CANHEIT 2011
The Nature of Technology

DNS Security

Russell Sutherland ~ I+TS ~ University of Toronto
russell.sutherland@utoronto.ca

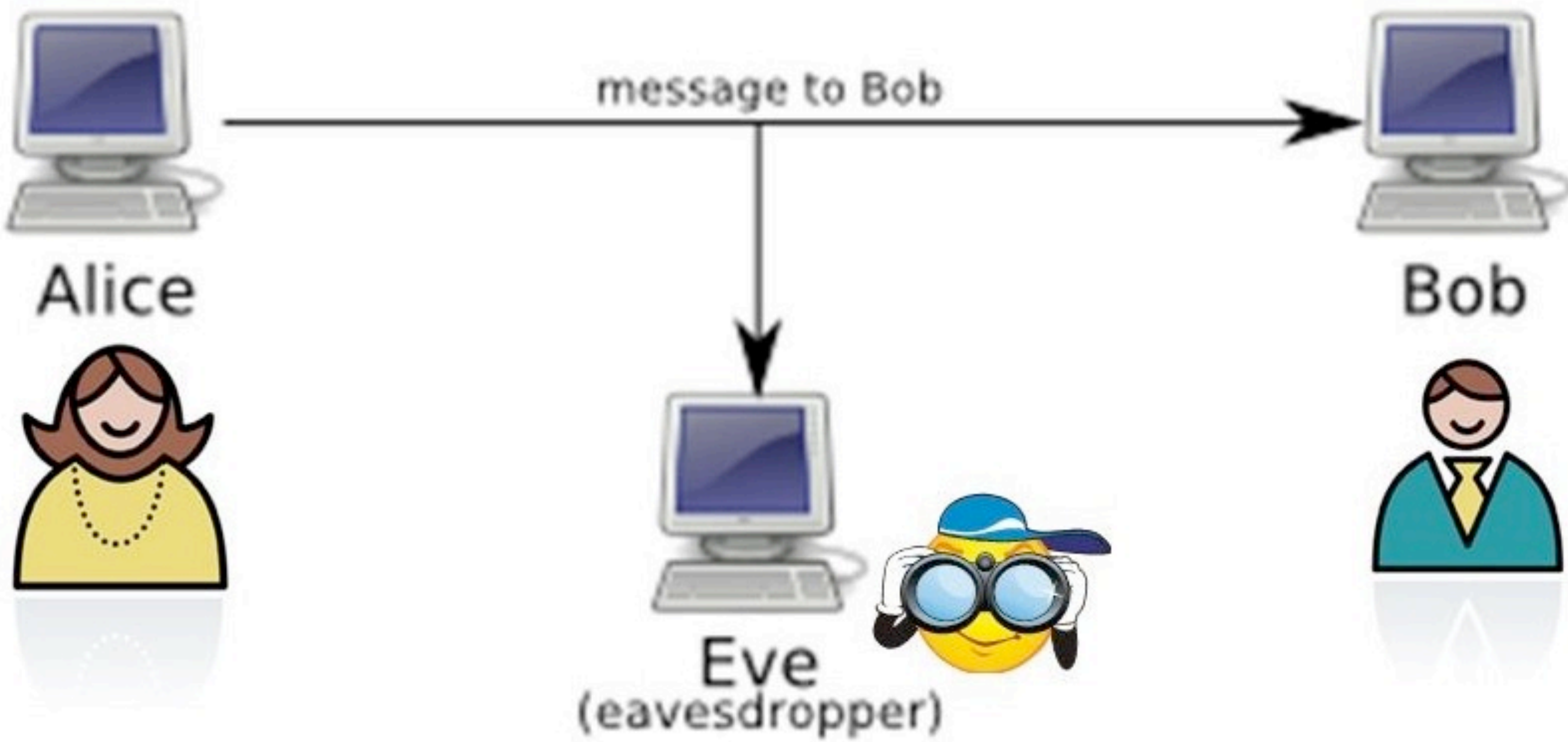
<0>

Caveat Emptor

Computer security
usually means...

Communication between two parties

But it's complicated


message to Bob
Alice
Bob
Eve
(eavesdropper)

Eve **is** the Wo(Man) in the Middle

3 goals of good computer security



Confidentiality…

despite espionage...

e.g. Eve wants to steal data

But to Eve it's all gibberish

Integrity…

despite corruption...

e.g. Eve wants to change data

Alice and Bob are NOT getting the wrong data

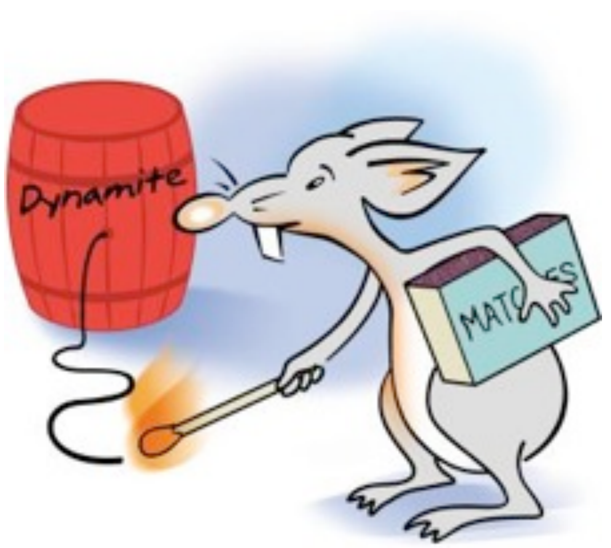
Forged data is detected

e.g. Not knowing that data has been corrupted is a violation of integrity

Availability...

despite sabotage...

e.g. Eve wants to destroy data



Bob and Alice are getting the right data

e.g. DoS attack is a violation of availability

e.g. Blocking data is a violation of availability

Computer security usually means…

Cryptography

Cryptography usually means…

Mathematics

Mathematics usually means...

Rigorous proofs

Rigorous proof
means ...

The masses* trust the few elite who “know”

* the intelligent, educated ones are included here

e.g.

Pierre de Fermat

Famous "Last" Theorem

Andrew Wiles

1637

1994/95

$$a^n + b^n \neq c^n$$

$$\{n \geq 3,\ \ a, b, c > 0\ \}\ a, b, c, n \in \mathbb{Z}$$

It takes a very great deal of mathematical knowledge to understand Wile’s proof; the original paper is hundreds of pages and when I tried to read it I couldn't get past page one; this highlights the fact that proof really has to do with authority and trust, not whether a computer can verify the mathematician's steps

Allan Reeve Wilks Ph.D., Statistician, AT&T Bell Labs
allan@research.att.com

Therefore …

it's good to remember

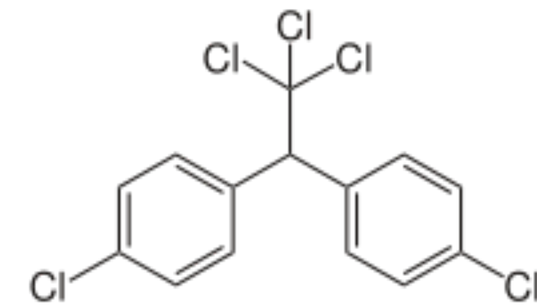
when it comes to security and cryptography in particular ...

There are professionals*, stuffed shirts, plumbers and actors

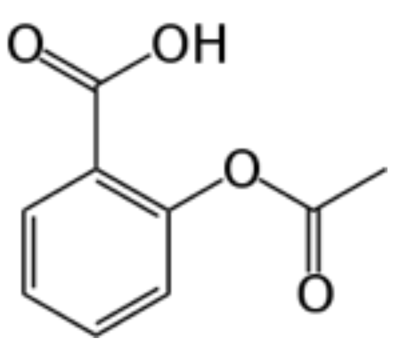
* Even the professionals do not always agree.

* This is certainly the case in DNS security.

<1>



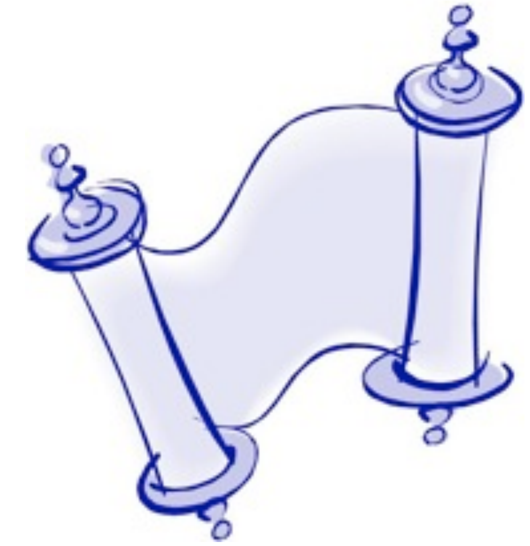
Nomenclature



DNS == Domain Name System

Stub Resolver

Caching Name Server



Authoritative Name Server

<2>

Function of the DNS

$$f(x) = \sqrt{a^2 - 4ab + b^2}$$

Name/Number Lookup Service

Map/Translate Names to Addresses*

* there are other important data /resource records

E.g.

www.mcgill.ca

www.mcgill.ca

132.216.177.140

A record

worldbank.int

worldbank.int

dns1.worldbank.org

dns2.worldbank.org

dns3.worldbank.org

dns4.worldbank.org

NS record

president@whitehouse.gov

president@whitehouse.gov

mail1.eop.gov.

mail2.eop.gov.

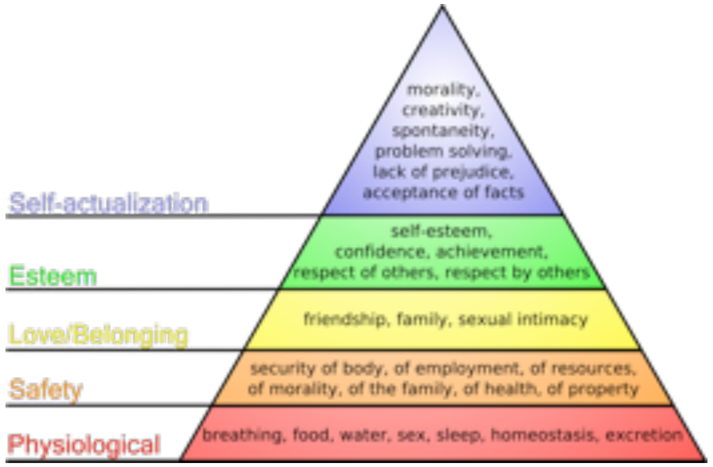
mail3.eop.gov.

mail4.eop.gov.

MX record

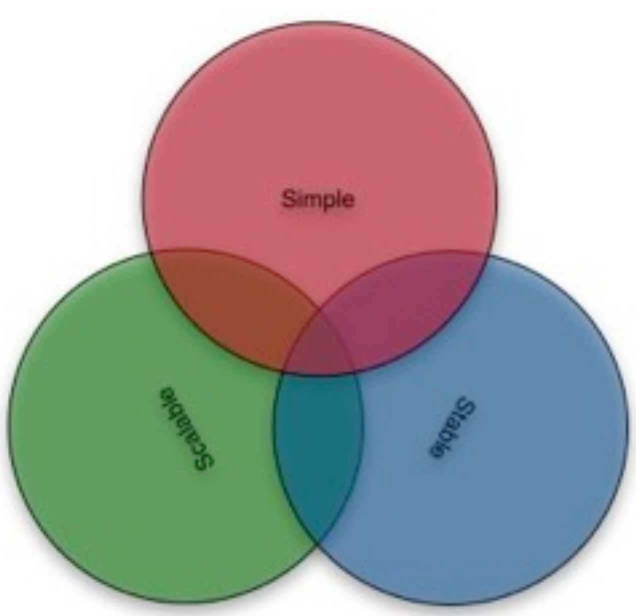
DNS Implementation

Hierarchical

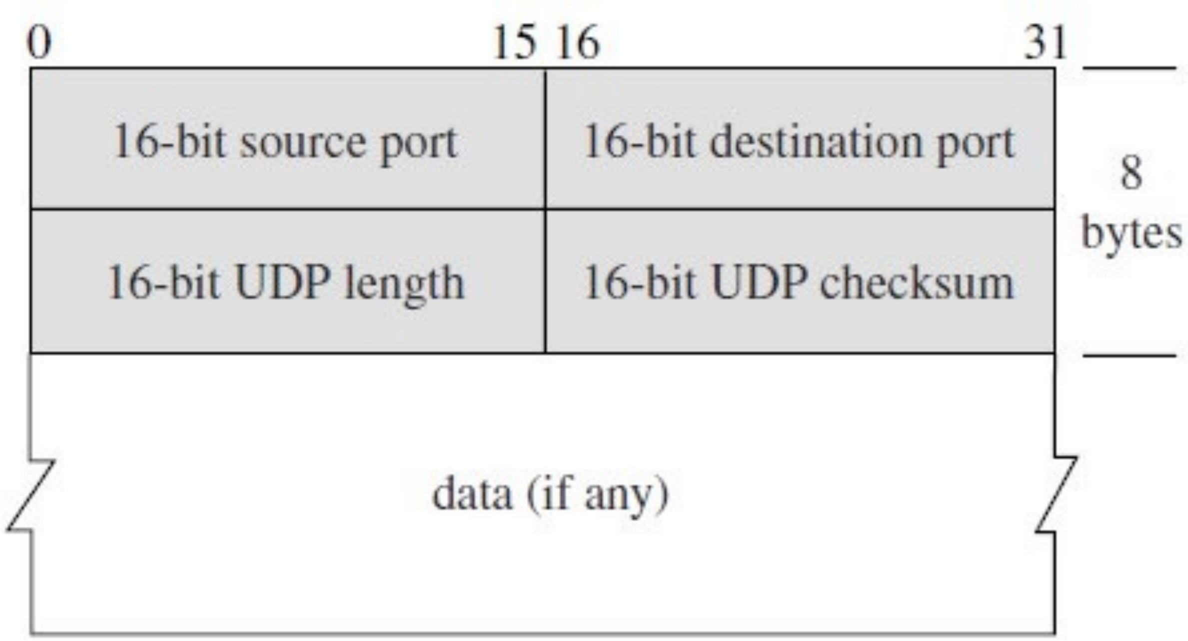


Globally Distributed

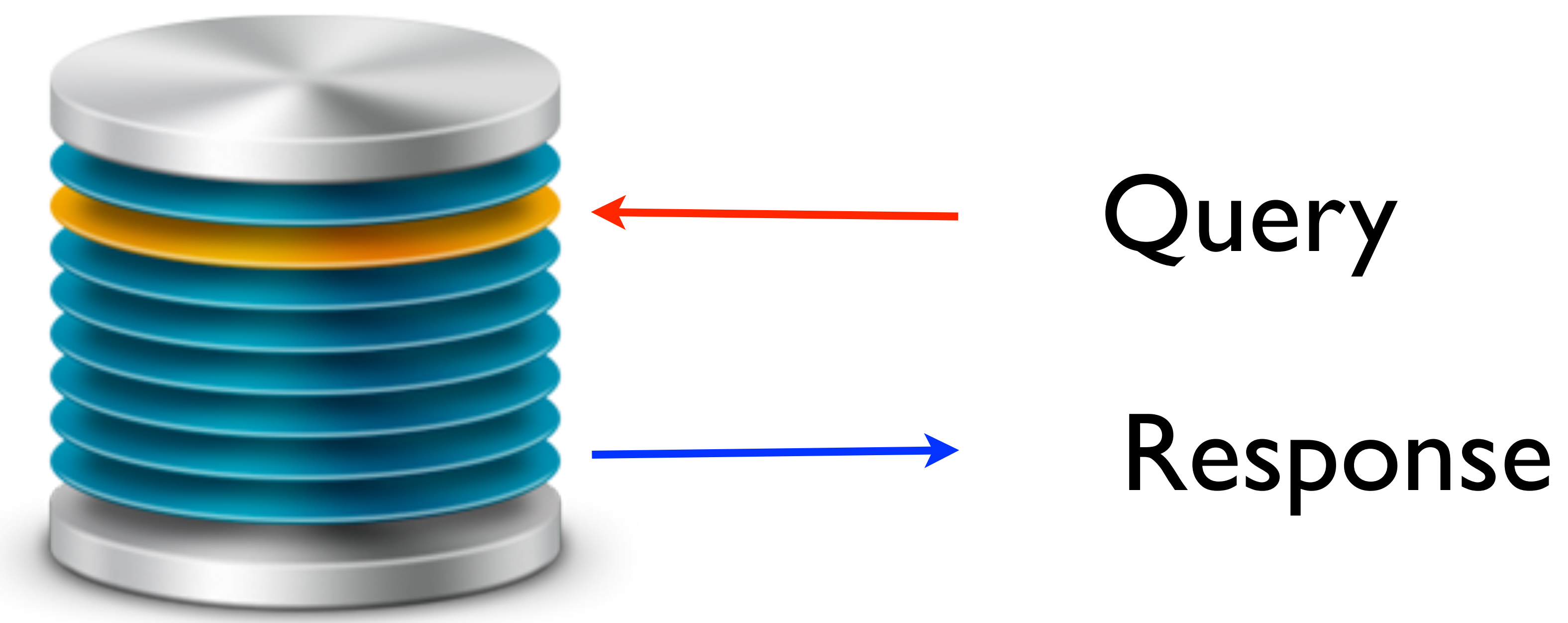
Scalable



Standard IP Protocol



Database



<4>

DNS Centrality & Criticality

DNS is a central anchor point of trust
for the entire Internet's infrastructure

DNS is a central anchor point of trust
for the entire Internet's infrastructure

Almost every user interaction deals with names.

Almost every user interaction deals with names.

president@utoronto.ca

https://www.royalbank.com/

Almost every Internet protocol interaction deals with numbers and addresses.

128.100.103.10

2001:beef:0666::2

2007: 24 Billion DNS Queries A Day

2008: 48 Billion DNS Queries A Day

Q: How secure is the Internet?

VeriSign Trusted

Q: Can Internet Mail be stolen?

A: Yes. And it's not too hard.

Mail client uses DNS, gets the wrong address for the remote mail server

Mail client uses DNS, attackers see and change the packets en-route

Q: Can Web Pages be Forged?

A: Yes. And it’s not too hard.

Browser sends DNS request, gets the wrong address and makes a HTTP connection to the bad guys server

Browser sends DNS request, makes a HTTP connection, attackers see and change the packets.

Q: How do we protect the DNS?

Q: Does cryptography solve the problem?

A: In theory... Yes!

A: In practice… ???

Q: Am I using cryptography?

Q: Are you using cryptography?

VeriSign™
Trusted

A: Sometimes yes; Normally no.

Q: Why is this so?

VeriSign Trusted

A: Most Internet Protocols do not support cryptography

Q: Why is this so?

A: Integration of cryptography is hard for protocol designers.

N.B. Some popular IP protocols do have cryptographic options!

VeriSign Trusted

e.g. HTTPS (RFC 2818)

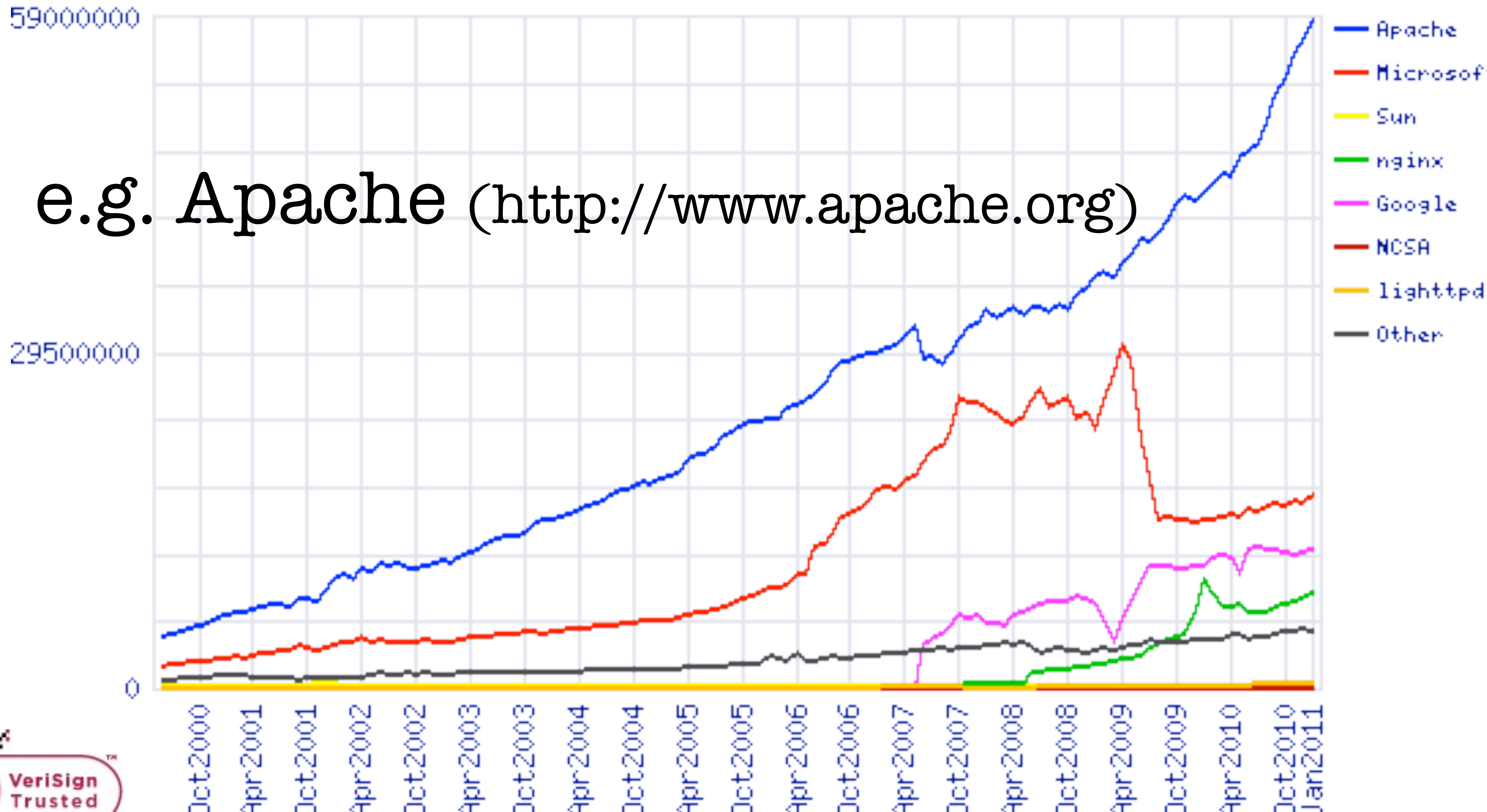
Q: Why do some implementations of these protocols do not support cryptography?

A: It's hard for software authors to implement the cryptography. Non cryptographic options are much easier.

N.B.

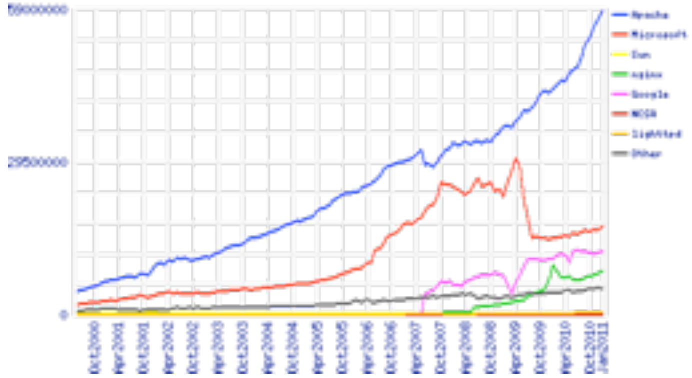
Some popular implementations do support cryptography!

e.g. Apache (http://www.apache.org)



VeriSign Trusted

Q: Why do 99% of Apache installations do NOT enable SSL



A: It’s harder and more costly for site administrators to turn it on and to keep it on.

BUYER BEWARE

Q: How secure are SSL certificates?

VeriSign Trusted™

Go Daddy®.COM

A: You tell me ...

Domain Access Verification

ra@godaddy.com <ra@godaddy.com>

To: Russell Sutherland <russell.sutherland@utoronto.ca>

Dear Secure Certificate Customer,

We have received a Certificate Signing Request for the following domain: theta.utoronto.ca.

Our query of the Whois database returned your name as the administrator for the domain in the certificate request.

In order to verify the validity of this request and that it was submitted by the entity to which the domain in the request is registered, please signify your final approval or disapproval of the certificate request by clicking the link below.

https://certs.godaddy.com/anonymous/domainapproval.seam?vk=3126963_dbb95e2dcbe3

Approval of the request will enable us to continue processing your request. Failure to approve the certificate request will lead to denial of the request.

If the above address does not appear as a clickable link, cut/copy and paste it into your browser's address bar.

If the Verification Page requests it, please use the following Verification Key: **3126963_dbb95e2dcbe3**
This part of our authentication process serves to ensure that only the entity/individual that controls the domain in the request can obtain a certificate for that domain.

If you encounter any problems or have any questions, our Customer Support department is ready to help, around-the-clock, seven days a week.

Customer Support:
E-Mail: ra@godaddy.com
Phone: 480.505.8852
Fax: 480.393.5009

For further information, log in to your account at https://certs.godaddy.com.

Q: How many certificate authorities does your browser trust?

A: ~ 1400 if your browser is Firefox or IE

N.B. Some important installations do support cryptography!

e.g. SourceForge has an SSL certificate and has set up SSL servers: https://sourceforge.net/account/

N.B. Cryptography is not enabled everywhere on the site!

e.g.
https://sourceforge.net/community gets redirected to http://sourceforge.net/community

Q: Why does SourceForge turn off SSL/cryptographic protection?

VeriSign Trusted

A: Enabling SSL for all transactions is costly in terms of CPU cycles/load.

A: SSL-acceleration is available but again costly ($$$).

Q: Why are cryptographic operations so expensive?

Q: Can cryptographic operations be made faster and still be correct?

Q: Can cryptographic operations be made fast enough to handle all of a www site's operation?

VeriSign Trusted

Q: Can cryptographic operations be made fast enough to handle all Internet transactions?

VeriSign Trusted

Q: Can Internet cryptography be easy to implement and manage?

Q: Can Internet cryptography be done in software?

VeriSign Trusted

Q: Can Internet cryptography be easy to add to Internet protocols?

Q: Will governments be afraid of universal Internet cryptography ?

