# Saving the Internet from doom (DNSSEC and IPv6)

Sofia, Bulgaria
September 2008

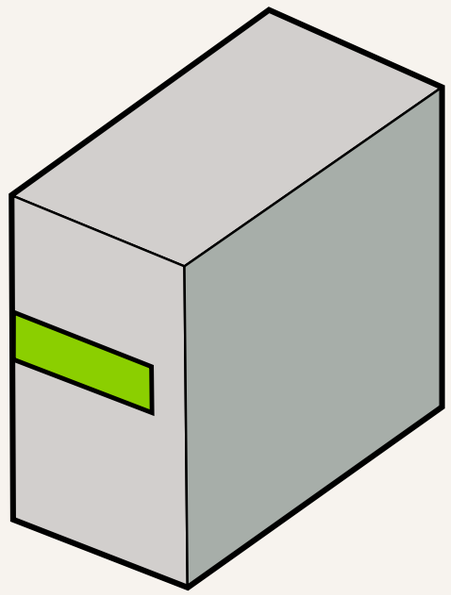
Kim Davies
Internet Assigned Numbers Authority


Internet Corporation for
Assigned Names & Numbers

# Agenda

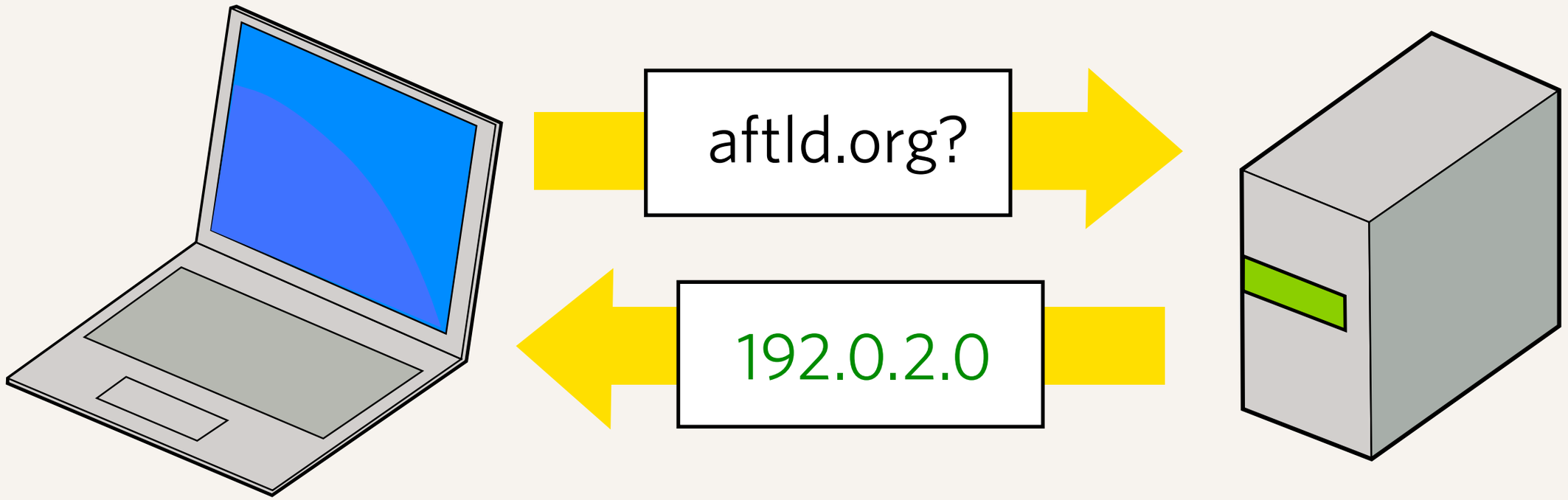
- How do you attack the DNS?
- How does DNSSEC help this?
- Work IANA is doing on DNSSEC
- IPv6 and TLDs

# How do you attack the DNS?



# A typical DNS query

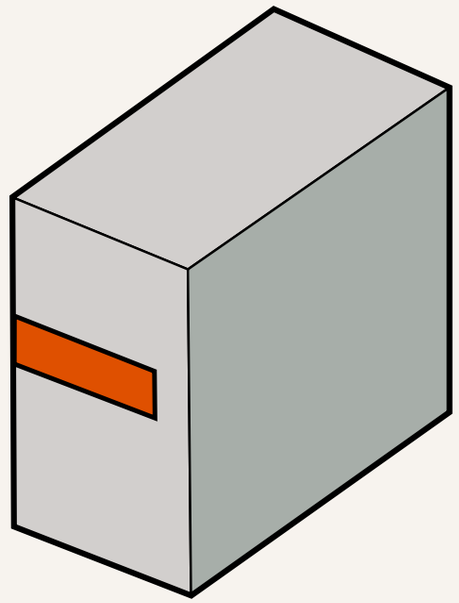

# A typical DNS query




# A typical DNS query

# The DNS is not secure

- A computer sends a “question” to a DNS server, asking a question like “What is the IP address for aftld.org?”
- The computer gets an answer, and completely trusts that it is correct.
- There are multiple ways that traffic on the Internet can be intercepted and rerouted, or impersonated, so that the answer given is false.

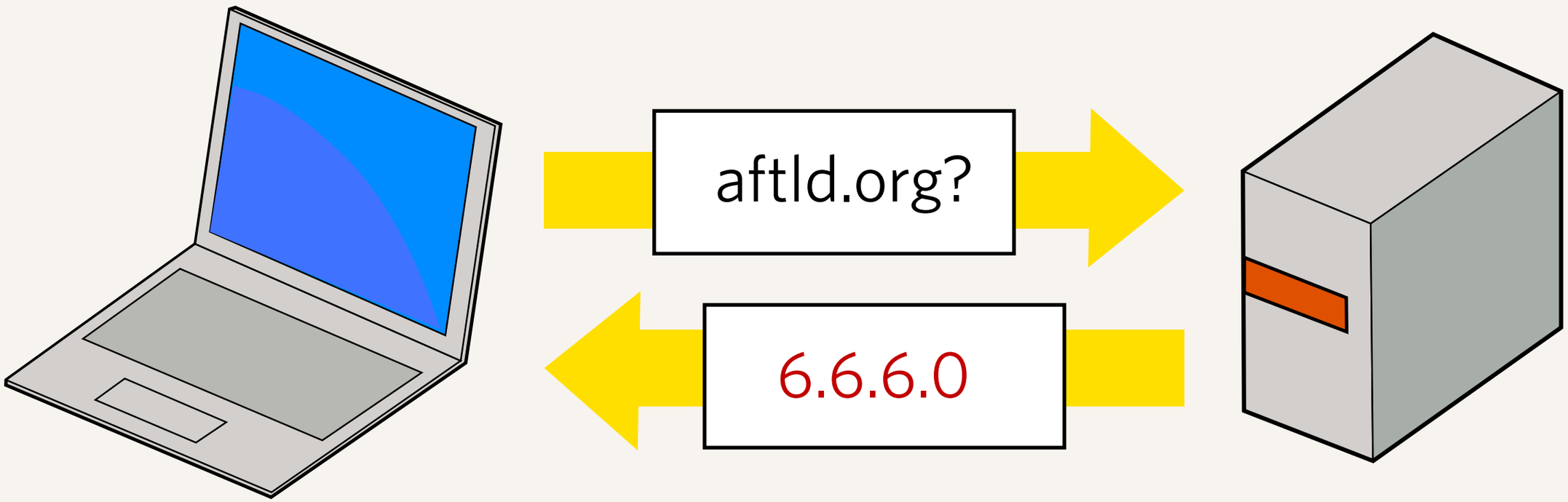


# Receiving the wrong answer

- Something in the network between the computer and the server has intercepted or redirected the traffic.

