

DNSSEC: Security in an insecure medium

7 December 2011

Patrick Jones

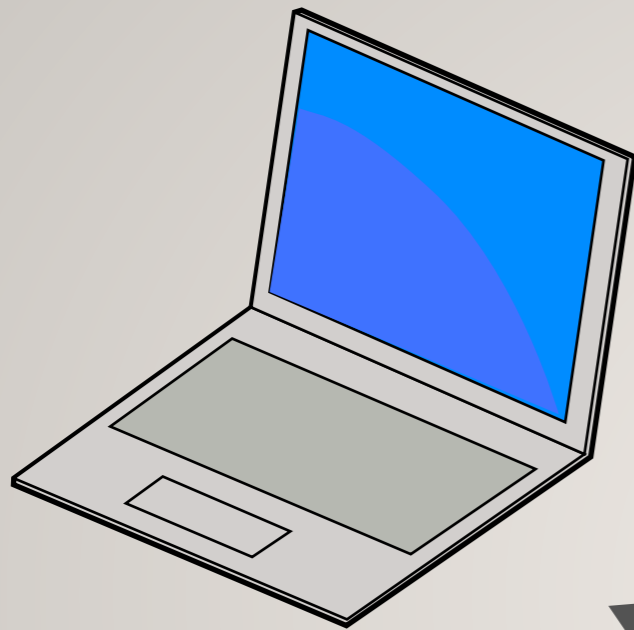
Senior Manager, Security

Presentation at CTU Ministerial Seminar



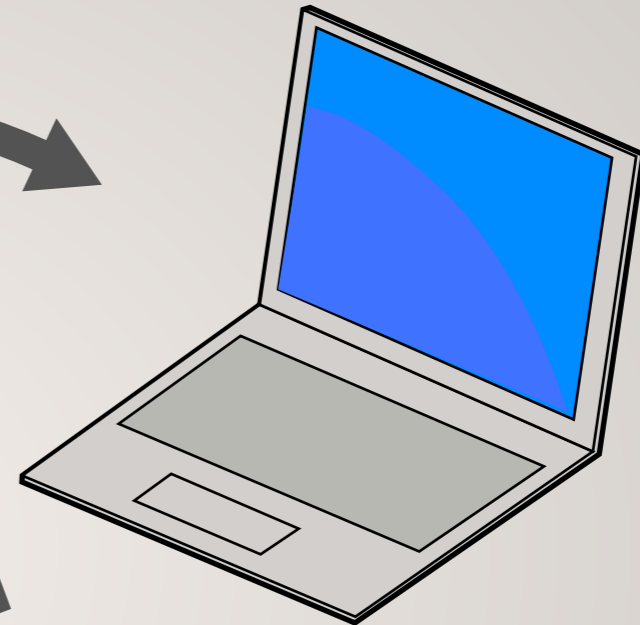
Internet Corporation for
Assigned Names &
Numbers

Background



96.126.96.181

to: 192.0.32.8
from: 205.214.212.63



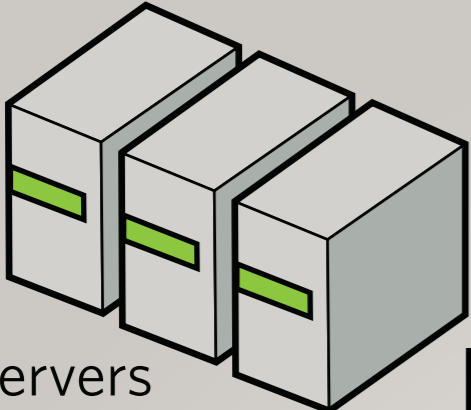
192.0.32.8

to: 205.214.212.63
from: 192.0.32.8

the "Internet"

How do you remember all these numbers?