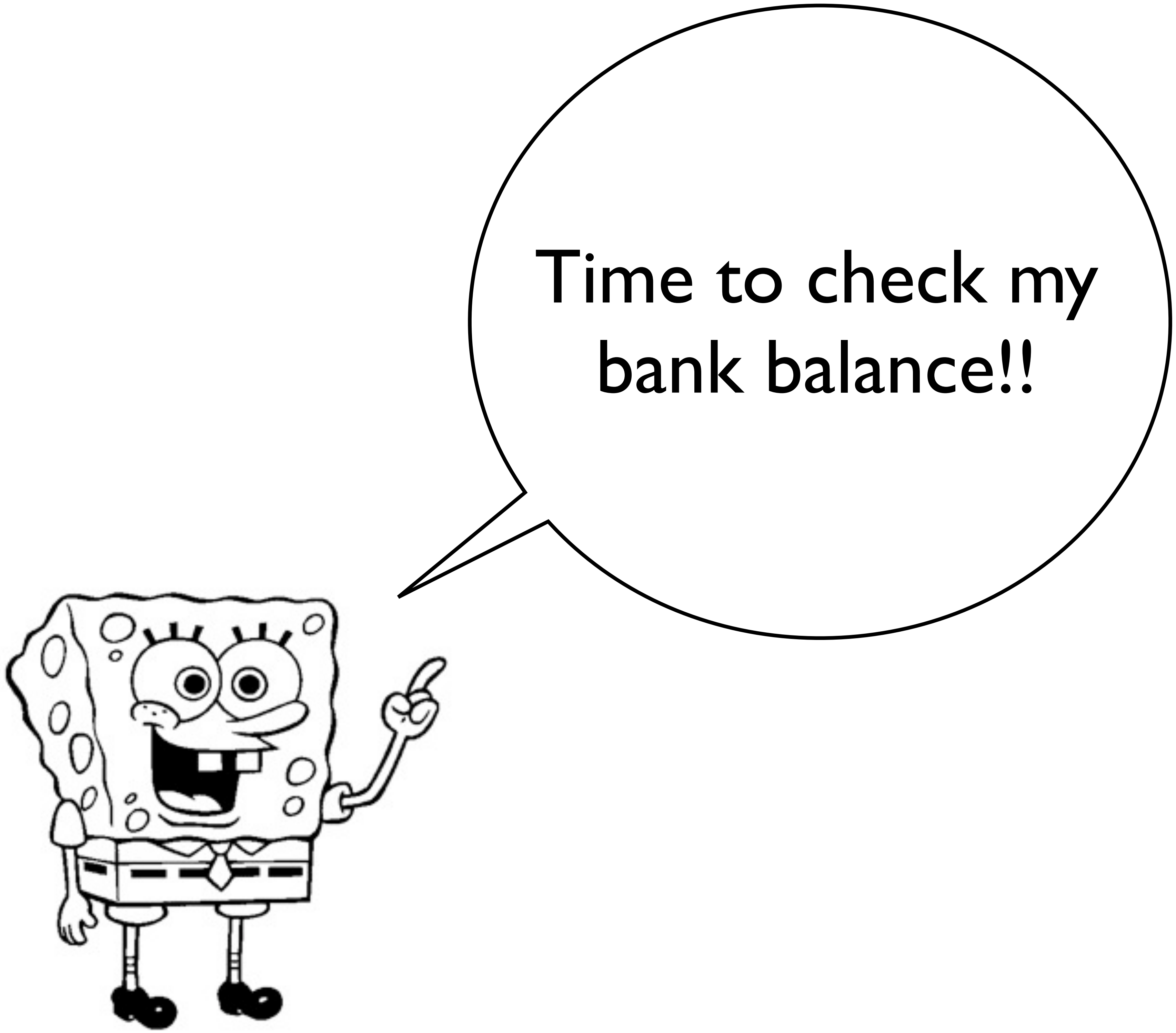
VeriSign Trusted

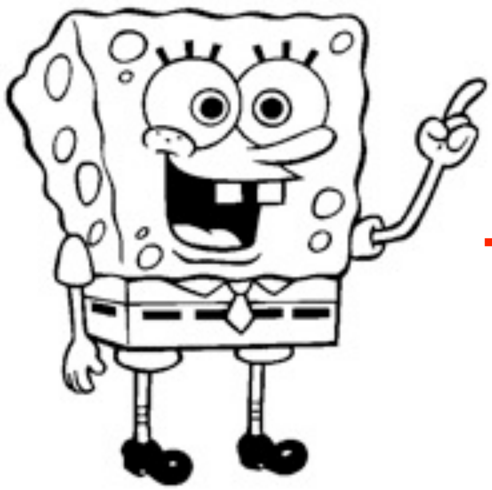
Q: Given gangsters and bad guys get to use cryptography can the average user have access to the same stuff?

VeriSign Trusted

<5>

A normal DNS transaction


Time to check my bank balance!!



www.cibc.ca


www.cibc.ca ?


I am going to assume Foxy meant:
www.cibc.ca.

I am going to assume
Foxy meant:

www.cibc.ca.

I am going to assume
Foxy meant:

www.cibc.ca.

That last dot is actually significant.


www.cibc.ca. ?

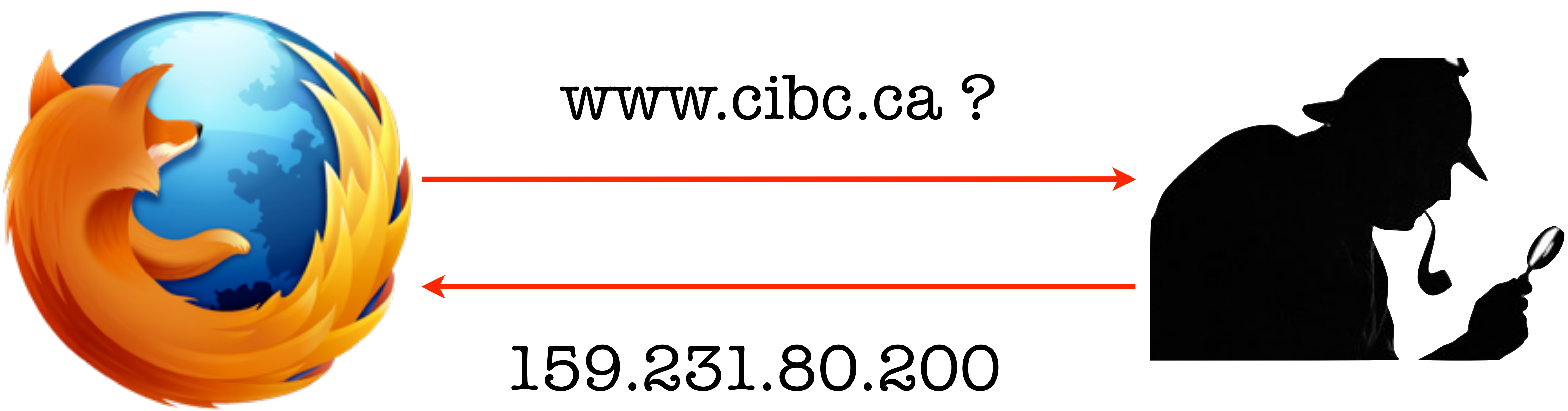

www.cibc.ca.?
Hmmm. Have I not seen that name before?

www.cibc.ca. ? Yes!

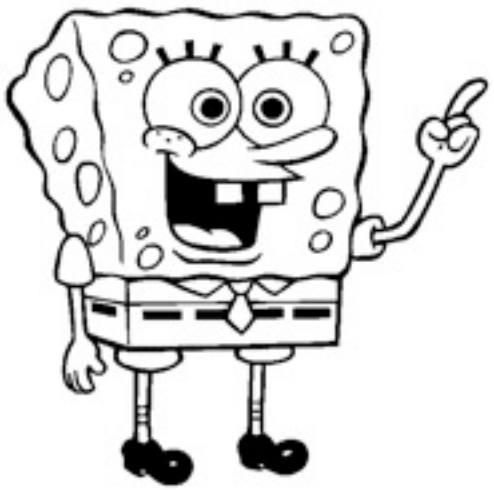
Here it is in my stash:

159.231.80.200


159.231.80.200
www.cibc.ca. ?


www.cibc.ca ?
159.231.80.200

Security Audit time …



Confidentiality ?

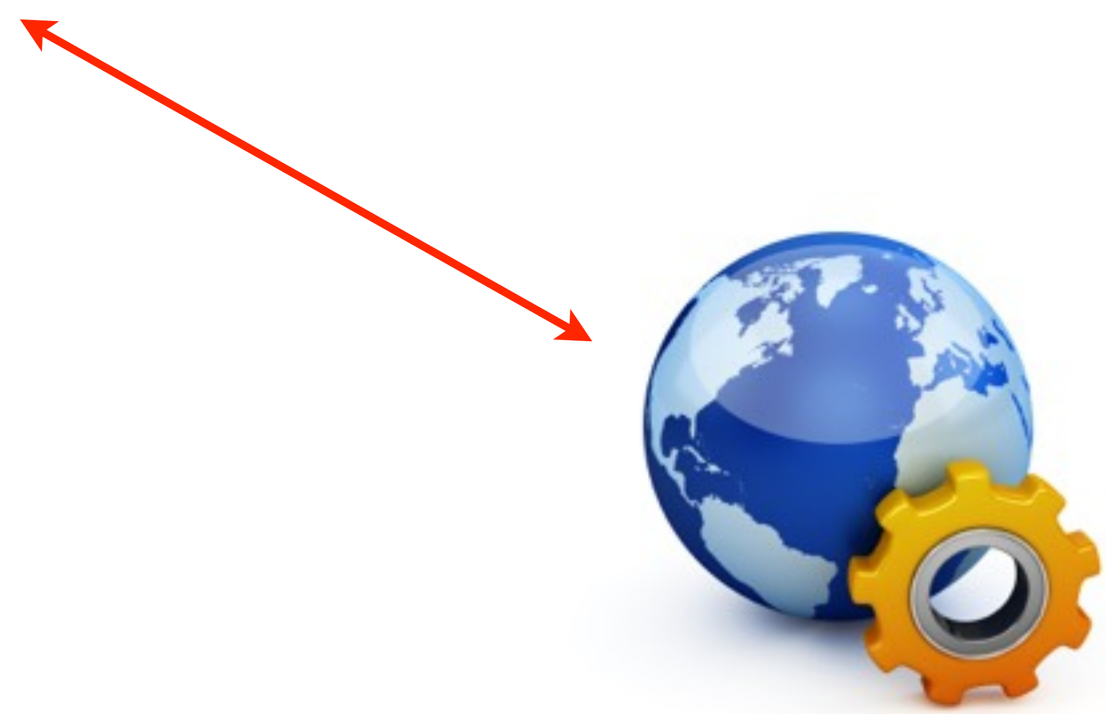
Integrity ?

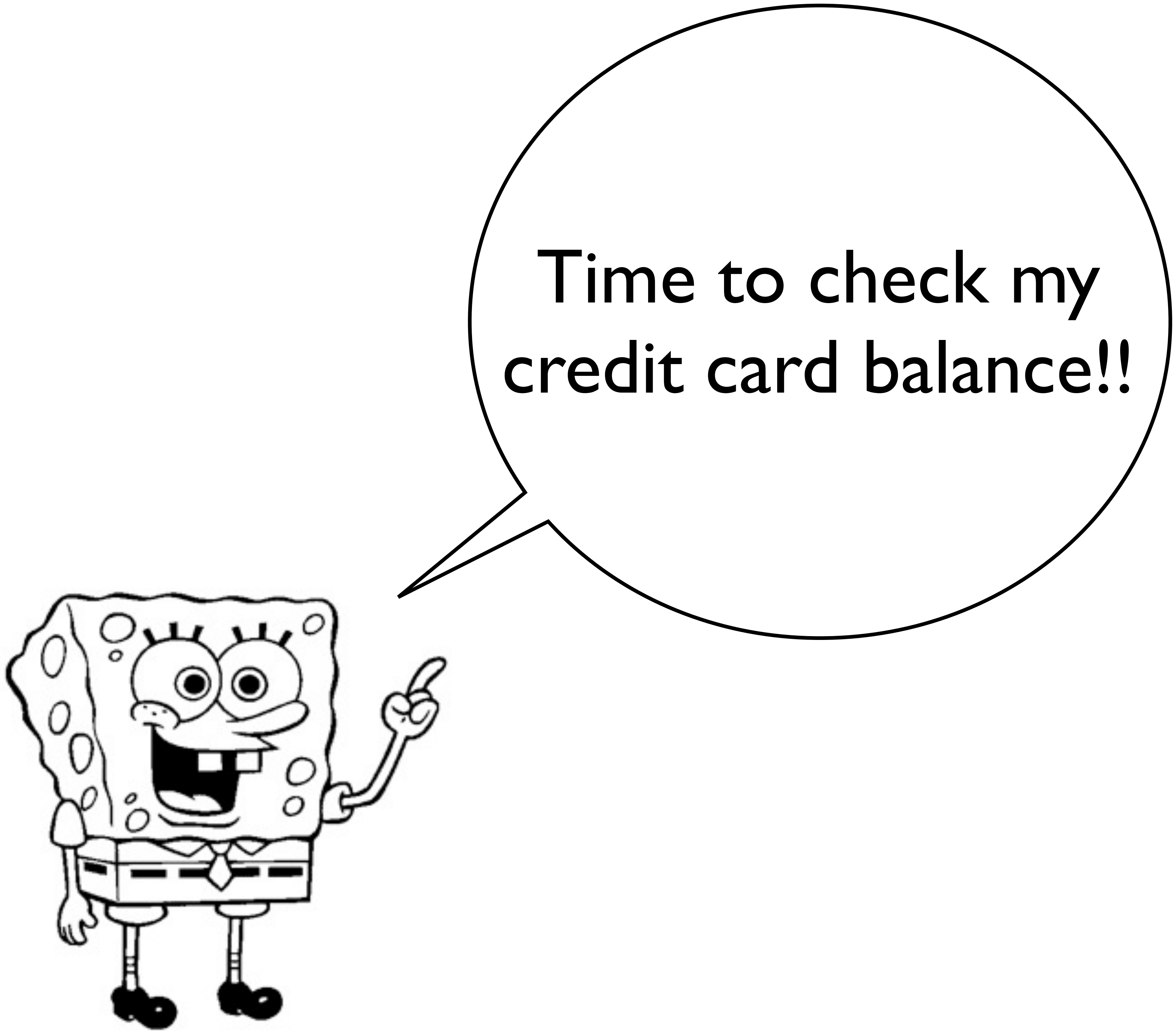
Availability ?

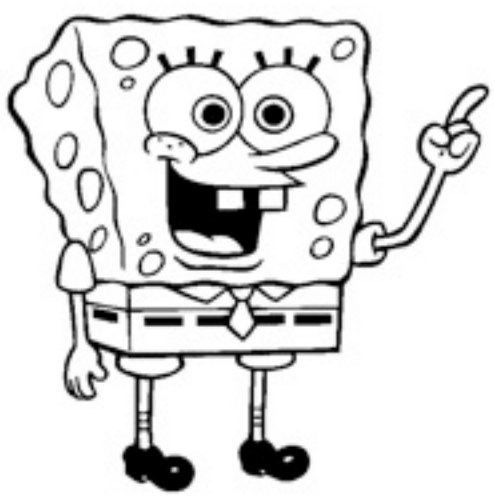
Confidentiality ?

Integrity ?

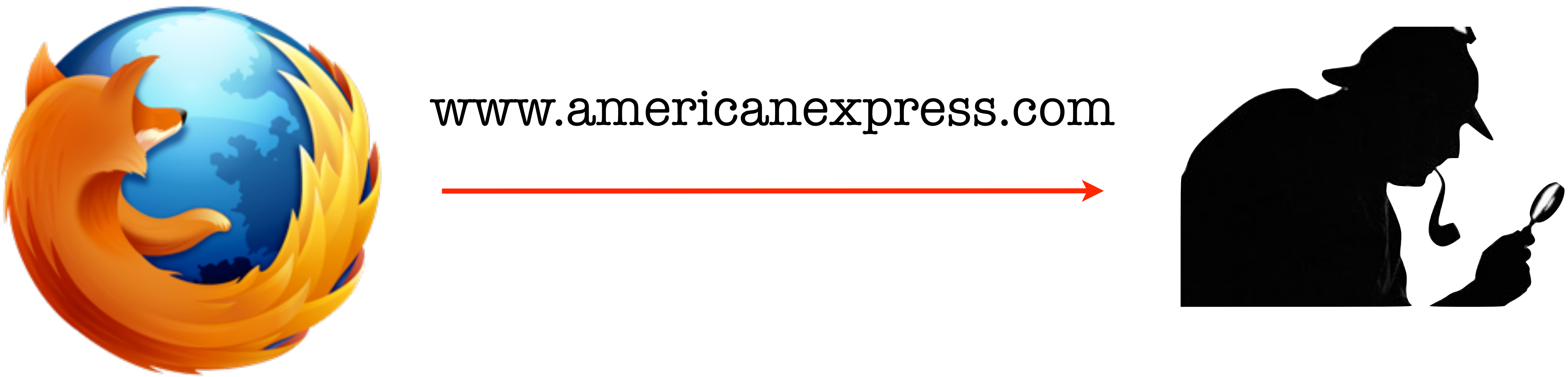
Availability ?




Time to check my credit card balance!!



www.americanexpress.com


www.americanexpress.com


People always forget that final dot. Sigh ...
www.americanexpress.com.

www.americanexpress.com. ?

www.americanexpress.com.

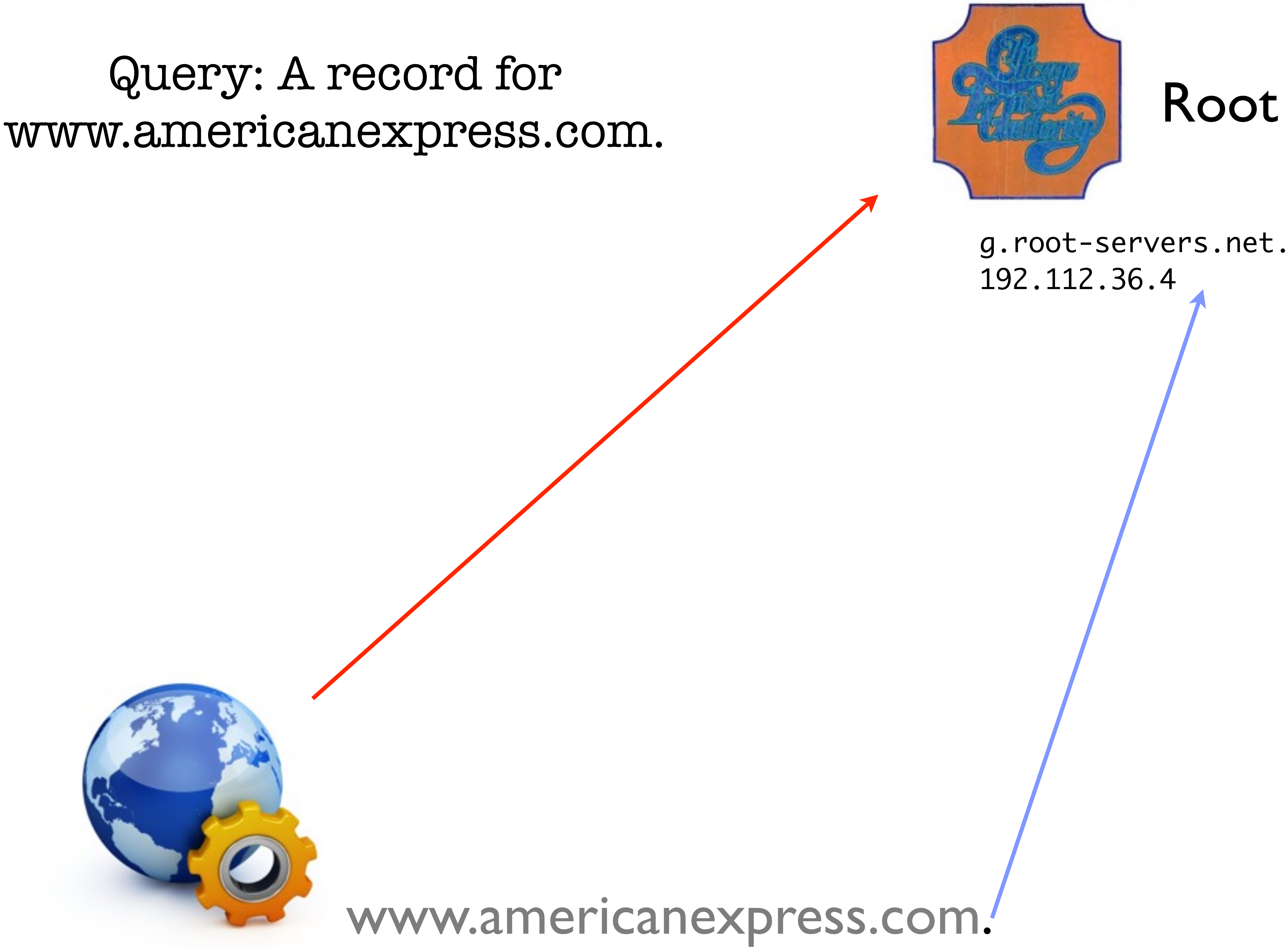
Hmmm. That looks like a new one. Let's check.


www.americanexpress.com.
Rats! I do not have that one stored. Time to go fish!

```
$ dig -t ns .

; <<>> DiG 9.7.0-P1 <<>> -t ns .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47571
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;.              IN  NS

;; ANSWER SECTION:
.           518375  IN  NS  g.root-servers.net.
.           518375  IN  NS  a.root-servers.net.
.           518375  IN  NS  e.root-servers.net.
.           518375  IN  NS  b.root-servers.net.
.           518375  IN  NS  k.root-servers.net.
.           518375  IN  NS  l.root-servers.net.
.           518375  IN  NS  c.root-servers.net.
.           518375  IN  NS  i.root-servers.net.
.           518375  IN  NS  d.root-servers.net.
.           518375  IN  NS  j.root-servers.net.
.           518375  IN  NS  f.root-servers.net.
.           518375  IN  NS  m.root-servers.net.
.           518375  IN  NS  h.root-servers.net.
```

```
$ dig +short -t ns .
g.root-servers.net.
a.root-servers.net.
e.root-servers.net.
b.root-servers.net.
k.root-servers.net.
l.root-servers.net.
c.root-servers.net.
i.root-servers.net.
d.root-servers.net.
j.root-servers.net.
f.root-servers.net.
m.root-servers.net.
h.root-servers.net.

$ dig +short -t a g.root-servers.net.
192.112.36.4
```

```
$ cat @
198.41.0.4
128.9.0.107
192.33.4.12
128.8.10.90
192.203.230.10
192.5.5.241
192.112.36.4
128.63.2.53
192.36.148.17
192.58.128.30
193.0.14.129
198.32.64.12
202.12.27.33
```


Query: A record for
www.americanexpress.com.
Root
g.root-servers.net.
192.112.36.4
www.americanexpress.com.

Query: A record for www.americanexpress.com.

Root

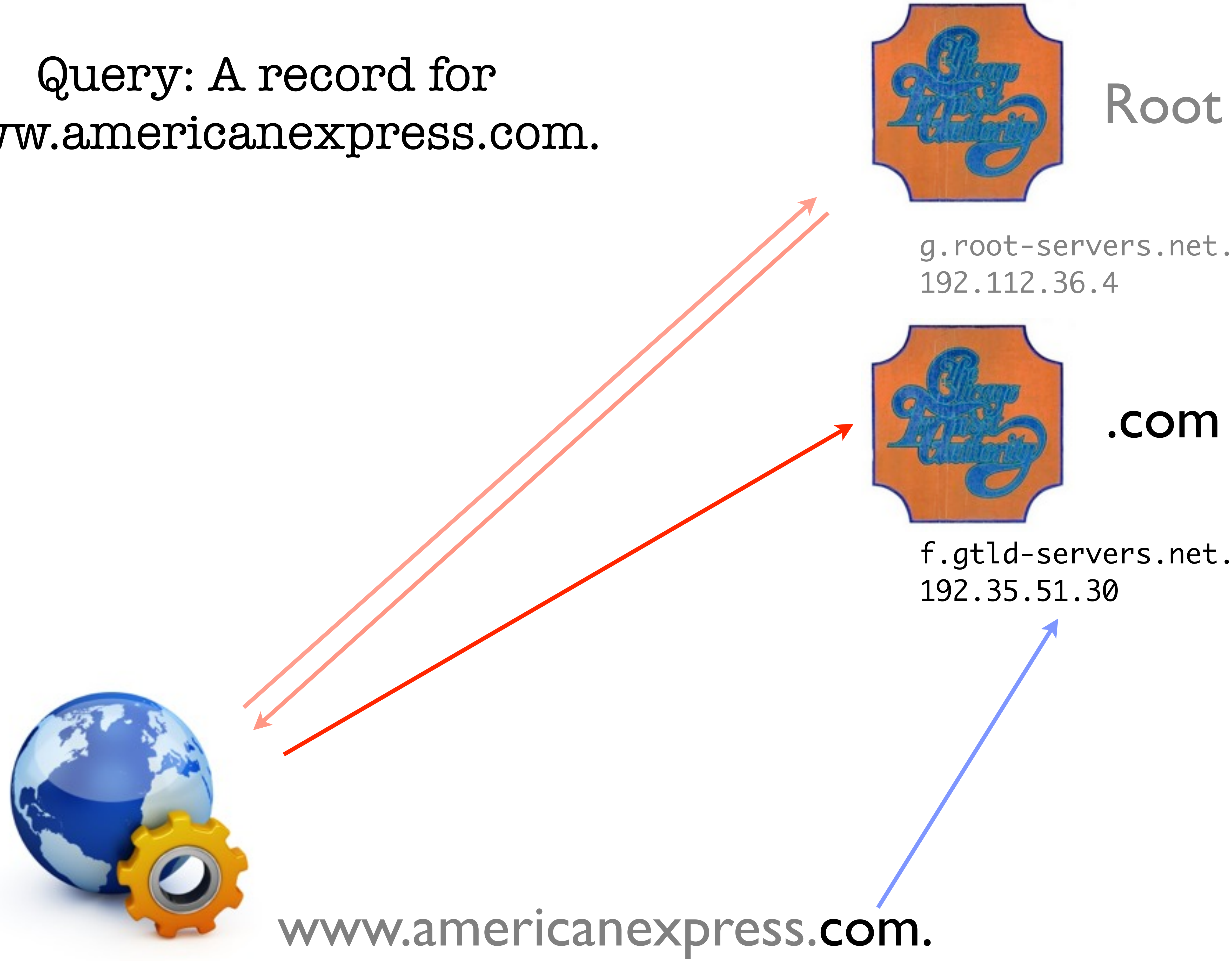
g.root-servers.net.
192.112.36.4

Response: NS records for com.

```
d.gtld-servers.net.
a.gtld-servers.net.
k.gtld-servers.net.
c.gtld-servers.net.
m.gtld-servers.net.
i.gtld-servers.net.
l.gtld-servers.net.
f.gtld-servers.net.
e.gtld-servers.net.
h.gtld-servers.net.
g.gtld-servers.net.
b.gtld-servers.net.
j.gtld-servers.net.
```

www.americanexpress.com.

Query: A record for
www.americanexpress.com.



Query: A record for
www.americanexpress.com.

Response: NS records for
americanexpress.com.