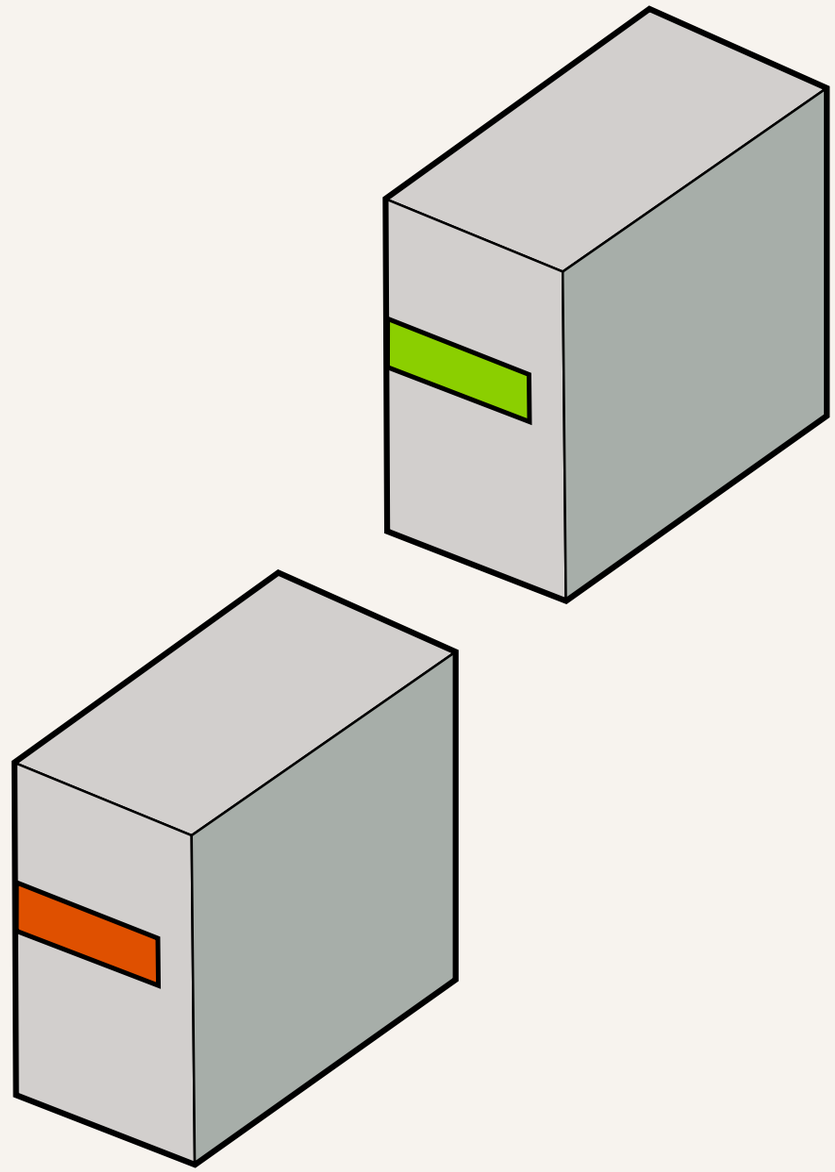

# Receiving the wrong answer

- Something in the network between the computer and the server has intercepted or redirected the traffic.



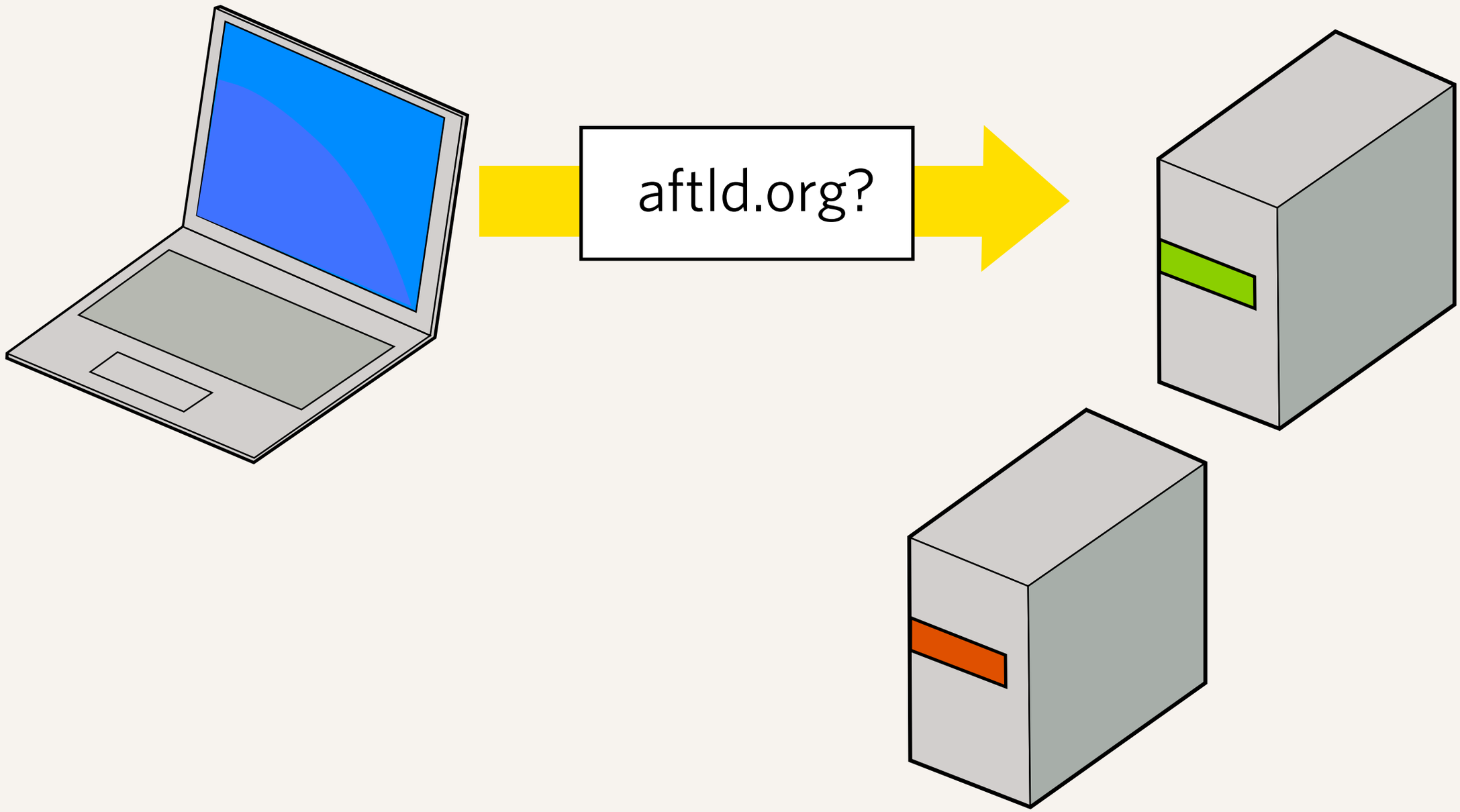

# Receiving the wrong answer

- Something in the network between the computer and the server has intercepted or redirected the traffic.