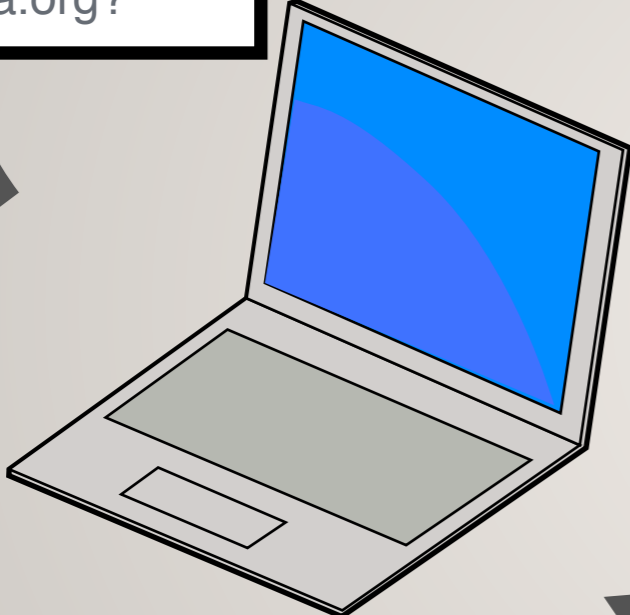
Using the DNS



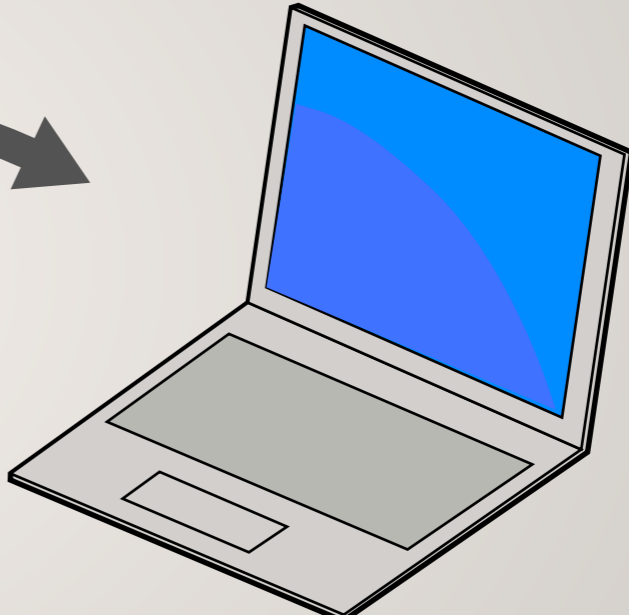
DNS servers

www.iana.org is at
192.0.32.8

where is
www.iana.org?



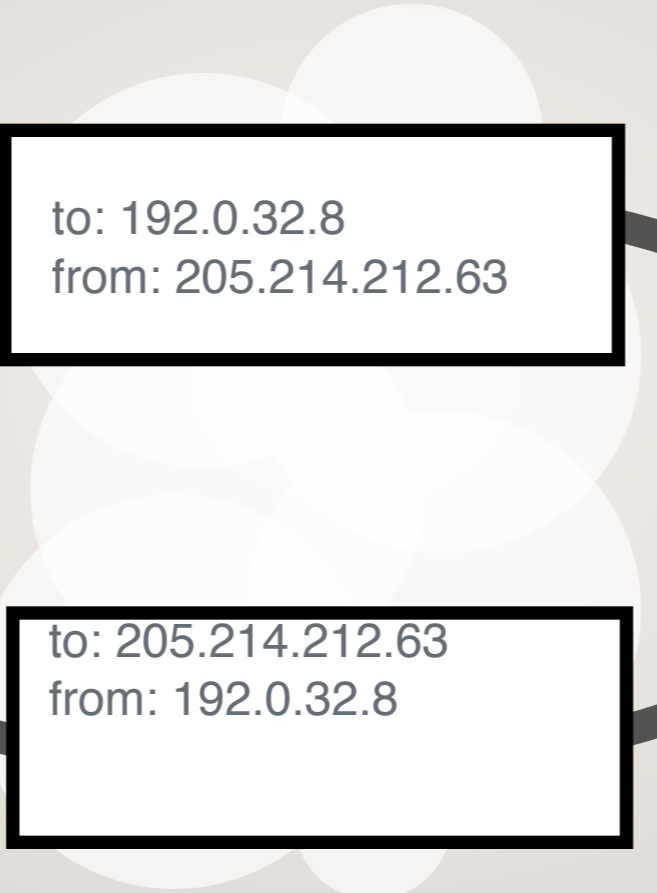
to: 192.0.32.8
from: 205.214.212.63



to: 205.214.212.63
from: 192.0.32.8

205.214.212.63
"caribsurf.com"

192.0.32.8
"www.iana.org"



