(Ab)use of DNS

Translating your Domains into IP Addresses...

and more.

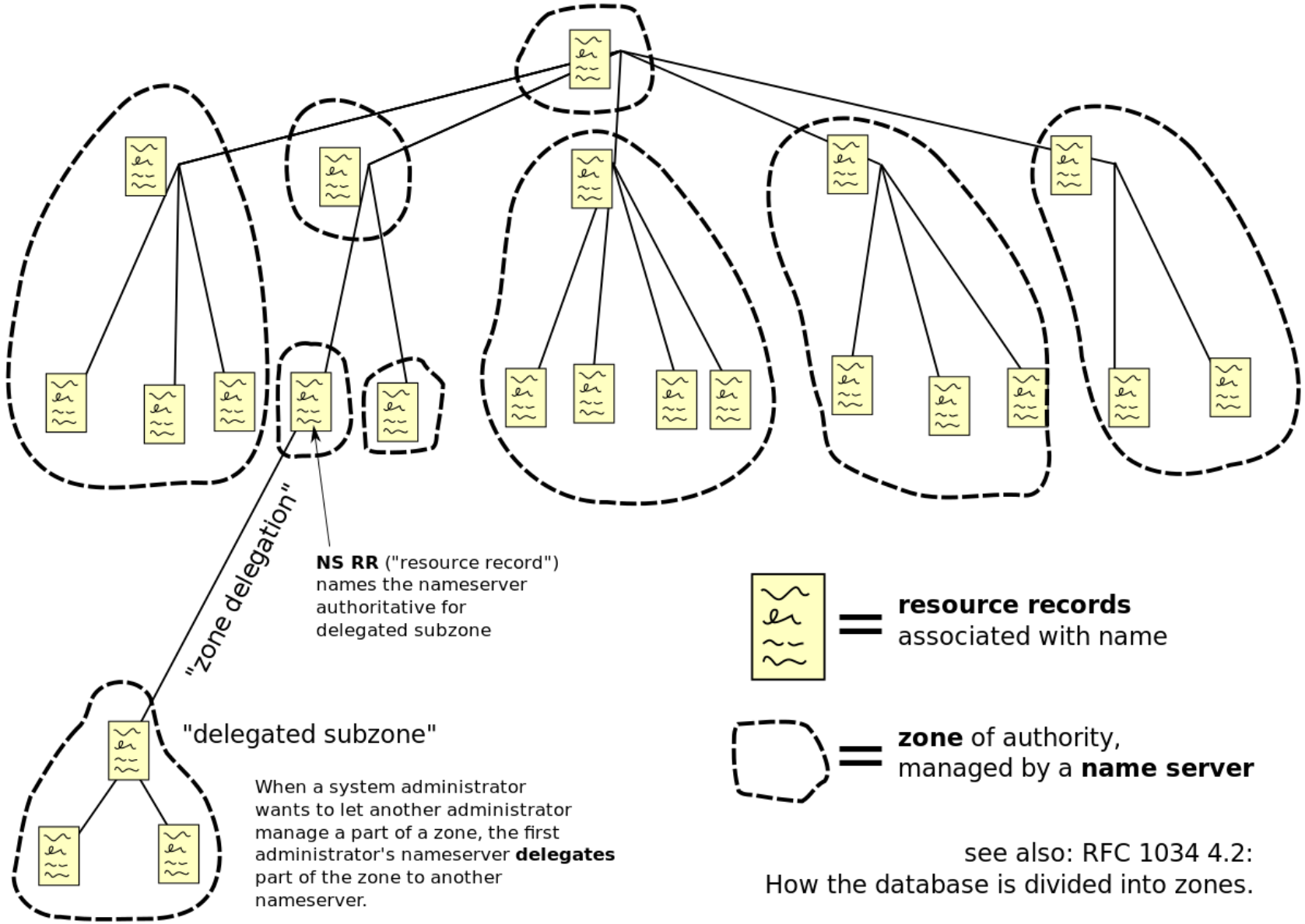
What is DNS?

- Hierarchical system of names
- Decentralized

DNS Zone

- Each Nameserver defines a "zone" of records
- e.g. `basis-ai.com` zone
- The zone may elect to delegate a child Nameserver for part of its zone (e.g. subdomain)

Domain Name Space



.

- The "root" of DNS
- Overseen by Internet Corporation for Assigned Names and Numbers (ICANN)
- "13" Name Servers
- More than that due to anycast
- Contains the Nameservers for Top Level Domains (TLDs)

Nameservers for `com.`

```
$ dig NS com.
;; QUESTION SECTION:
;com.                           IN      NS

;; ANSWER SECTION:
com.                    171845  IN      NS      j.gtld-servers.net.
com.                    171845  IN      NS      i.gtld-servers.net.
com.                    171845  IN      NS      f.gtld-servers.net.
com.                    171845  IN      NS      a.gtld-servers.net.
com.                    171845  IN      NS      l.gtld-servers.net.
com.                    171845  IN      NS      g.gtld-servers.net.
com.                    171845  IN      NS      k.gtld-servers.net.
com.                    171845  IN      NS      h.gtld-servers.net.
com.                    171845  IN      NS      m.gtld-servers.net.
com.                    171845  IN      NS      b.gtld-servers.net.
com.                    171845  IN      NS      e.gtld-servers.net.
com.                    171845  IN      NS      c.gtld-servers.net.
com.                    171845  IN      NS      d.gtld-servers.net.

;; ADDITIONAL SECTION:
c.gtld-servers.net.     85436   IN      A       192.26.92.30
d.gtld-servers.net.     85436   IN      A       192.31.80.30
j.gtld-servers.net.     85436   IN      A       192.48.79.30
i.gtld-servers.net.     85436   IN      A       192.43.172.30
f.gtld-servers.net.     85436   IN      A       192.35.51.30
a.gtld-servers.net.     85436   IN      A       192.5.6.30
l.gtld-servers.net.     85437   IN      A       192.41.162.30
g.gtld-servers.net.     85436   IN      A       192.42.93.30
k.gtld-servers.net.     85437   IN      A       192.52.178.30
h.gtld-servers.net.     85436   IN      A       192.54.112.30
m.gtld-servers.net.     85437   IN      A       192.55.83.30
b.gtld-servers.net.     85436   IN      A       192.33.14.30
e.gtld-servers.net.     85436   IN      A       192.12.94.30
```

Fully Qualified Domain Name (FQDN)