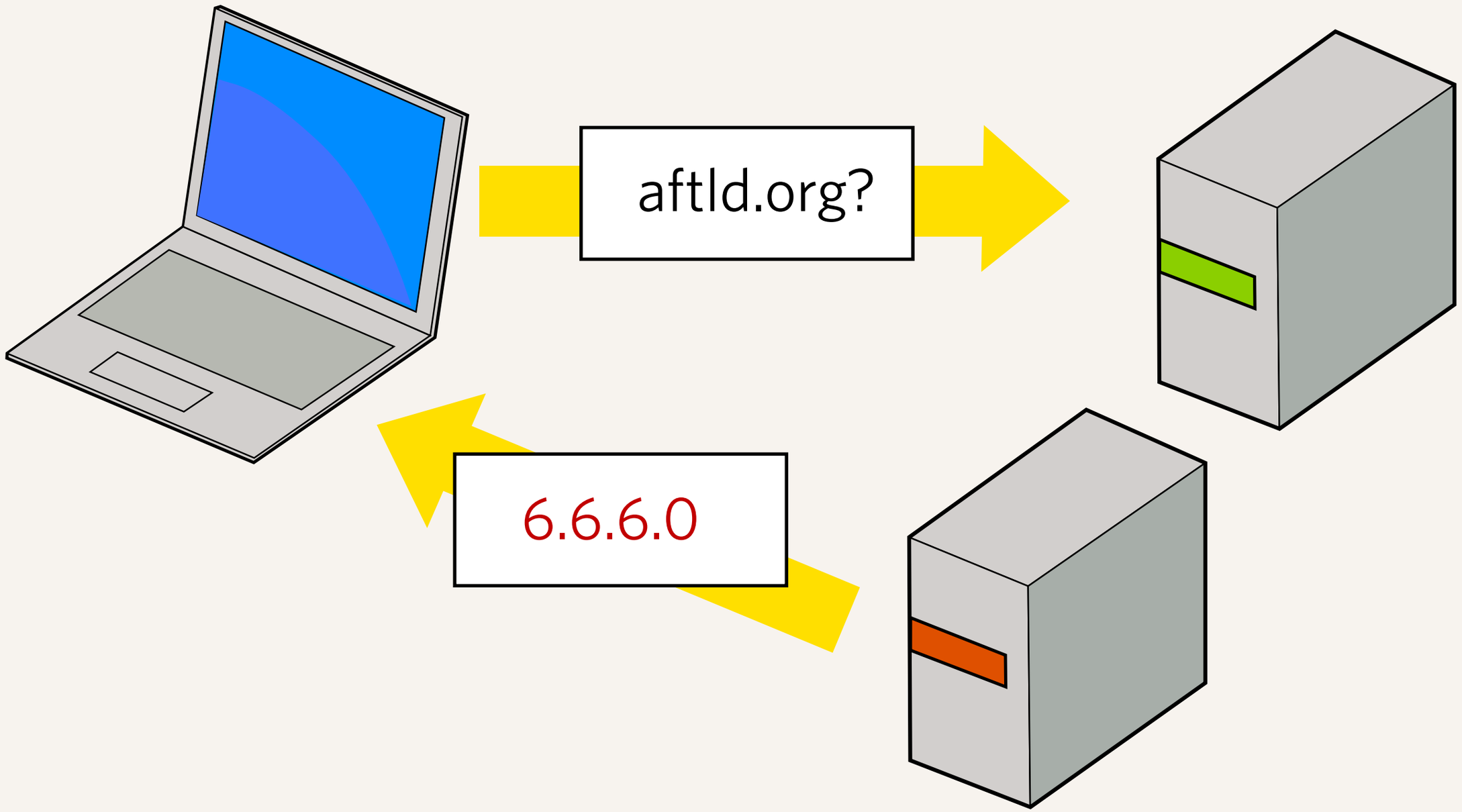
# Receiving the wrong answer

- A server on the network responds with the wrong answer, quicker than the correct server can give the right answer.



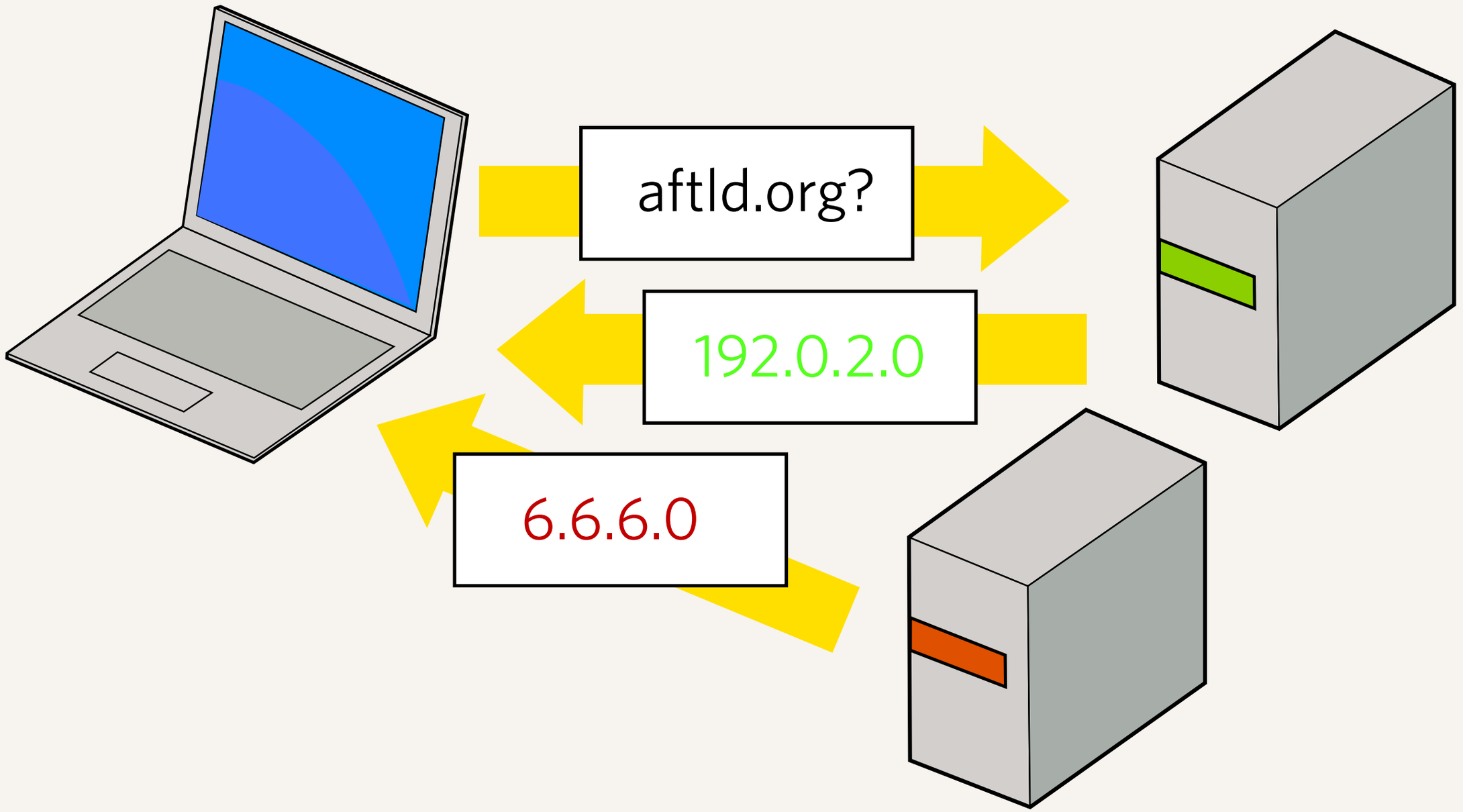

# Receiving the wrong answer

- A server on the network responds with the wrong answer, quicker than the correct server can give the right answer.




# Receiving the wrong answer

- A server on the network responds with the wrong answer, quicker than the correct server can give the right answer.




# Receiving the wrong answer

- A server on the network responds with the wrong answer, quicker than the correct server can give the right answer.

# Cache poisoning

- If the answers are stored in a cache, the wrong answer gets remembered and served to future lookups.
  - This is the typical configuration at ISPs, etc.
  - One successful cache poisoning attack with therefore affect many users.

