DNSSEC and Routing Security

London, February 2009

Leo Vegoda
Internet Assigned Numbers Authority

Internet Corporation for
Assigned Names & Numbers

Agenda

- A primer on DNSSEC
- Work IANA is doing on DNSSEC
- Status of DNSSEC signing
- A primer on BGP (routing between ISPs)
- Status of routing security work

This presentation focuses on key concepts

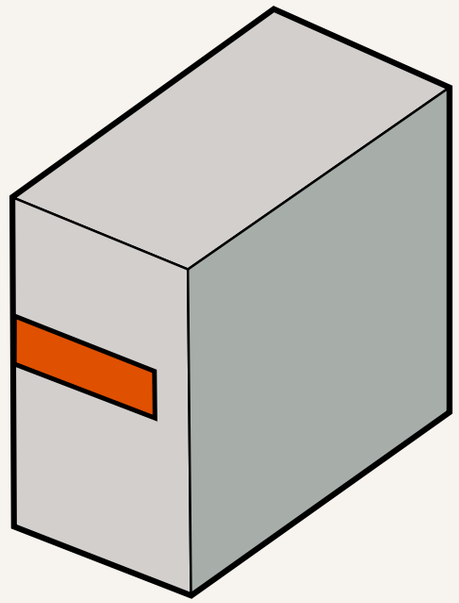
- Some of the technical concepts and language have been simplified
  - The aim is to explain the basic concepts without being confused by implementation details

What is DNSSEC?

How does it work?