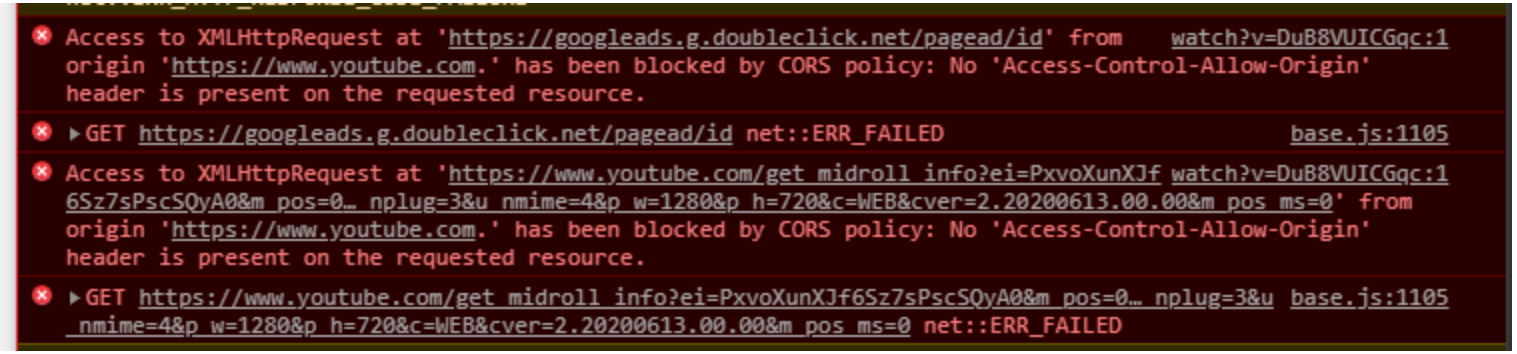
- Technically `basis-ai.com` is really `basis-ai.com.`

```
$ dig basis-ai.com

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;basis-ai.com.                  IN      A

;; ANSWER SECTION:
basis-ai.com.           300     IN      A       35.244.177.213
```

- Resolvers usually add the `.` for you or some local default (e.g. local service discovery)

YouTube Advertisement Blocking

- Visit `www.youtube.com.` instead!



Source

- Not sure if this is a bug in CORS implementation,
- or actually from the specification. 🤔

DNS Architecture

- Decentralised Name Servers
- Starts from the root
- Parent layer will contain NS record for the child layer

-

```
$ dig +noall +answer NS .
.                       494556  IN      NS      h.root-servers.net.
.                       494556  IN      NS      e.root-servers.net.
.                       494556  IN      NS      j.root-servers.net.
.                       494556  IN      NS      i.root-servers.net.
.                       494556  IN      NS      f.root-servers.net.
.                       494556  IN      NS      b.root-servers.net.
.                       494556  IN      NS      m.root-servers.net.
.                       494556  IN      NS      l.root-servers.net.
.                       494556  IN      NS      d.root-servers.net.
.                       494556  IN      NS      k.root-servers.net.
.                       494556  IN      NS      a.root-servers.net.
.                       494556  IN      NS      g.root-servers.net.
.                       494556  IN      NS      c.root-servers.net.

b.root-servers.net.     75913   IN      A       199.9.14.201
b.root-servers.net.     113885  IN      AAAA    2001:500:200::b
m.root-servers.net.     73453   IN      A       202.12.27.33
m.root-servers.net.     73453   IN      AAAA    2001:dc3::35
l.root-servers.net.     102000  IN      A       199.7.83.42
l.root-servers.net.     113885  IN      AAAA    2001:500:9f::42
d.root-servers.net.     94581   IN      A       199.7.91.13
d.root-servers.net.     113885  IN      AAAA    2001:500:2d::d
k.root-servers.net.     100634  IN      A       193.0.14.129
k.root-servers.net.     113885  IN      AAAA    2001:7fd::1
a.root-servers.net.     73415   IN      A       198.41.0.4
a.root-servers.net.     74384   IN      AAAA    2001:503:ba3e::2:30
g.root-servers.net.     102000  IN      A       192.112.36.4
g.root-servers.net.     113885  IN      AAAA    2001:500:12::d0d
c.root-servers.net.     79345   IN      A       192.33.4.12
c.root-servers.net.     113885  IN      AAAA    2001:500:2::c
h.root-servers.net.     102000  IN      A       198.97.190.53
h.root-servers.net.     113885  IN      AAAA    2001:500:1::53
e.root-servers.net.     99652   IN      A       192.203.230.10
e.root-servers.net.     113885  IN      AAAA    2001:500:a8::e
j.root-servers.net.     80188   IN      A       192.58.128.30
j.root-servers.net.     113885  IN      AAAA    2001:503:c27::2:30
i.root-servers.net.     102000  IN      A       192.36.148.17
i.root-servers.net.     113885  IN      AAAA    2001:7fe::53
f.root-servers.net.     102000  IN      A       192.5.5.241
f.root-servers.net.     113891  IN      AAAA    2001:500:2f::f
```

`.com.`

```
$ dig +noall +answer NS basis-ai.com.
basis-ai.com.           21600   IN      NS      ns-cloud-a4.googledomains.com.
basis-ai.com.           21600   IN      NS      ns-cloud-a1.googledomains.com.
basis-ai.com.           21600   IN      NS      ns-cloud-a2.googledomains.com.
basis-ai.com.           21600   IN      NS      ns-cloud-a3.googledomains.com.
```

basis-ai.com.

```
$ dig NS bedrock.basis-ai.com

;; QUESTION SECTION:
;bedrock.basis-ai.com.          IN      NS

;; ANSWER SECTION:
bedrock.basis-ai.com.   21600   IN      NS      ns-cloud-c2.googledomains.com.
bedrock.basis-ai.com.   21600   IN      NS      ns-cloud-c3.googledomains.com.
bedrock.basis-ai.com.   21600   IN      NS      ns-cloud-c4.googledomains.com.
bedrock.basis-ai.com.   21600   IN      NS      ns-cloud-c1.googledomains.com.

;; ADDITIONAL SECTION:
ns-cloud-c1.googledomains.com. 297122 IN A      216.239.32.108
ns-cloud-c1.googledomains.com. 298185 IN AAAA   2001:4860:4802:32::6c
ns-cloud-c2.googledomains.com. 297126 IN A      216.239.34.108
ns-cloud-c2.googledomains.com. 298296 IN AAAA   2001:4860:4802:34::6c
ns-cloud-c3.googledomains.com. 297156 IN A      216.239.36.108
ns-cloud-c3.googledomains.com. 298253 IN AAAA   2001:4860:4802:36::6c
ns-cloud-c4.googledomains.com. 296994 IN A      216.239.38.108
ns-cloud-c4.googledomains.com. 298327 IN AAAA   2001:4860:4802:38::6c
```

bedrock.basis-ai.com

```
$ dig bedrock.basis-ai.com

;; QUESTION SECTION:
;bedrock.basis-ai.com.          IN      A

;; ANSWER SECTION:
bedrock.basis-ai.com.   300     IN      A       35.240.210.204
```

Types of DNS Records - `A` and `AAAA`

```
$ dig www.google.com

;; QUESTION SECTION:
;www.google.com.                        IN      A

;; ANSWER SECTION:
www.google.com.         114     IN      A       172.217.194.105
www.google.com.         114     IN      A       172.217.194.99
www.google.com.         114     IN      A       172.217.194.106
www.google.com.         114     IN      A       172.217.194.103
www.google.com.         114     IN      A       172.217.194.147
www.google.com.         114     IN      A       172.217.194.104

$ dig AAAA www.google.com

;; QUESTION SECTION:
;www.google.com.                        IN      AAAA

;; ANSWER SECTION:
www.google.com.         109     IN      AAAA    2404:6800:4003:c04::69
```

Types of DNS Records - `MX`

```
$ dig MX basis-ai.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> MX basis-ai.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63394
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;basis-ai.com.                  IN      MX

;; ANSWER SECTION:
basis-ai.com.           3600    IN      MX      5 alt2.aspmx.l.google.com.
basis-ai.com.           3600    IN      MX      10 alt3.aspmx.l.google.com.
basis-ai.com.           3600    IN      MX      10 alt4.aspmx.l.google.com.
basis-ai.com.           3600    IN      MX      1 aspmx.l.google.com.
basis-ai.com.           3600    IN      MX      5 alt1.aspmx.l.google.com.

;; ADDITIONAL SECTION:
aspmx.l.google.com.     195     IN      A       74.125.24.26
aspmx.l.google.com.     195     IN      AAAA    2404:6800:4003:c04::1a
```

