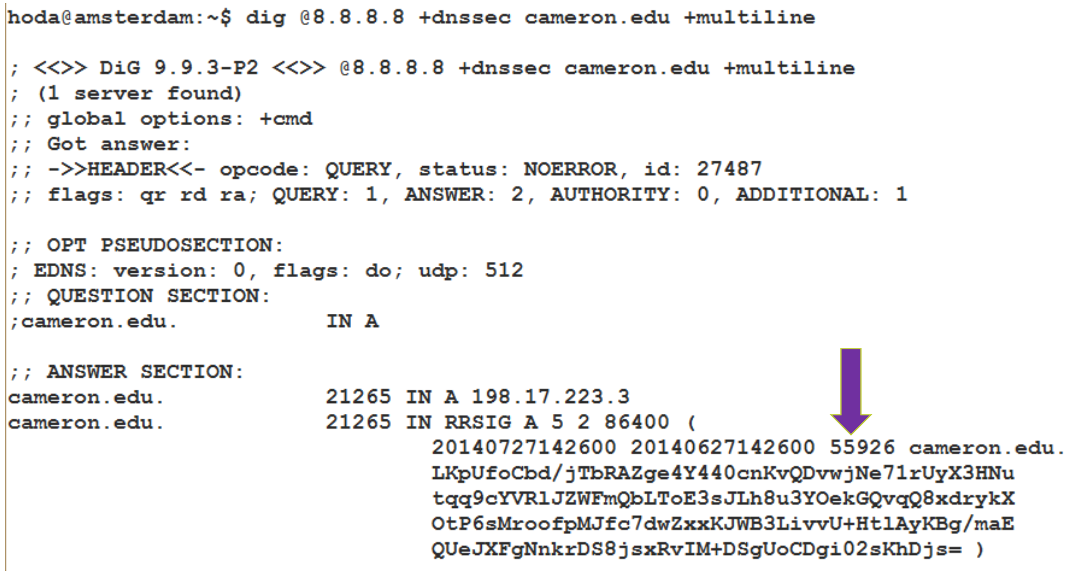
```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec letsmove.gov +multiline

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec letsmove.gov +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4803
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;letsmove.gov.           IN A

;; ANSWER SECTION:
letsmove.gov.            19 IN A 72.247.8.242
letsmove.gov.            19 IN A 72.247.8.200
letsmove.gov.            19 IN RRSIG A 7 2 20 (
                                 20140704110635 20140701100635 46286 letsmove.gov.
                                 DzT5lyLI0b7Eb3fw+kiCNpoT+zrQEdJ1HzcRVHmMBjpK
                                 pSEtR4jZ9WWFXO1pInETVEXnIAkeoEV5+G1IDgZg50dK
                                 SvN2Ss952ky2SSiEIl3woax60Z0vVA4raxrqij8hpF7G
                                 616YfQsR6LFLTzNpjcXdst5kDuvF2b8wKcDctds= )
```

Consistent: Different Data in Nameservers

- Differences in RRSIG
  - Multiple ZSK keys and signing with different keys



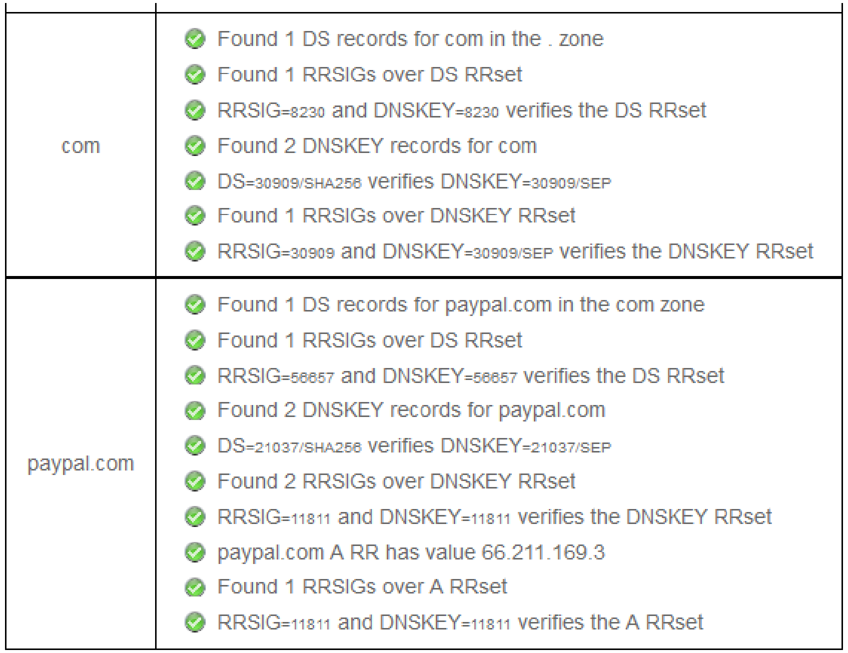
```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec cameron.edu +multiline

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec cameron.edu +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2339
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;cameron.edu.            IN A

;; ANSWER SECTION:
cameron.edu.             14118 IN A 198.17.223.3
cameron.edu.             14118 IN RRSIG A 5 2 86400 (
                                 20140712122015 20140612122015 19800 cameron.edu.
                                 i+Tf1Q81KInqVlvMv8uh3Lv+TBWk3/xrJD5ZZh7Ibddx
                                 JFsSUK01nNPey83kNhPVHyW1jQqVAW3D/GqtnfA/Pcrd
                                 QFvRMp1I+sGFVdAQ7ofeSw0AfZhfyWL1JSNZLdyMaE3m
                                 3etrxdp7YojsrROCUGXGfcqolyipy/ylmZLX/Wc= )
```



```
hoda@amsterdam:~$ dig @8.8.8.8 +dnssec cameron.edu +multiline

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 +dnssec cameron.edu +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27487
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;cameron.edu.            IN A

;; ANSWER SECTION:
cameron.edu.             21265 IN A 198.17.223.3
cameron.edu.             21265 IN RRSIG A 5 2 86400 (
                                 20140727142600 20140627142600 55926 cameron.edu.
                                 LKpUfoCbd/jTbRAZge4Y440cnKvQDvwjNe71rUyX3HNu
                                 tqq9cYVR1JZWFmQbLToE3sJLh8u3YOekGQvqQ8xdrykX
                                 OtP6sMroofpMJfc7dwZxxKJWB3LivvU+Ht1AyKBg/maE
                                 QUeJXFgNnkrDS8jsxRvIM+DSgUoCDgi02sKhDjs= )
```