The DNS is not secure

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

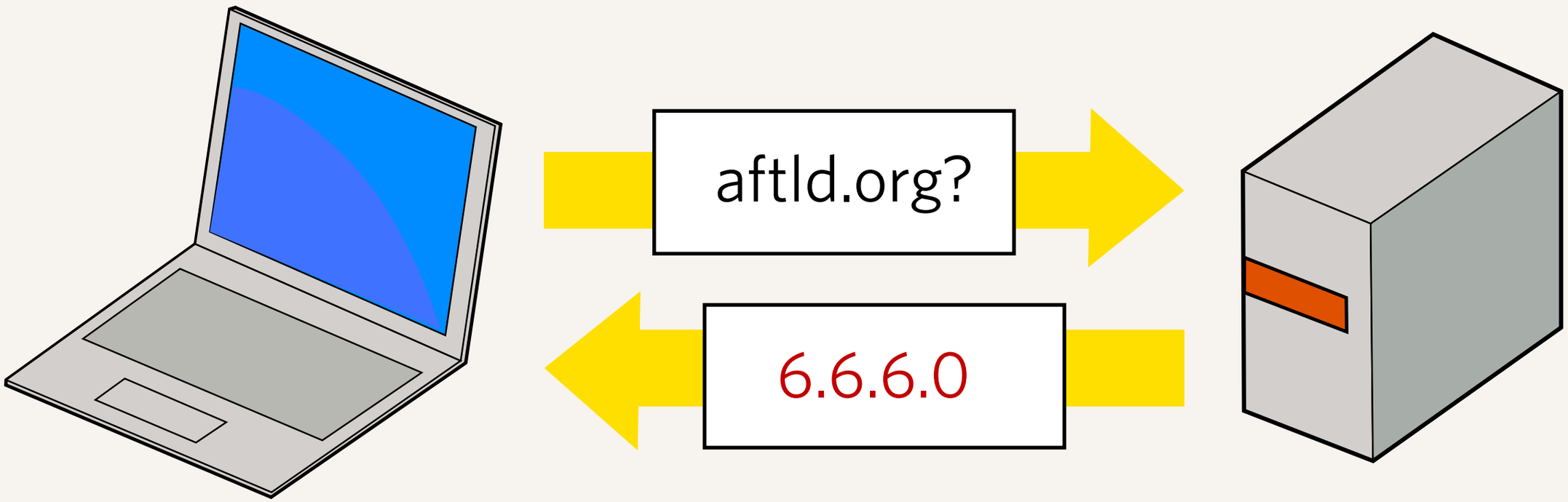


Receiving the wrong answer

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

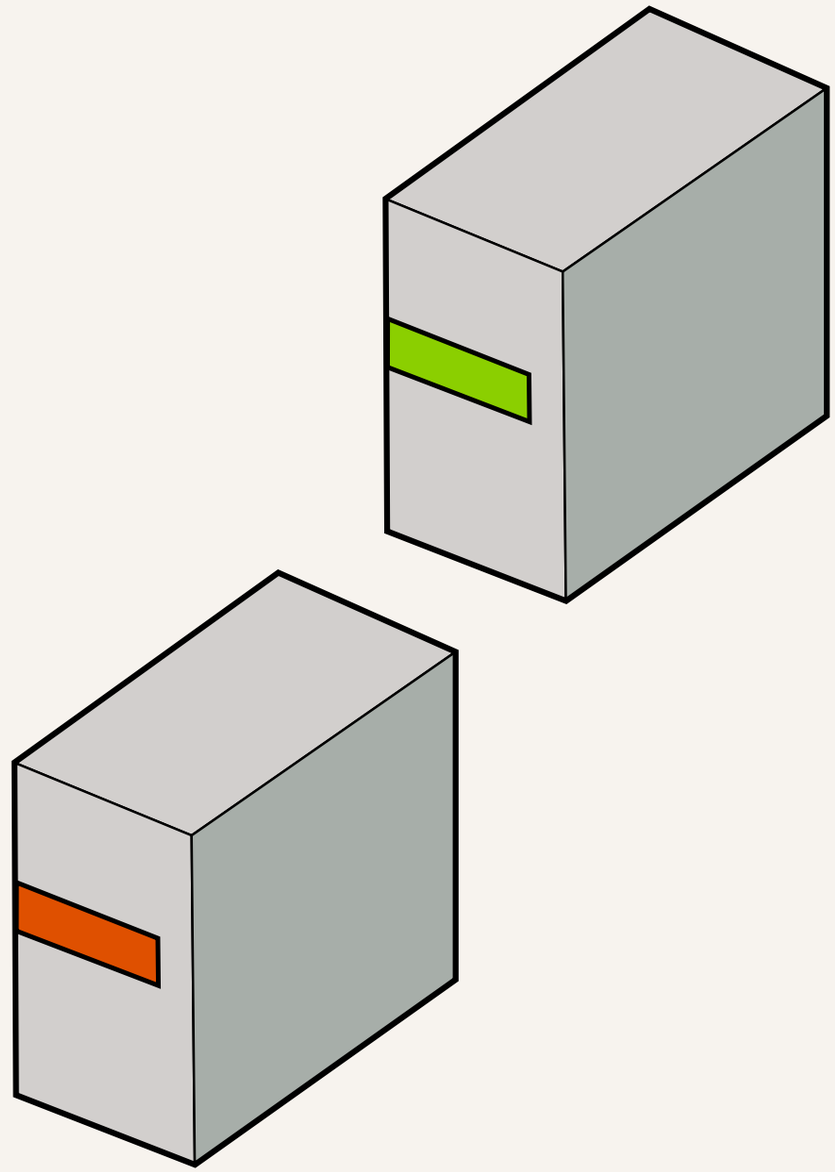
Receiving the wrong answer