Types of DNS Records - `CNAME`

```
$ dig auth.basis-ai.com

;; QUESTION SECTION:
;auth.basis-ai.com.             IN      A

;; ANSWER SECTION:
auth.basis-ai.com.      3600    IN      CNAME   bdrk-cd-cm6eaqua5yzksmql.edge.tenants.auth0.com.
bdrk-cd-cm6eaqua5yzksmql.edge.tenants.auth0.com. 300 IN CNAME tenants.auth0.com.
tenants.auth0.com.      60      IN      A       54.71.132.32
tenants.auth0.com.      60      IN      A       44.228.7.2
tenants.auth0.com.      60      IN      A       52.12.28.200
```

Types of DNS Records - `CAA`

```
$ dig CAA auth.basis-ai.com

;; QUESTION SECTION:
;auth.basis-ai.com.             IN      CAA

;; ANSWER SECTION:
auth.basis-ai.com.      3568    IN      CNAME   bdrk-cd-cm6eaqua5yzksmql.edge.tenants.auth0.com.
bdrk-cd-cm6eaqua5yzksmql.edge.tenants.auth0.com. 268 IN CNAME tenants.auth0.com.
tenants.auth0.com.      60      IN      CAA     0 issue "letsencrypt.org"
tenants.auth0.com.      60      IN      CAA     0 issue "amazon.com"
tenants.auth0.com.      60      IN      CAA     0 issue "amazonaws.com"
tenants.auth0.com.      60      IN      CAA     0 issue "amazontrust.com"
tenants.auth0.com.      60      IN      CAA     0 issue "awstrust.com"
tenants.auth0.com.      60      IN      CAA     0 issue "comodoca.com"
```

Types of DNS Records - `TXT` aka master of (Ab)use

```
# Demonstrate domain control
$ dig TXT basis-ai.com

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;basis-ai.com.                  IN      TXT

;; ANSWER SECTION:
basis-ai.com.           3600    IN      TXT     "google-site-verification=80hiIqAESYhPJXpCUhzij24RjxOVWjRoWNguO6UTWA8"
basis-ai.com.           3600    IN      TXT     "google-site-verification=lTJdfZNdjSedLBKIOxoJeBsECEIYN2HpS89GuZ-yA2Y"
basis-ai.com.           3600    IN      TXT     "v=spf1 include:_spf.google.com include:sendgrid.net include:4788637.spf03.hubspotemail.net ~all"
```

`TXT` (Ab)use - Identity and Ownership Verification

- Used extensively over the internet to verify ownership of domain
- Used by Certificate Authorities to verify ownership and control of domain before issuing certificates (e.g. ACME protocol used by Let's Encrypt)
- Works by placing certain values in `TXT` records, manually or programmatically

`TXT` (Ab)use - DMARC

- System of using DNS Records to validate who is allowed to send email as the domain

`spf`

- Allowed list of email server addresses to send emails from

```
basis-ai.com.           3600    IN      TXT     "v=spf1 include:_spf.google.com include:sendgrid.net include:4788637.spf03.hubspotemail.net ~all"
```

`TXT` (Ab)use - DMARC

DKIM

- Lists public keys to verify email signatures
- Emails will specify a "selector" for the key being used

```
$ dig TXT google._domainkey.basis-ai.com

;; QUESTION SECTION:
;google._domainkey.basis-ai.com.        IN      TXT

;; ANSWER SECTION:
google._domainkey.basis-ai.com. 3600 IN TXT     "v=DKIM1;" "k=rsa;"
"p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCaJeDDAhBDSP0H1DiYu1aqMM12v1pXdpc0//eW/
bttioNKsVfHnOcrIkAchBOiJF2KTmLGVNFzNbvTNS7eOGn4Vre82jeXpx9SDgu5DxbU3OK6jO7tnT3HnybqGivcRbtr1YXfWKWOSdySoKxZXU1PlH95IFUJRVU3337H/OYW+QIDAQAB"
```

`TXT` (Ab)use - DMARC

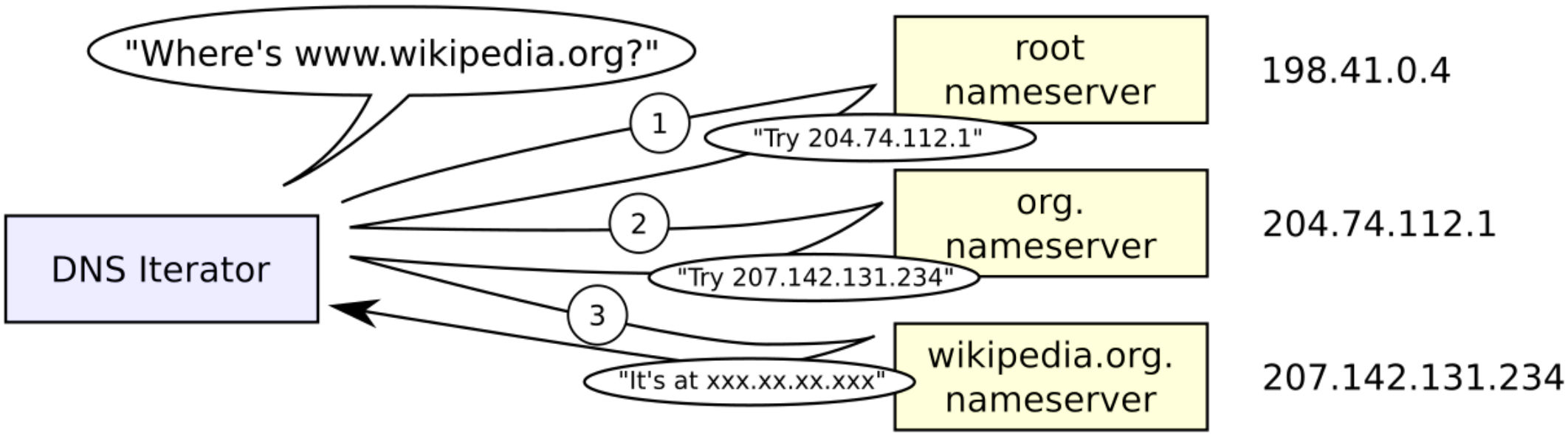
- DMARC policy tells recipients what to do with suspicious emails that fail either SPF or DKIM checks

```
$ dig TXT _dmarc.basis-ai.com

;; QUESTION SECTION:
;_dmarc.basis-ai.com.           IN      TXT

;; ANSWER SECTION:
_dmarc.basis-ai.com.    3600    IN      TXT     "v=DMARC1;" "p=quarantine;" "sp=reject;" "adkim=s;"
"aspf=r;" "rua=mailto:dmarc@basis-ai.com,mailto:awjeb3c7@ag.ap.dmarcian.com"
```

Read more

Resolving

- Sending DNS Queries to a DNS Server, usually on port 53
- When you connect to your network, your gateway's DHCP server usually sets itself as the DNS server
- Your Gateway will then use the DNS server assigned to it by your ISP DHCP
- Iteratively by the client
- Or done recursively where the DNS server sends queries "upstream"


"Where's www.wikipedia.org?"
DNS Iterator
1
"Try 204.74.112.1"
root nameserver
198.41.0.4
2
"Try 207.142.131.234"
org. nameserver
204.74.112.1
3
"It's at xxx.xx.xx.xxx"
wikipedia.org. nameserver
207.142.131.234

DNS Caching

- Results are cached with a TTL
- Reduce load on the root servers
- Updates to Nameservers will take time to propogate.