Internet addressing

- ▶ IP Addresses

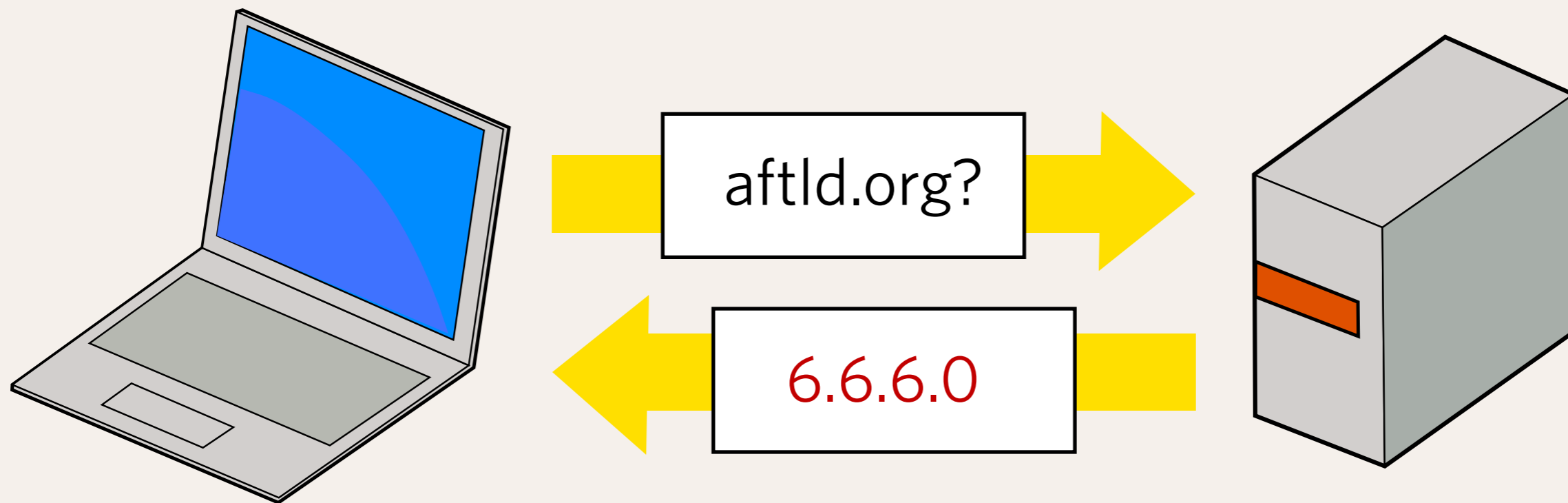
- ▶ Each computer on the Internet has a unique address like “192.0.32.8”. This is how Internet traffic is correctly routed to the right destination

- ▶ Domain Names

- ▶ These numbers are hard to remember, in the early 1980s, the “DNS” was invented, giving each to remember names like “iana.org”. These are converted to IP addresses automatically by your computer by talking to DNS servers.