Root

g.root-servers.net.
192.112.36.4

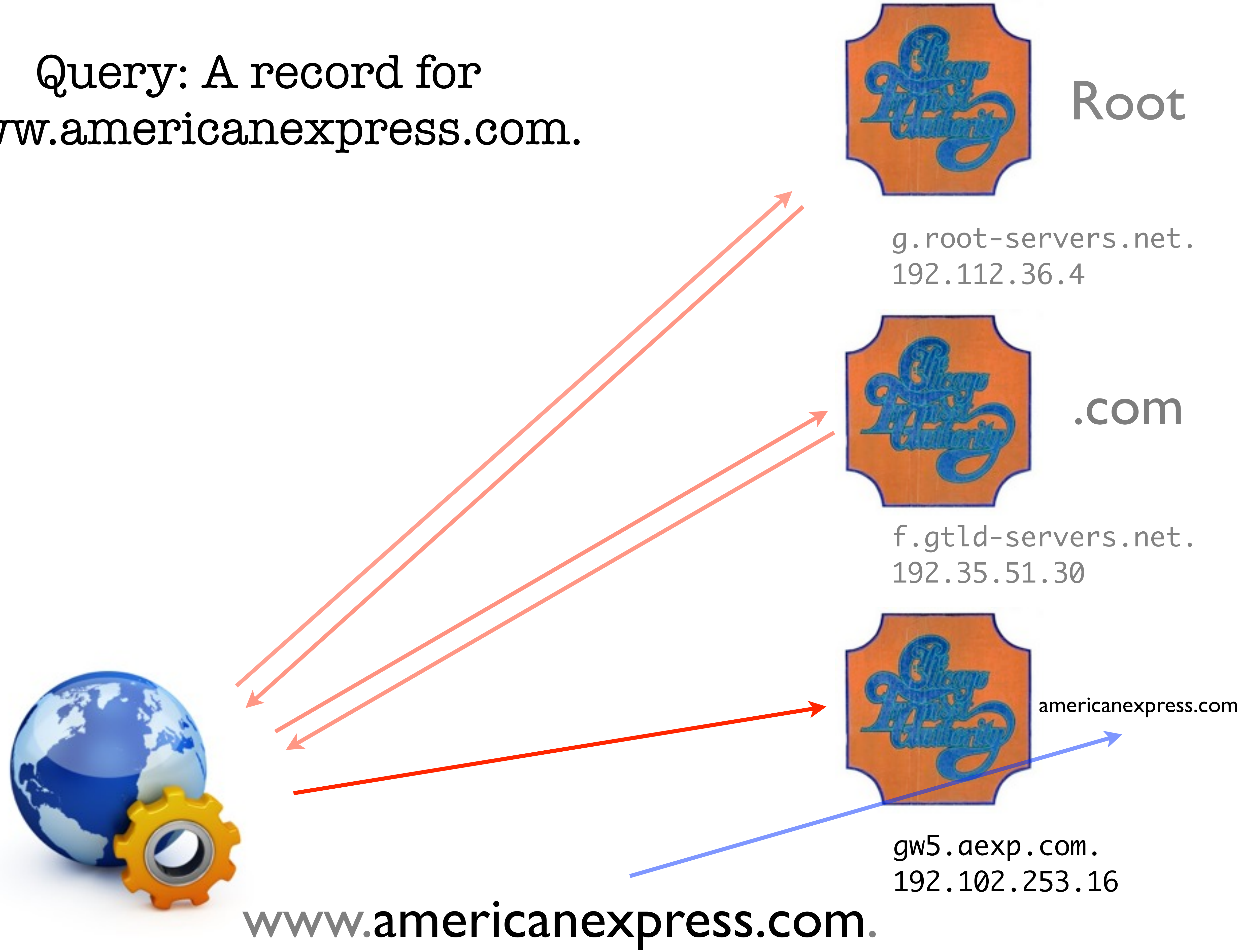
.com

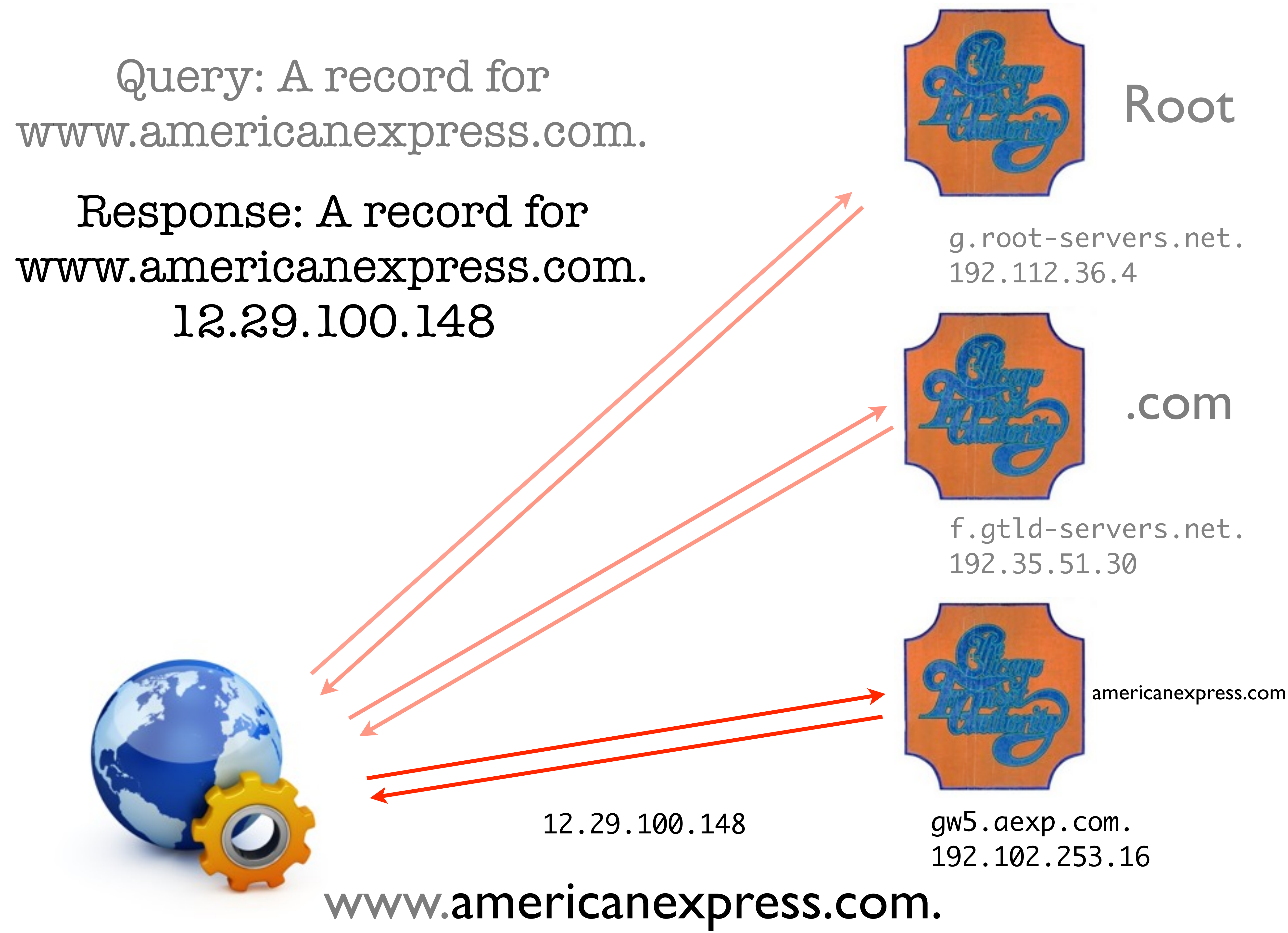
f.gtld-servers.net.
192.35.51.30

gw4.aexp.com.
gw5.aexp.com.
gw.aexp.com.
gw2.aexp.com.
gw3.aexp.com.

www.americanexpress.com.

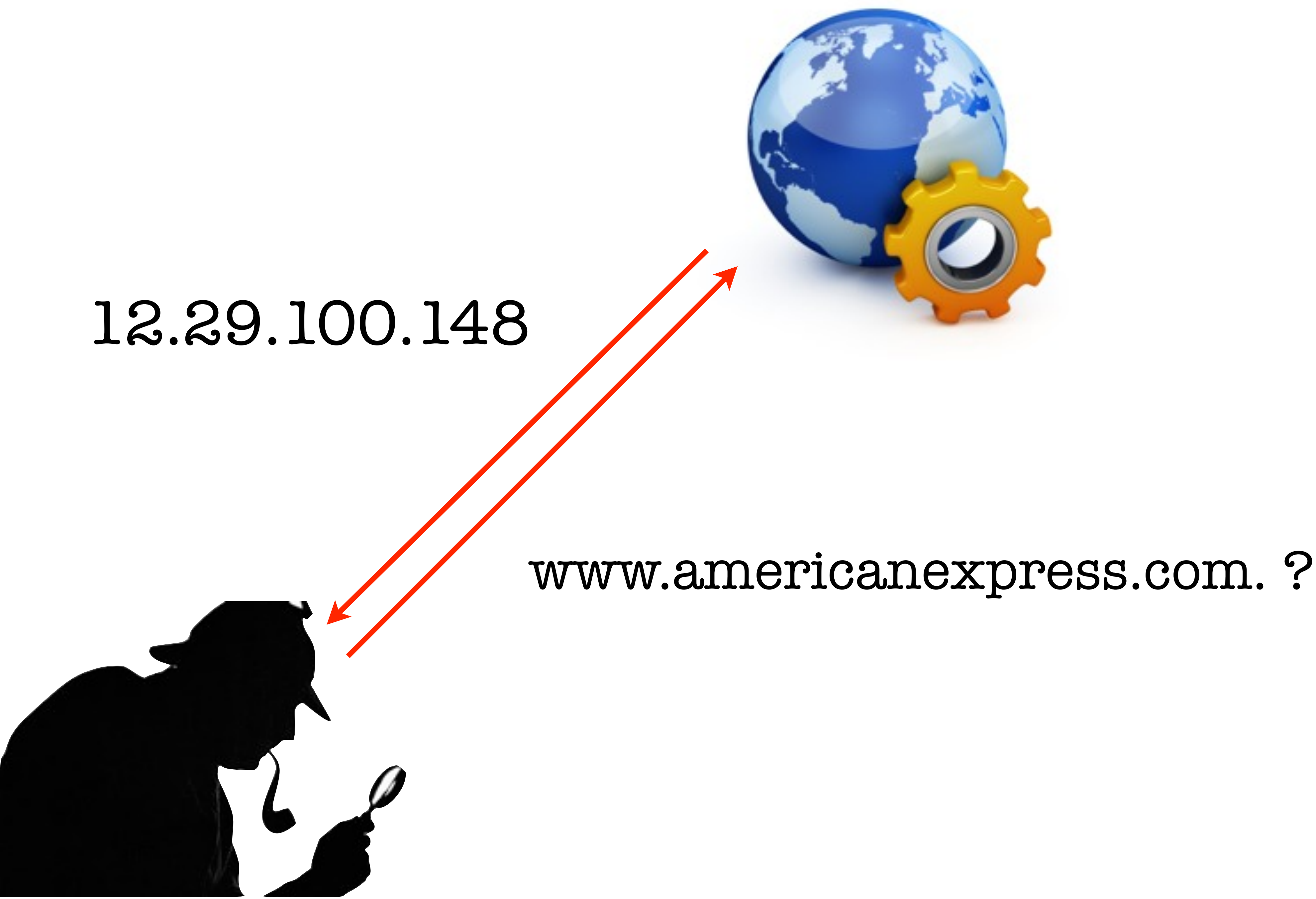
Query: A record for www.americanexpress.com.

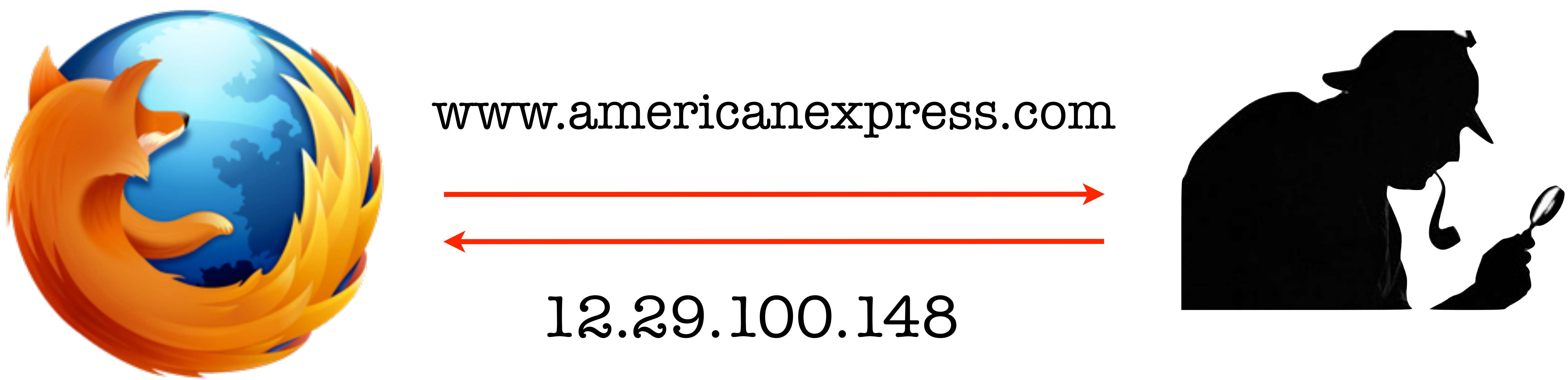



Query: A record for
www.americanexpress.com.
Response: A record for
www.americanexpress.com.
12.29.100.148
Root
g.root-servers.net.
192.112.36.4
.com
f.gtld-servers.net.
192.35.51.30
americanexpress.com
12.29.100.148
gw5.aexp.com.
192.102.253.16
www.americanexpress.com.

www.americanexpress.com.
12.29.100.148

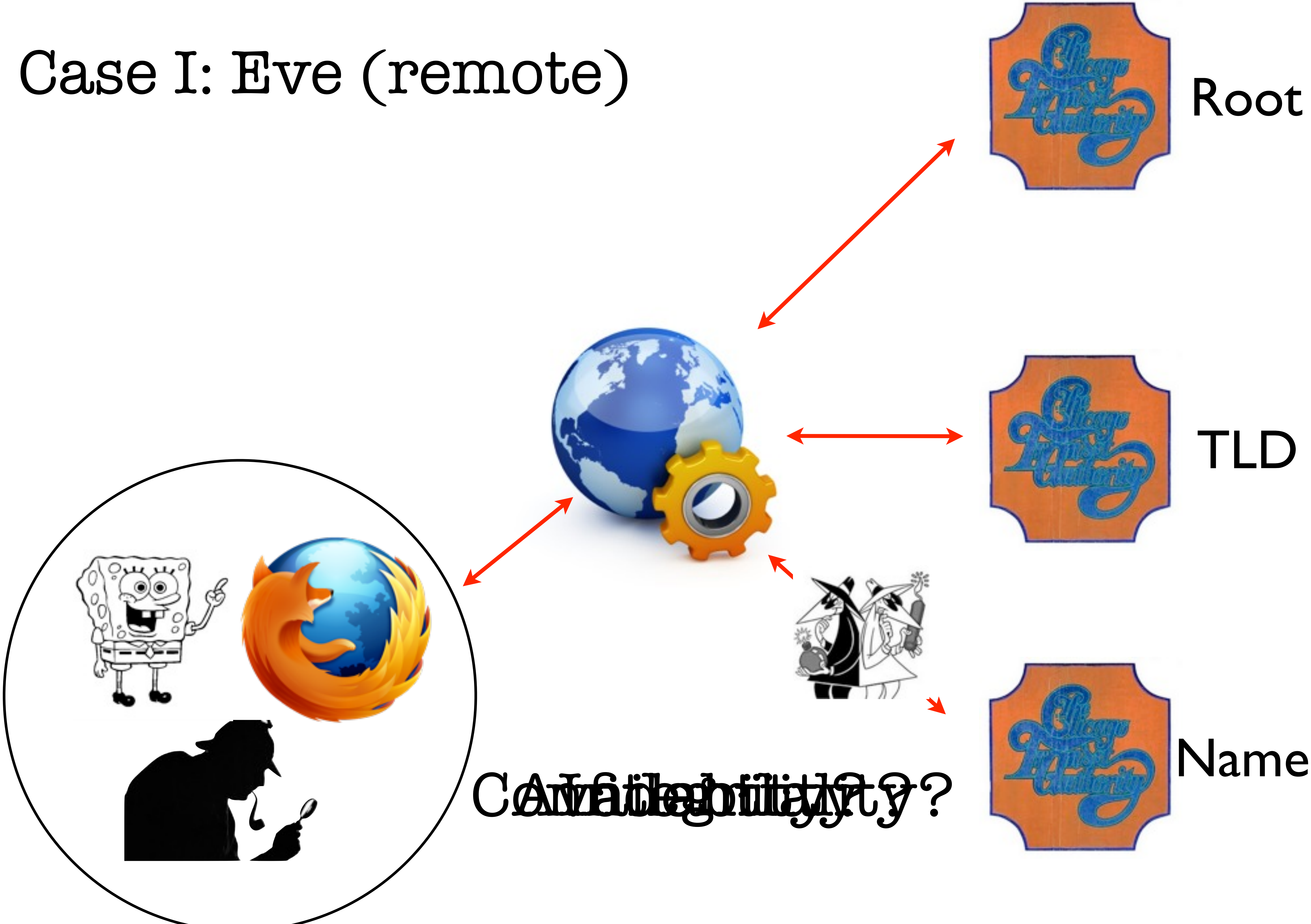
That took a bit of work. Let's
store it in our local stash.


12.29.100.148
www.americanexpress.com. ?


www.americanexpress.com
12.29.100.148

Security Audit time ...

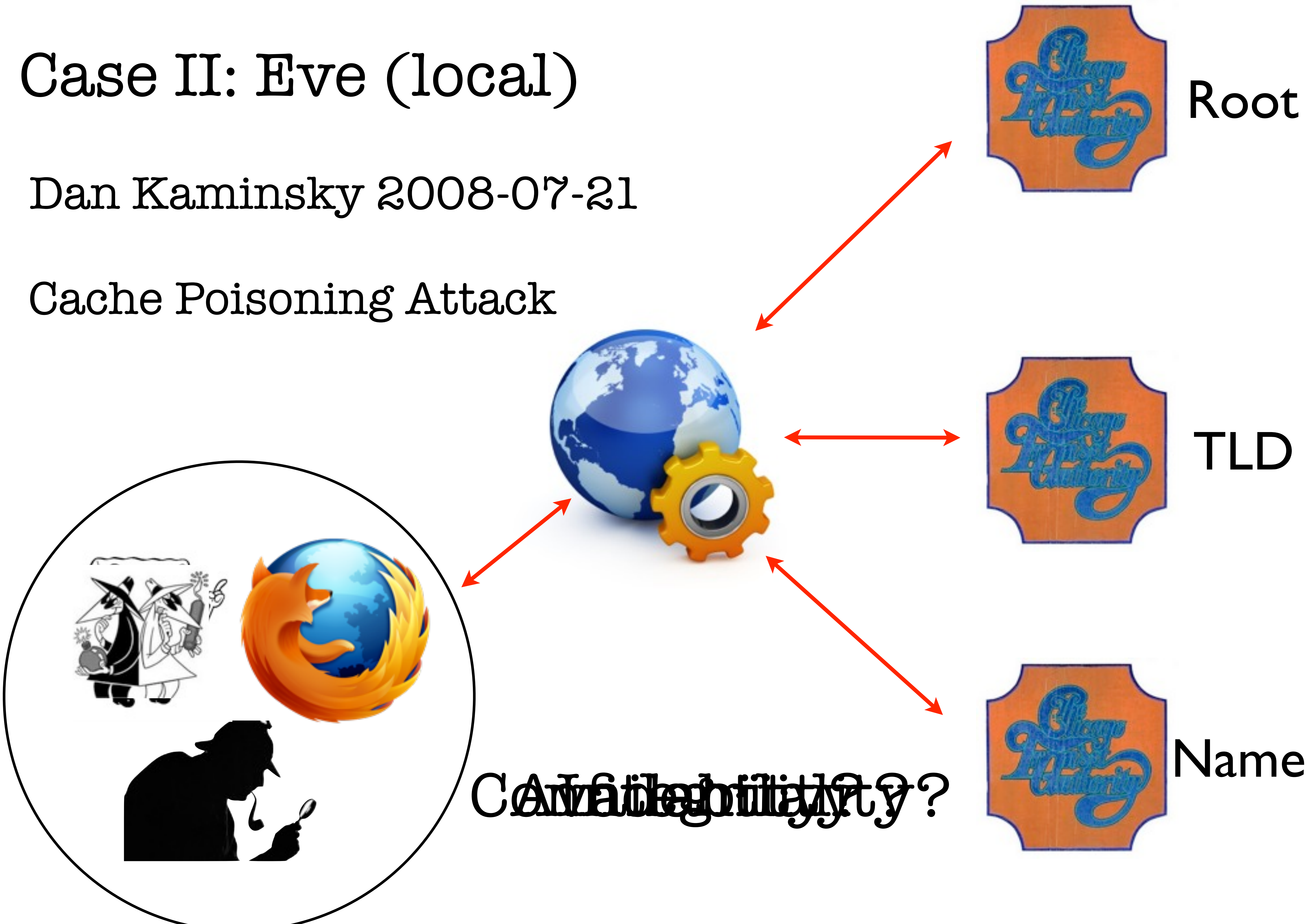
Case I: Eve (remote)



Case II: Eve (local)

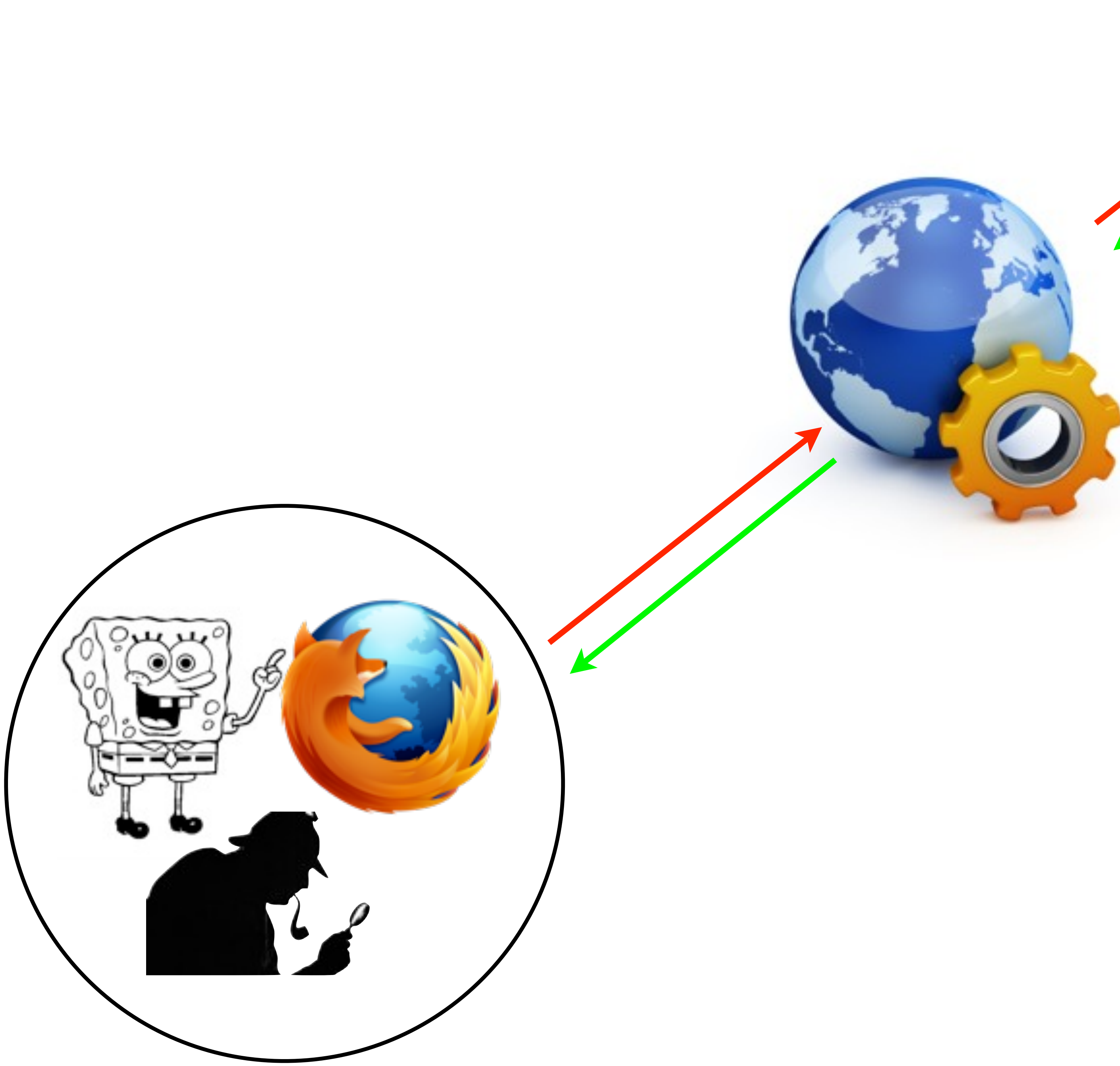
Dan Kaminsky 2008-07-21

Cache Poisoning Attack



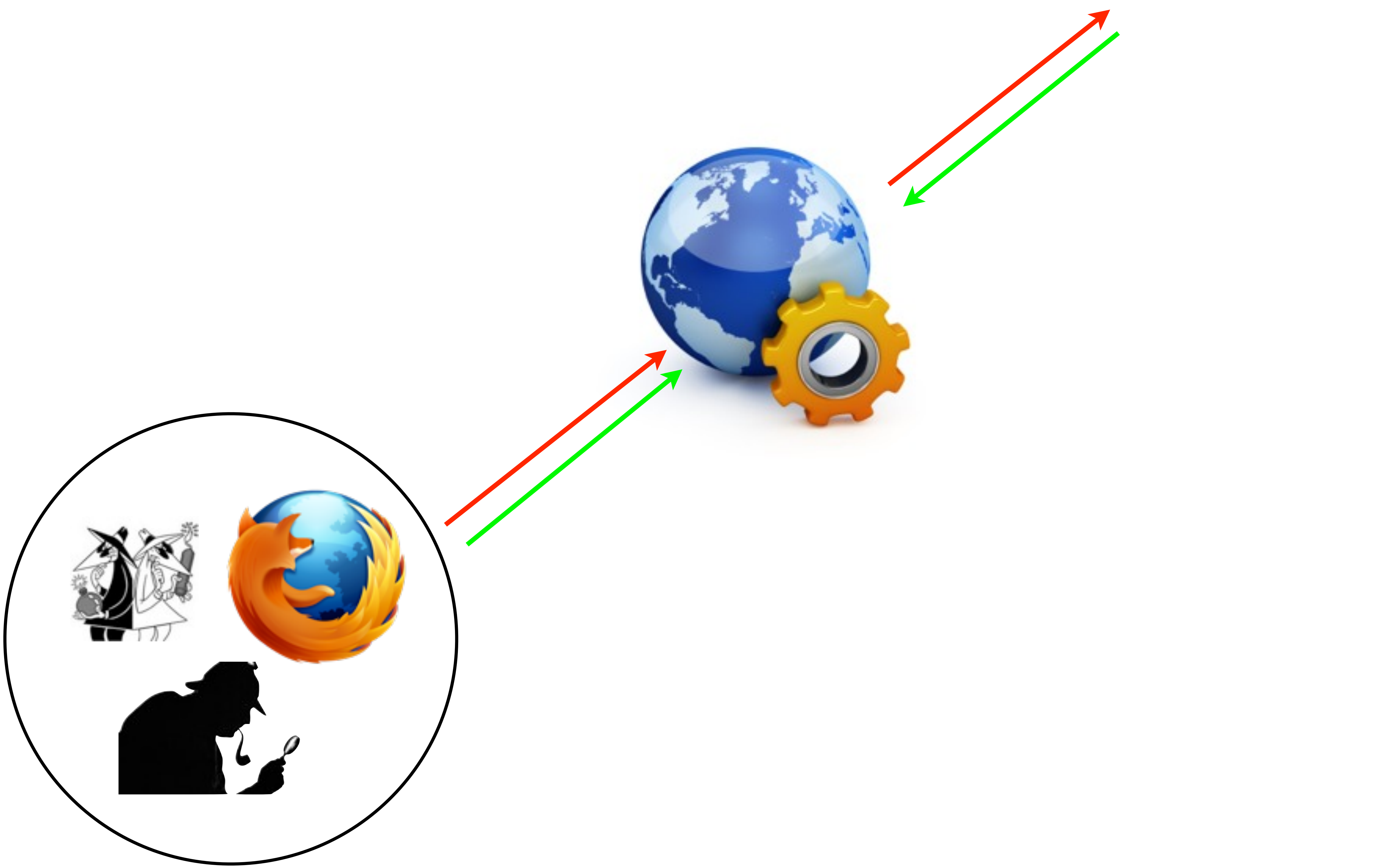
Cache Poisoning Attack

Normal Case: Alice - Bob

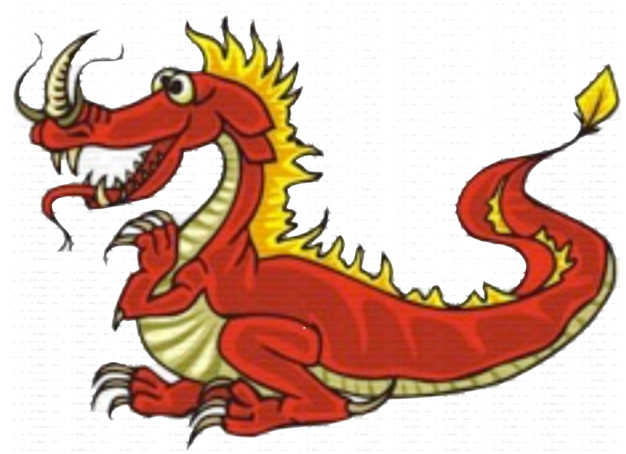


Cache Poisoning Attack

Imposter Case: Eve - Bob



Houston, we really do have a problem!