DNS Usage - Censorship!

```
# Ashley Madison
$ dig @dnssec1.singnet.com.sg www.amson.icu

;; QUESTION SECTION:
;www.amson.icu.                 IN      A

$ dig @8.8.8.8 www.amson.icu

;; QUESTION SECTION:
;www.amson.icu.                 IN      A

;; ANSWER SECTION:
www.amson.icu.          1798    IN      A       192.64.119.168
```

DNS Usage - Censorship!

- Even more nefarious in Indonesia!
- Packet sniffing will intercept and hijack plaintext DNS requests to `8.8.8.8`!
- Use DNS over TLS (DOT) or DNS over HTTPS (DOH)

DNS Usage - Ad blocking with Pi-hole

```
$ dig @8.8.8.8 js.hs-analytics.net

;; QUESTION SECTION:
;js.hs-analytics.net.           IN      A

;; ANSWER SECTION:
js.hs-analytics.net.    286     IN      A       104.17.67.176
js.hs-analytics.net.    286     IN      A       104.17.71.176
js.hs-analytics.net.    286     IN      A       104.17.69.176
js.hs-analytics.net.    286     IN      A       104.17.70.176
js.hs-analytics.net.    286     IN      A       104.17.68.176

$ dig js.hs-analytics.net

;; QUESTION SECTION:
;js.hs-analytics.net.           IN      A
```


Pi-hole
hostname: raspberrypi
Pi-hole
Status
Active
Temp: 70.4 °C
Load: 0.06 0.03 0.01
Memory usage: 56.5 %
MAIN NAVIGATION
Dashboard
Query Log
Long term data
Whitelist
Blacklist
Group Management
Disable
Tools
Network
Settings
Local DNS Records
Logout
Donate
Help
Total queries (17 clients)
17,925
Queries Blocked
859
Percent Blocked
4.8%
Domains on Blocklist
94,541
Total queries over last 24 hours
800
600
400
200
0
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
Client activity over last 24 hours
800
600
400
200
0
12:00
14:00
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
Query Types
A (IPv4)
AAAA (IPv6)
ANY
SRV
SOA
PTR
TXT
NAPTR
Queries answered by
blocklist
cache
localhost
Top Permitted Domains
Domain
Hits
Frequency
ccc-api.cloudapp.net
409
autopush.prod.mozaws.net
327
profile.accounts.firefox.com
290
mail.google.com
285
Top Blocked Domains
Domain
Hits
Frequency
telemetry.dropbox.com
374
mobile.pipe.aria.microsoft.com
176
www.youtube.com
89
ping.ui.com
34

Problems

- DNS Cache Poisoning
- No way to validate DNS Records
- Lack of DNS Query Privacy (e.g. Indonesia DNS hijacking!)

DNSSEC

- Digitally sign DNS records
- Implemented with *more* DNS record types
- Not all TLDs support (e.g. `.ai` does not)

Reading Materials

- `dig` + DNSSEC
- DNSSEC
- Cloudflare Post

Resource Record (RR)

```
basis-ai.com.          3398    IN      TXT     "google-site-verification=lTJdfZNdjSedLBKIOxoJeBsECEIYN2HpS89GuZ-yA2Y"
```

Components:

1. Owner: `basis-ai.com`
2. Type: `TXT`
3. Class: `IN` (Internet)
4. TTL: 3398
5. rdata - the data

RRSet

- A set of Resource Records

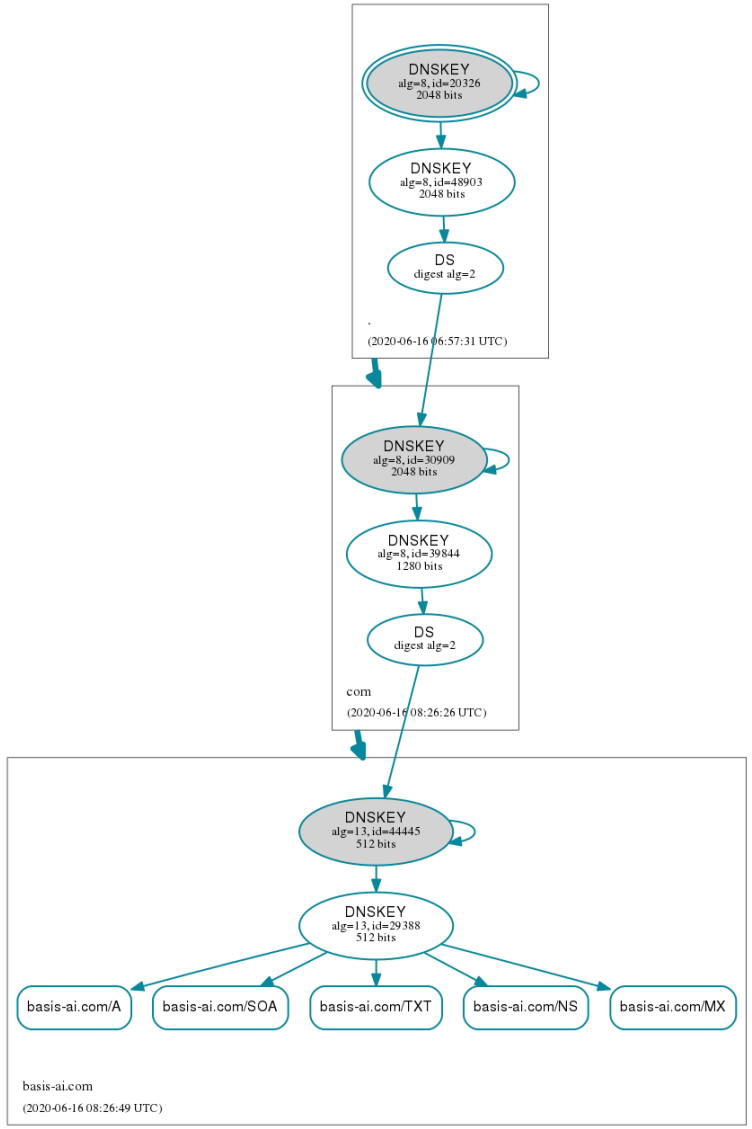
```
$ dig TXT basis-ai.com

;; QUESTION SECTION:
;basis-ai.com.                  IN      TXT

;; ANSWER SECTION:
basis-ai.com.           3600    IN      TXT     "v=spf1 include:_spf.google.com include:sendgrid.net include:4788637.spf03.hubspotemail.net ~all"
basis-ai.com.           3600    IN      TXT     "google-site-verification=80hiIqAESYhPJXpCUhzij24RjxOVWjRoWNguO6UTWA8"
basis-ai.com.           3600    IN      TXT     "google-site-verification=lTJdfZNdjSedLBKIOxoJeBsECEIYN2HpS89GuZ-yA2Y"
```