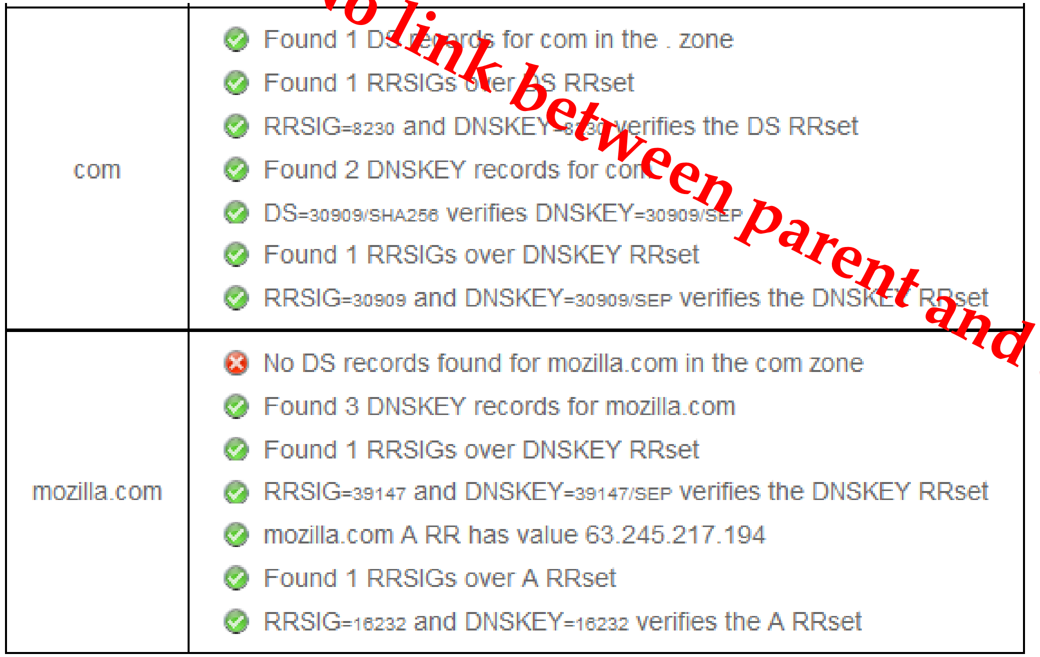
Consistent Data in Nameservers

- ~76% of the asked domains return RRSIGs with AD flag
- ~24% of the asked domains return RRSIGs with no AD flag