There be many DNS dragons…

Passive Attacks

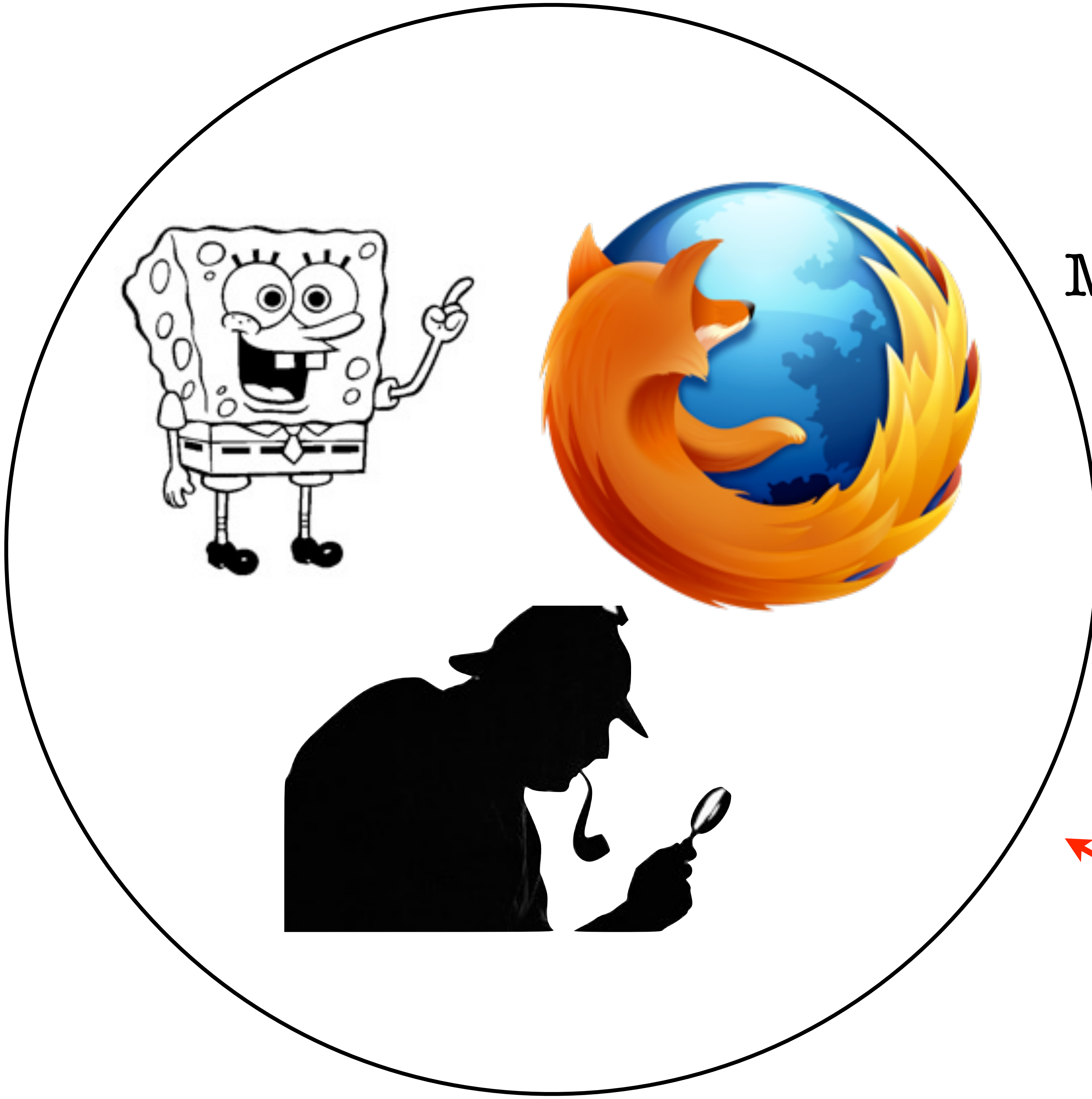
Man in Middle collects data regarding users queries

Active Attacks

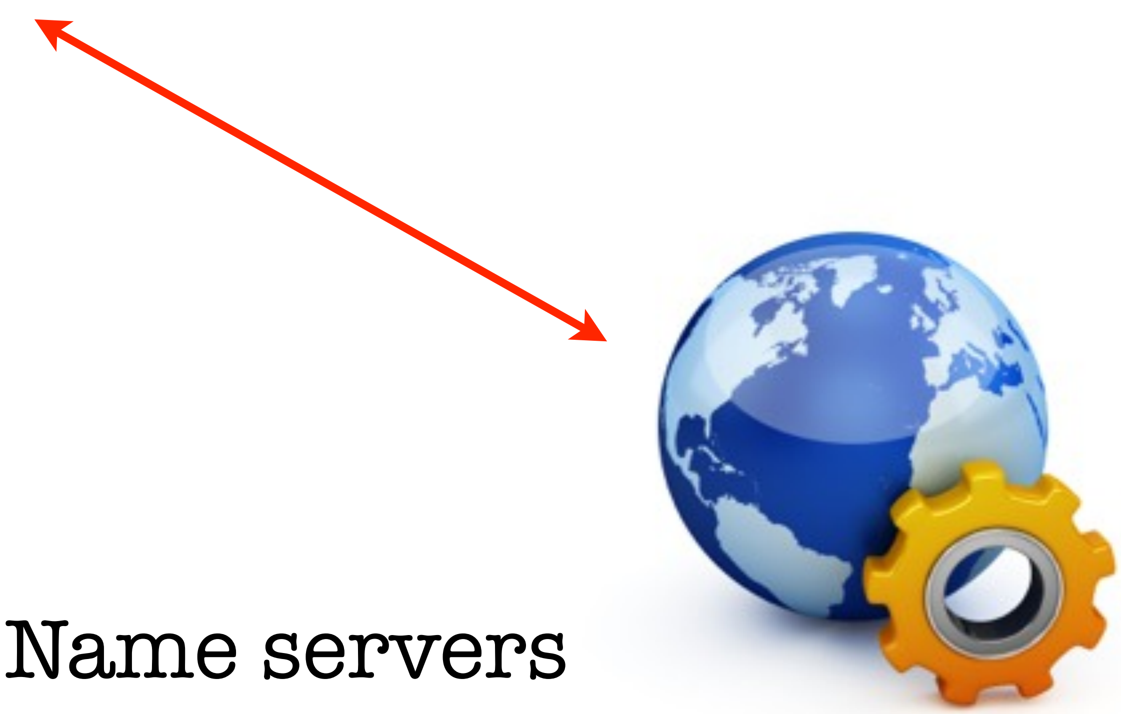
Man in Middle changes data

Active Attacks

Man in Middle changes data



Passive Attacks



Devious users can poison Caching Name servers

Solutions

For passive cache poisoning attacks

$$2^{16} = 65536$$

Random Query IDs makes guessing difficult

$$2^{16} * 2^{11} = 2^{27} = 134217728$$

Random QIDS & SRC ports minimizes risk

Modify DNS to use Cryptographic Tools

Confidentiality…

Would thwart passive man in the middle attacks

Integrity…

Would thwart all of the spoofing attacks

<6>

DNS Security Extensions

aka DNSSEC

What is it?

"The DNS Security extensions provide origin authentication and integrity protection for DNS data, as well as a means of public key distribution. These extensions do not provide confidentiality."

“ It is a set of extensions to DNS, which provide:

a. origin authentication of DNS data
b. data integrity
c. authenticated denial of existence ”

History

1987: Regular DNS standardized [RFC 1034,1035]

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light
[Steve Bellovin, Bell Laboratories]

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions
[RFC 2065]

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065
implementation problems

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

2001: RFC2535 key handling operational problems.
Restart! Writing, Drafting, Publishing

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

2001: RFC2535 key handling operational problems.

2005: 3 new RFCs: 4033,4034, 4035: DNSSEC-bis

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

2001: RFC2535 key handling operational problems.

2005: 3 new RFCs: 4033,4034, 4035: DNSSEC-bis

2005: First ccTLD implements DNSSEC: .se

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

2001: RFC2535 key handling operational problems.

2005: 3 new RFCs: 4033,4034, 4035: DNSSEC-bis

2005: First ccTLD implements DNSSEC: .se

2010: All root name servers are DNSSEC ready

1987: Regular DNS standardized [RFC 1034,1035]

1990: DNS vulnerabilities come to light

1995: Steve Bellovin makes public the vulnerabilities

1995: IETF strikes a DNSEXT working group

1997: IETF Domain Name Security Extensions [RFC 2065]

1999: RFC 2535 supercedes RFC 2065

1999: end of year, ISC ships bind with RFC2535 exts.

2001: RFC2535 key handling operational problems.

2005: 3 new RFCs: 4033,4034, 4035: DNSSEC-bis

2005: First ccTLD implements DNSSEC: .se

2010: All root name servers are DNSSEC ready

2012: .ca name servers are DNSSEC ready

Recent Uptake

End of 2009: ~1000

End of 2010: ~2500

Number of registered domains: ~200,000,000

DNSSEC: Objectives

<0>

N.B:

DNSSEC is designed to detect attacks and not necessarily to prevent them.

<1>

Origin Authentication of DNS Data

Client can trust that the authoritative name server really is the authority for a certain zone.

Authenticity is a case of Integrity

Origin Authentication of DNS Data

Client can trust that the authoritative name server really is the authority for a certain zone.

<2>

Data Integrity

Either end can detect if query or response has been modified by an unauthorized third party

Data Integrity

Either end can detect if query or response has been modified by an unauthorized third party

<3>

Authenticated Denial of Existence

The client can be sure not only of the response from data which exists but also that certain data does NOT exist.

Authenticated Denial of Existence

The client can be sure not only of the response from data which exists but also that certain data does NOT exist.

This is necessary to prevent certain forms of attacks

<4>

Backward Compatibility with Regular DNS

DNSSEC and non DNSSEC environments both need to interoperate.

DNSSEC: Non Objectives

<1>


Confidentiality

All DNSSEC traffic is plaintext

… that all data in the DNS is thus visible. Accordingly, DNSSEC is not designed to provide confidentiality, access control lists, or other means of differentiating between inquirers.

RFC 4033

… that all data in the DNS is thus visible. Accordingly, DNSSEC is not designed to provide confidentiality, access control lists, or other means of differentiating between inquirers.

RFC 4033

This design decision has security implications


Availability

DNSSEC provides no protection against denial of service attacks. Security-aware resolvers and security-aware name servers are vulnerable to an additional class of denial of service attacks based on cryptographic operations.

RFC 4033

DNSSEC provides **no protection against denial of service attacks**. Security-aware resolvers and security-aware name servers are **vulnerable** to an **additional class of denial of service attacks** based on cryptographic operations.

RFC 4033

There are no extra features, over and above regular DNS, to prevent DoS or buffer overflow attacks

DNSSEC Specifications

New Resource Records

Regular Resource Records

NS - name server delegation

A - IP address

MX - mail server name & priority

CNAME - name alias

TXT - text description

SOA - start of authority

New Resource Records

DNSSEC uses public key cryptography to sign and authenticate DNS resource record sets (RRsets).

RFC 4034

DNSSEC uses public key cryptography to sign and authenticate DNS resource record sets (RRsets).

RFC 4034

DNSKEY - for storing public keys

A zone signs its authoritative RRsets by using a private key and stores the corresponding public key in a DNSKEY RR.

RFC 4034

A zone signs its authoritative RRsets by using a private key and stores the corresponding public key in a DNSKEY RR.

RFC 4034

Note:

The DNSKEY RR is only intended to store DNS related public keys. It MUST NOT be used to store generic public keys and certificates

RFC 4034

DNSKEY - algorithms are also stored

```
# dig +multiline vix.com DNSKEY

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11667
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vix.com.                IN DNSKEY

;; ANSWER SECTION:
vix.com.                 2894 IN DNSKEY 257 3 5 (
                                 AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/
                                 A+U+h7F3EtblBDJVs/LgtdjsE3JHak51iRaELLOoEvVe
                                 RIIa1UjNvXIeia+QV1nlSas8LcXya0XOYA2Jfxez0pEW
                                 ArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
                                 ) ; key id = 26437
vix.com.                 2894 IN DNSKEY 256 3 5 (
                                 BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5
                                 vViM2+fh93XF1SqJaAaqgX6PszTPUlElvuTV2xTV4uQj
                                 UTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9PgAOc
                                 z2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9D
                                 lw==
                                 ) ; key id = 63066
```

```
# dig +multiline vix.com DNSKEY

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11667
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vix.com.                IN DNSKEY

;; ANSWER SECTION:
vix.com.                 2894 IN DNSKEY 257 3 5 (
                                 AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/
                                 A+U+h7F3EtblBDJVs/LgtdjsE3JHak51iRaELLOoEvVe
                                 RIIa1UjNvXIeia+QV1nlSas8LcXya0XOYA2Jfxez0pEW
                                 ArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
                                 ) ; key id = 26437
vix.com.                 2894 IN DNSKEY 256 3 5 (
                                 BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5
                                 vViM2+fh93XF1SqJaAaqgX6PszTPUlElvuTV2xTV4uQj
                                 UTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9PgAOc
                                 z2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9D
                                 lw==
                                 ) ; key id = 63066
```

```
# dig +multiline vix.com DNSKEY

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11667
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vix.com.                IN DNSKEY

;; ANSWER SECTION:
vix.com.                 2894 IN DNSKEY 257 3 5 (
                                 AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/
                                 A+U+h7F3EtblBDJVs/LgtdjsE3JHak51iRaELLOoEvVe
                                 RIIa1UjNvXIeia+QV1nlSas8LcXya0XOYA2Jfxez0pEW
                                 ArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
                                 ) ; key id = 26437
vix.com.                 2894 IN DNSKEY 256 3 5 (
                                 BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5
                                 vViM2+fh93XF1SqJaAaqgX6PszTPUlElvuTV2xTV4uQj
                                 UTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9PgAOc
                                 z2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9D
                                 lw==
                                 ) ; key id = 63066
```

```
# dig +multiline vix.com DNSKEY

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11667
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;vix.com.                IN DNSKEY

;; ANSWER SECTION:
vix.com.                 2894 IN DNSKEY 257 3 5 (
                                 AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/
                                 A+U+h7F3EtblBDJVs/LgtdjsE3JHak51iRaELLOoEvVe
                                 RIIa1UjNvXIeia+QV1nlSas8LcXya0XOYA2Jfxez0pEW
                                 ArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
                                 ) ; key id = 26437
vix.com.                 2894 IN DNSKEY 256 3 5 (
                                 BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5
                                 vViM2+fh93XF1SqJaAaqgX6PszTPUlElvuTV2xTV4uQj
                                 UTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9PgAOc
                                 z2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9D
                                 lw==
                                 ) ; key id = 63066
```

RRSIG - signatures are stored here

Signature: DNS data + owners private key

RRSIG - other fields as well

RRSIG - sig. inception time

RRSIG - sig. expiration time

RRSIG - type covered

RRSIG - algorithm

RRSIG - key tag

RRSIG - signers name

RRSIG - Data signature

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c/3b
+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437 vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMBZxZ
aivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY= ;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

```
# drill -D vix.com @ns.sql1.vix.com. rrsig
;; QUESTION SECTION:
;; vix.com.     IN      RRSIG

;; ANSWER SECTION:
vix.com.        3600    IN      RRSIG   A 5 2 3600 20110629030401 20110331030401 63066 vix.com.
CsxzLHeqDLi2XXKqGALXYn4lbmZrqkDzCYegv6EiZQFpPHG8oVdxvqJDCczpVHF3mykB05uHntpyoOS4om34l8fkIuVKViE6c
/3b+j3jiJIfXbFYPqM501NChRf/SwkBqsmKRj4jbTp3jCicUG6M3lyNWe5B2CjVd9hEUmzrbjY=
;{id = 63066}

vix.com.        3600    IN      RRSIG   MX 5 2 3600 20110629030401 20110331030401 63066 vix.com.
urjAd1NVJKNfUOI/l0aJRNEQJJfexjnwRTcyzcZmVvxnV5FlqlT9O4aIzcKMPnM2L3FWpf
+F0Tzfjr9Cb46pUHrj9LApaKxAH7RTOGKz7t2kVd8bD62LbhkFiVVlvqVTBBIhHinzAx8wPSCaU2saAt4fYc
+0w86it8IKBuwZyjE= ;{id = 63066}

vix.com.        3600    IN      RRSIG   DNSKEY 5 2 3600 20110629030401 20110331030401 26437
vix.com.
QvyoIbB1fTtge9aBTj88oBBFUnfLdGxGoyABG3bkPDAiDB5TUgJa68UDcF5k9c5fQEHZA6rd52QRxkPKyOhb5Reh64cZMjzMB
ZxZaivxX+W+hmkEk9ztSgWaotNBw2RHechItBI4/IPZWRXGNPr1IIduI8KC+dm96tf404BraAU= ;{id =
26437}
```

NSEC - Next SECure Record

NSEC - to accommodate negative authentication requests

NSEC - indicates all zones for which the name server is authoritative

NSEC - assume the following zones:

alpha.org
charlie.org
delta.org

NSEC - A query for beta.org will yield:

alpha.org NSEC charlie.org

NSEC3 : RFC5155 : 2008-02

NSEC3 - like NSEC but to prevent tree walking

NSEC3 - instead of actual names, the hash of the name is given

```
# drill -D rps.vix.com @ns.sql1.vix.com A
;; QUESTION SECTION:
;; rps.vix.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
vix.com.        3600    IN      SOA     ns.lah1.vix.com. hostmaster.vix.com. 2011033116 3600 1800
604800 3600
vix.com.        3600    IN      RRSIG   SOA 5 2 3600 20110629030401 20110331030401 63066 vix.com.
fPpFeE/Y/1HfFtKTAjfWlBQafC2i4qf5gYewmr0fQHzH7xIYmvx
+rpenaKfr4By2R01Dh5q6kKgB3DR7G9swmAXcAVB5TzvQ6UcmjXcGGZPw+HUwUSIAt6q559YMKxSN6DTeh7/
kNlLPtoPZqSmz7rxIr0USe2VwAYDznGtlzdQ= ;{id = 63066}
vix.com.        3600    IN      NSEC    ns-lah1._meta.vix.com. A NS SOA MX TXT AAAA RRSIG NSEC
DNSKEY
vix.com.        3600    IN      RRSIG   NSEC 5 2 3600 20110629030401 20110331030401 63066
vix.com. Hm3dfubDRTtF8BrztQ3X2tCc5IJ7+JO3cB8F5rQhDAyzBz7XcOESJrwyUCk8YL/
w3i360fUuhN3MahOdTzrzoAMxWp90yM5MRbRSzUQwQ
+73cRbq2C2YEfsYPatPiL9vHnc5Wvo9xtrFEjiWK7qcHgBwO3SrXPsUYzn8seB8DtA= ;{id = 63066}
relay.vix.com.  3600    IN      NSEC    server99.vix.com. CNAME RRSIG NSEC
relay.vix.com.  3600    IN      RRSIG   NSEC 5 3 3600 20110629030401 20110331030401 63066
vix.com. SrJ3NLPntXcN+SpT9igyoEyQYznsomsbAxqfXutF5o0VDfaeHZvB2LZC7+HjCAwwH6F7YWItdRVFt4PVQ6/
ouZ2K7r2RLoaMyaaHAJzhq4EN503AoFD7ONcMyVV4BIzI6vsquORSPW8H03ym/OkZOaQG0Bw2UFW/Q6Pwx4xVbKA= ;{id =
63066}
```

```
# drill -D rps.vix.com @ns.sql1.vix.com
;; QUESTION SECTION:
;; rps.vix.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
vix.com.        3600    IN      SOA     ns.lah1.vix.com. hostmaster.vix.com. 2011033116 3600 1800
604800 3600
vix.com.        3600    IN      RRSIG   SOA 5 2 3600 20110629030401 20110331030401 63066 vix.com.
fPpFeE/Y/1HfFtKTAjfWlBQafC2i4qf5gYewmr0fQHzH7xIYmvx
+rpenaKfr4By2R01Dh5q6kKgB3DR7G9swmAXcAVB5TzvQ6UcmjXcGGZPw+HUwUSIAt6q559YMKxSN6DTeh7/
kNlLPtoPZqSmz7rxIr0USe2VwAYDznGtlzdQ= ;{id = 63066}
vix.com.        3600    IN      NSEC    ns-lah1._meta.vix.com. A NS SOA MX TXT AAAA RRSIG NSEC
DNSKEY
vix.com.        3600    IN      RRSIG   NSEC 5 2 3600 20110629030401 20110331030401 63066
vix.com. Hm3dfubDRTtF8BrztQ3X2tCc5IJ7+JO3cB8F5rQhDAyzBz7XcOESJrwyUCk8YL/
w3i360fUuhN3MahOdTzrzoAMxWp90yM5MRbRSzUQwQ
+73cRbq2C2YEfsYPatPiL9vHnc5Wvo9xtrFEjiWK7qcHgBwO3SrXPsUYzn8seB8DtA= ;{id = 63066}
relay.vix.com.  3600    IN      NSEC    server99.vix.com. CNAME RRSIG NSEC
relay.vix.com.  3600    IN      RRSIG   NSEC 5 3 3600 20110629030401 20110331030401 63066
vix.com. SrJ3NLPntXcN+SpT9igyoEyQYznsomsbAxqfXutF5o0VDfaeHZvB2LZC7+HjCAwwH6F7YWItdRVFt4PVQ6/
ouZ2K7r2RLoaMyaaHAJzhq4EN503AoFD7ONcMyVV4BIzI6vsquORSPW8H03ym/OkZOaQG0Bw2UFW/Q6Pwx4xVbKA= ;{id =
63066}
```

```
# drill -D rps.vix.com @ns.sql1.vix.com
;; QUESTION SECTION:
;; rps.vix.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
vix.com.        3600    IN      SOA     ns.lah1.vix.com. hostmaster.vix.com. 2011033116 3600 1800
604800 3600
vix.com.        3600    IN      RRSIG   SOA 5 2 3600 20110629030401 20110331030401 63066 vix.com.
fPpFeE/Y/1HfFtKTAjfWlBQafC2i4qf5gYewmr0fQHzH7xIYmvx
+rpenaKfr4By2R01Dh5q6kKgB3DR7G9swmAXcAVB5TzvQ6UcmjXcGGZPw+HUwUSIAt6q559YMKxSN6DTeh7/
kNlLPtoPZqSmz7rxIr0USe2VwAYDznGtlzdQ= ;{id = 63066}
vix.com.        3600    IN      NSEC    ns-lah1._meta.vix.com. A NS SOA MX TXT AAAA RRSIG NSEC
DNSKEY
vix.com.        3600    IN      RRSIG   NSEC 5 2 3600 20110629030401 20110331030401 63066
vix.com. Hm3dfubDRTtF8BrztQ3X2tCc5IJ7+JO3cB8F5rQhDAyzBz7XcOESJrwyUCk8YL/
w3i360fUuhN3MahOdTzrzoAMxWp90yM5MRbRSzUQwQ
+73cRbq2C2YEfsYPatPiL9vHnc5Wvo9xtrFEjiWK7qcHgBwO3SrXPsUYzn8seB8DtA= ;{id = 63066}
relay.vix.com.  3600    IN      NSEC    server99.vix.com. CNAME RRSIG NSEC
relay.vix.com.  3600    IN      RRSIG   NSEC 5 3 3600 20110629030401 20110331030401 63066
vix.com. SrJ3NLPntXcN+SpT9igyoEyQYznsomsbAxqfXutF5o0VDfaeHZvB2LZC7+HjCAwwH6F7YWItdRVFt4PVQ6/
ouZ2K7r2RLoaMyaaHAJzhq4EN503AoFD7ONcMyVV4BIzI6vsquORSPW8H03ym/OkZOaQG0Bw2UFW/Q6Pwx4xVbKA=
;{id = 63066}
```

```
# drill -D rps.vix.com @ns.sql1.vix.com
;; QUESTION SECTION:
;; rps.vix.com. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
vix.com.        3600    IN      SOA     ns.lah1.vix.com. hostmaster.vix.com. 2011033116 3600 1800 
604800 3600
vix.com.        3600    IN      RRSIG   SOA 5 2 3600 20110629030401 20110331030401 63066 vix.com. 
fPpFeE/Y/1HfFtKTAjfWlBQafC2i4qf5gYewmr0fQHzH7xIYmvx
+rpenaKfr4By2R01Dh5q6kKgB3DR7G9swmAXcAVB5TzvQ6UcmjXcGGZPw+HUwUSIAt6q559YMKxSN6DTeh7/
kNlLPtoPZqSmz7rxIr0USe2VwAYDznGtlzdQ= ;{id = 63066}
vix.com.        3600    IN      NSEC    ns-lah1._meta.vix.com. A NS SOA MX TXT AAAA RRSIG NSEC 
DNSKEY
vix.com.        3600    IN      RRSIG   NSEC 5 2 3600 20110629030401 20110331030401 63066 
vix.com. Hm3dfubDRTtF8BrztQ3X2tCc5IJ7+JO3cB8F5rQhDAyzBz7XcOESJrwyUCk8YL/
w3i360fUuhN3MahOdTzrzoAMxWp90yM5MRbRSzUQwQ
+73cRbq2C2YEfsYPatPiL9vHnc5Wvo9xtrFEjiWK7qcHgBwO3SrXPsUYzn8seB8DtA= ;{id = 63066}
relay.vix.com.  3600    IN      NSEC    server99.vix.com. CNAME RRSIG NSEC
relay.vix.com.  3600    IN      RRSIG   NSEC 5 3 3600 20110629030401 20110331030401 63066 
vix.com. SrJ3NLPntXcN+SpT9igyoEyQYznsomsbAxqfXutF5o0VDfaeHZvB2LZC7+HjCAwwH6F7YWItdRVFt4PVQ6/
ouZ2K7r2RLoaMyaaHAJzhq4EN503AoFD7ONcMyVV4BIzI6vsquORSPW8H03ym/OkZOaQG0Bw2UFW/Q6Pwx4xVbKA= ;{id = 
63066}
```

DS - Delegation Signer

DS:

A key signed by the parent zone to indicate stuff down in the hierarchy can be trusted

DS:

The parent zone stores the key tag, algorithm and a digest/hash of the DNSKEY in the child zone.