RRSig

- One Signature for the RRSet
- Recursively validated to root

```
$ dig +dnssec TXT basis-ai.com

;; QUESTION SECTION:
;basis-ai.com.                  IN      TXT

;; ANSWER SECTION:
basis-ai.com.           3009    IN      TXT     "v=spf1 include:_spf.google.com include:sendgrid.net include:4788637.spf03.hubspotemail.net ~all"
basis-ai.com.           3009    IN      TXT     "google-site-verification=80hiIqAESYhPJXpCUhzij24RjxOVWjRoWNguO6UTWA8"
basis-ai.com.           3009    IN      TXT     "google-site-verification=lTJdfZNdjSedLBKIOxoJeBsECEIYN2HpS89GuZ-yA2Y"
basis-ai.com.           3009    IN      RRSIG   TXT 13 2 3600 20200704054318 20200612054318 29388 basis-ai.com. uSSmYuWSH+5wWhWUk2LY1oik
+nxwIXSfy5f97fjKLTM7AHV28Vud8G6V MMfm1azcGTi682Xs03fRiQZjOKiqfQ==
```

Source


DNSKEY
alg=8, id=20326
2048 bits
DNSKEY
alg=8, id=48903
2048 bits
DS
digest alg=2
.
(2020-06-16 06:57:31 UTC)
DNSKEY
alg=8, id=30909
2048 bits
DNSKEY
alg=8, id=39844
1280 bits
DS
digest alg=2
com
(2020-06-16 08:26:26 UTC)
DNSKEY
alg=13, id=44445
512 bits
DNSKEY
alg=13, id=29388
512 bits
basis-ai.com/A
basis-ai.com/SOA
basis-ai.com/TXT
basis-ai.com/NS
basis-ai.com/MX
basis-ai.com
(2020-06-16 08:26:49 UTC)

DNSKEY

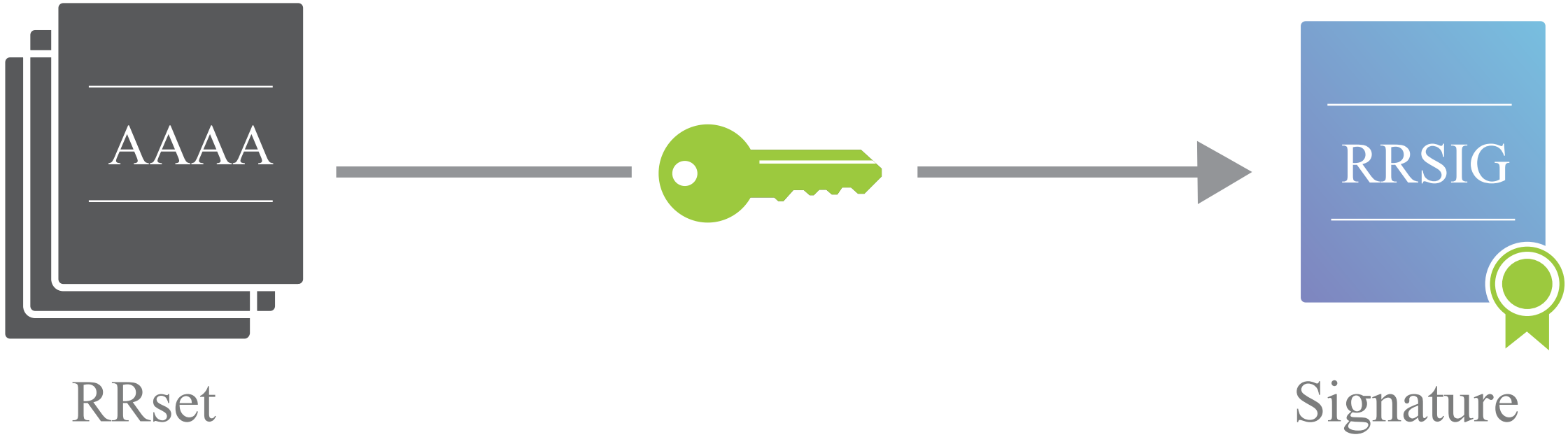
```
$ dig +dnssec DNSKEY basis-ai.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> +dnssec DNSKEY basis-ai.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24699
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;basis-ai.com.                  IN      DNSKEY

;; ANSWER SECTION:
basis-ai.com.           222     IN      DNSKEY  257 3 13 sK8vHLxnYzqu9ox+LLwHSlUeZe/TZi0xMIMEUtIvbJtBXqEcSlNKAaKx nQv6RCYGN3oI/
FSS4EXyHinfutfoYw==
basis-ai.com.           222     IN      DNSKEY  256 3 13 yYSfQi6LaGU70sbBgh3Oacl0dVSXhvCbMbgrKDot6pc3u0w62SvO456d WJ5Yy1Nme+iTWH0yj3SO/
IGA89TjrQ==
basis-ai.com.           222     IN      RRSIG   DNSKEY 13 2 300 20200704054318 20200612054318 44445 basis-ai.com. 5Fw5yqwW7IszfoaO
+qxX96x4bQAo2rhpGxP7b1ua8aL9gIP6000F79BM LrhzS5VbQ8ixAeAKy/fjS1IOvy36iA==
```

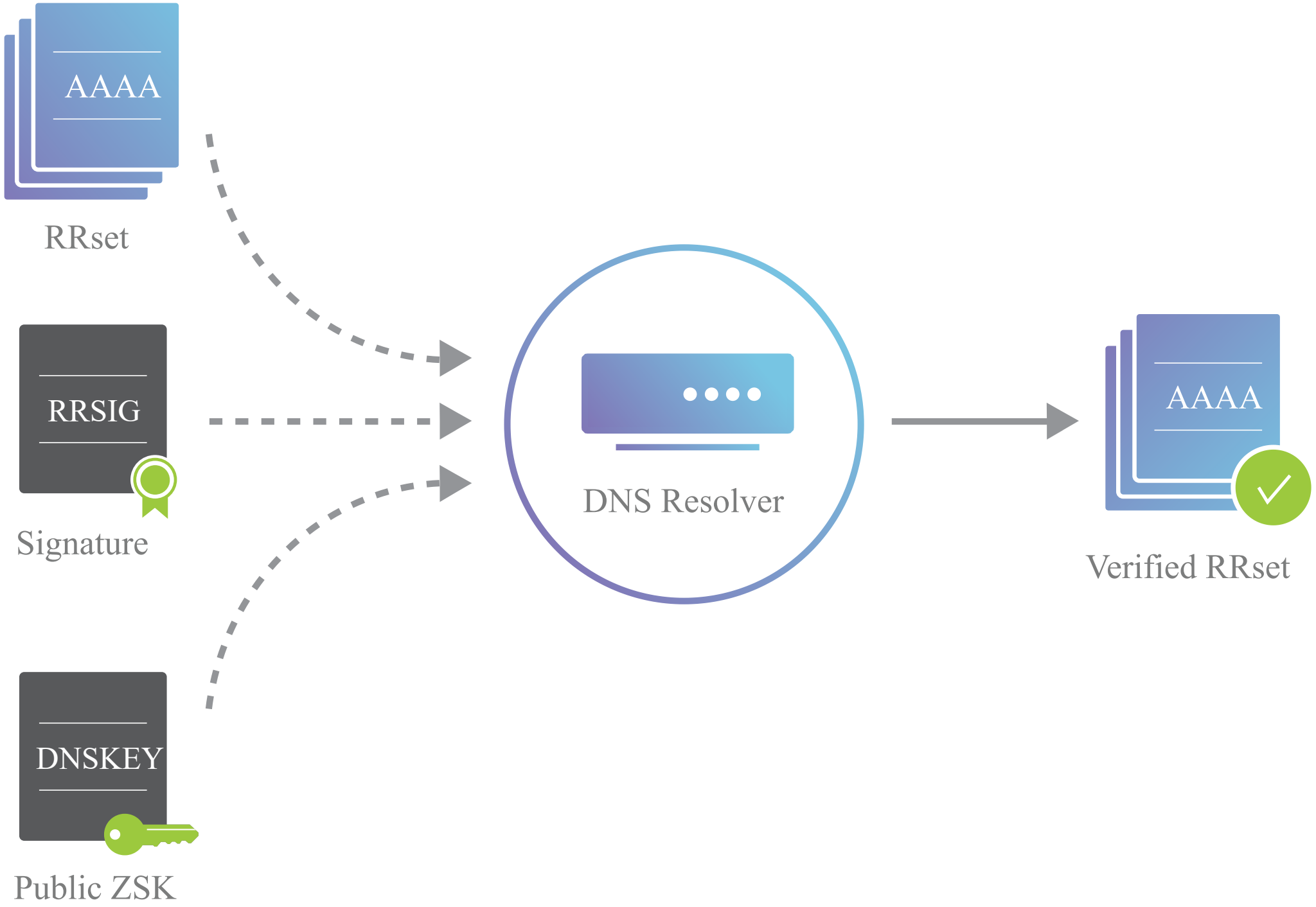
- Flags: Zone Signing Key (257) vs Key Signing Key (256)
- Protocol: Fixed to 3
- Algorithm: See list
- Public Key Material