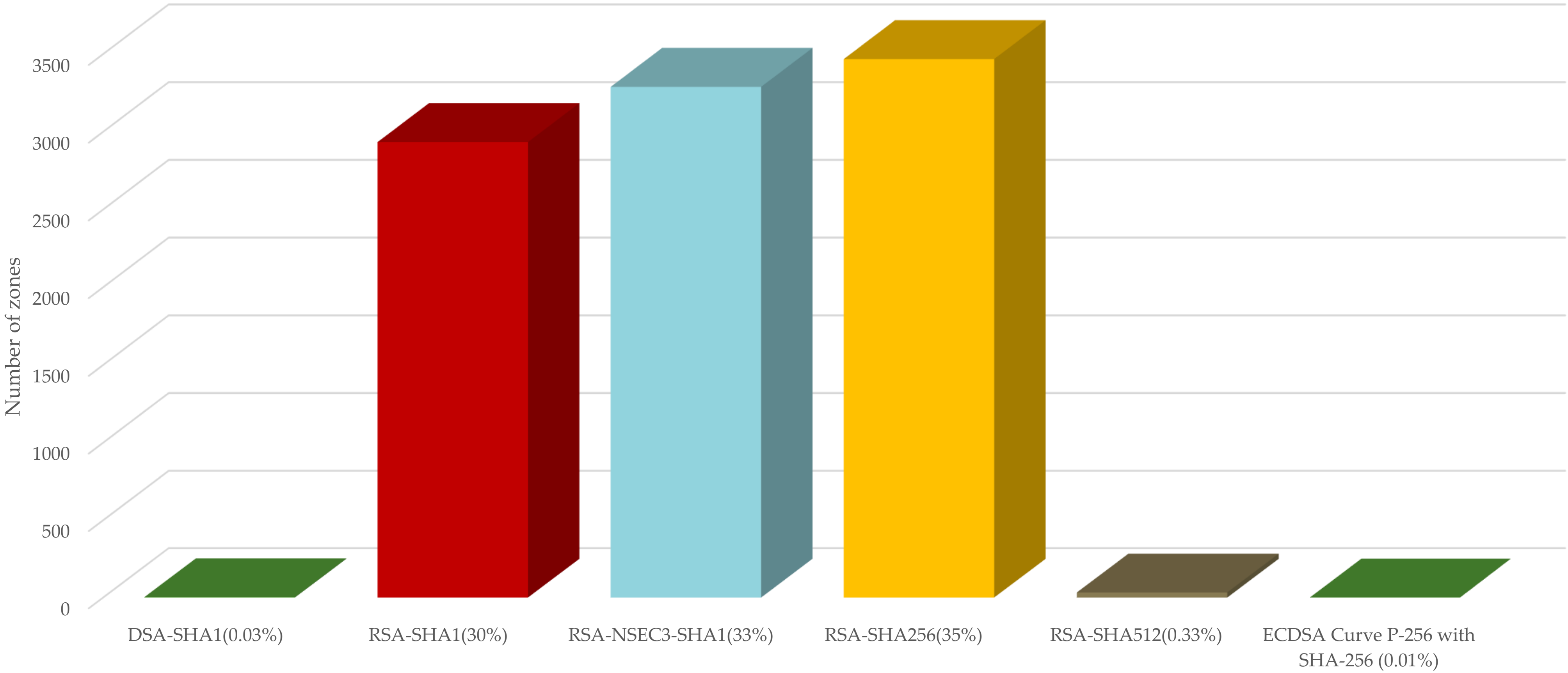
com	✓ Found 1 DS records for com in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=8230 and DNSKEY=8230 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=30909/SHA256 verifies DNSKEY=30909/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
paypal.com	✓ Found 1 DS records for paypal.com in the com zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=56657 and DNSKEY=56657 verifies the DS RRset ✓ Found 2 DNSKEY records for paypal.com ✓ DS=21037/SHA256 verifies DNSKEY=21037/SEP ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=11811 and DNSKEY=11811 verifies the DNSKEY RRset ✓ paypal.com A RR has value 66.211.169.3 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=11811 and DNSKEY=11811 verifies the A RRset

No link between parent and child



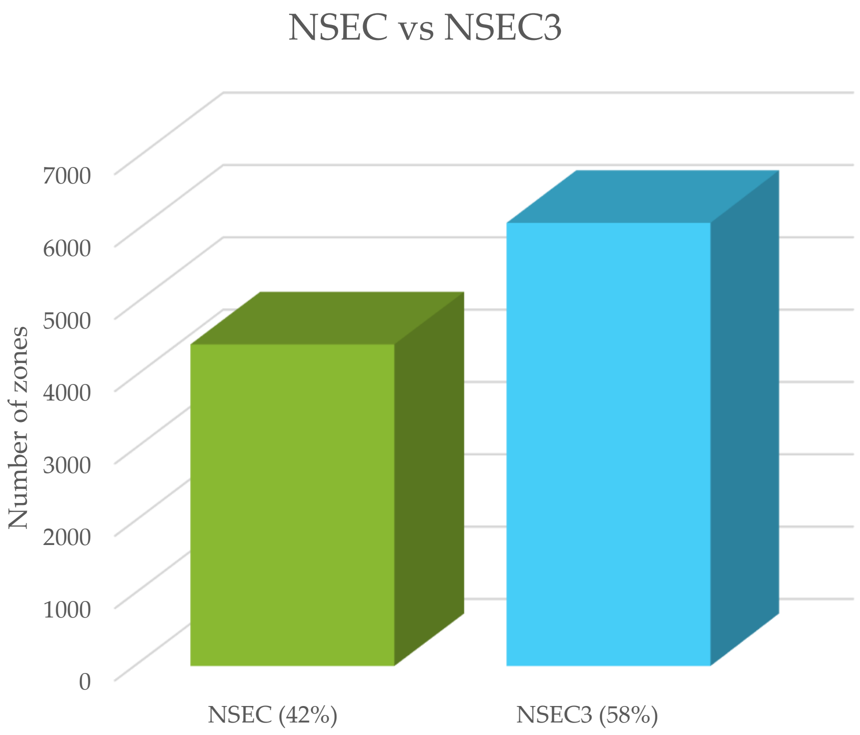
com	✓ Found 1 DS records for com in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=8230 and DNSKEY=8230 verifies the DS RRset ✓ Found 2 DNSKEY records for com ✓ DS=30909/SHA256 verifies DNSKEY=30909/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
mozilla.com	✗ No DS records found for mozilla.com in the com zone ✓ Found 3 DNSKEY records for mozilla.com ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=39147 and DNSKEY=39147/SEP verifies the DNSKEY RRset ✓ mozilla.com A RR has value 63.245.217.194 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=16232 and DNSKEY=16232 verifies the A RRset