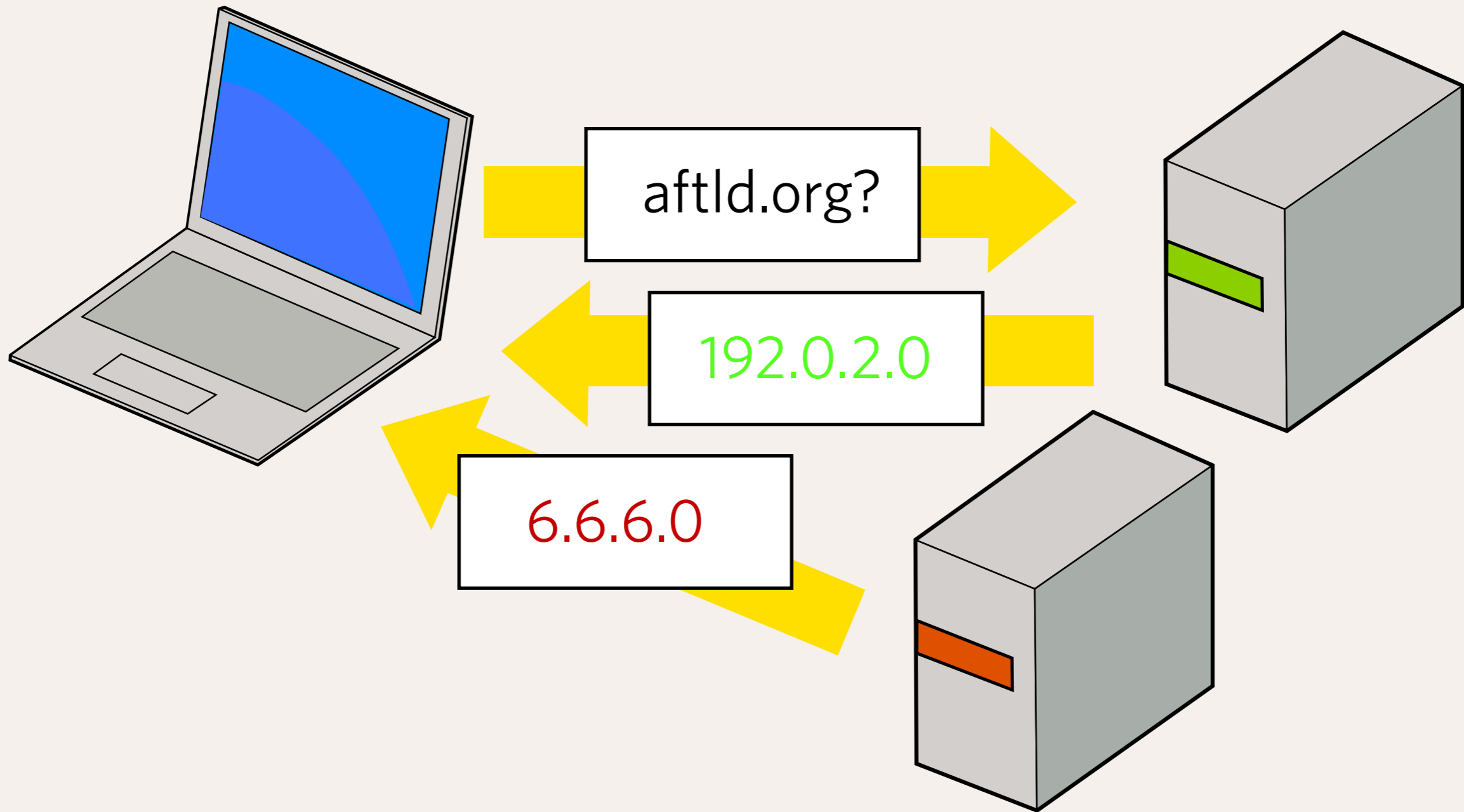
The DNS is not secure

- ▶ A computer sends a “question” to a DNS server, asking a question like “What is the IP address for iana.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, 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.