# Cross pollination

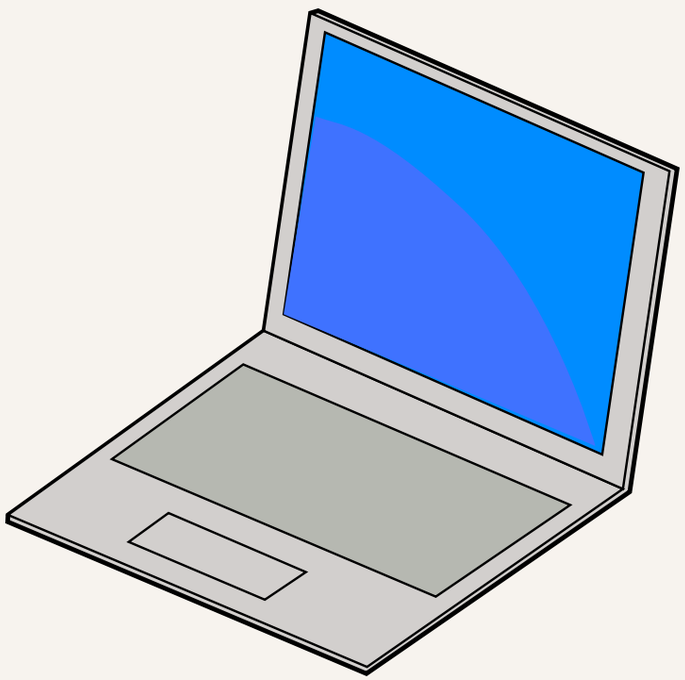
- If the cache is also authoritative for a domain, it can also give the wrong answers for answers within that domain.

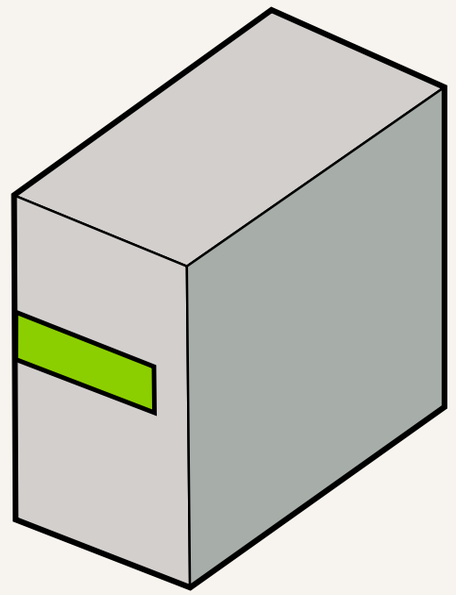
# What do I do?

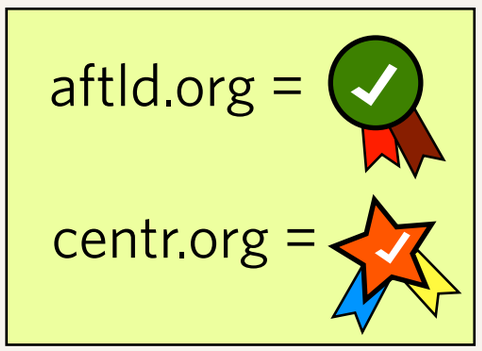
- Short term
  - Do not offer open recursive name servers
  - Definitely do not offer open recursive name servers that are also authorities at the same time
    - Patch recursive name servers for maximum entropy (source port randomisation, etc.)
    - http://recursive.iana.org/
- Longer term
  - Introduce security to the DNS…

# What DNSSEC provides

- DNSSEC provides proof that the data has not been modified in transit from the DNS zone publisher (the registry) to the end-user
- It does this by providing additional information, something like a “seal of origin”, that can be verified as being correct or not.

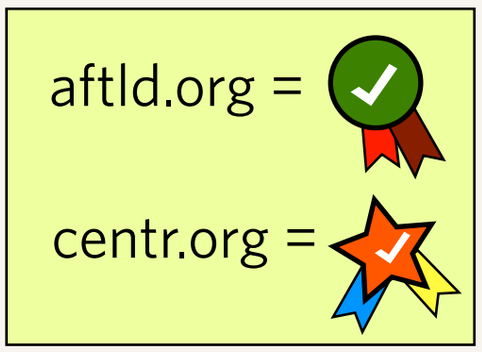






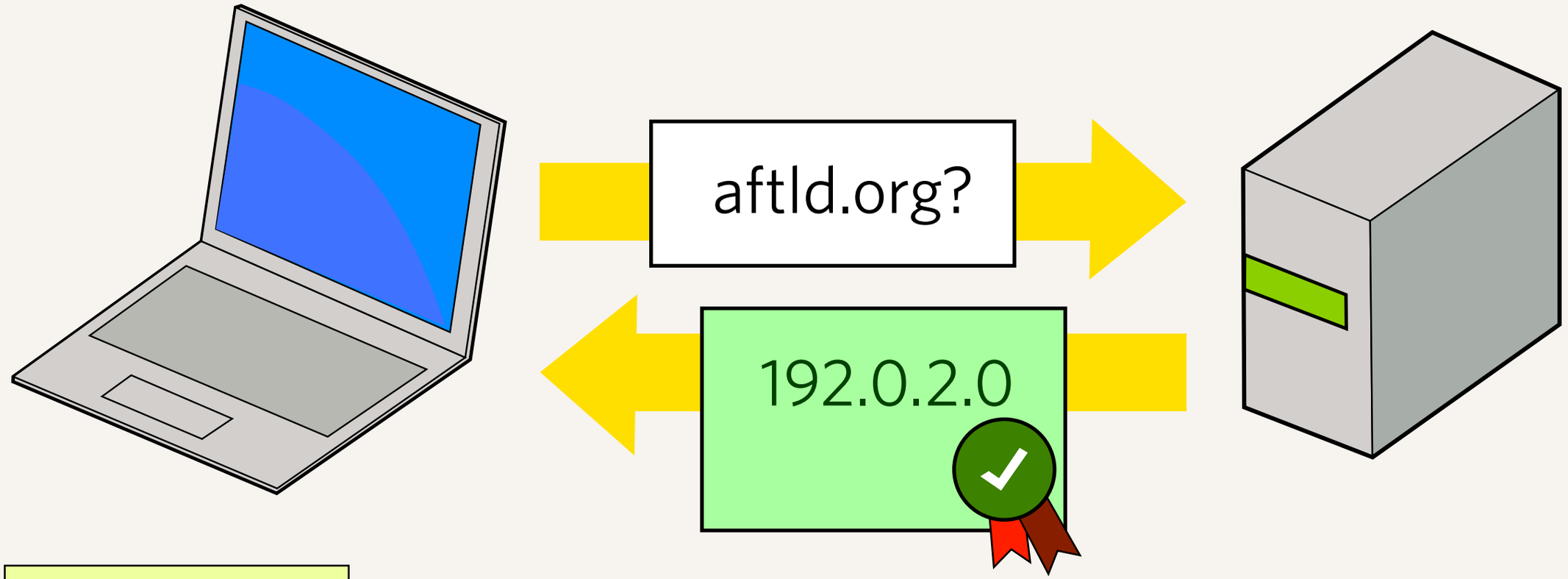

# A DNSSEC secured transaction

- Check against a known set of signatures, and if there is a match, is a valid answer.