Other checks: Common DNSSEC Algorithms



Other checks: NSEC and NSEC3

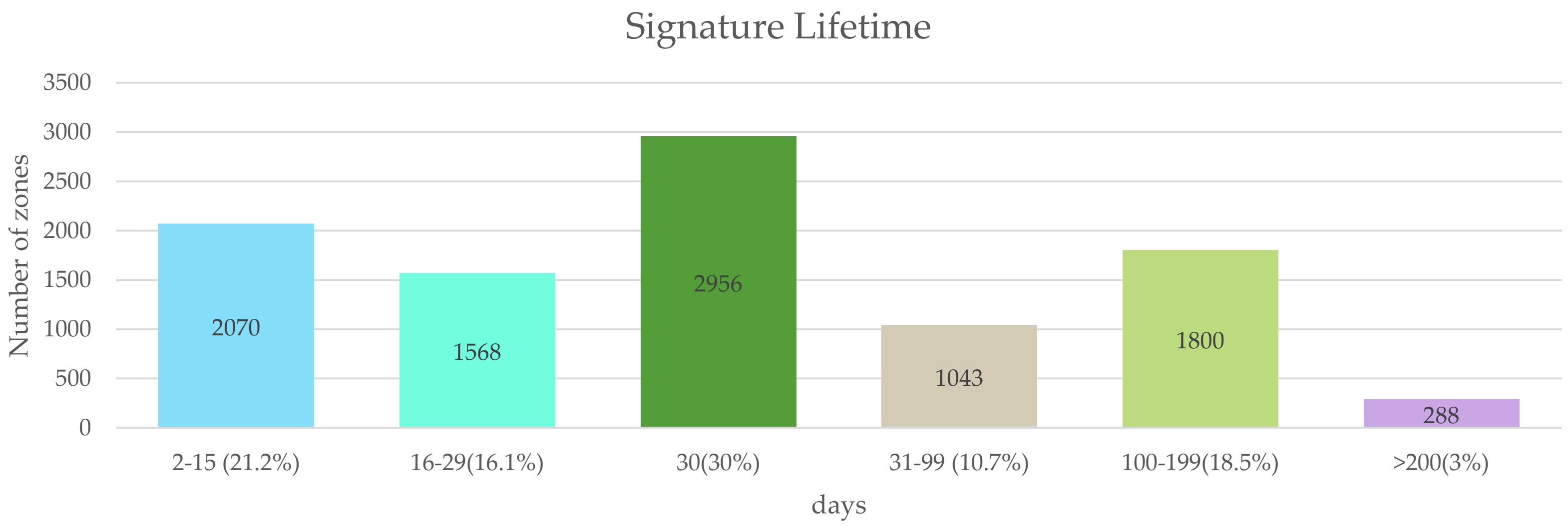
- Proof of non-existence
  - Pre-calculated records
  - NSEC vs NSEC3



Other checks: DNSSEC RRSIG Lifetime

- Signature lifetimes
  - Default value: Inception time 1 hour before
  - Default value: Expiration 30 days from now
  - Vary between 2 and 3,600 days