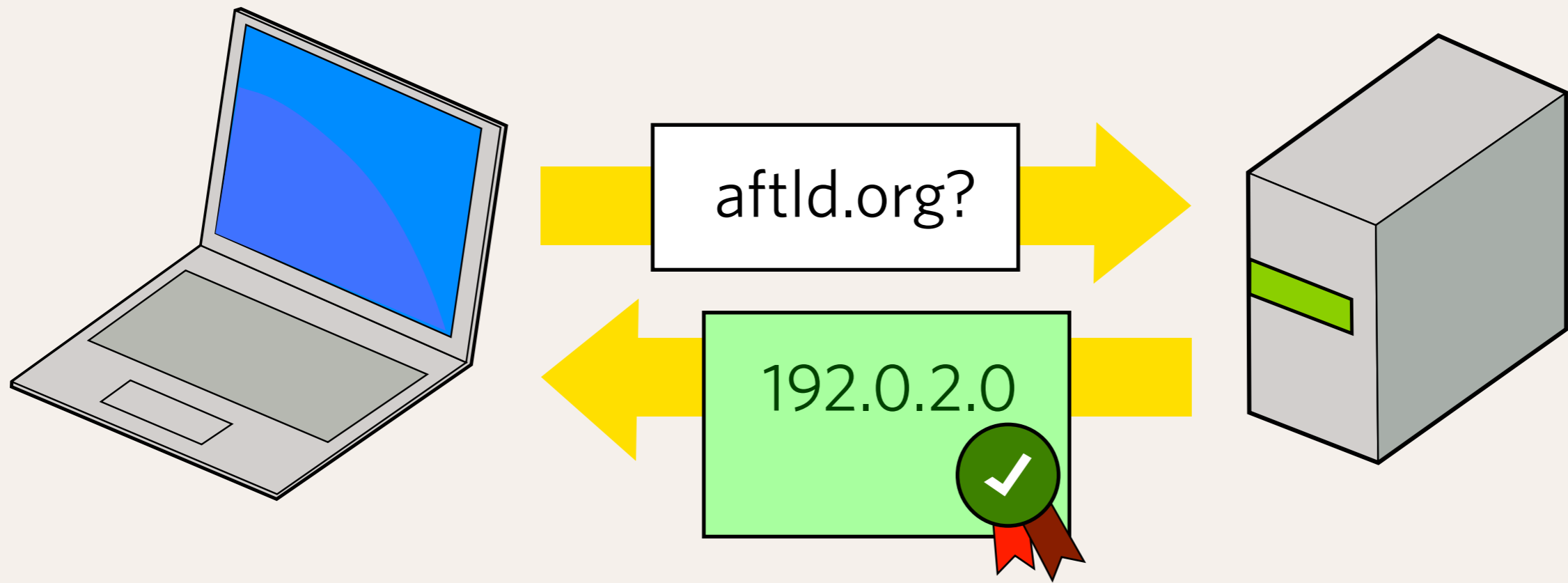


Receiving the wrong answer

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

What DNSSEC provides

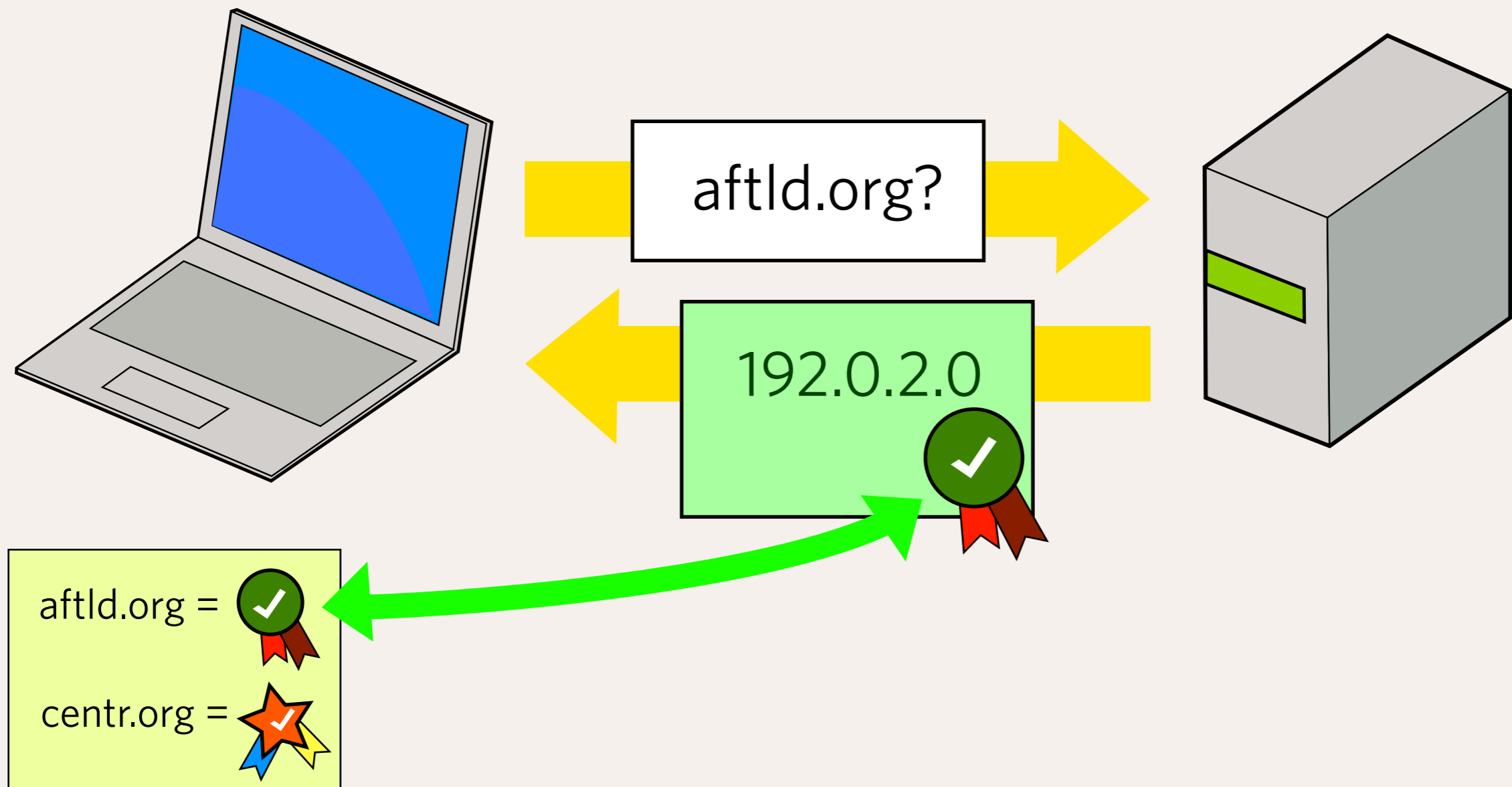
- ▶ DNSSEC provides proof that the data has not been modified in transit from the DNS zone publisher (the registry) to the end-user
- ▶ It does this by providing additional information, something like a “seal of origin”, that can be verified as being correct or not.