DS:

The parent zone then signs the DS record and creates a corresponding RRSIG record

```
# drill -s -D vix.com DNSKEY
;; ANSWER SECTION:

vix.com.        3600    IN      DNSKEY  257 3 5
AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/A+U+h7F3EtblBDJVs/
LgtdjsE3JHak51iRaELLOoEvVeRIIa1UjNvXIei+QV1nlSas8LcXya0XOYA2Jfxez0p
EWArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
;{id = 26437 (ksk), size = 1024b}

vix.com.        3600    IN      DNSKEY  256 3 5
BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5vViM2+fh93XF1SqJaAaq
gX6PszTPUlElvuTV2xTV4uQjUTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9P
gAOcz2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9Dlw==
;{id = 63066 (zsk), size = 1024b}

; vix.com.      3600    IN      DS      26437 5 1
483cca94fd7e2aa30f4fca34ccf0db4ddc601388
; xidaf-sidan-gazol-vupap-fofag-zudif-gufyz-bikag-talyk-begom-muxox

; vix.com.      3600    IN      DS      63066 5 1
8229b0484396f12015de1cb7e3267ed1f109060a
; xobid-nusog-mebon-kusid-bihyt-velyr-lomid-kizut-ceseb-nacab-puxux
```

vix.com.

com.

```
# drill -s -D vix.com DNSKEY
;; ANSWER SECTION:

vix.com.        3600    IN      DNSKEY  257 3 5
AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/A+U+h7F3EtblBDJVs/
LgtdjsE3JHak51iRaELLOoEvVeRIIa1UjNvXIei+QV1nlSas8LcXya0XOYA2Jfxez0p
EWArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
;{id = 26437 (ksk), size = 1024b}

vix.com.        3600    IN      DNSKEY  256 3 5
BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5vViM2+fh93XF1SqJaAaq
gX6PszTPUlElvuTV2xTV4uQjUTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9P
gAOcz2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9Dlw==
;{id = 63066 (zsk), size = 1024b}

; vix.com.      3600    IN      DS      26437 5 1
483cca94fd7e2aa30f4fca34ccf0db4ddc601388
; xidaf-sidan-gazol-vupap-fofag-zudif-gufyz-bikag-talyk-begom-muxox

; vix.com.      3600    IN      DS      63066 5 1
8229b0484396f12015de1cb7e3267ed1f109060a
; xobid-nusog-mebon-kusid-bihyt-velyr-lomid-kizut-ceseb-nacab-puxux
```

```
# drill -s -D vix.com DNSKEY
;; ANSWER SECTION:

vix.com.        3600    IN      DNSKEY  257 3 5
AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/A+U+h7F3EtblBDJVs/
LgtdjsE3JHak51iRaELLOoEvVeRIIa1UjNvXIei+QV1nlSas8LcXya0XOYA2Jfxez0p
EWArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
;{id = 26437 (ksk), size = 1024b}

vix.com.        3600    IN      DNSKEY  256 3 5
BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5vViM2+fh93XF1SqJaAaq
gX6PszTPUlElvuTV2xTV4uQjUTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9P
gAOcz2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9Dlw==
;{id = 63066 (zsk), size = 1024b}

; vix.com.      3600    IN      DS      26437 5 1
483cca94fd7e2aa30f4fca34ccf0db4ddc601388
; xidaf-sidan-gazol-vupap-fofag-zudif-gufyz-bikag-talyk-begom-muxox

; vix.com.      3600    IN      DS      63066 5 1
8229b0484396f12015de1cb7e3267ed1f109060a
; xobid-nusog-mebon-kusid-bihyt-velyr-lomid-kizut-ceseb-nacab-puxux
```

```
# drill -s -D vix.com DNSKEY
;; ANSWER SECTION:

vix.com.        3600    IN      DNSKEY  257 3 5
AwEAAbKW5zsYMBUX4MS0yq3MNm4312c7WEF1Af2Iy2O/A+U+h7F3EtblBDJVs/
LgtdjsE3JHak51iRaELLOoEvVeRIIa1UjNvXIei+QV1nlSas8LcXya0XOYA2Jfxez0p
EWArN1QLhkgVDPAsEwKLzYfVjW78CFlOZnYxbBWXwKgb4z
;{id = 26437 (ksk), size = 1024b}

vix.com.        3600    IN      DNSKEY  256 3 5
BEAAAAO6wBt1U39U8meHca3JBCWixBi8BvZLMJZp51/5vViM2+fh93XF1SqJaAaq
gX6PszTPUlElvuTV2xTV4uQjUTaFv8qDnsjbfXVusE1v+OaQpSVuP8GjI28cGi9P
gAOcz2ACdiD2XVbYKUDTJb+pqoE/o3Z6FjKf6ByTkJUI5x9Dlw==
;{id = 63066 (zsk), size = 1024b}

; vix.com.      3600    IN      DS      26437 5 1
483cca94fd7e2aa30f4fca34ccf0db4ddc601388
; xidaf-sidan-gazol-vupap-fofag-zudif-gufyz-bikag-talyk-begom-muxox

; vix.com.      3600    IN      DS      63066 5 1
8229b0484396f12015de1cb7e3267ed1f109060a
; xobid-nusog-mebon-kusid-bihyt-velyr-lomid-kizut-ceseb-nacab-puxux
```

.CA Recommended DNSSEC Key Parameters

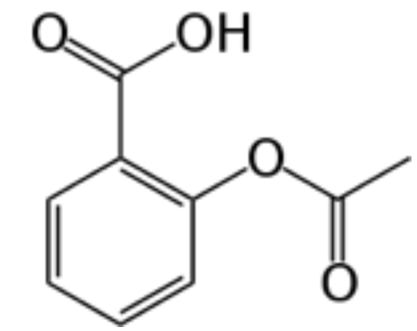
Parameter	Value
Key Signing Key (KSK)	2048 RSA
KSK Rollover Schedule	once per year
KSK Algorithm	RSA/SHA/256
Zone Signing Key (ZSK)	1024-bit RSA
ZSK Rollover Schedule	once per month
ZSK Signature Algorithm	RSA/SHA/256
Authenticated Proof of Non Existence	NSEC3 with opt-out

DNSSEC - Traversal

Caching Name Server

DNSSEC aware

RFC 4035



recursive
name
server

resolver

client (aka)
stub resolver

caching

authority

DNSSEC - Bootstrapping

Assumption - Root Zone has been signed

Assumption - Public Keys are available

FACT - Root keys available since: 2010-07-15

DNSSEC - Fetch and Validate Root Keys

This is a manual process.