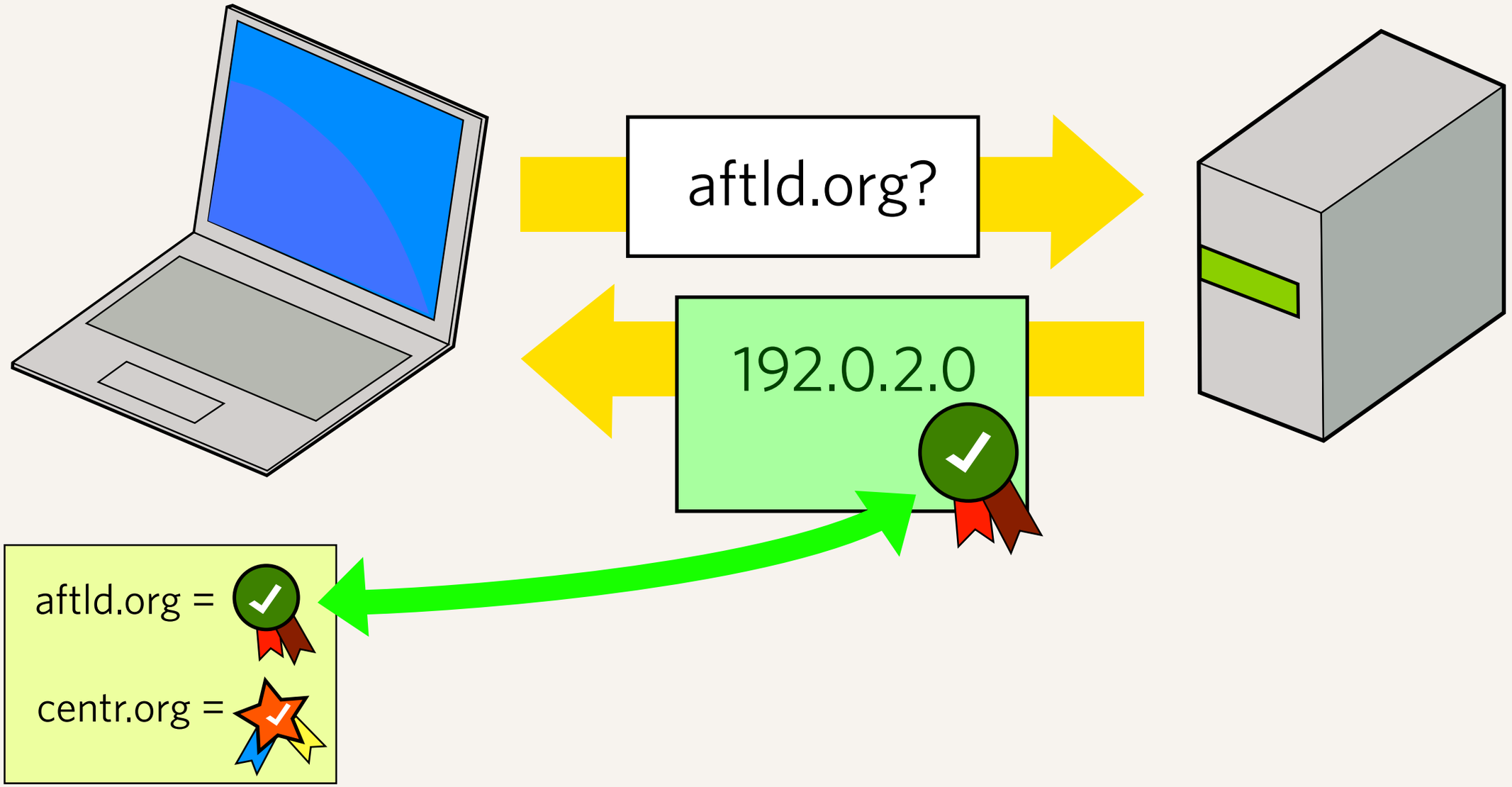

# A DNSSEC secured transaction

- Check against a known set of signatures, and if there is a match, is a valid answer.




# A DNSSEC secured transaction

- Check against a known set of signatures, and if there is a match, is a valid answer.




# A DNSSEC secured transaction

- Check against a known set of signatures, and if there is a match, is a valid answer.

# Maintaining a list of signatures for every domain does not scale

- How could every computer maintain a list of every certificate for every domain it needs to verify?
- There needs to be a better way...

aftld.org =

centr.org =

iana.org?

192.0.2.0

# Using a chain of trusted certificates

aftld.org =

centr.org =

**root**

.org =

iana.org?

192.0.2.0

# Using a chain of trusted certificates

aftld.org =

centr.org =

**root**

.org =

iana.org?

192.0.2.0

# Using a chain of trusted certificates

aftld.org =

centr.org =

**root**

.org =

iana.org?

192.0.2.0

**.org**

iana.org =

# Using a chain of trusted certificates

aftld.org =

centr.org =

**root**

.org =

iana.org?

192.0.2.0

**.org**

iana.org =

# Using a chain of trusted certificates

aftld.org =

centr.org =

root =

iana.org?

192.0.2.0

**root**

.org =

**.org**

iana.org =

# Using a chain of trusted certificates

aftld.org =

centr.org =

root =

**root**

.org =

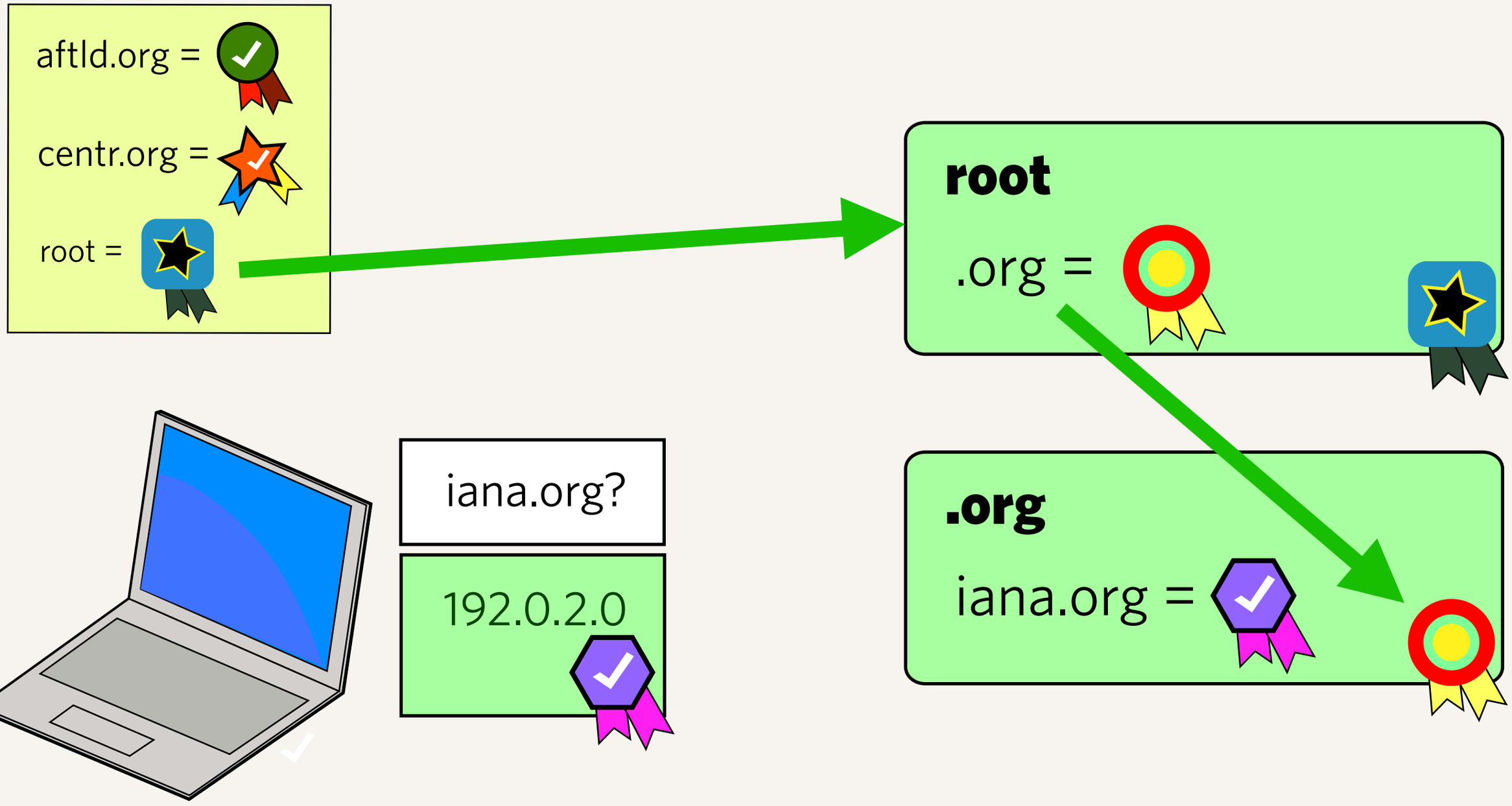
iana.org?