A DNSSEC secured transaction

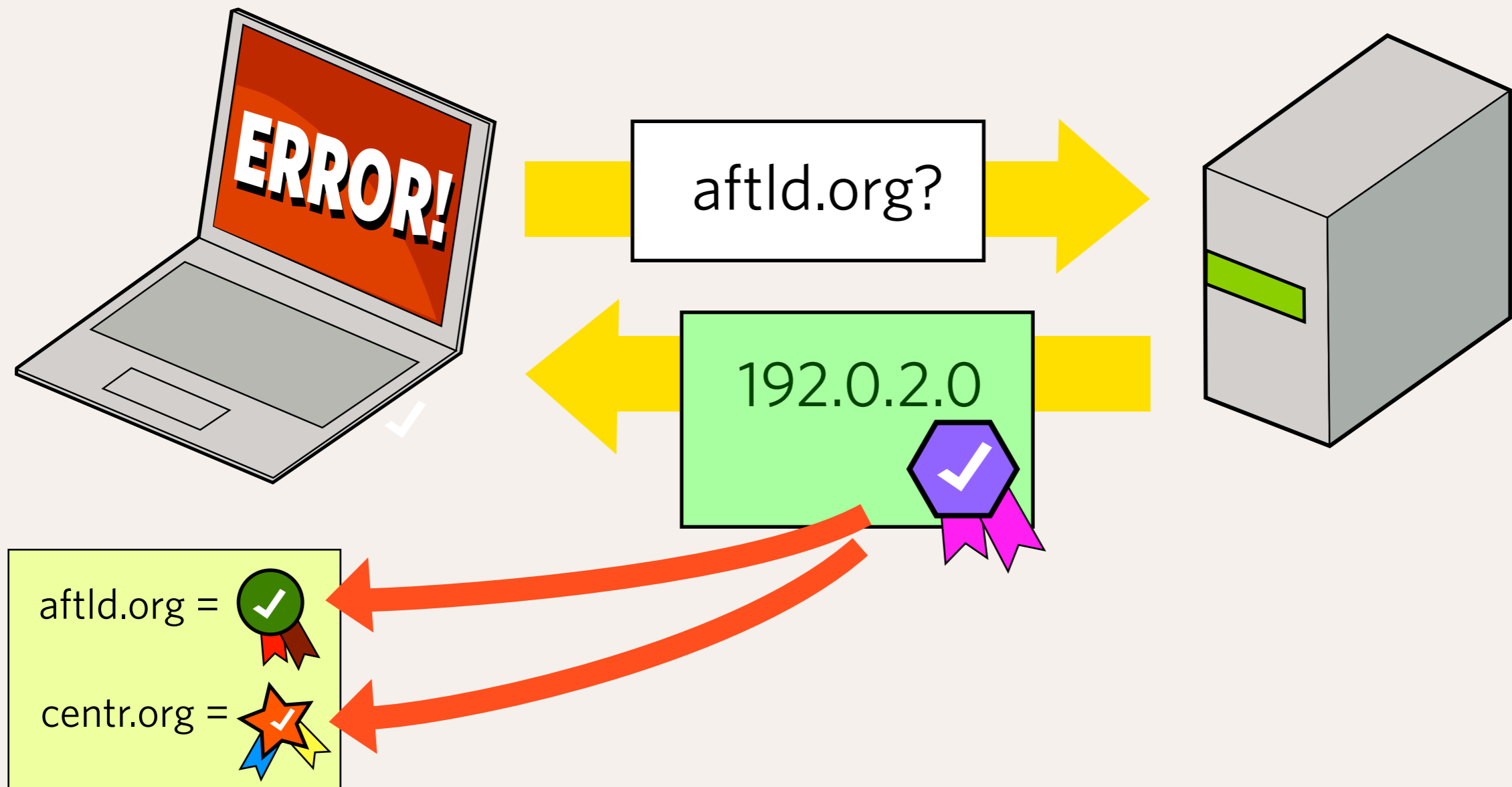
Verifying the DNS is correct

- ▶ The DNS response is only considered correct if the attached signature can be verified against a known set of good signatures.
- ▶ But, how does each computer know what are good signatures?
 - ▶ Each domain has a unique signature