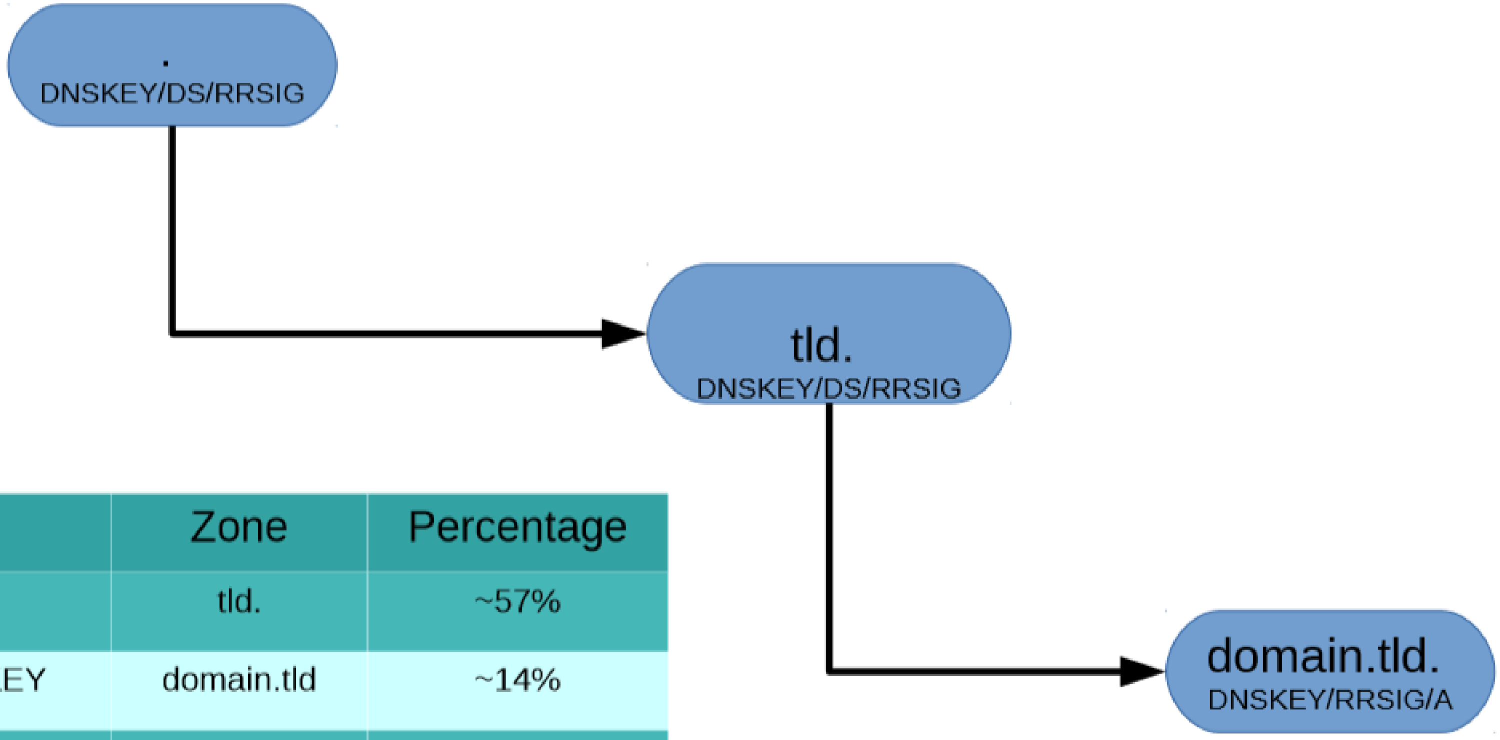
- Be sure about your servers accurate time
  - Validating resolvers has to check signature validity time



DNSSEC Misconfiguration

- **Missing DS** – no link between parent and child
- **Mismatch DS** – No DNSKEY matching DS in parent zone
  - None of DNSKEY records could be validated by any of DS records, the DNSKEY RRset was not signed by any keys in the chain-of-trust (the DNSSEC chain-of-trust is broken at this point)
- **Missing DNSKEY** – DNSKEY not available to validate RRSIG
- **Missing NSEC** – NSEC RRs not returned by authoritative server
  - No NSEC records in response, no NSEC record could prove that no records of type A
- **Missing RRSIG** – RRSIGs not returned by some servers
- **Bogus RRSIG** - if the zone was signed with different keys than the ones that are published in the zone data
  - DNSSEC signatures did not validate the RRset
- **Expired RRSIG** – Signature in RRSIG are expired
  - DNSSEC signatures did not validate the RRset