192.0.2.0

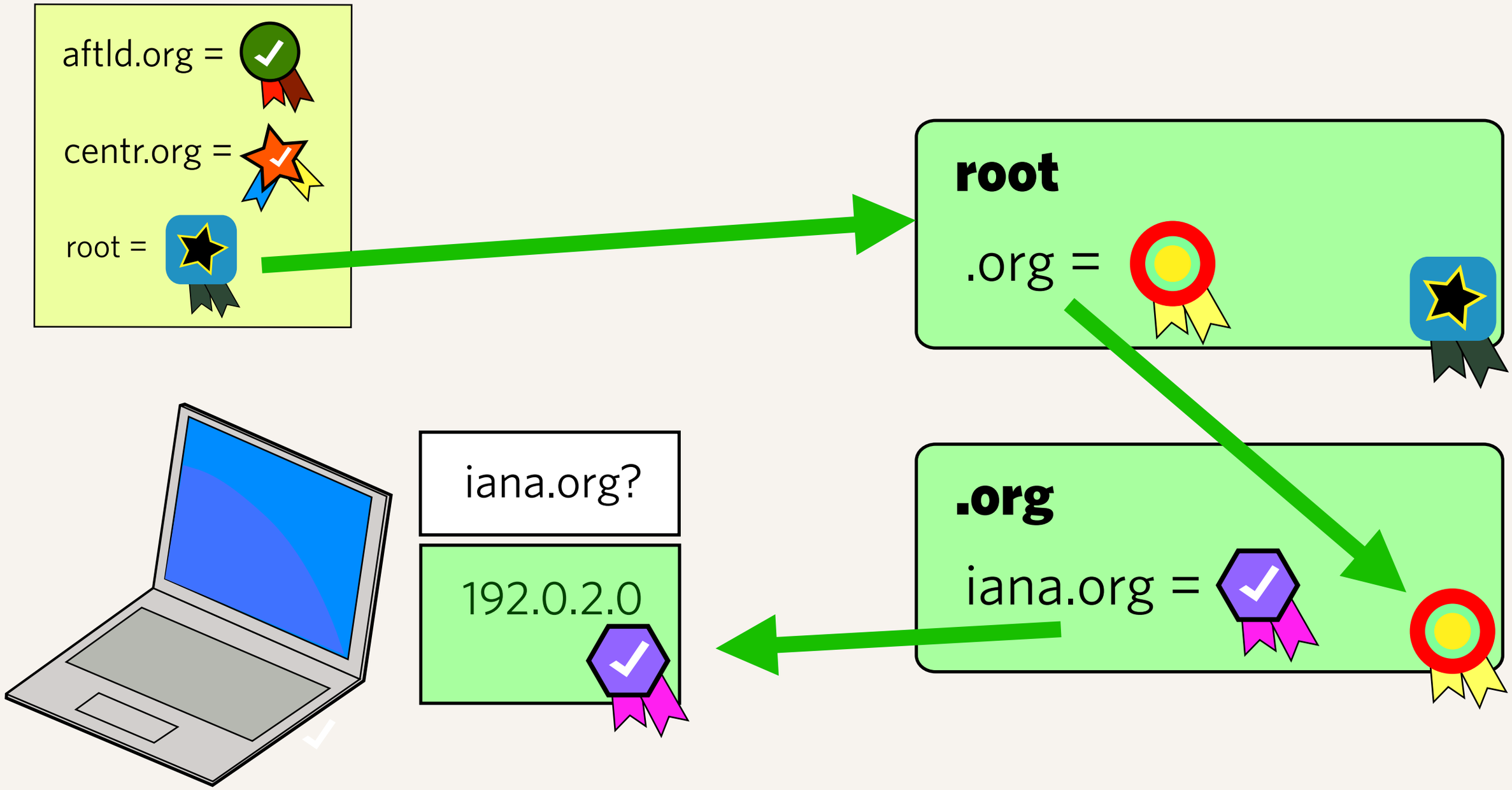
**.org**

iana.org =

# Using a chain of trusted certificates




# Using a chain of trusted certificates




# Using a chain of trusted certificates

# The chain of trust

- By using the hierarchical property of the DNS, you can use DNSSEC to check certificates without knowing the certificate of every single domain
  - Computers can learn certificates by tracing from a trusted key down the DNS delegation chain
- Of course, this only works if each level of the DNS deploys DNSSEC…
  - For this to work, registries need to keep a list of signatures of its child zones, and publish them in their own signed zone

# In summary:

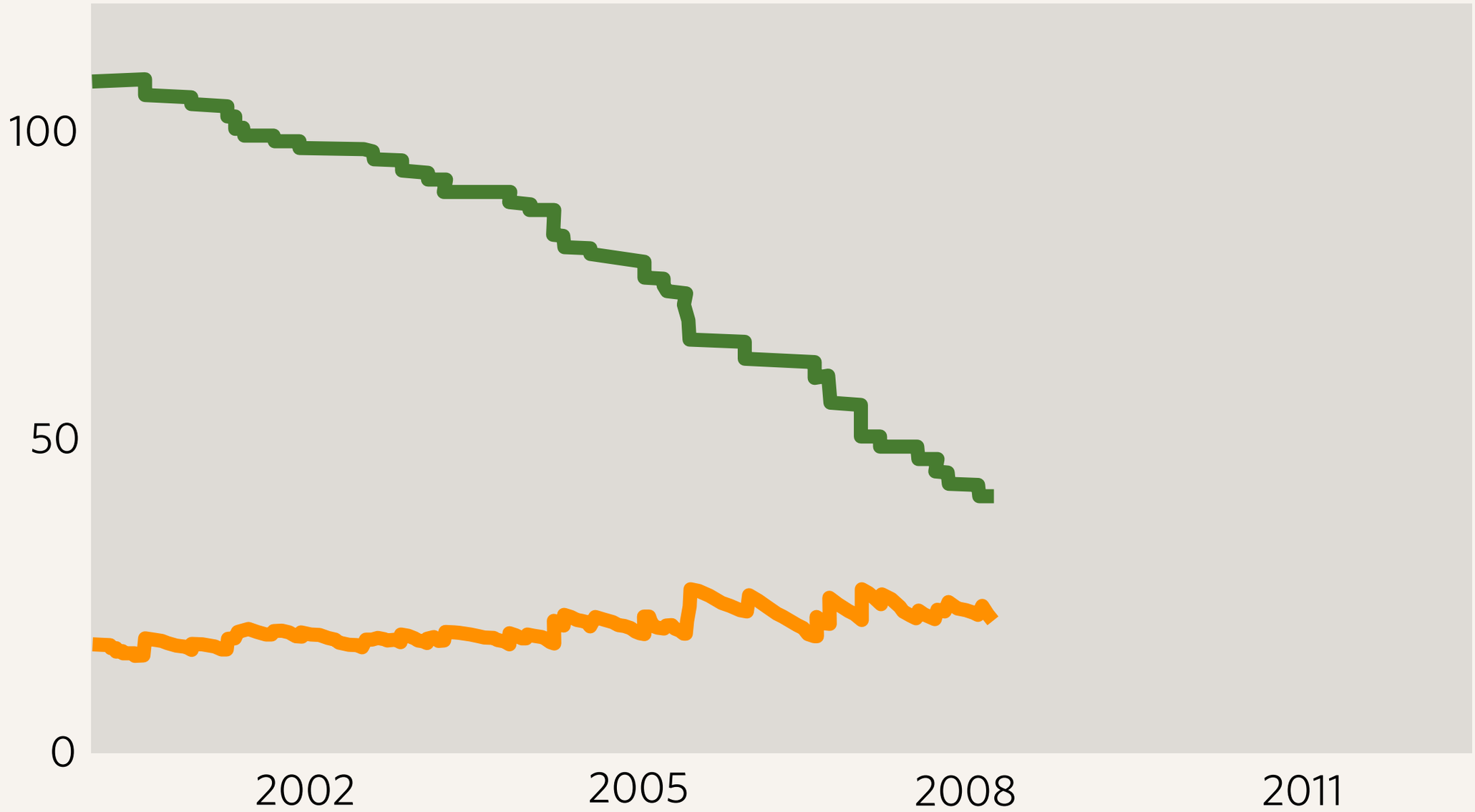
- To deploy DNSSEC fully, zone managers need to:
  - Sign their zone with a certificate
  - Publish the certificates of their child zones
  - Share their certificate with their parent zone
- The administration of these is much of the reason why DNSSEC has been difficult to deploy
  - And why “signing the root” is considered so important — it theoretically allows a single signature to verify the whole DNS!