Zone Signing Key (ZSK)

- Can be rotated by the domain owner easily
- ZSK used to sign all non DNSKEY RRSets
- The appropriate DNSKEY RR is used to validate the RRSIGs

```
basis-ai.com.           222     IN      DNSKEY  256 3 13 yYSfQi6LaGU70sbBgh3Oacl0dVSXhvCbMbgrKDot6pc3u0w62SvO456d WJ5Yy1Nme+iTWH0yj3SO/
IGA89TjrQ==
```

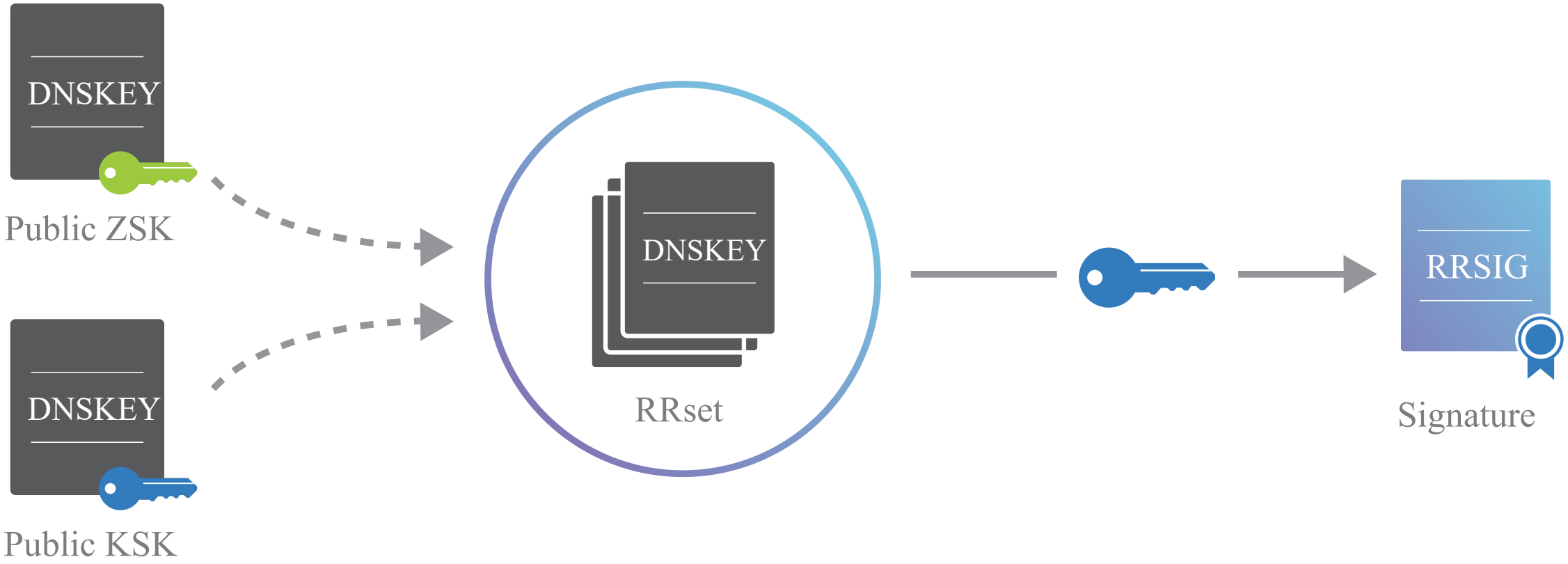


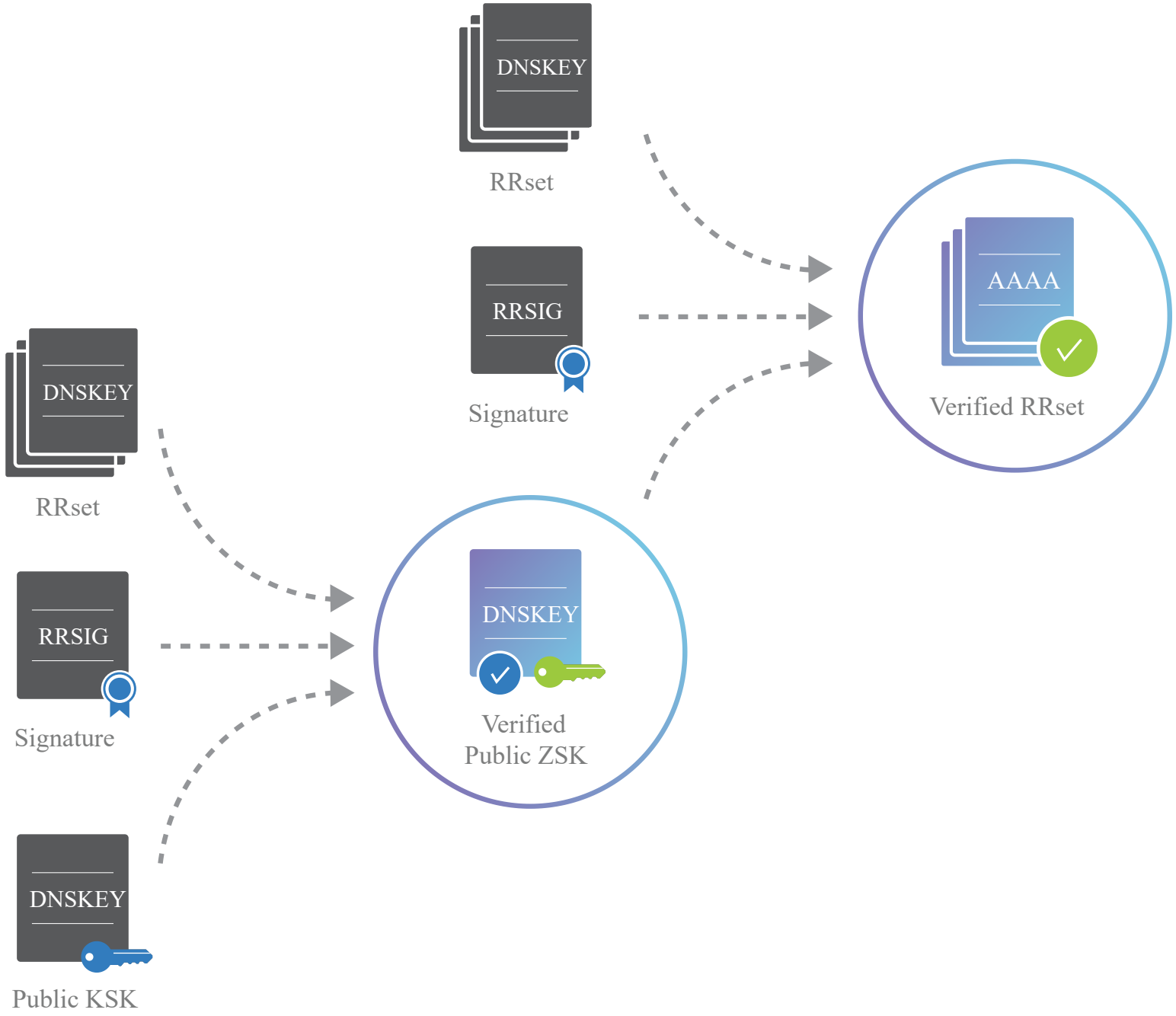

AAAA
RRset
RRSIG
Signature
DNSKEY
Public ZSK
DNS Resolver
AAAA
Verified RRset

Key Signing Key (KSK)