Guide: http://data.iana.org/root-anchors/draft-icann-dnssec-trust-anchor.txt

Complete trust anchor: https://data.iana.org/root-anchors/root-anchors.xml

PGP signature: https://data.iana.org/root-anchors/root-anchors.asc

DNSSEC - Traversal

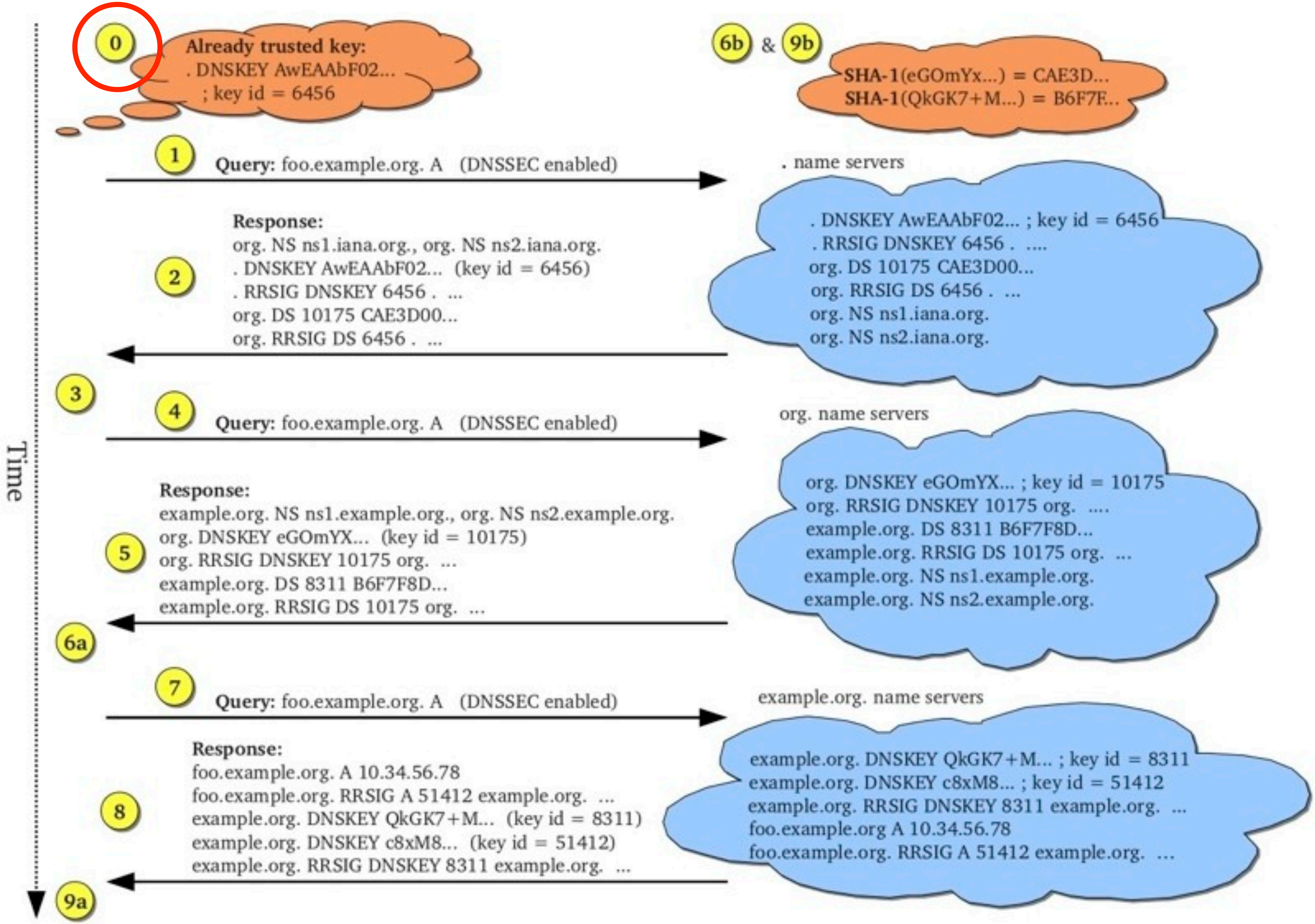


Figure 3.4: *Graphical representation of a DNSSEC traversal*

0

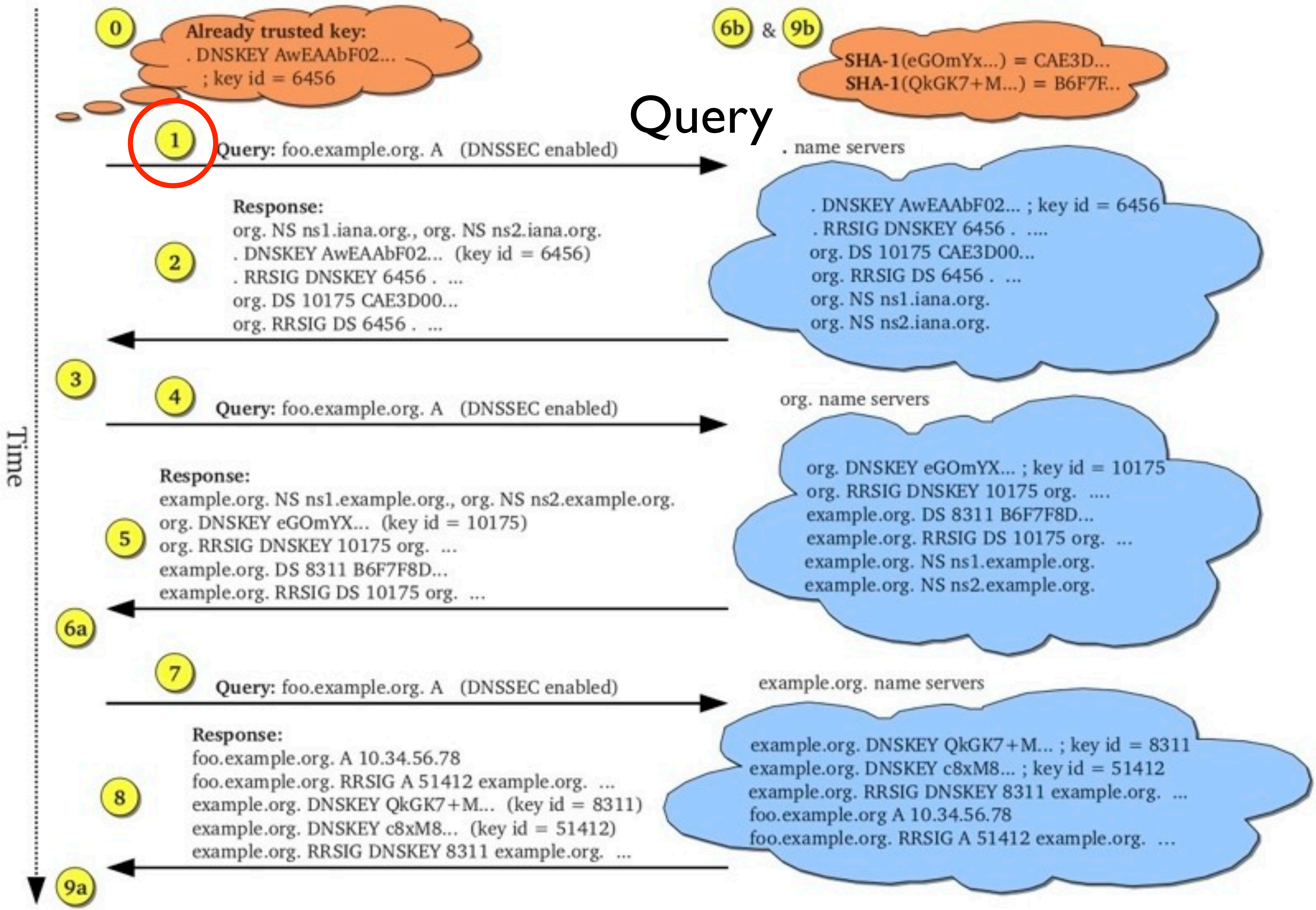


Figure 3.4: *Graphical representation of a DNSSEC traversal*

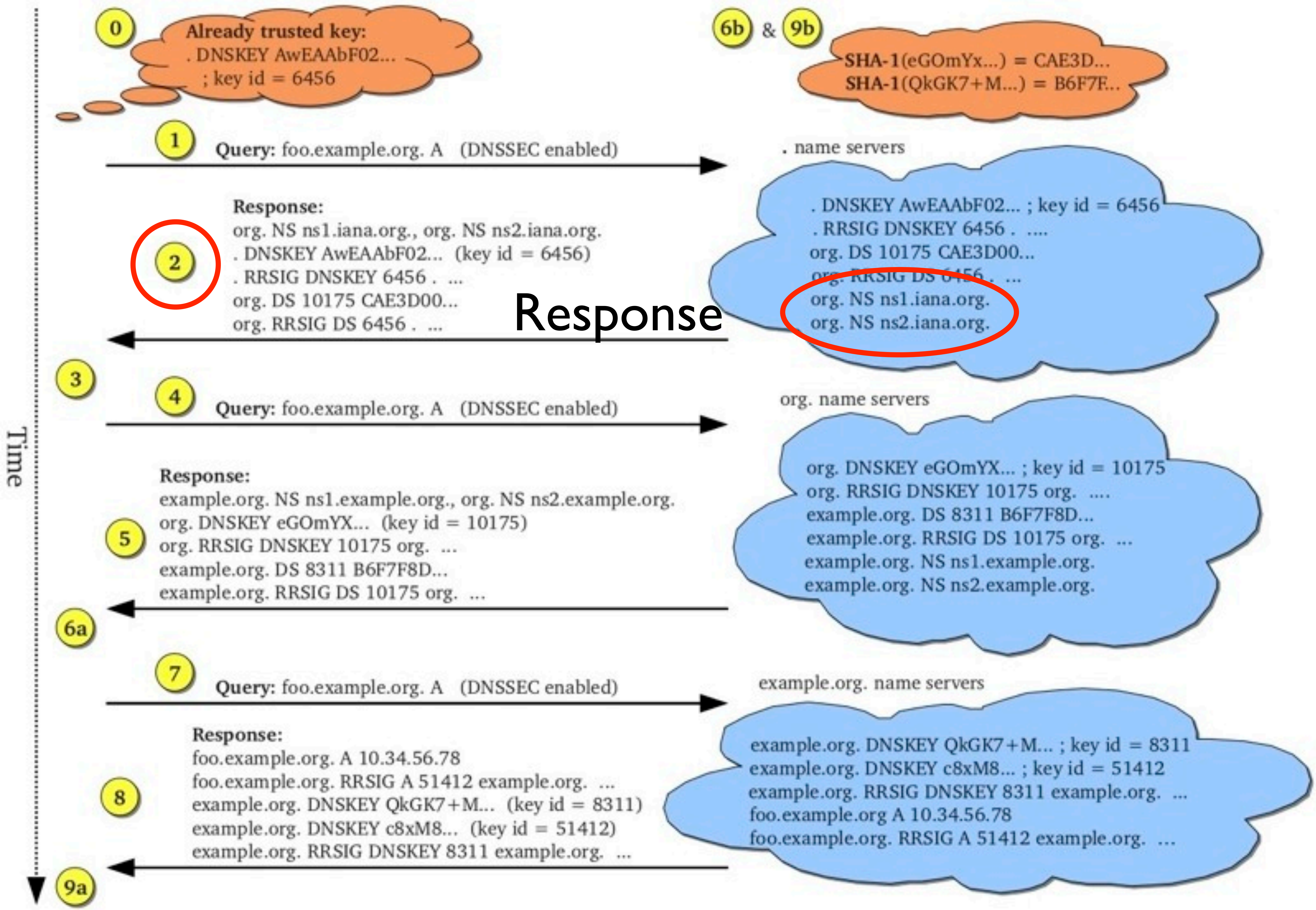


Figure 3.4: *Graphical representation of a DNSSEC traversal*

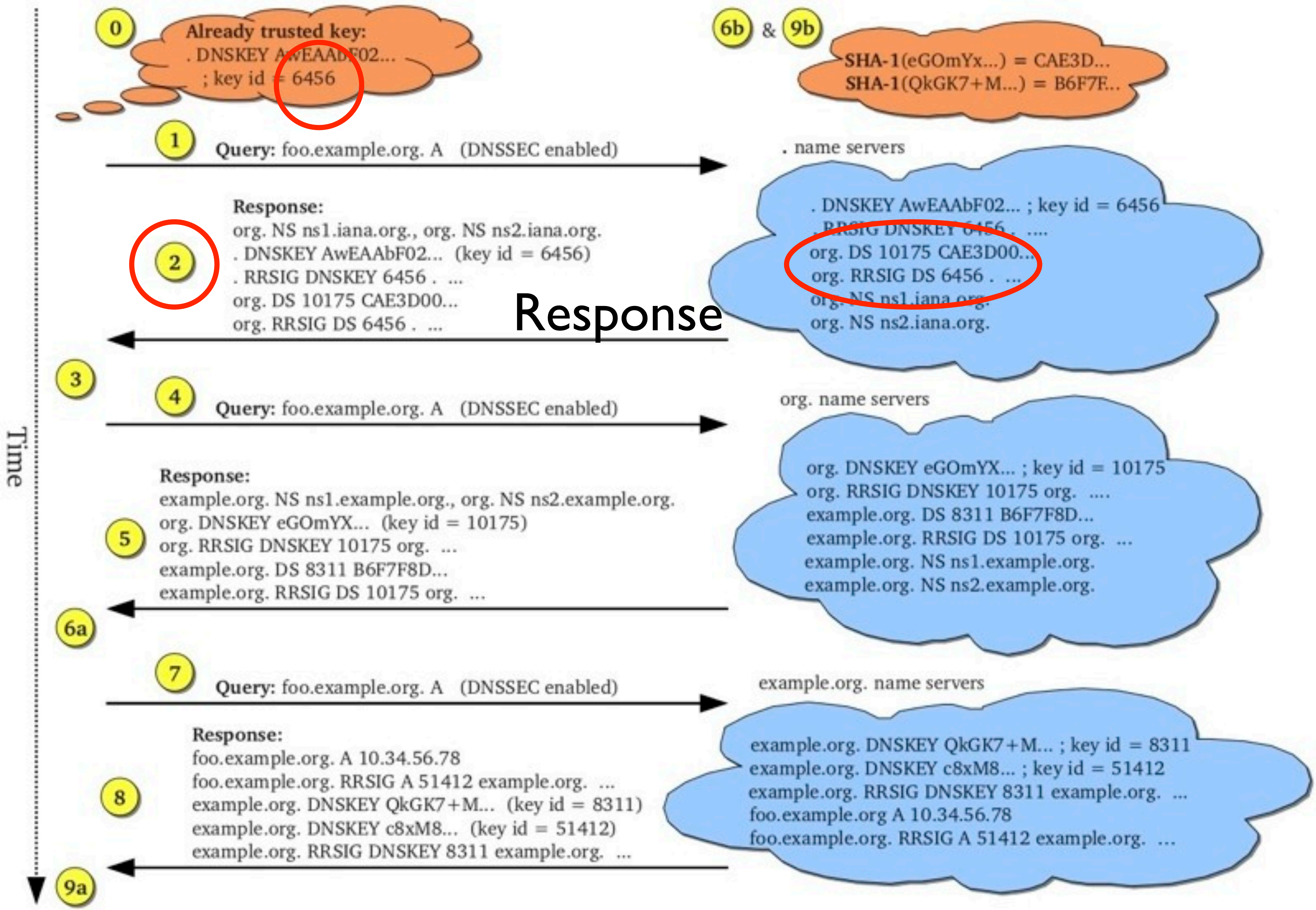


Figure 3.4: *Graphical representation of a DNSSEC traversal*

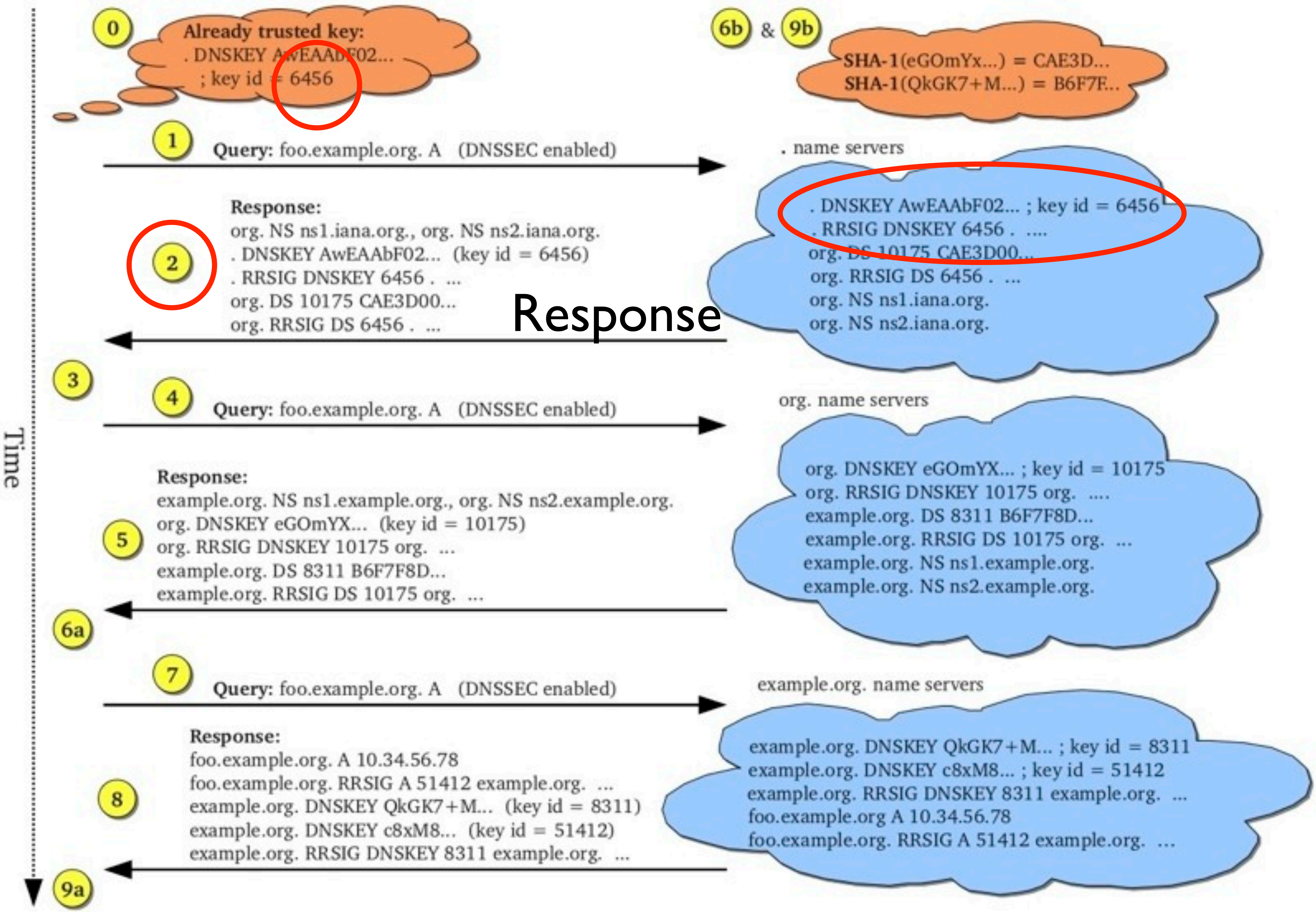


Figure 3.4: *Graphical representation of a DNSSEC traversal*

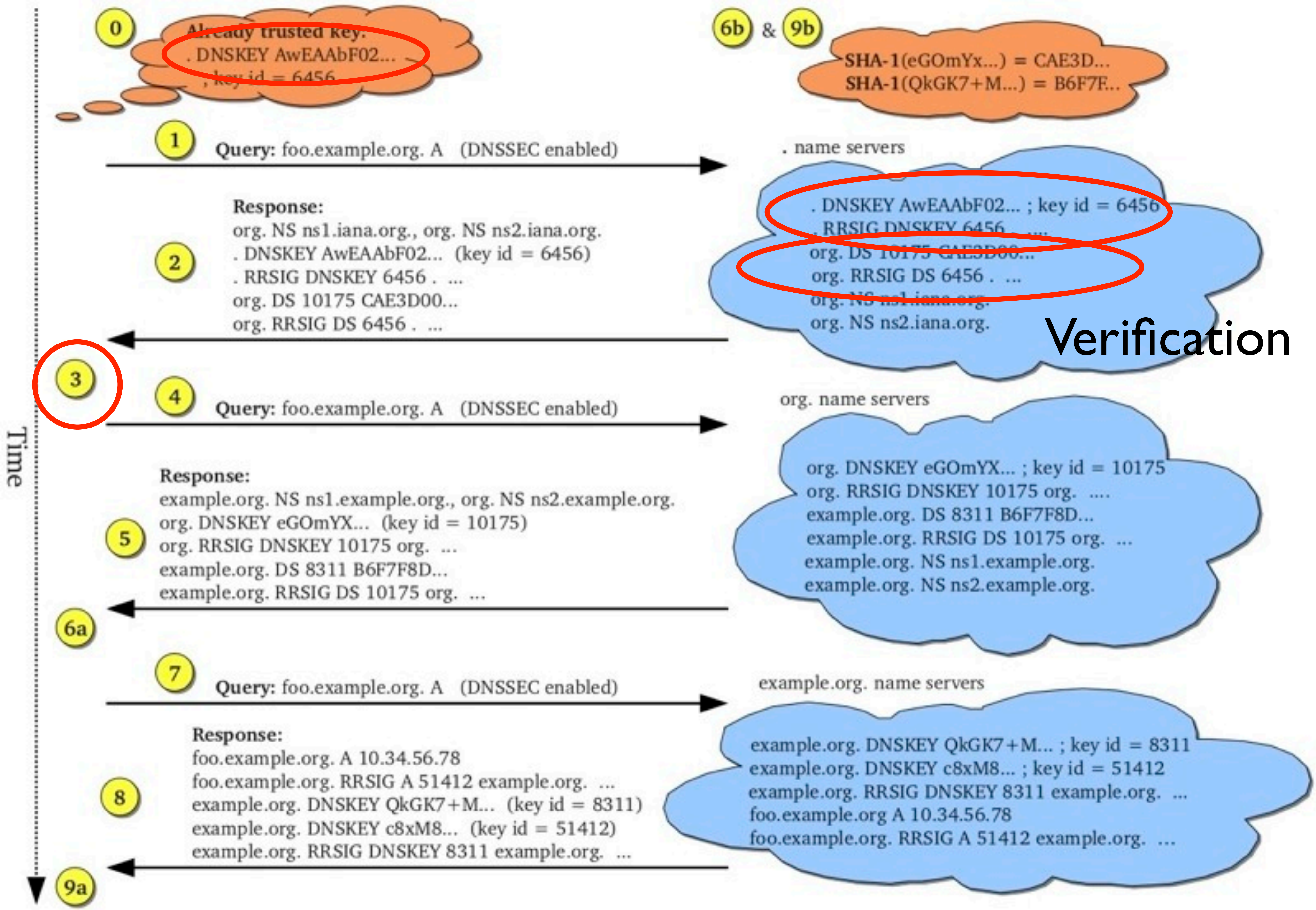


Figure 3.4: *Graphical representation of a DNSSEC traversal*

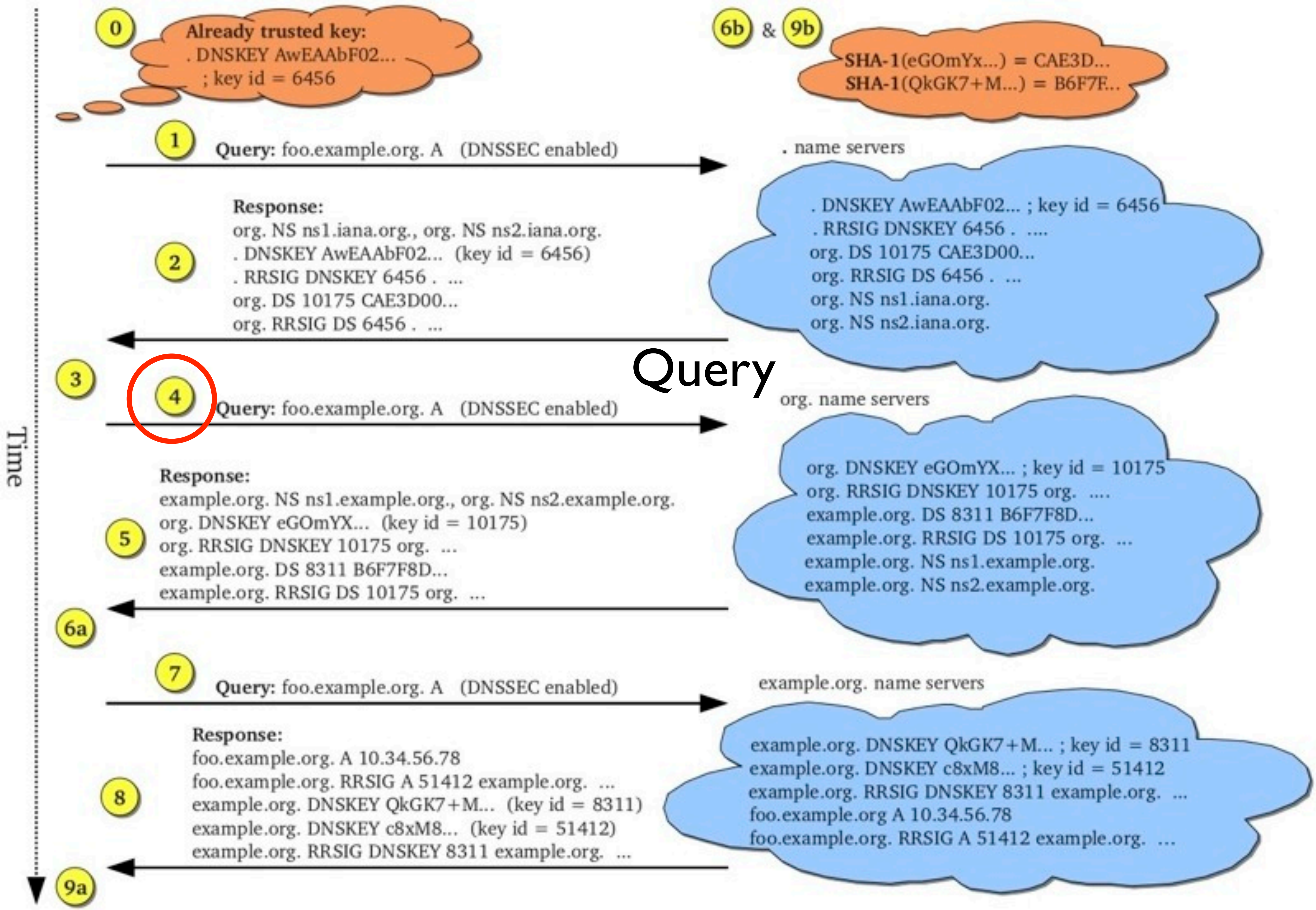


Figure 3.4: *Graphical representation of a DNSSEC traversal*

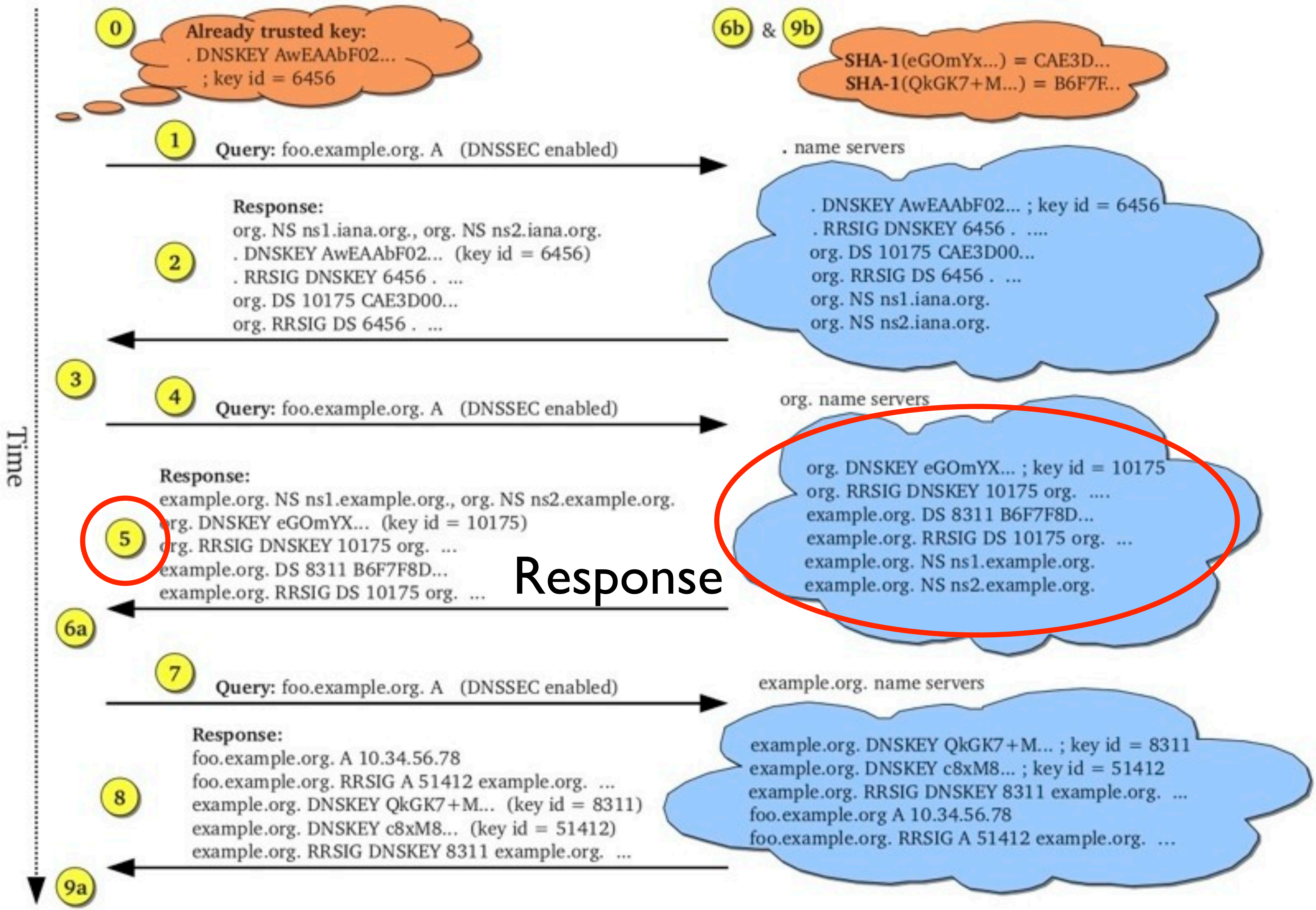


Figure 3.4: *Graphical representation of a DNSSEC traversal*

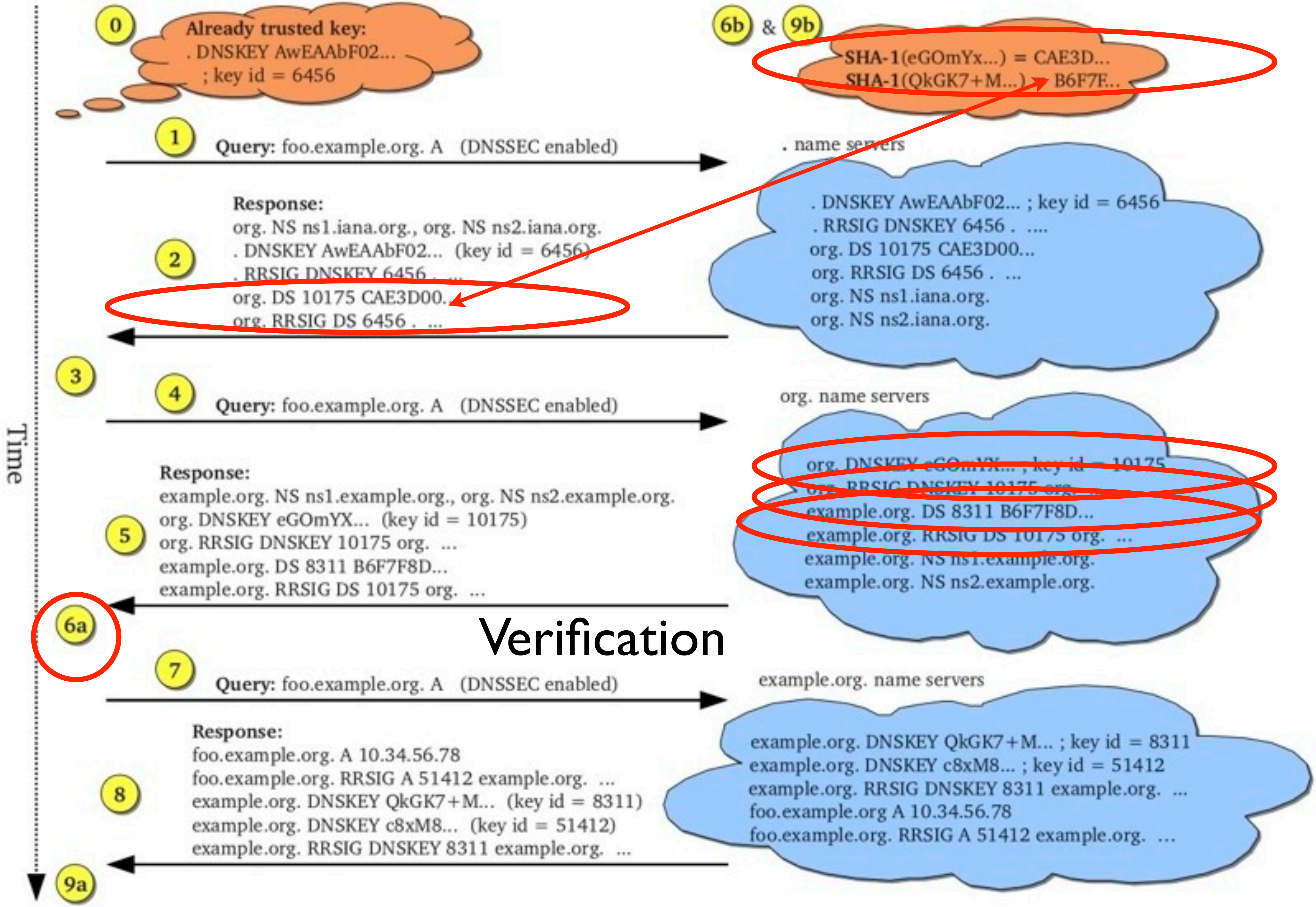


Figure 3.4: *Graphical representation of a DNSSEC traversal*

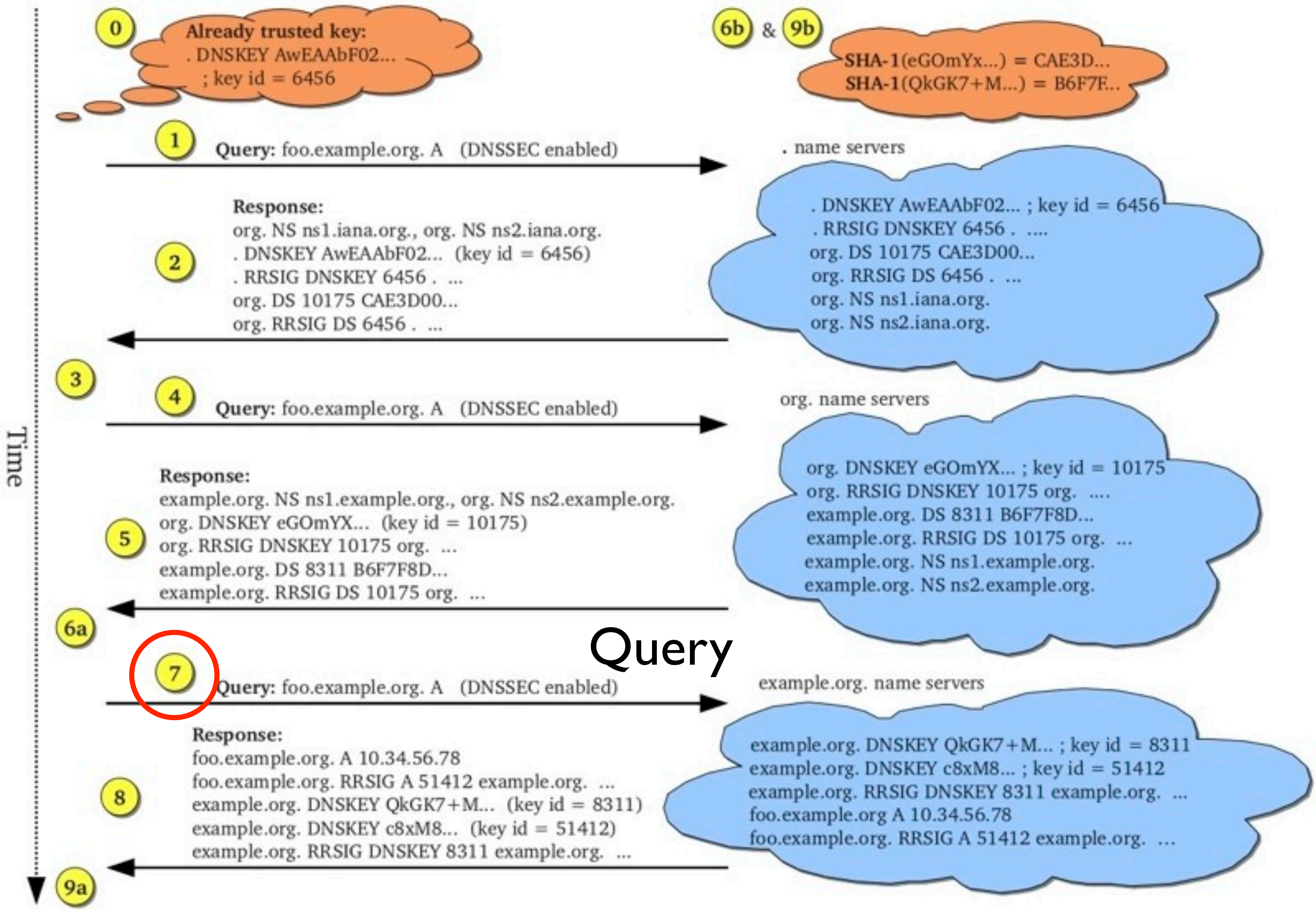


Figure 3.4: *Graphical representation of a DNSSEC traversal*

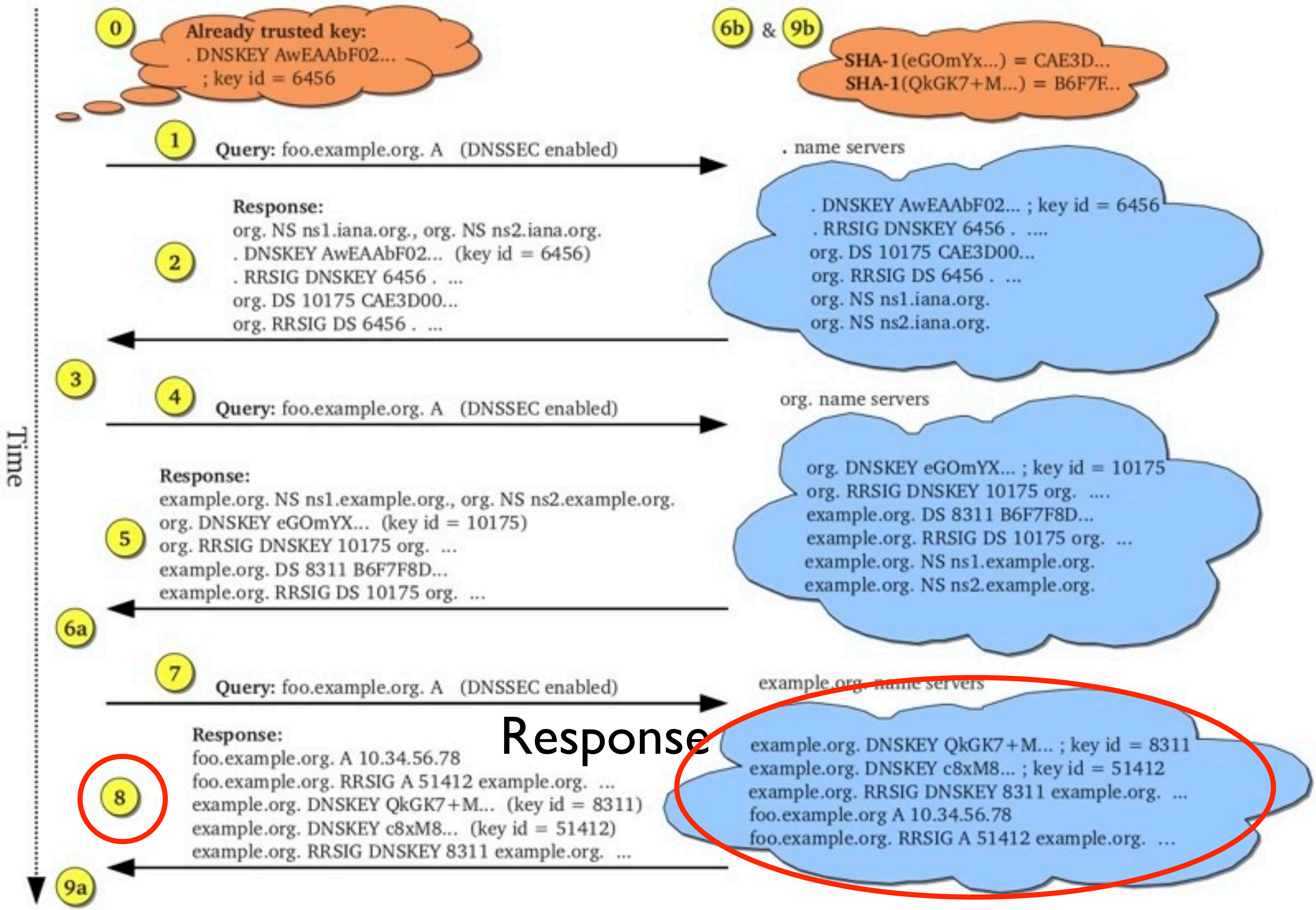


Figure 3.4: *Graphical representation of a DNSSEC traversal*

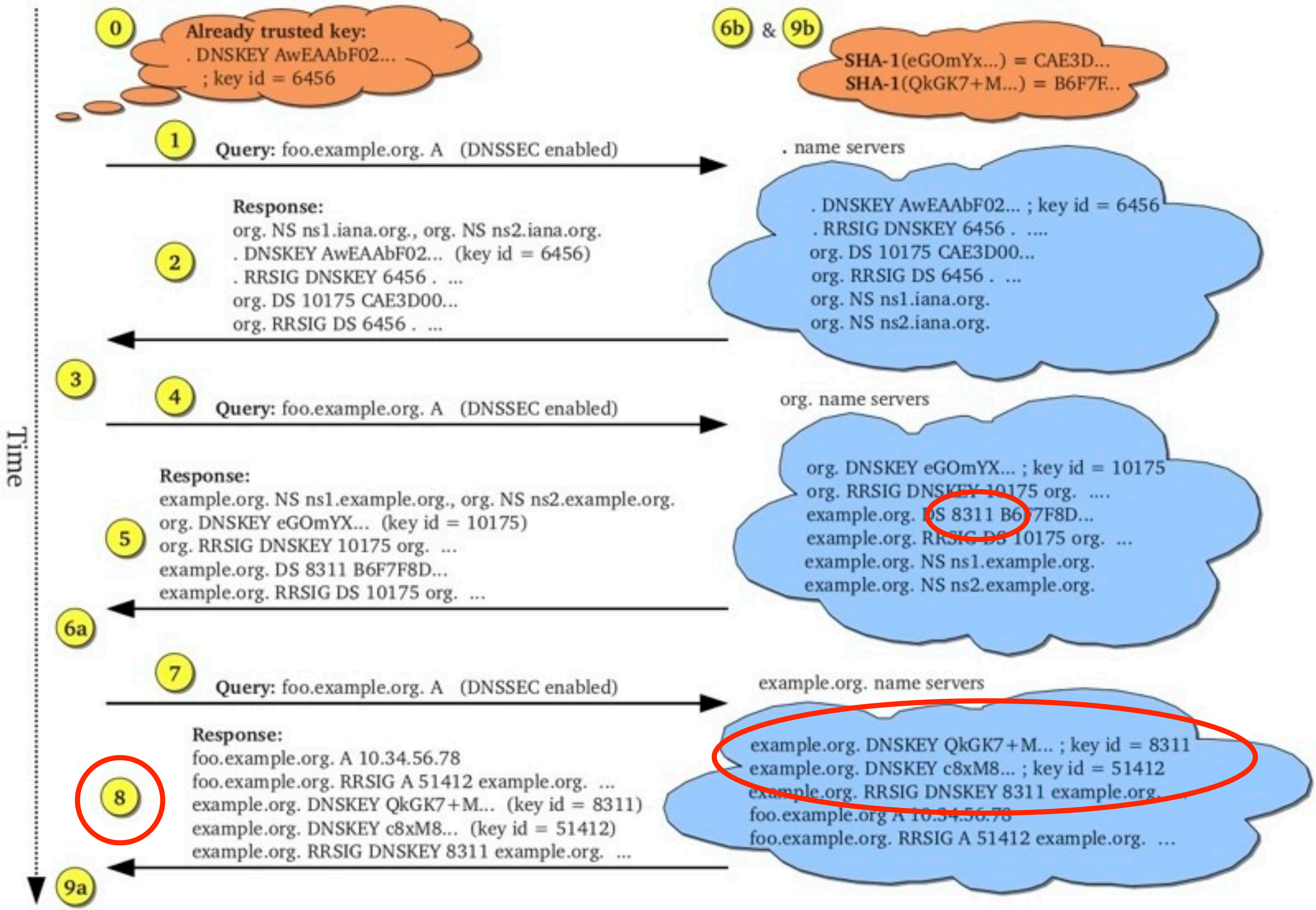


Figure 3.4: *Graphical representation of a DNSSEC traversal*

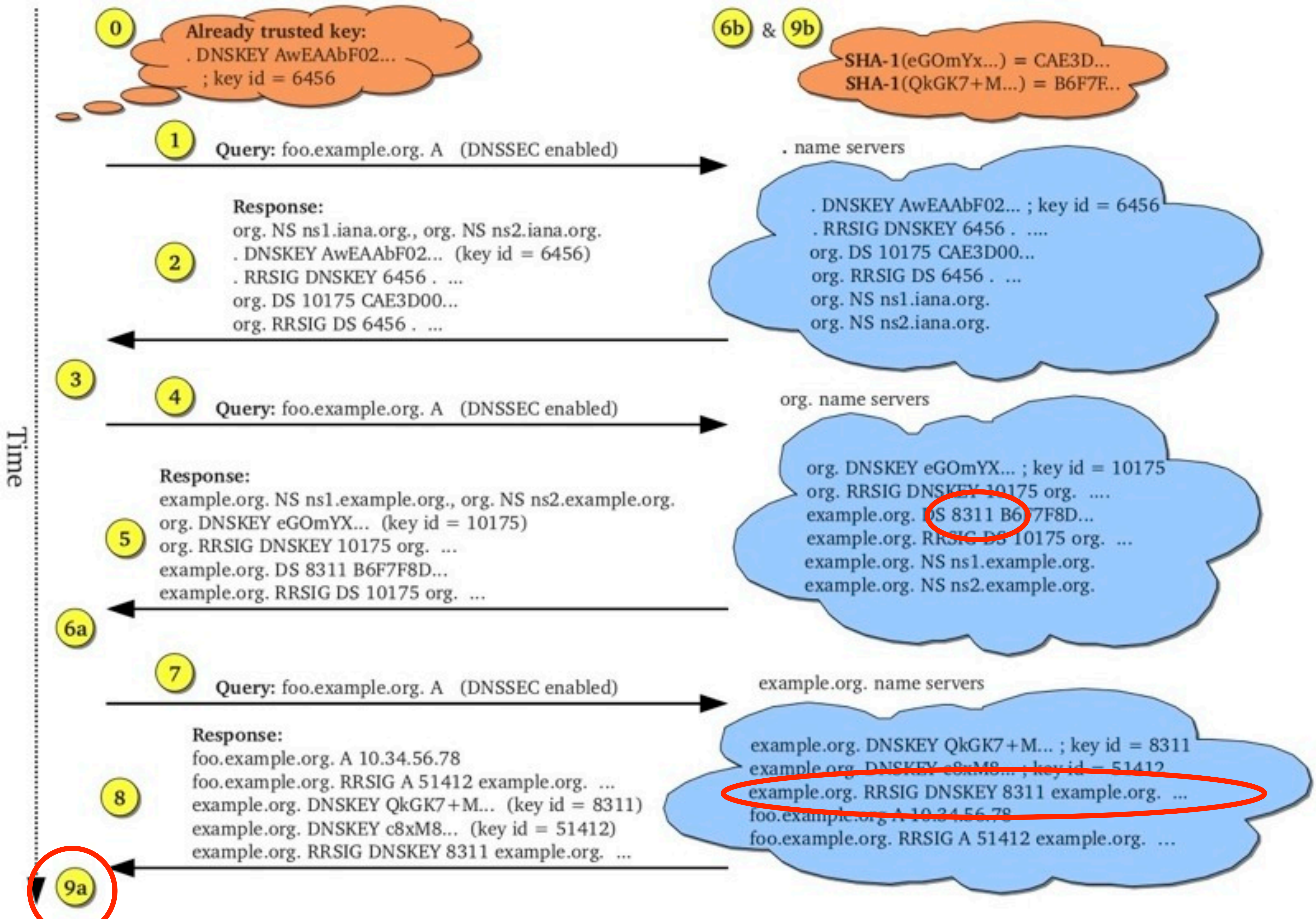


Figure 3.4: *Graphical representation of a DNSSEC traversal*

9a

DNSSEC - Management

<1>

Generate a Key Signing Pair*

* KSK: Larger is better as the life time may be long

<2>

Create a MD of the KSK for the Boss*

* Whoever administers the zone above in the hierarchy

Generate a Zone Signing Pair*

* ZSK is authenticated by signing with the KSK.

<4>

Create the NSEC/NSEC3 RRs

<5>

Create RRSIGs for all RRs using the ZSK

<6>

Recreate RRSIGs when editing RRs or upon expiry *

* NTP is important for proper DNSSEC

<7>

Recreate ZSK/KSK from time to time and resign

<8>

time, disk, bandwidth,memory requirements time, disk, bandwidth,memory requirements

hours, 4-12x, 90% -> 400%,10-200%

DNSSEC - Security

3 goals of good computer security



Confidentiality

Integrity

Availability

Confidentiality?


FAIL

Integrity?


Mostly
WINNING

DNSSEC - Prevents Active MiM attacks *

* given all links in the DNS query-response are DNSSEC aware

DNSSEC - Allows for replay attacks.

DNSSEC - Crypto brute force attacks

DNSSEC - How safe is RSA/SHA-1?