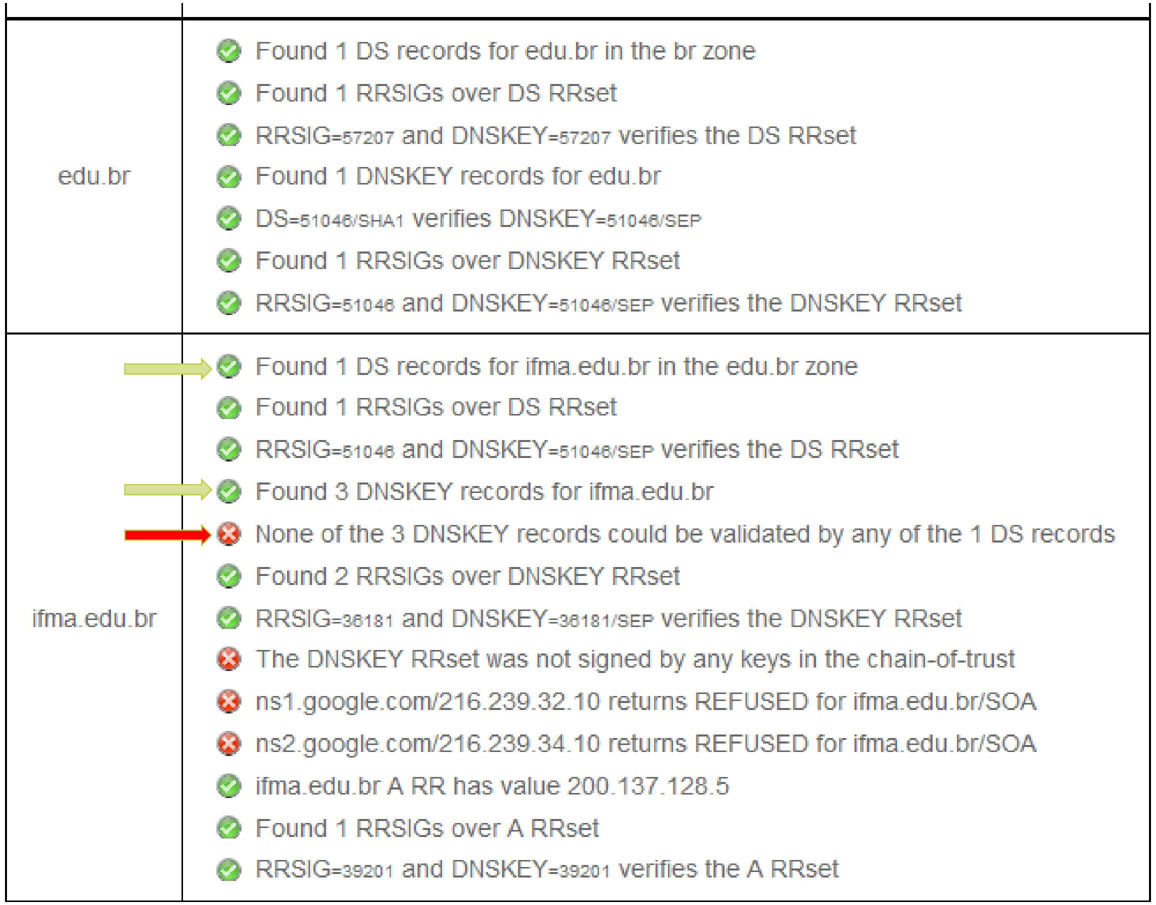
Delegation Errors



Error	Zone	Percentage
Missing DS	tld.	~57%
Missing DNSKEY	domain.tld	~14%
Signature Expired	domain.tld	~13.5%
Other	tld./domain.tld	~15.4%

DS Mismatch

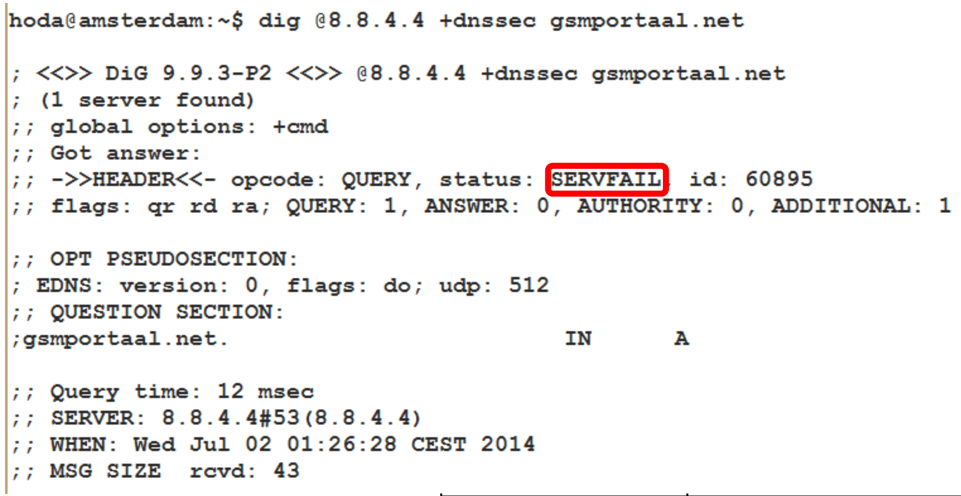
```
hoda@amsterdam:~$ dig @8.8.4.4 +dnssec ifma.edu.br

; <<>> DiG 9.9.3-P2 <<>> @8.8.4.4 +dnssec ifma.edu.br
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 45774
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;ifma.edu.br.                   IN      A

;; Query time: 522 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Wed Jul 02 01:25:22 CEST 2014
;; MSG SIZE  rcvd: 40
```