- Used to sign DNSKEY RRSets
- The appropriate DNSKEY RR is used to validate the RRSIG of the DNSKEY
- Harder to rotate

```
basis-ai.com.           222     IN      DNSKEY  257 3 13 sK8vHLxnYzqu9ox+LLwHSlUeZe/TZi0xMIMEUtIvbJtBXqEcSlNKAaKx nQv6RCYGN3oI/
FSS4EXyHinfutfoYw==
```



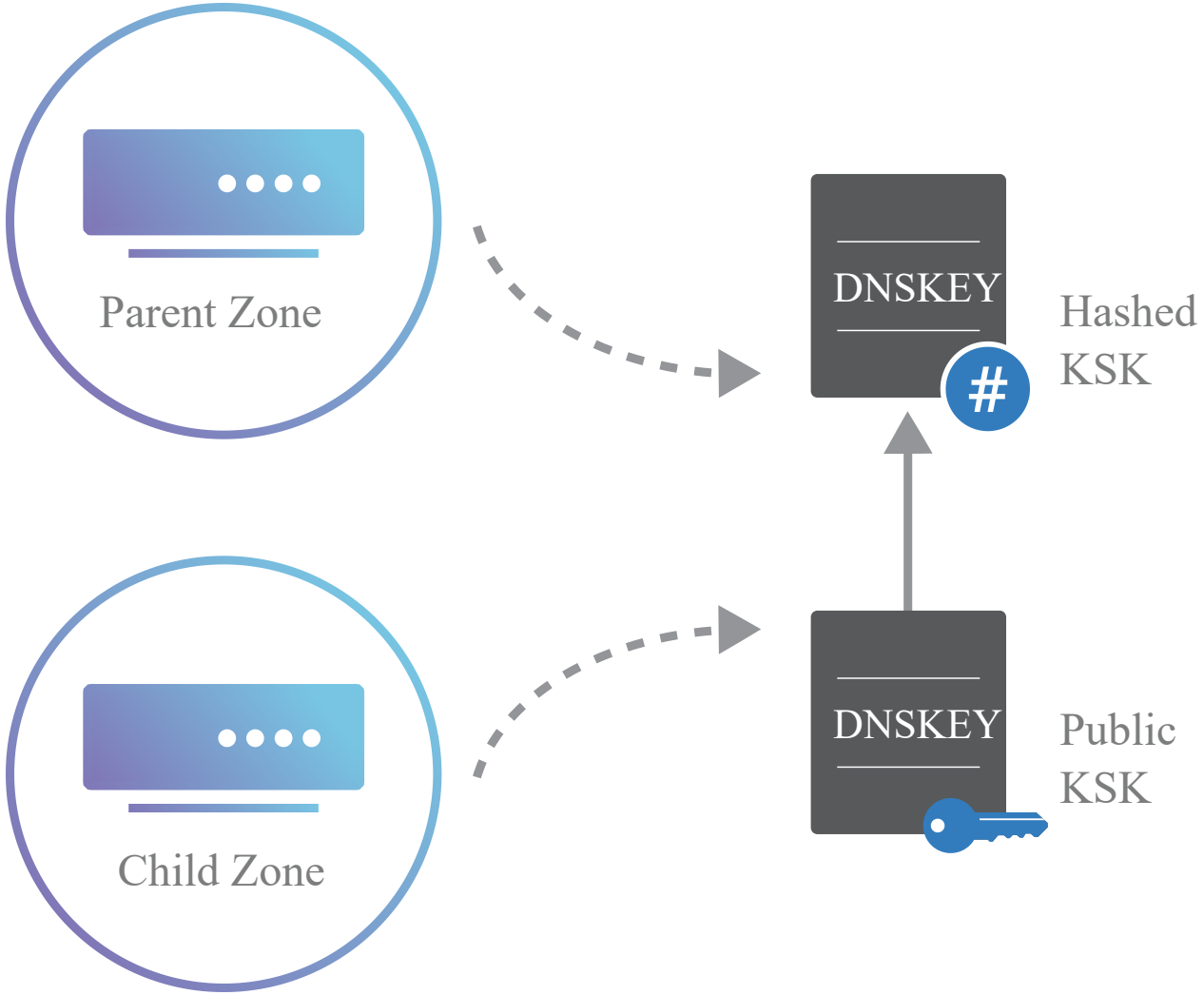

DNSKEY
RRset
RRSIG
Signature
AAAA
Verified RRset
DNSKEY
RRset
RRSIG
Signature
DNSKEY
Verified
Public ZSK
DNSKEY
Public KSK

DS Record

- The KSK is embedded in a DS record that is submitted "upwards" (i.e. to `com.`)