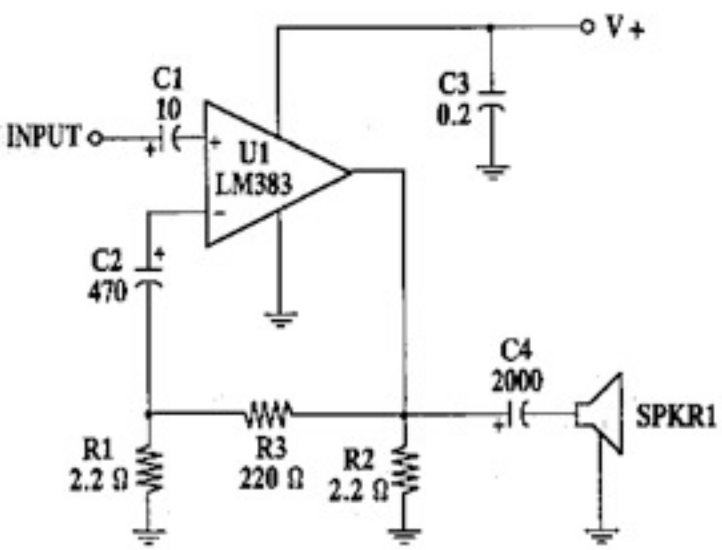
Availability

Potential and Risk of

DNSSEC - Creates other types of attacks

DNSSEC - Enhances DoS/Availability attacks

DNSSEC - Amplification Attack



```
# drill -D se. @a.ns.se. DNSKEY
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 37009
;; flags: qr aa rd ; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; se.	IN	DNSKEY

;; ANSWER SECTION:
se.	3600	IN	DNSKEY	256 3 5 AwEAAYUDNvoT6yfrNra/7d2c7ZoSBphCxjs5xrpPbAPi8F6aP/
oC2W9xPaXa5BXcEhneMwiabUBErF4LWFkSher5z2mrPN/3/YH/78IGwMMWV2wxOAtzbLkhuXWTh7cjH2u5sR8xvVeAQgAV0fGCE/ykvj6bF2pvj1r/
5KRY0izG7PAZ ;{id = 57240 (zsk), size = 1024b}
se.	3600	IN	DNSKEY	256 3 5 AwEAAdZgee2x1z9yHDWAfJ3oqAnwoU/v/awpObk6lCnxtoZ6ukq6+OxgYOdusS7qCHf
+LcBRCsAehpQJAWzL7c4xRrs2PT4/z4jZMtfa1EX6hN+s0ZXjxYwR7WdqVje4/Jtn2krpUvE+jjIyegQ+DKFkbxawGJ5pG3EgU3B0MSvEonMT ;{id =
12973 (zsk), size = 1024b}
se.	3600	IN	DNSKEY	257 3 5 AwEAAbaxTum9L7z1DmPiXPk0QZ2/qUM3to210Caey/ycZuvQ8Mh/
dgGpwBmyZB9xZSkaCLa2Mw6pmDLrjK9hWOffq5PXRVm9RrcA/eIEBEvbQzkY5sFkWAczNAs58Oscxi+/
Gd5KfuVi3lJpYgJwwa2JB4doZ00IXywcCn0VTz0Hsl/lqpA2Bqj+e
+ATzA5hWyiNyHPjiYvyMCkSXTiGgFVVuG8H3N6Us8uSABuO2UoFQeQi6YikIiCbf1FfCzr4vBIRXW6MaDs8kqAAadKjLk3i39dviL/
YeyGUvq9Dan9PsvkwQejKN/7J0yCr2nYXfwGGCHkcBKkagv79EaRlZigUCp8= ;{id = 39547 (ksk), size = 2048b}
se.	3600	IN	DNSKEY	257 3 5 AwEAAb6IEZ2ETrgngbjONAC1Ob4dRs/jD0MYPcMXRzQlo/eqo5AHXvqPaav+rgA3q
+I6zvWYFTMUPxNT2wdJwV4R7VbXb3pBfYPBzeacqPaWSbw4W1BFdYyOWKe0sw3gvwD62dLGbykQAqx5gUYZ8gBtFXDsJe/x+JvenC/
wmz7yW6mxpn3Tzd60vE6wjXhnBs62905xckOBskVx6dI
+dMLoXNG2p5tpXfT4dGrA10SFWVb2C9QTaFww9fP60QqVoYz1xU1Z5BXa5ZB1O8I4rHYGtDYU36n0UhCG4nWnTJgUbNRsN3CeeTplkZ94JS8jMsdA0x983
VIn5stGU1W4juyDqF0= ;{id = 7649 (ksk), size = 2048b}
se.	3600	IN	RRSIG	DNSKEY 5 1 3600 20110409220345 20110403210548 7649 se. U8IIYExbbCcxYeTfQQGB/
jEYuKnVFlG2c8bojkvt3U7fNx7l7Z3IUdEuLxATR4+xw3aKmGdfioC6EXNt5UmcOoUNxyf6t4zhEMmV9/LDXxUlASDIBmk/e5RWTCFeiY
+BU2nY2Rir8owku5C+Rk9bJDx886VhnKj4qD0MJB2Xep1WmFqnPQ8siTEb/rYJ1h/3ao4wWim8lMNttTY4SQC+A7sEAFlY7vN2D73W0lAVIEde/
sh6ARQEgv+YqPTYbN2Wae7tzyI1efr0Ih8suSF8DjUoLeWnFhbSzAbAooS4CegiF/Kkc+2MwuFLtzuYeZVAZnegAZuAH81N833owMfShw== ;{id =
7649}
se.	3600	IN	RRSIG	DNSKEY 5 1 3600 20110410160345 20110404150548 39547 se.
E3uA3bUSOhBNTWoqARj6fSrFdxvaGDjSQRipT5Em+HUX4NO9TR2/02tweeA8QKII3bKBRfZ1r56blLK9nqOelv3UhPgEbwHwmdpC9fHbRi9FCX
+hL5UuZWCUqcwnu3rTLRIckpAGf+LOnuXyurwHauVhb2ij1QQ9W/A1a4dddDwbiFxgg0Lo5xaTmA8ixw4Z59AvM5WudWHv5X1yG0VX3dDNoHFbD
+PdOBuZ0ZZg4XnYKFAWBu6gUPsgTkhCrF+q+9k+0d9duybXXrDEJnOBu+YVEVu1ECtdekvGPV+UWOA/SOLfLWPNPPjjgu/
JsMeKLIbgEvQIsu6zpaZvc1l8ng== ;{id = 39547}
```

```
# drill -D se. @a.ns.se. DNSKEY
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 37009
;; flags: qr aa rd ; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; se.  IN      DNSKEY

;; ANSWER SECTION:
se.     3600    IN      DNSKEY  256 3 5 AwEAAYUDNvoT6yfrNra/7d2c7ZoSBphCxjs5xrpPbAPi8F6aP/
oC2W9xPaXa5BXcEhneMwiabUBErF4LWFkSher5z2mrPN/3/YH/78IGwMMWV2wxOAtzbLkhuXWTh7cjH2u5sR8xvVeAQgAV0fGCE/ykvj6bF2pvj1r/
5KRY0izG7PAZ ;{id = 57240 (zsk), size = 1024b}
se.     3600    IN      DNSKEY  256 3 5 AwEAAdZgee2x1z9yHDWAfJ3oqAnwoU/v/awpObk6lCnxtoZ6ukq6+OxgYOdusS7qCHf
+LcBRCsAehpQJAWzL7c4xRrs2PT4/z4jZMtfa1EX6hN+s0ZXjxYwR7WdqVje4/Jtn2krpUvE+jjIyegQ+DKFkbxawGJ5pG3EgU3B0MSvEonMT ;{id =
12973 (zsk), size = 1024b}
se.     3600    IN      DNSKEY  257 3 5 AwEAAbaxTum9L7z1DmPiXPk0QZ2/qUM3to210Caey/ycZuvQ8Mh/
dgGpwBmyZB9xZSkaCLa2Mw6pmDLrjK9hWOffq5PXRVm9RrcA/eIEBEvbQzkY5sFkWAczNAs58Oscxi+/
Gd5KfuVi3lJpYgJwwa2JB4doZ00IXywcCn0VTz0Hsl/lqpA2Bqj+e
+ATzA5hWyiNyHPjiYvyMCkSXTiGgFVVuG8H3N6Us8uSABuO2UoFQeQi6YikIiCbf1FfCzr4vBIRXW6MaDs8kqAAadKjLk3i39dviL/
YeyGUvq9Dan9PsvkwQejKN/7J0yCr2nYXfwGGCHkcBKkagv79EaRlZigUCp8= ;{id = 39547 (ksk), size = 2048b}
se.     3600    IN      DNSKEY  257 3 5 AwEAAb6IEZ2ETrgngbjONAC1Ob4dRs/jD0MYPcMXRzQlo/eqo5AHXvqPaav+rgA3q
+I6zvWYFTMUPxNT2wdJwV4R7VbXb3pBfYPBzeacqPaWSbw4W1BFdYyOWKe0sw3gvwD62dLGbykQAqx5gUYZ8gBtFXDsJe/x+JvenC/
wmz7yW6mxpn3Tzd60vE6wjXhnBs62905xckOBskVx6dI
+dMLoXNG2p5tpXfT4dGrA10SFWVb2C9QTaFww9fP60QqVoYz1xU1Z5BXa5ZB1O8I4rHYGtDYU36n0UhCG4nWnTJgUbNRsN3CeeTplkZ94JS8jMsdA0x983
VIn5stGU1W4juyDqF0= ;{id = 7649 (ksk), size = 2048b}
se.     3600    IN      RRSIG   DNSKEY 5 1 3600 20110409220345 20110403210548 7649 se. U8IIYExbbCcxYeTfQQGB/
jEYuKnVFlG2c8bojkvt3U7fNx7l7Z3IUdEuLxATR4+xw3aKmGdfioC6EXNt5UmcOoUNxyf6t4zhEMmV9/LDXxUlASDIBmk/e5RWTCFeiY
+BU2nY2Rir8owku5C+Rk9bJDx886VhnKj4qD0MJB2Xep1WmFqnPQ8siTEb/rYJ1h/3ao4wWim8lMNttTY4SQC+A7sEAFlY7vN2D73W0lAVIEde/
sh6ARQEgv+YqPTYbN2Wae7tzyI1efr0Ih8suSF8DjUoLeWnFhbSzAbAooS4CegiF/Kkc+2MwuFLtzuYeZVAZnegAZuAH81N833owMfShw== ;{id =
7649}
se.     3600    IN      RRSIG   DNSKEY 5 1 3600 20110410160345 20110404150548 39547 se.
E3uA3bUSOhBNTWoqARj6fSrFdxvaGDjSQRipT5Em+HUX4NO9TR2/02tweeA8QKII3bKBRfZ1r56blLK9nqOelv3UhPgEbwHwmdpC9fHbRi9FCX
+hL5UuZWCUqcwnu3rTLRIckpAGf+LOnuXyurwHauVhb2ij1QQ9W/A1a4dddDwbiFxgg0Lo5xaTmA8ixw4Z59AvM5WudWHv5X1yG0VX3dDNoHFbD
+PdOBuZ0ZZg4XnYKFAWBu6gUPsgTkhCrF+q+9k+0d9duybXXrDEJnOBu+YVEVu1ECtdekvGPV+UWOA/SOLfLWPNPPjjgu/
JsMeKLIbgEvQIsu6zpaZvc1l8ng== ;{id = 39547}
```

Response:Query = 120:1

Average amplification factor: 30x

DNSCurve

DNSCurve: Rationale

DNSSEC: 15 years in the making

DNSSEC: does not solve all the security issues

mathematician
cryptologist
programmer

DNSCurve: History

DNSCurve: Proposed in 2008

DNSCurve: Objectives

Confidentiality

All DNS payload data is encrypted

IP, UDP, TCP headers are plaintext

Encryption Methods

Does not use standard RSA

Does use ECC*

* Elliptic-Curve Cryptography

Specifically: Curve25519

Curve25519 is Open/Free

Curve25519 is fast enough for real time encryption

RSA-1024 requires ~ 2^80 operations to break

How large computationally speaking is 2^80?

x 1 year == 2^69

2048 x 1 year == 2^80

2003: 1024-bit RSA deemed breakable

2003: RSA Labs recommends 2048-bit RSA for the remainder of the decade

2005: NSA recommends ECC for all public-key cryptography and withdrawing previous recommendations of RSA.

2007: NIST recommends 2048-bit RSA

2010: US gov. recommends 2048-bit RSA

Curve25519 == 3000 bit RSA

ECC-256 requires 2^128 operations

ECC-256: no attack degradation on 25 years

Confidentiality?

Integrity…

All DNS Queries and Responses are authenticated, cryptographically

Authenticity is guaranteed as well as non-repudiation

Uses nonces* in all communication to prevent replay attacks

* one time use number

Backwards compatible with regular DNS services

Integrity?

Availability

Server: several authoritative servers

Client: Non-authenticated/Rogue DNS servers are rejected

Client: some amplification is produced

Availability

Protocol Specification

Two data formats of are used

Streamlined Format

Custom & Efficient

Query Format

```
                                 1  1  1  1  1  1
   0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Q| 6| f| n| v| W| j| 8|
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|               CLIENT PUBLIC KEY               |
|                                               |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|            CLIENT NONCE           |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
/                                               /
/               CRYPTOGRAPHIC BOX               /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Response Format

```
                                          1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| R| 6| f| n| v| W| J| 8|
+--+--+--+--+--+--+--+--+--+--+--+--+
|             CLIENT NONCE          |
+--+--+--+--+--+--+--+--+--+--+--+--+
|             SERVER NONCE          |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
/                                               /
/                 CRYPTOGRAPHIC BOX             /
/                                               /
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

TXT-Format

DNSCurve: Key Usage

No new RRs are introduced

DNSSEC: RRs provide the keys

DNSCurve: No new RRs

How do we get the name server keys?

"If it were not for key management,
Cryptography would be easy!"

“note -- i think dnssec is terribly ugly but i have come to terms with that and am pushing forward with it because i want what it can do for the world.”

Paul Vixie, BIND/DNSSEC author/architect

Keys are obtained from existing RRs!

Server pub keys are hidden in NS records

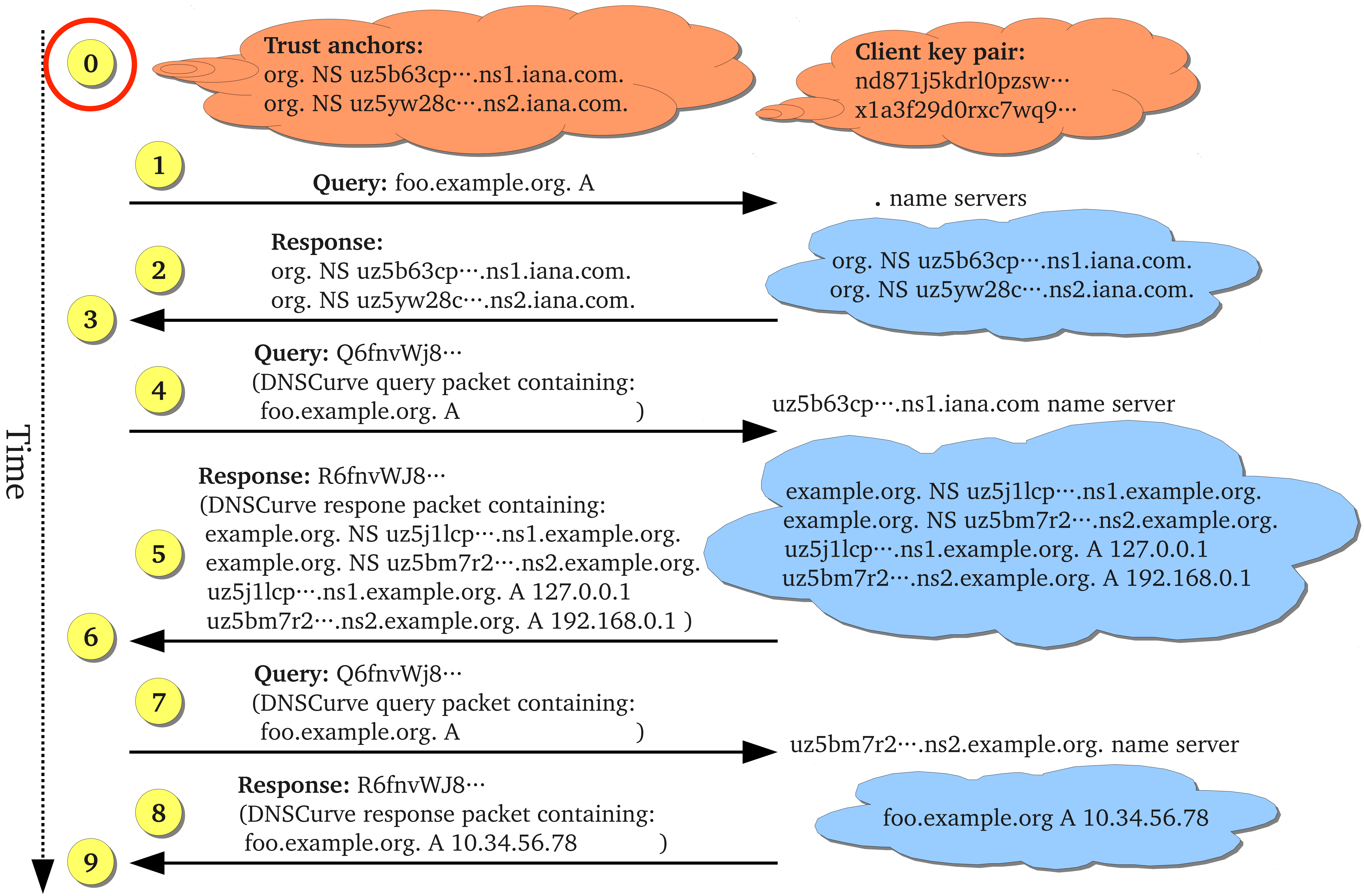
E.g. example.org

Regular DNS: ns1.example.org

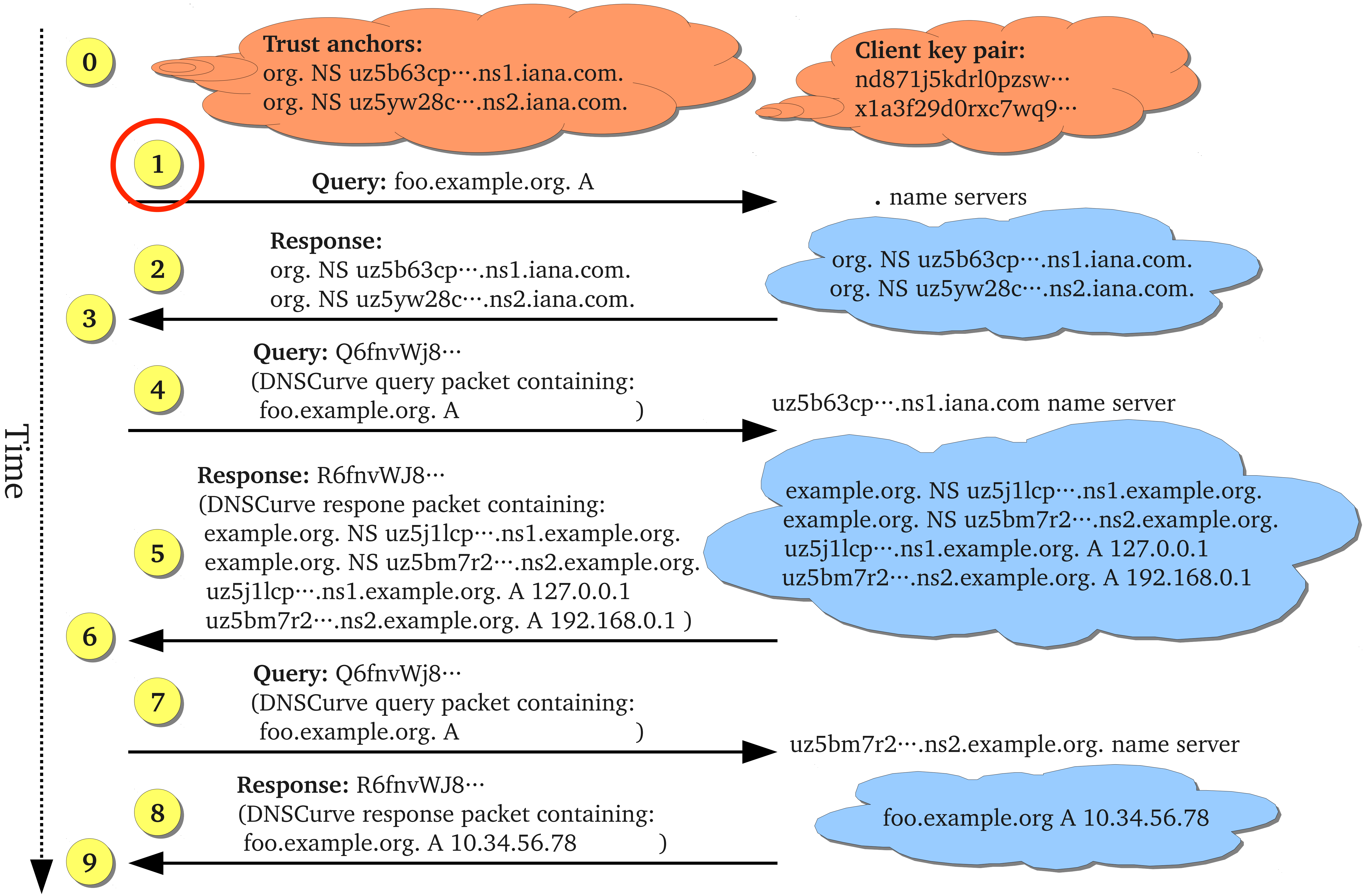
DNScurve:

uz5dkhm9g380kyx9slmktyvmb1h0ck7whwzc5uqvl8f1cwfp8zl3ub.ns1.example.org

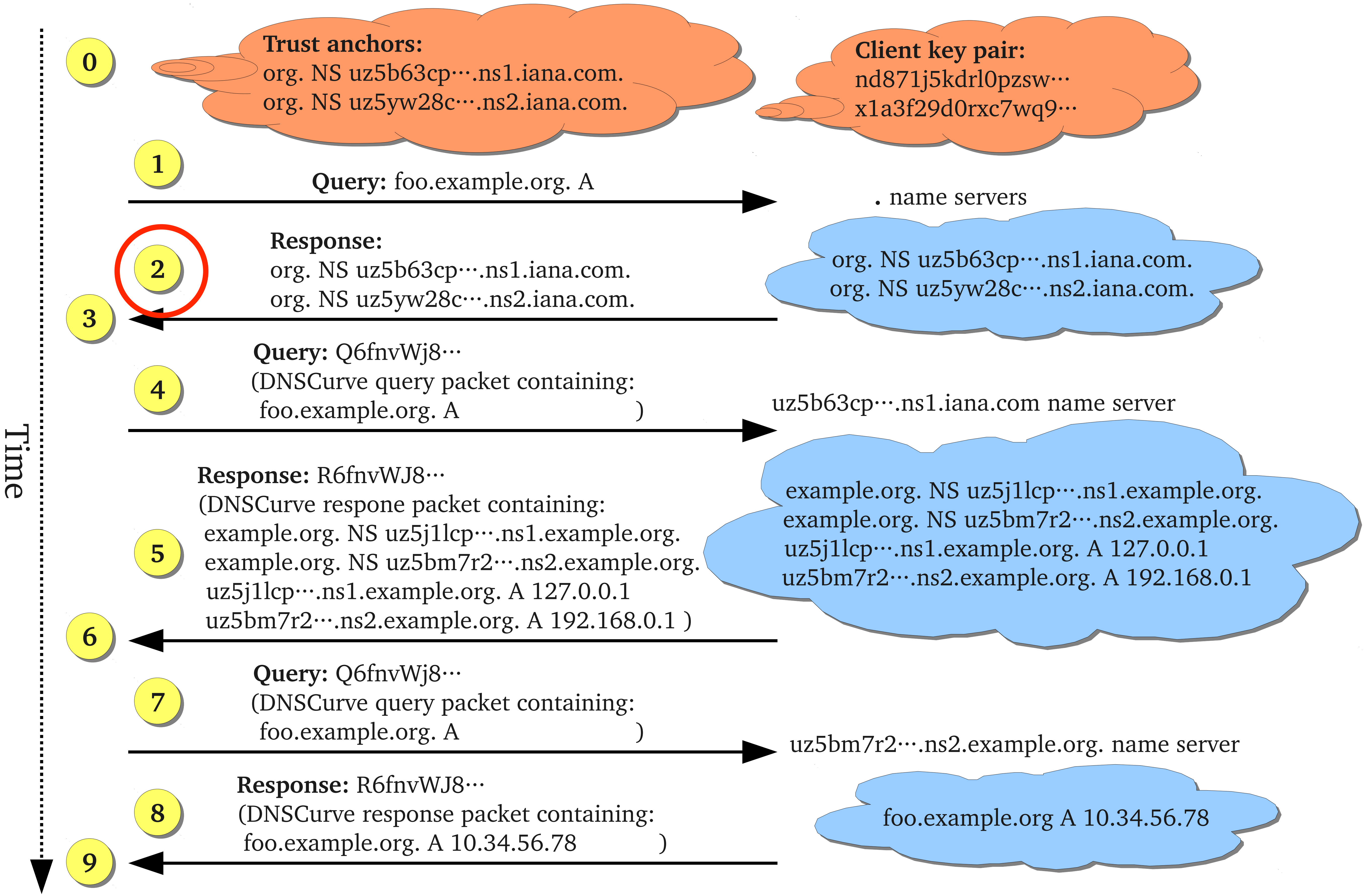
DNSCurve: Traversal



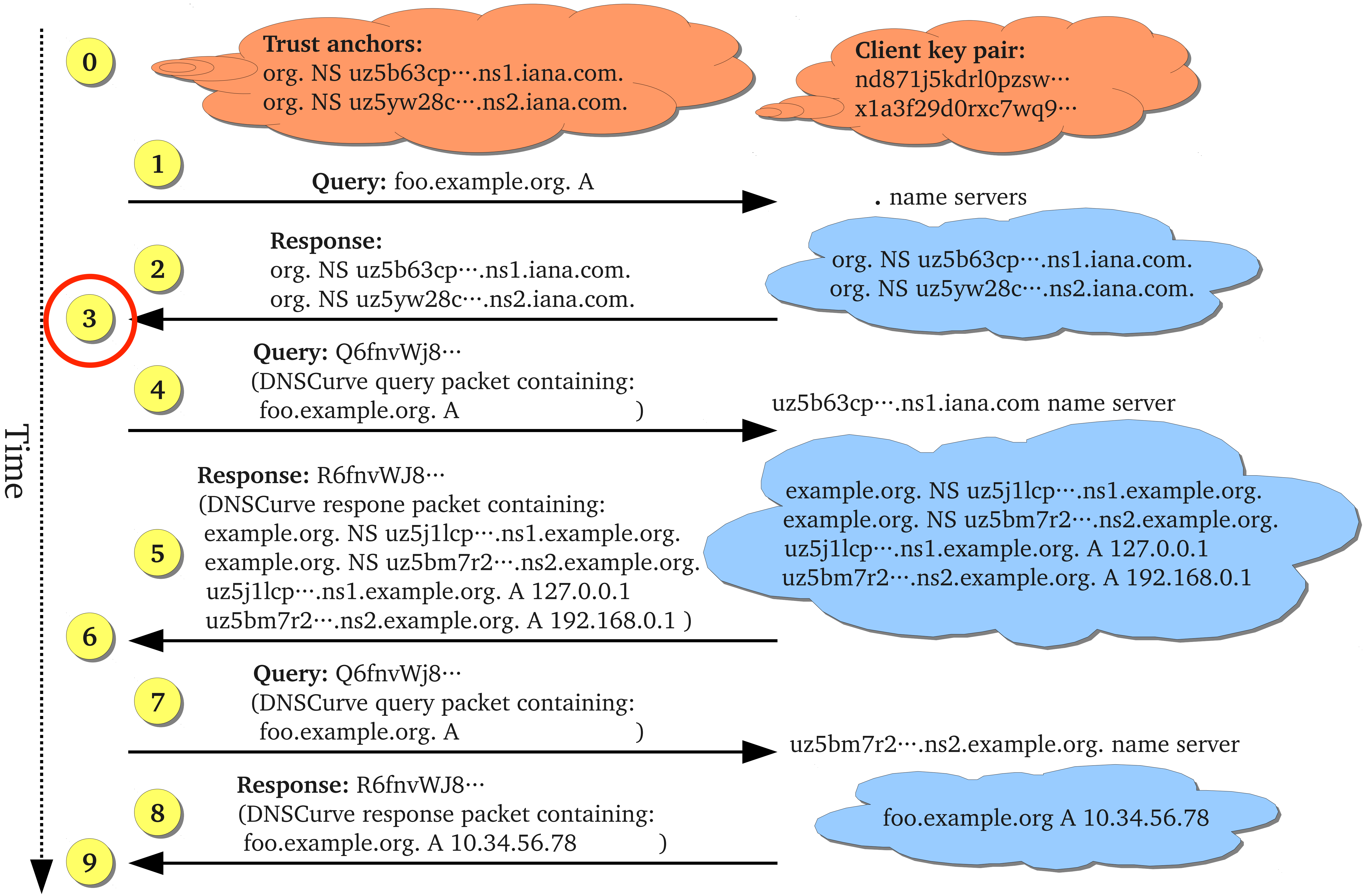
Graphical representation of a DNSCurve traversal