Verifying against a list of signatures

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

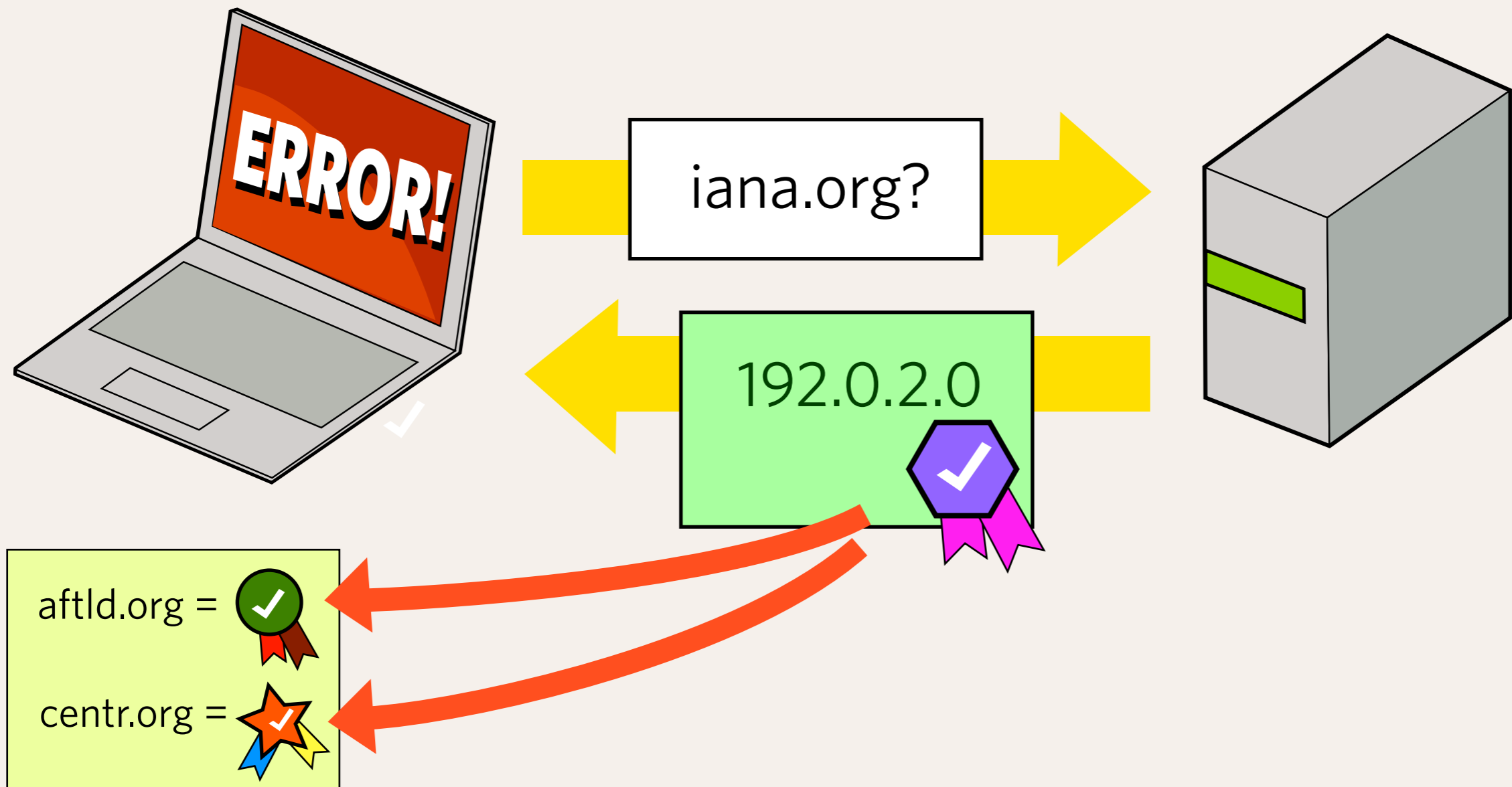


Verifying against a list of signatures

- ▶ Check against a list of known good signatures, if it fails, do not allow

That works great, but...

- What if the domain is not `aftld.org` or `centr.org`?