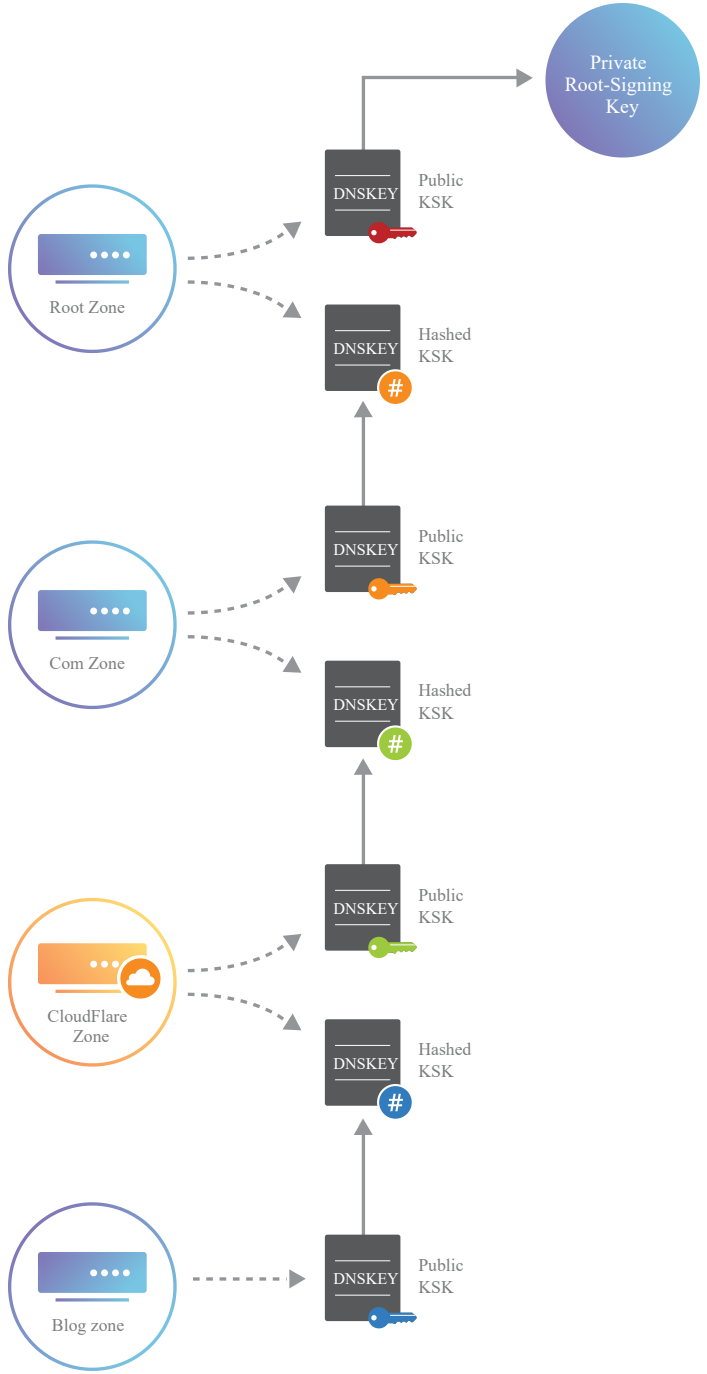
```
$ dig +dnssec DS basis-ai.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> +dnssec DS basis-ai.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19654
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;basis-ai.com.                  IN      DS

;; ANSWER SECTION:
basis-ai.com.           86400   IN      DS      44445 13 2 9B05C6EA7028958C69F8E47410E7BD3E782C60B41519192CF75D0648 E0200191
basis-ai.com.           86400   IN      RRSIG   DS 8 2 86400 20200621055752 20200614044752 39844 com.
FXLj45HvljmJI6aKW3M9V6vcX4G8iYEtA2yHkmAeZKB7AhMECdfOOzT0 bQ7oDgA8qgowmhxSfM9rEz9gZM3VP/I38HscP5mVB5n6pmVx3TdJx8cX ptQvGl3Px6d/
whdAoH7hmUk8gnNPl8xfRZfcNGjqxw/g7Gi55KqF9kJB Xuon21Bjg8H7uF6EwprAh9K5ybn0DL9HbkEbSxYNNBf7NA==
```

- Key tag of DNSSKEY: some numeric identifier
- Algorithm
- Digest Algorithm
- Digest of DNSSKEY RR containing the KSK


Parent Zone
Child Zone
DNSKEY
#
Hashed
KSK
DNSKEY
Public
KSK

DS Record of `.com`

```
$ dig +dnssec DS com

;; QUESTION SECTION:
;com.                           IN      DS

;; ANSWER SECTION:
com.                    33224   IN      DS      30909 8 2 E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF C41A5766
com.                    33224   IN      RRSIG   DS 8 1 86400 20200628170000 20200615160000 48903 . GZ8NQtY
+xGXh1NnD1GOeeC6KDbETHDtlStzJSEmaFXplSb8KWzfg5SIN ilLGGEXFBtkktbf5v3KH6bhkt3r7LS90E5nzinZcUWHETxkBG+fdGj+z
+aU4AW5pjYxhnVGaeBEMS6yJN3gfdfgJguH5ajAC9lZs83Ed7dhzvONy a7tx4U2kC5zpY95HrvJZmtKxaEsPfy7Z2BSqrLGPMVlsQsY7UdGdM5Ox
Ey4U4q2KRIQMwwXxxR4AnwdBF7jfewM7AEQ/oNiLMisFj6gqxadGwT7t 0blsyjQ2wbzZmL55Ck33uZwHZXN8T2bA98eDUR8x+rCBpyo28qTBiOiG 3nmeBQ==
```


Private
Root-Signing
Key
DNSKEY
Public
KSK
Root Zone
DNSKEY
Hashed
KSK
#
DNSKEY
Public
KSK
Com Zone
DNSKEY
Hashed
KSK
#
DNSKEY
Public
KSK
CloudFlare
Zone
DNSKEY
Hashed
KSK
#
DNSKEY
Public
KSK
Blog zone

Root Key

Immensely powerful key at the root of the internet...

```
$ dig DNSKEY .

;; QUESTION SECTION:
;.                              IN      DNSKEY

;; ANSWER SECTION:
.                       120698  IN      DNSKEY  256 3 8 AwEAAc4qsciJ5MdMUIu4n/pSTsSiU9OCyAanPTe5TcMX4v1hxhpFwiTG
QUv3BXT6IAO4litrZKTUaj4vitqHW1+RQsHn3k/gSvt7FwyQwpy0mEnS hBgr6RQiGtlBODNY67sTl+W8M/b6SLTAaaDri3BO5u6wrDs149rMELJA doVBjmXW
+zRH3kZzh3lwyTZsYtk7L+3DYbTiiHq+sRB4F9XoBPAz5Psv 4q4EiPq07nW3acbW84zTz3CyQUmQkJT9VB1oUKHz6sNoyccqzcMX4q1G
HAYpQ7FAXlKMxidoN1Ay5DWANgTmgJXzKhcI2nIZoq1x3yq4814O1LQd 9QP68gI37+0=
.                       120698  IN      DNSKEY  257 3 8 AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3 +/
4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF 0jLHwVN8efS3rCj/
EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd RUfhHdY6+cn8HFRm
+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN R1AkUTV74bU=
```

Root Signing Ceremony

- Securely stored in two locations
- Multiple participants perform only parts of the ceremony
- Participants of various affliations
- Audited by two Big Four
- Keys are stored in safes requiring multiple (physical) keys
- Very complicated process!


Hardware Failure

No Record and Enumeration

- How to verify the absence of a record?
- "Next Secure Record": `NSEC` or `NSEC3`
- But now an attacker can enumerate the records...
- Read more here

Encrypted DNS

DNS over HTTPS (DOH)

- Wrap DNS in HTTPS over port 443
- Looks just like HTTPS traffic (pros and cons)
- Better privacy since they cannot be differentiated

DNS over TLS (DOT)

- Wrap DNS UDP Datagrams in TLS over port 853
- Distinct traffic (pros and cons)
- Better control by network administrators (filtering malicious traffic for e.g.)

Conclusion

- DNS is extremely important
- Unfortunately used as a source of "identity" on the internet
- Protect it at all cost!