# Signing the root

# IANA has been asked to sign the root zone

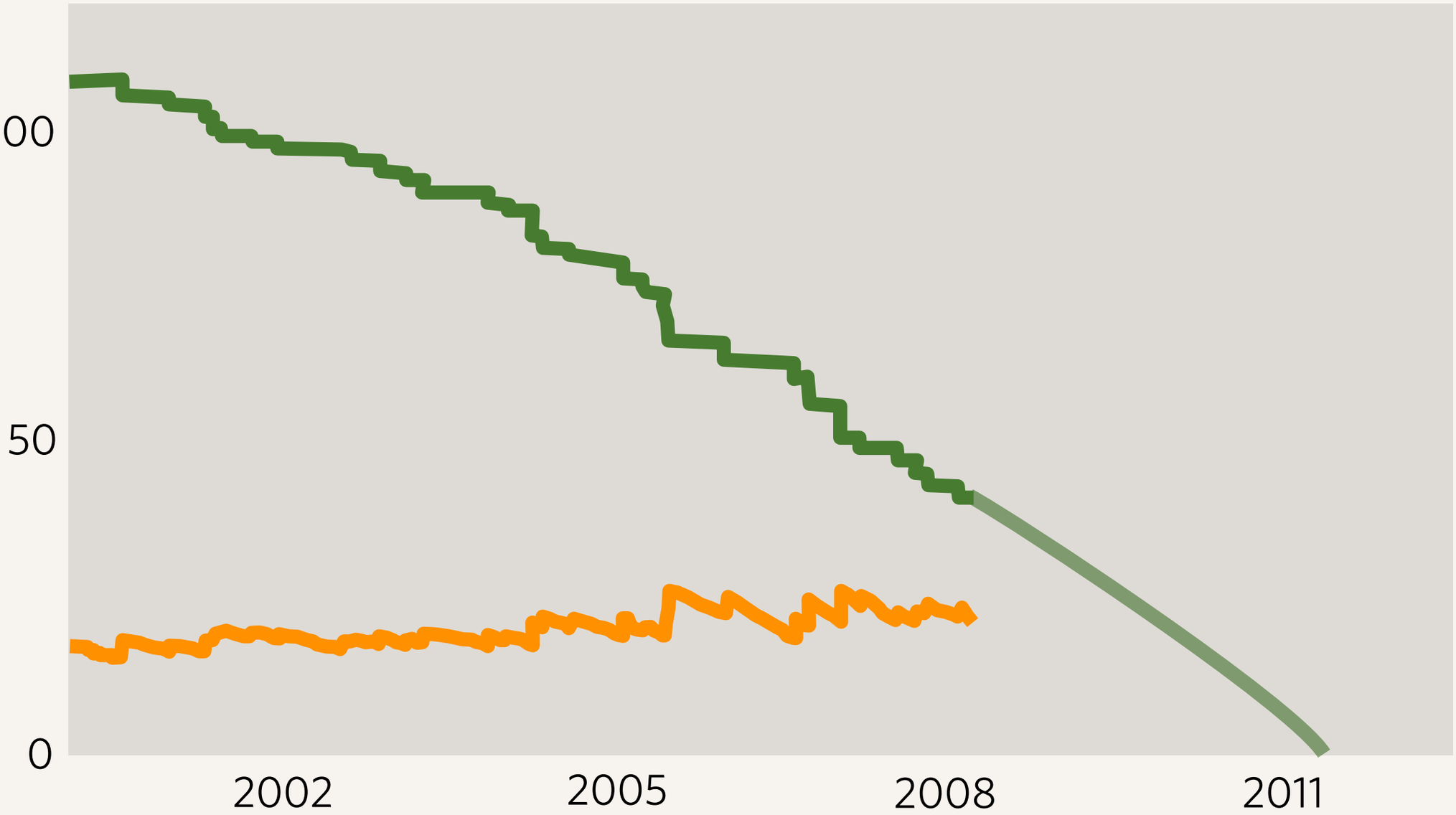
- Several entities have formally asked ICANN to sign the root zone (RIPE, .SE, APNIC)
- IANA has been signing the root experimentally for over a year
- However, as IANA does not directly publish the root, it can not currently make this a production service
- Working on obtaining permission from USDOC to let us sign the root zone