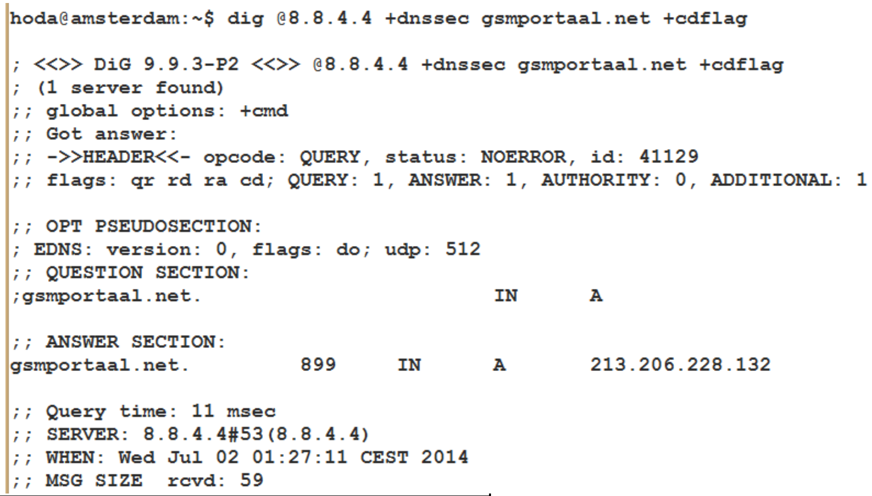
edu.br	✓ Found 1 DS records for edu.br in the br zone
	✓ Found 1 RRSIGs over DS RRset
	✓ RRSIG=57207 and DNSKEY=57207 verifies the DS RRset
	✓ Found 1 DNSKEY records for edu.br
	✓ DS=51046/SHA1 verifies DNSKEY=51046/SEP
	✓ Found 1 RRSIGs over DNSKEY RRset
	✓ RRSIG=51046 and DNSKEY=51046/SEP verifies the DNSKEY RRset
ifma.edu.br	✓ Found 1 DS records for ifma.edu.br in the edu.br zone
	✓ Found 1 RRSIGs over DS RRset
	✓ RRSIG=51046 and DNSKEY=51046/SEP verifies the DS RRset
	✓ Found 3 DNSKEY records for ifma.edu.br
	✗ None of the 3 DNSKEY records could be validated by any of the 1 DS records
	✓ Found 2 RRSIGs over DNSKEY RRset
	✓ RRSIG=36181 and DNSKEY=36181/SEP verifies the DNSKEY RRset
	✗ The DNSKEY RRset was not signed by any keys in the chain-of-trust
	✗ ns1.google.com/216.239.32.10 returns REFUSED for ifma.edu.br/SOA
	✗ ns2.google.com/216.239.34.10 returns REFUSED for ifma.edu.br/SOA
	✓ ifma.edu.br A RR has value 200.137.128.5
	✓ Found 1 RRSIGs over A RRset
	✓ RRSIG=39201 and DNSKEY=39201 verifies the A RRset

DNSKEY Missing

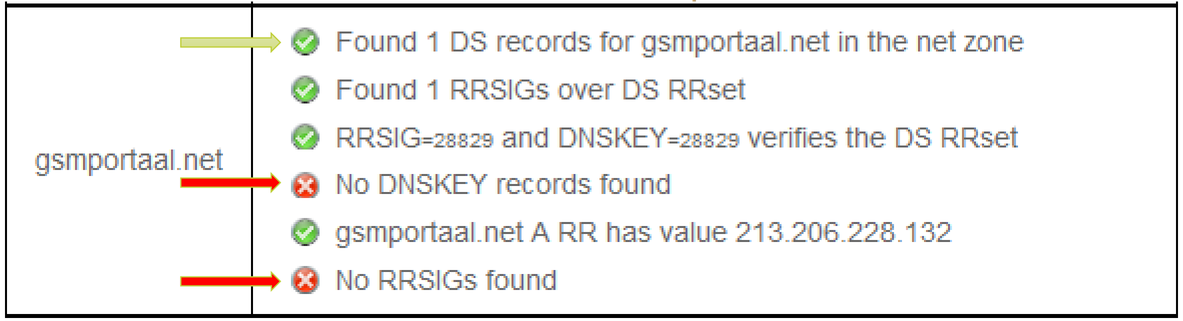
Turn DNSSEC off but forgot to interact with parent to remove the DS record: found 25 domains



```
hoda@amsterdam:~$ dig @8.8.4.4 +dnssec gsmportaal.net

; <<>> DiG 9.9.3-P2 <<>> @8.8.4.4 +dnssec gsmportaal.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 60895
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;gsmportaal.net.                        IN      A

;; Query time: 12 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Wed Jul 02 01:26:28 CEST 2014
;; MSG SIZE  rcvd: 43
```

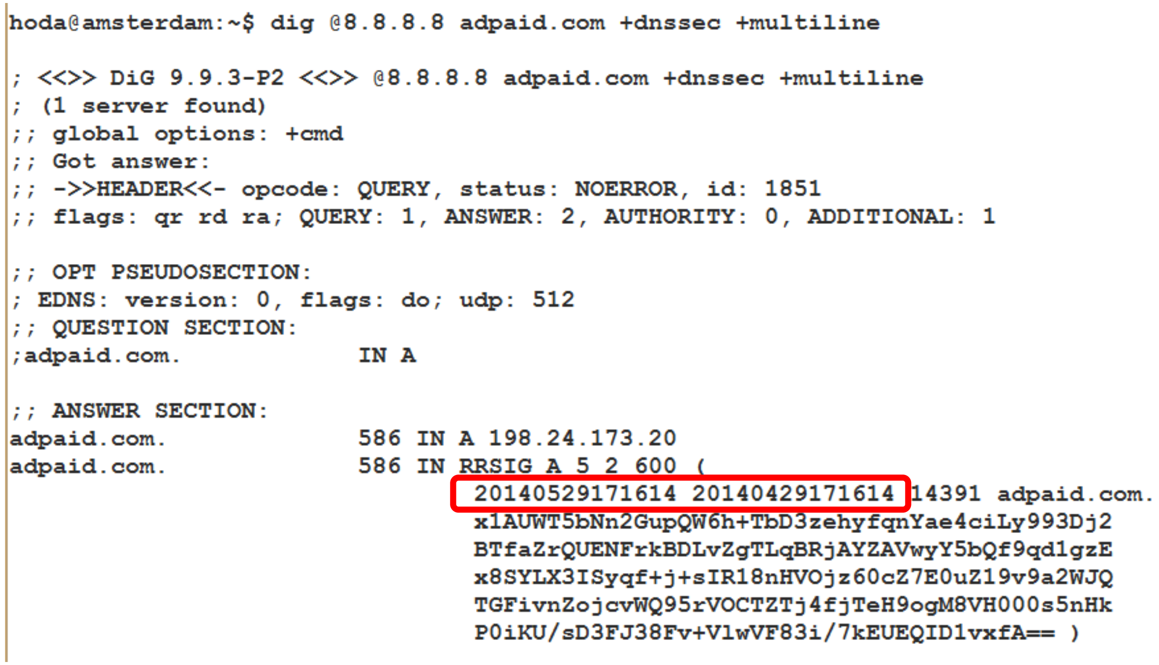


```
hoda@amsterdam:~$ dig @8.8.4.4 +dnssec gsmportaal.net +cdflag

; <<>> DiG 9.9.3-P2 <<>> @8.8.4.4 +dnssec gsmportaal.net +cdflag
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41129
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;gsmportaal.net.                        IN      A

;; ANSWER SECTION:
gsmportaal.net.         899     IN      A       213.206.228.132

;; Query time: 11 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: Wed Jul 02 01:27:11 CEST 2014
;; MSG SIZE  rcvd: 59
```