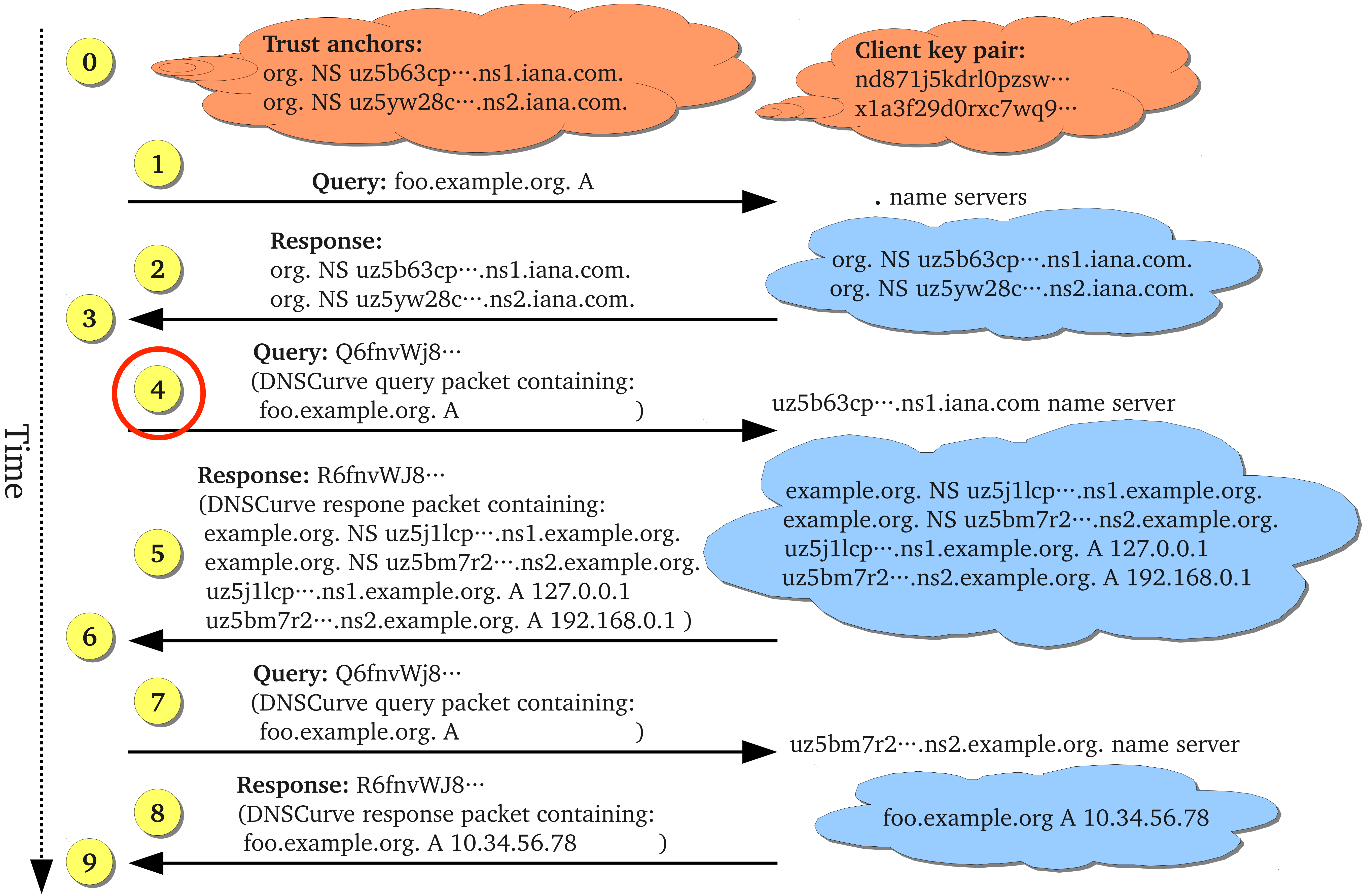
Graphical representation of a DNSCurve traversal



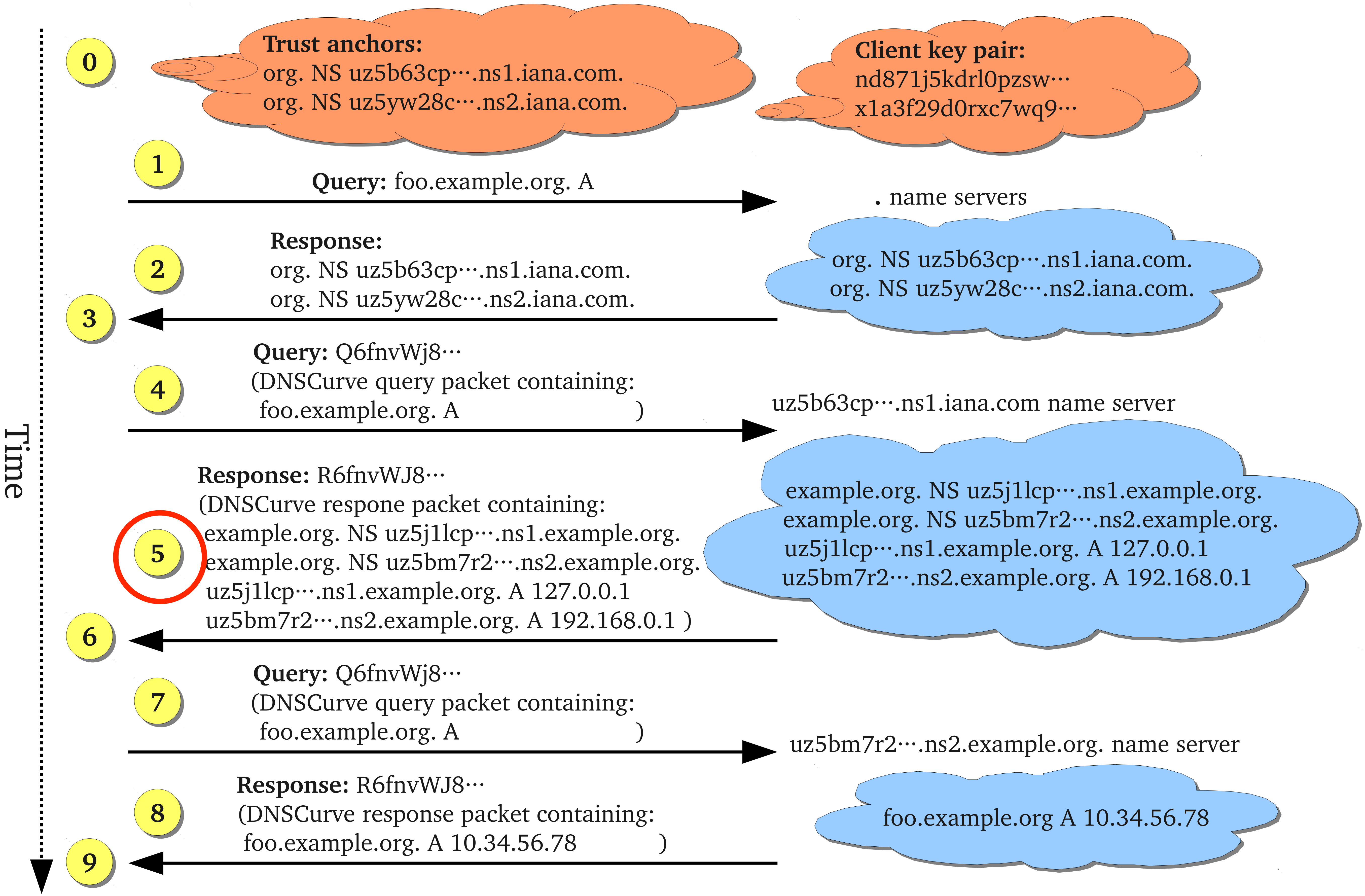
Graphical representation of a DNSCurve traversal



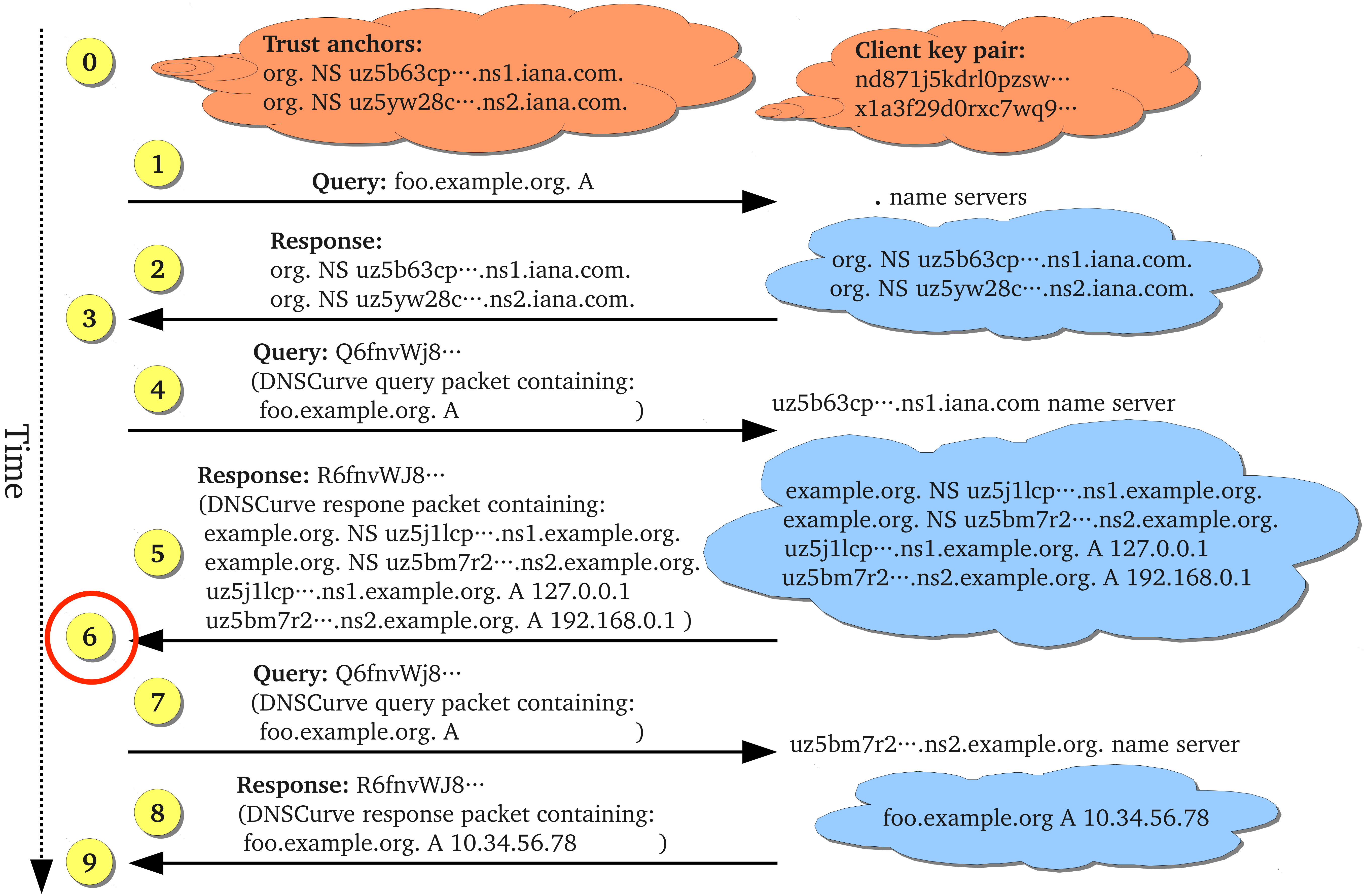
Graphical representation of a DNSCurve traversal



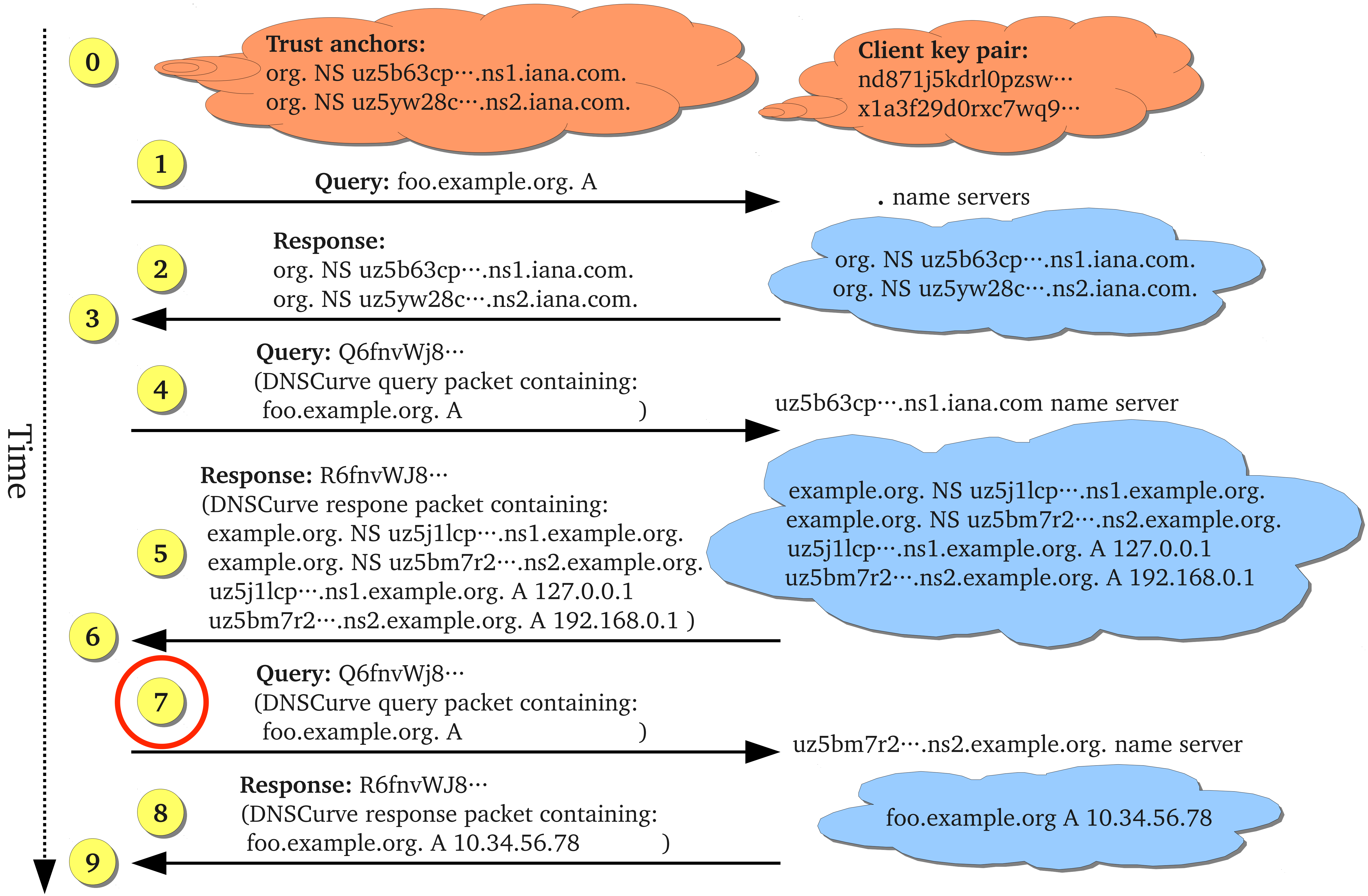
Graphical representation of a DNSCurve traversal



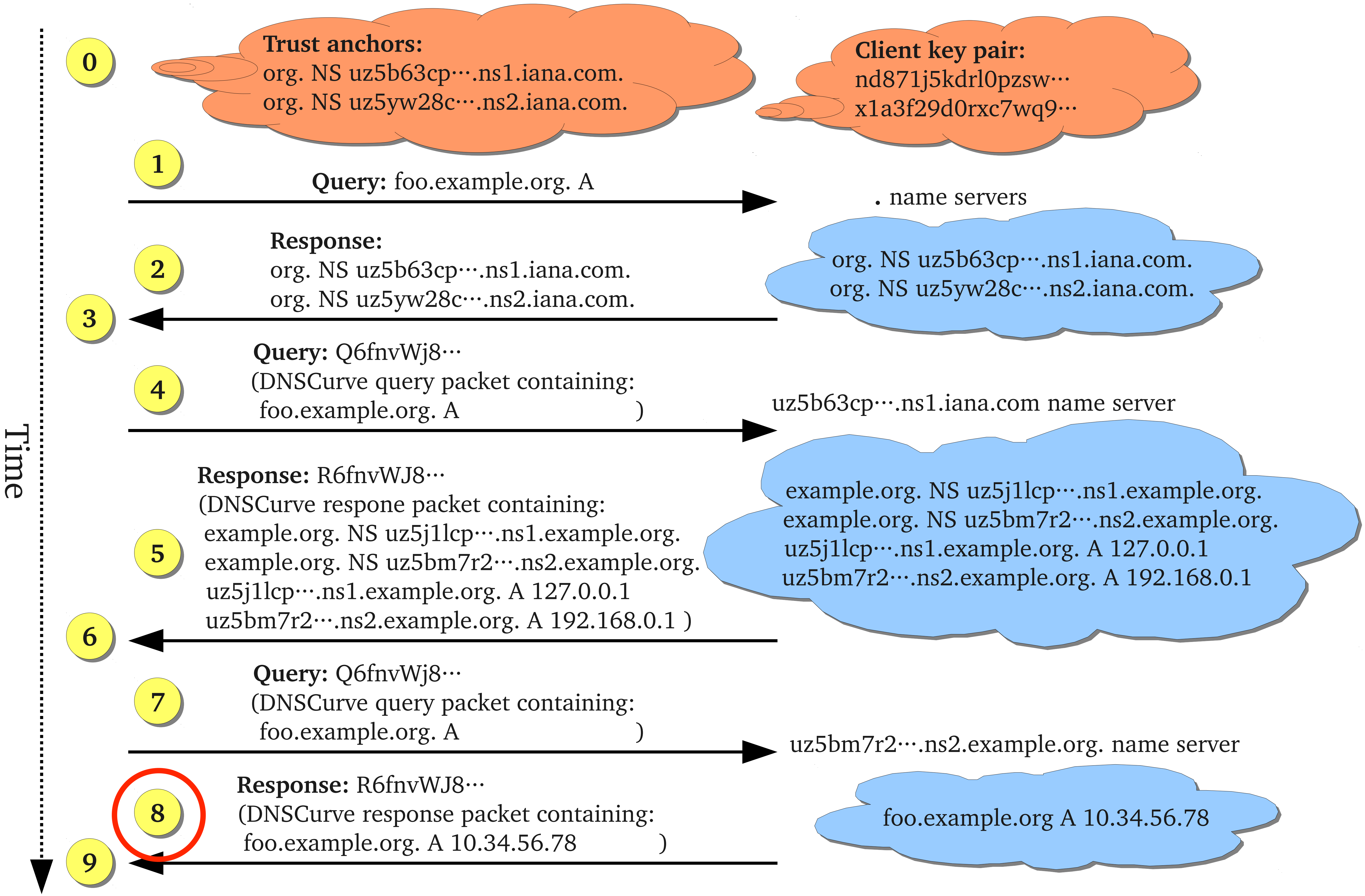
Graphical representation of a DNSCurve traversal



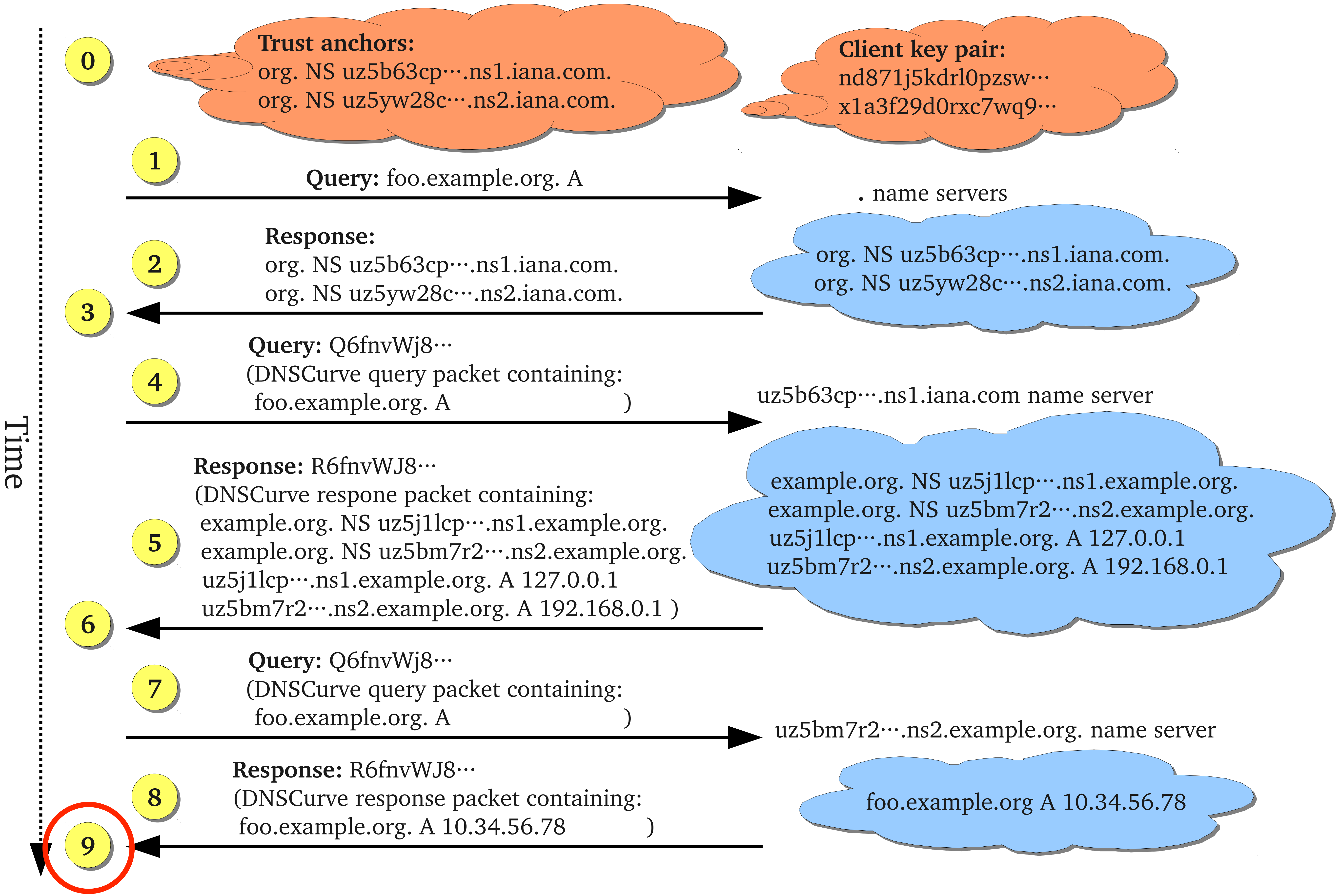
Graphical representation of a DNSCurve traversal



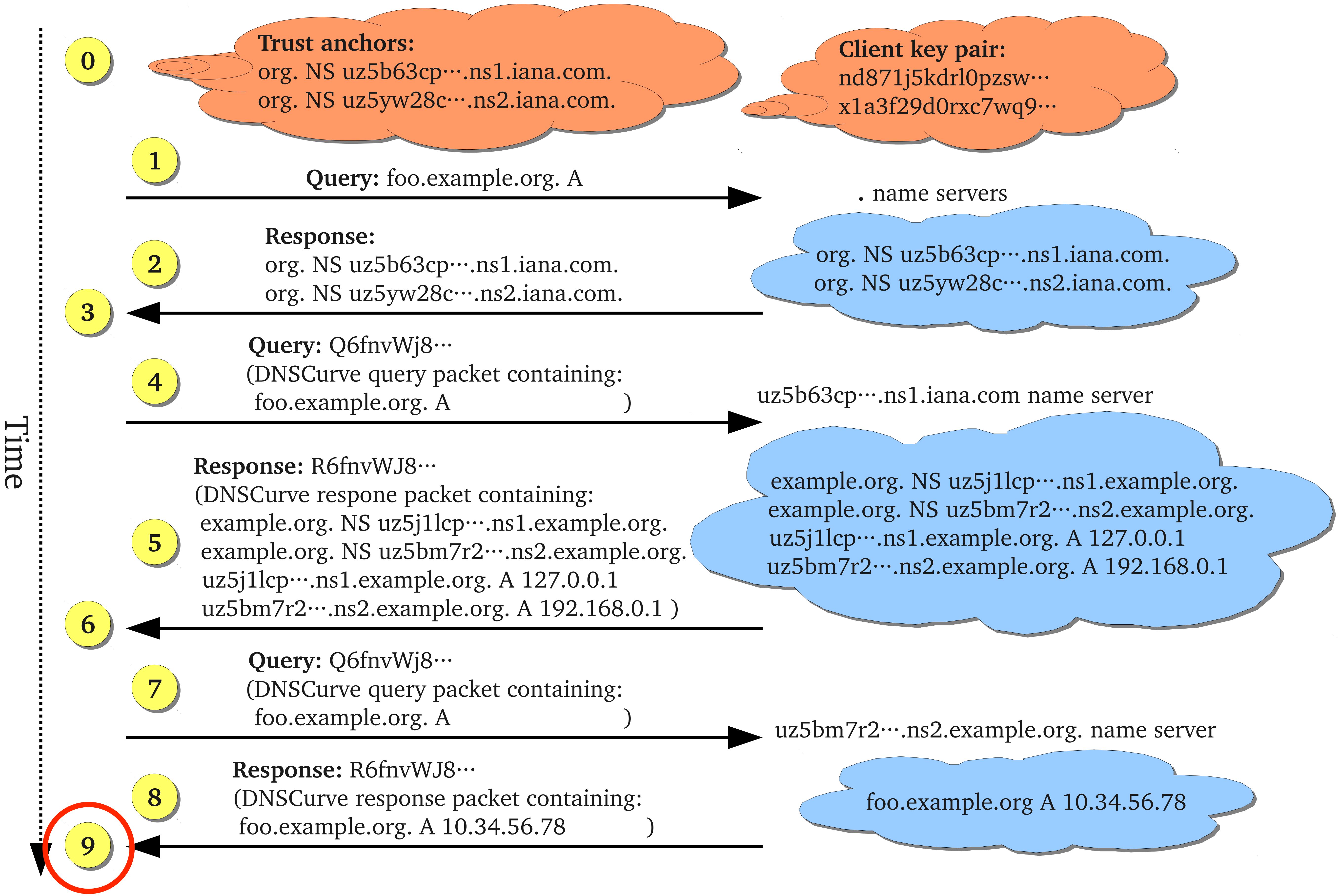
Graphical representation of a DNSCurve traversal



Graphical representation of a DNSCurve traversal



Graphical representation of a DNSCurve traversal



Graphical representation of a DNSCurve traversal

Conclusions....

DNSSEC is big and messy

DNSSEC solves some security problems

but creates some significant others

DNSSEC has problems with the last mile

Given HTTPS, what exactly does DNSSEC offer?

DNSCurve is less messy

DNSCurve solves more problems than DNSSEC

DNSCurve is a more general solution

Both DNSSEC & DNSCurve need to be tested and tried locally.