# IPv6



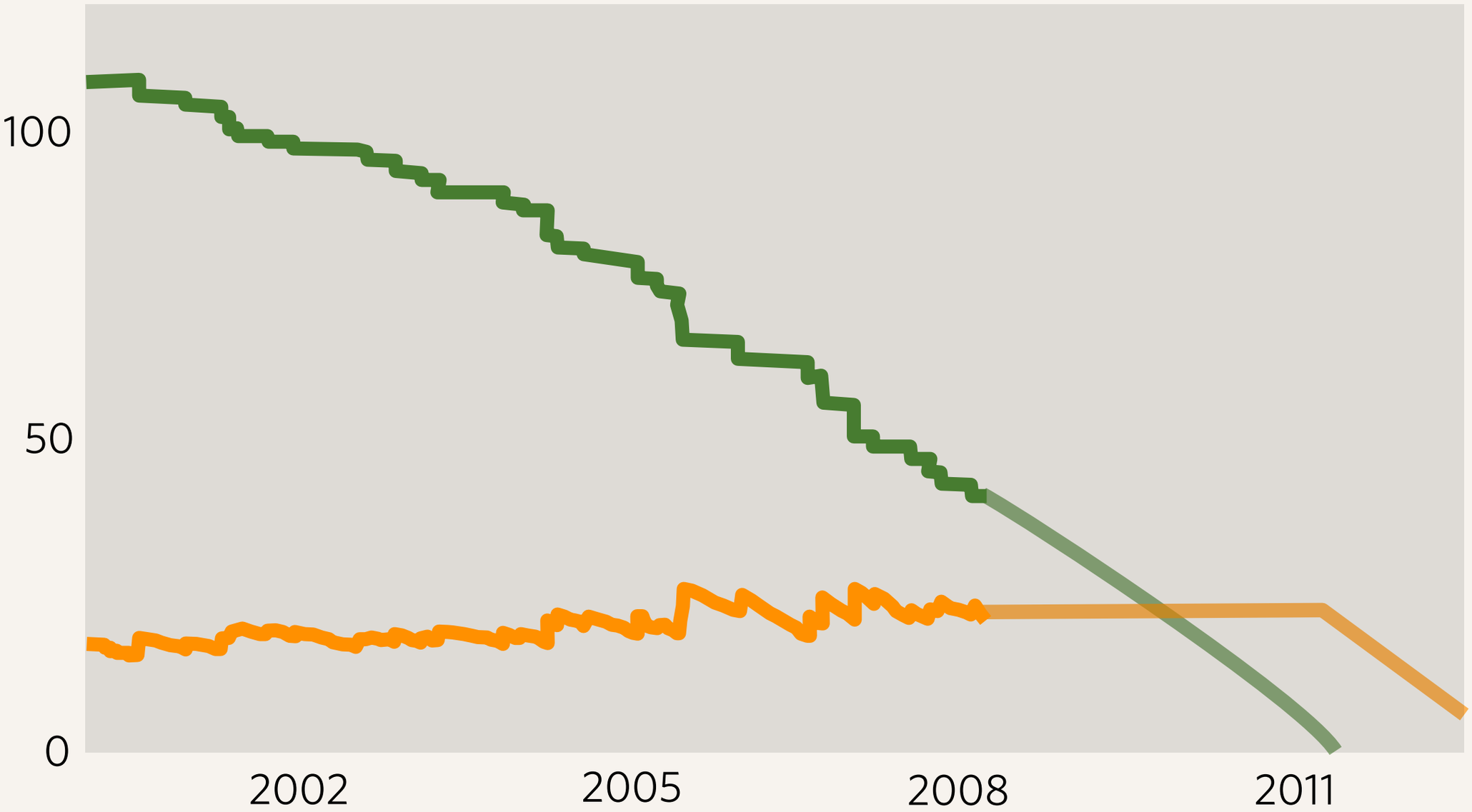

# IPv4 Availability

- Dwindling stocks ...




# IPv4 Availability

- Dwindling stocks ...

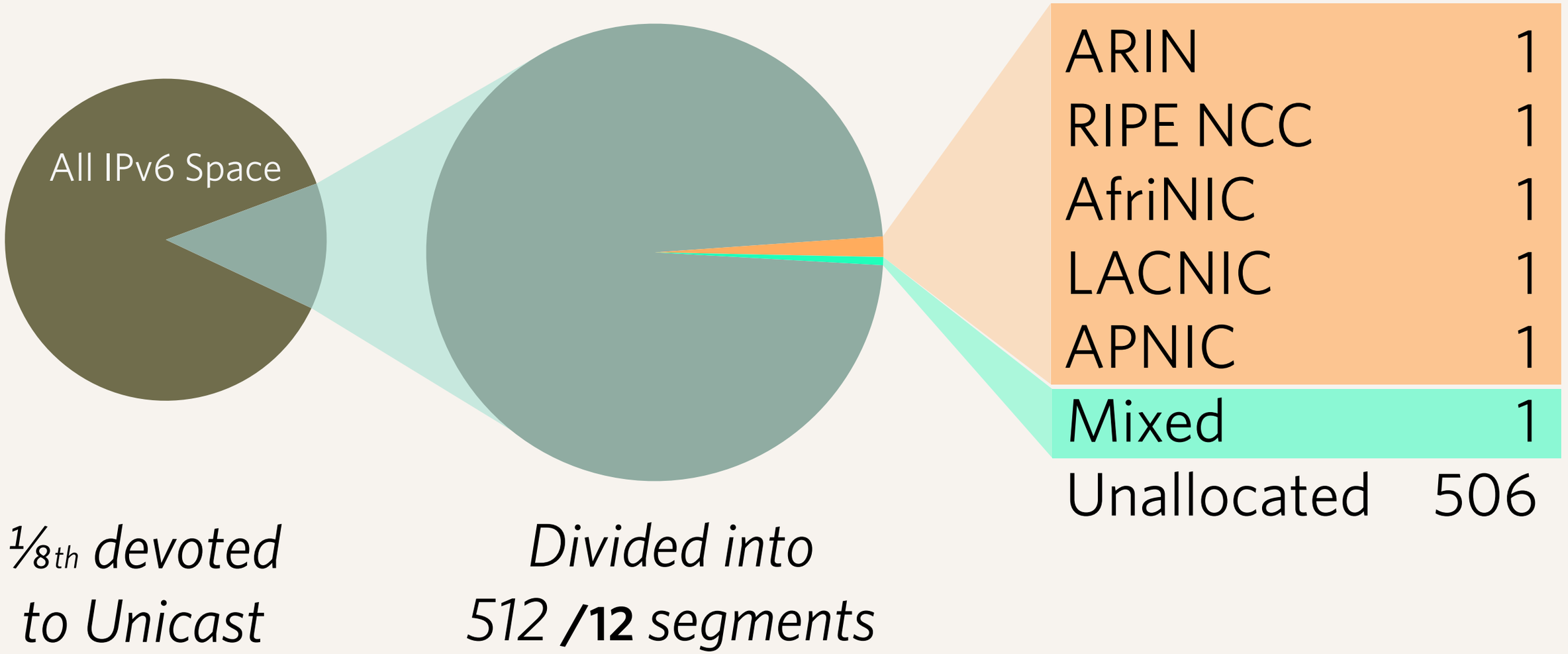



# IPv4 Availability

- Dwindling stocks ...

# IPv6 in a nutshell

- 128-bit address space
  - 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses
- IANA still has lots in reserve




*1/8th devoted to Unicast*

*Divided into 512 **/12** segments*

# IPv6 Availability

- Approximately 1% of Unicast designated space is allocated to RIRs.

# IPv6: the short story

- IPv4 address space is running out
  - Current estimates, next couple of years
- IPv6 is the new numbering technology that will provide for growth of IP addressing needs
- The two numbering technologies are not mutually compatible, you must support IPv6 in addition to IPv4 to be accessible to IPv6 clients.

# IPv6 adoption by TLD operators

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities
- 22 TLDs have 3 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities
- 22 TLDs have 3 IPv6 authorities
- 34 TLDs have 2 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities
- 22 TLDs have 3 IPv6 authorities
- 34 TLDs have 2 IPv6 authorities
- 49 TLDs have only 1 IPv6 authorities

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities
- 22 TLDs have 3 IPv6 authorities
- 34 TLDs have 2 IPv6 authorities
- 49 TLDs have only 1 IPv6 authorities
  - Would not meet IANA minimum diversity requirements for production deployment for IPv4

# IPv6 adoption by TLD operators

- 5 TLDs have 6 IPv6 authorities
- 11 TLDs have 5 IPv6 authorities
- 5 TLDs have 4 IPv6 authorities
- 22 TLDs have 3 IPv6 authorities
- 34 TLDs have 2 IPv6 authorities
- 49 TLDs have only 1 IPv6 authorities
  - Would not meet IANA minimum diversity requirements for production deployment for IPv4
- 155 TLDs have no IPv6 authorities at all!

# Don't be a hindrance to IPv6 adoption

- Allow AAAA glue records in your zone
- Provide your zone over IPv6 transit
- Encourage registrars to allow AAAA glue records from registrants
  - It is no use if your registry supports it, if your registrars do not.
  - Registry support is bad, registrar support is worse!

# Thanks!

kim.davies@icann.org