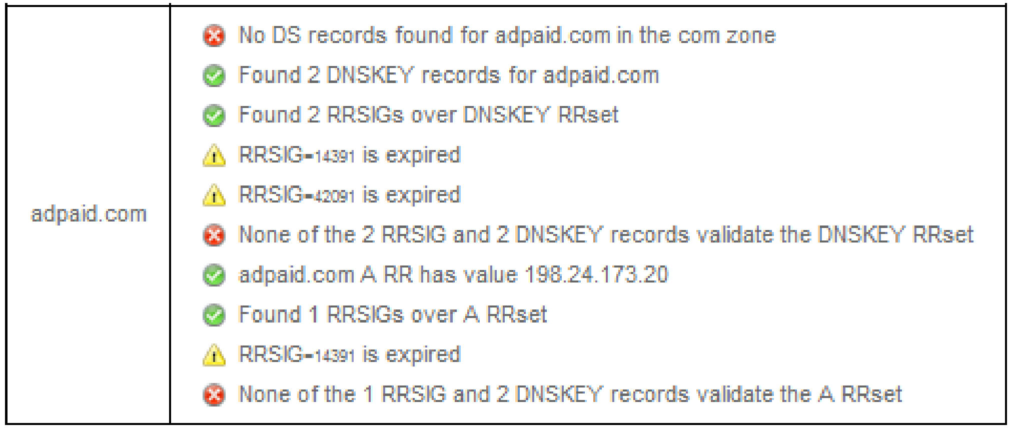


gsmportaal.net	✓ Found 1 DS records for gsmportaal.net in the net zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=28829 and DNSKEY=28829 verifies the DS RRset ✗ No DNSKEY records found ✓ gsmportaal.net A RR has value 213.206.228.132 ✗ No RRSIGs found

RRSIG Expired Dates



```
hoda@amsterdam:~$ dig @8.8.8.8 adpaid.com +dnssec +multiline

; <<>> DiG 9.9.3-P2 <<>> @8.8.8.8 adpaid.com +dnssec +multiline
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1851
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;adpaid.com.                IN A

;; ANSWER SECTION:
adpaid.com.                 586 IN A 198.24.173.20
adpaid.com.                 586 IN RRSIG A 5 2 600 (
                                 20140529171614 20140429171614 14391 adpaid.com.
                                 x1AUWT5bNn2GupQW6h+TbD3zehyfqnYae4ciLy993Dj2
                                 BTfaZrQUENFrkBDLvZgTLqBRjAYZAVwyY5bQf9qd1gzE
                                 x8SYLX3ISyqf+j+sIR18nHVOjz60cZ7E0uZ19v9a2WJQ
                                 TGFivnZojcvWQ95rVOCTZTj4fjTeH9ogM8VH000s5nHk
                                 P0iKU/sD3FJ38Fv+V1wVF83i/7kEUEQID1vxfA== )
```



adpaid.com	✗ No DS records found for adpaid.com in the com zone ✓ Found 2 DNSKEY records for adpaid.com ✓ Found 2 RRSIGs over DNSKEY RRset ⚠ RRSIG=14391 is expired ⚠ RRSIG=42091 is expired ✗ None of the 2 RRSIG and 2 DNSKEY records validate the DNSKEY RRset ✓ adpaid.com A RR has value 198.24.173.20 ✓ Found 1 RRSIGs over A RRset ⚠ RRSIG=14391 is expired ✗ None of the 1 RRSIG and 2 DNSKEY records validate the A RRset

Regular re-signing is part of the administrators' tasks (not only when changes occur)

Recommendation & Conclusion

- Our results showed that few administrators have deployed and maintained DNSSEC properly due to its burden and difficulties
  - Use scripts and online tools for checking the healthiness of the zone and monitor the zone regularly
  - Automate regular process as much as possible
  - Keep all nameservers' data updated to avoid inconsistencies

Any Questions?