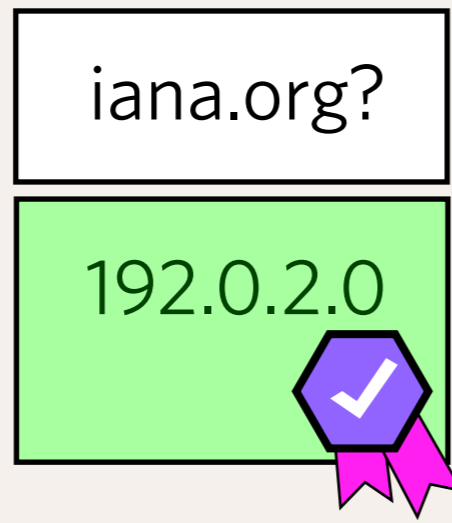
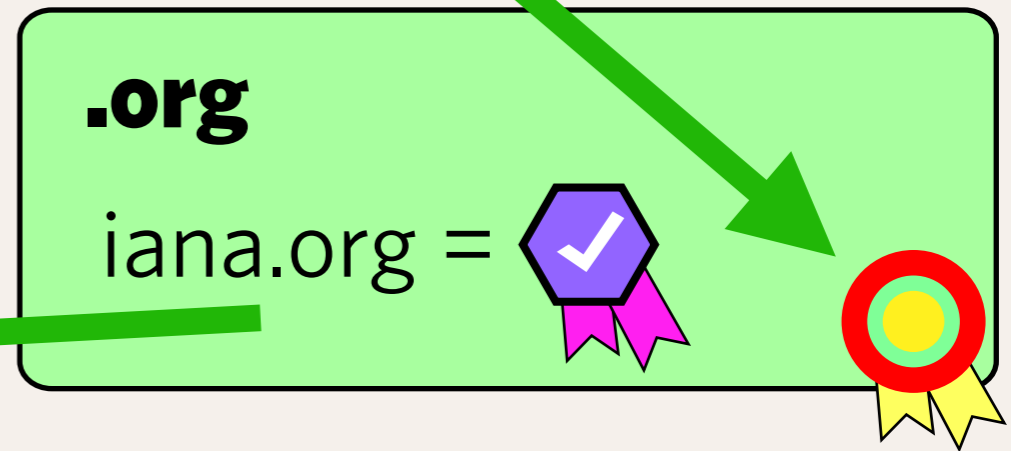
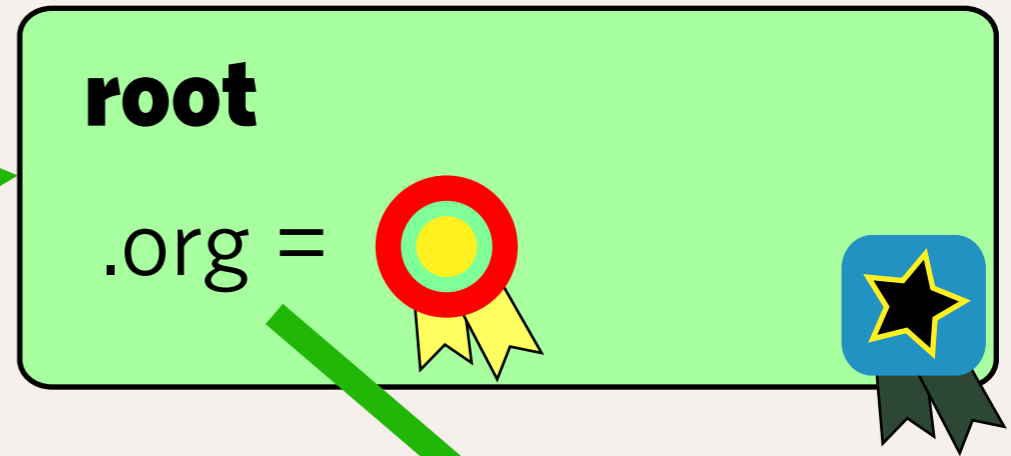
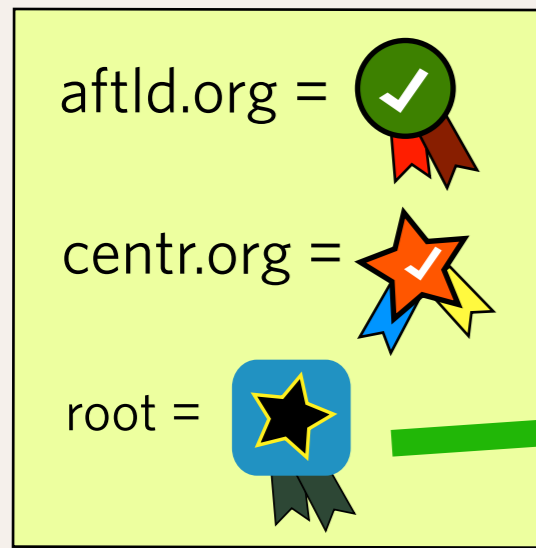


Verifying against a list of signatures

- What if it is not a domain you know about?

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...



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” was considered so important — it allows a single signature to verify the whole DNS!

Thanks!

Original Presentation by Kim Davies, Manager of Root Zone Services at ICANN
kim.Davies@icann.org

patrick.Jones@icann.org