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



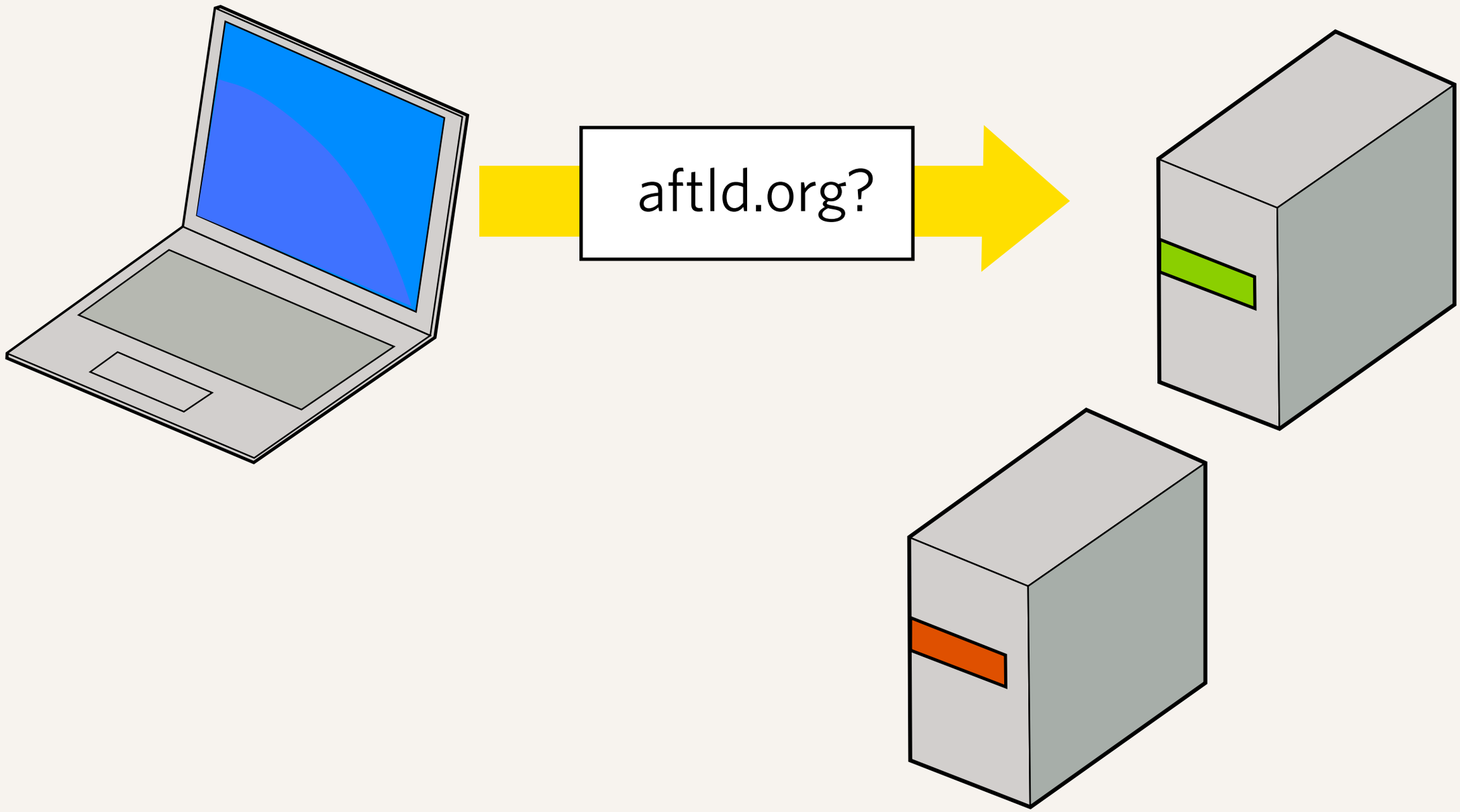
Receiving the wrong answer

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



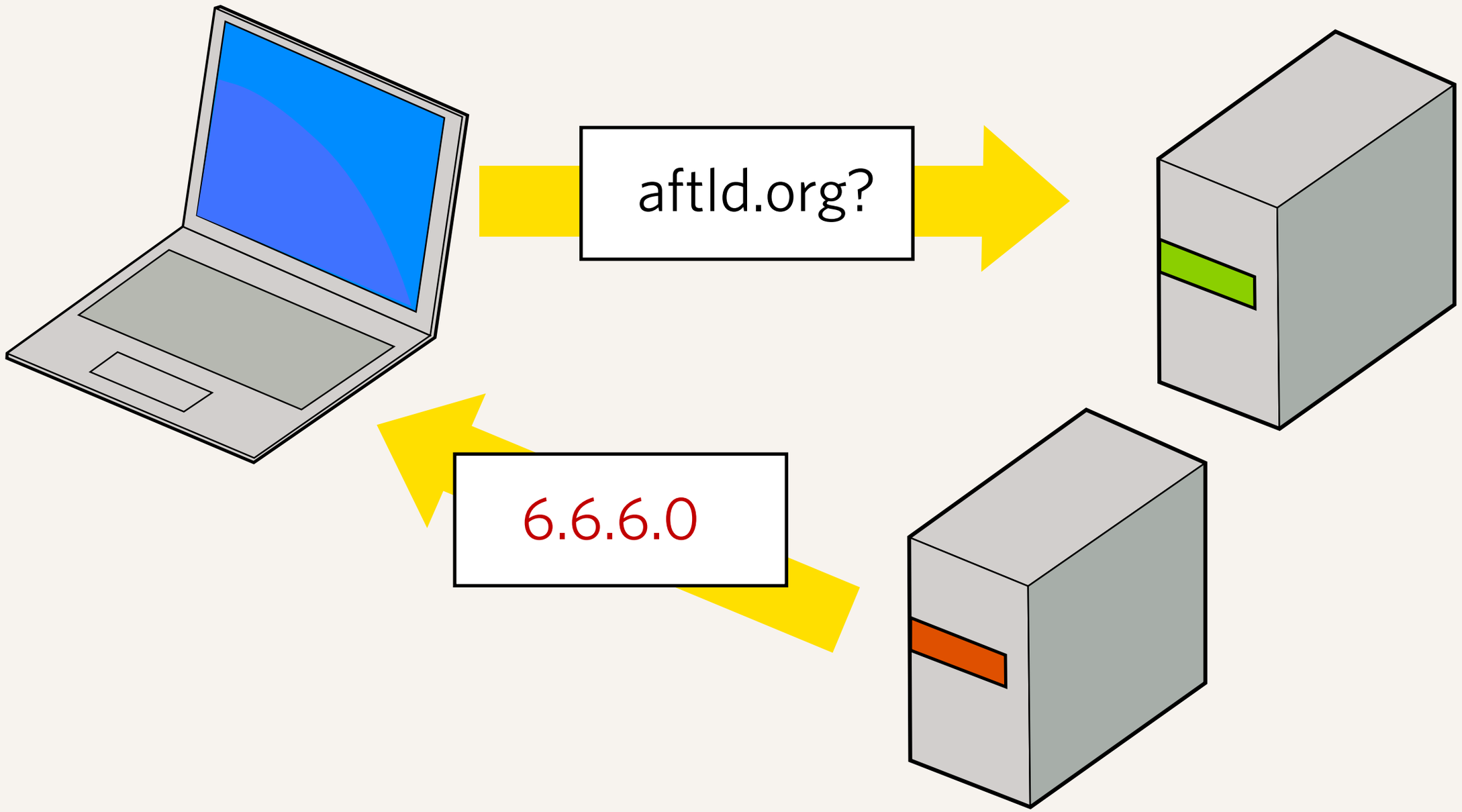
Receiving the wrong answer

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



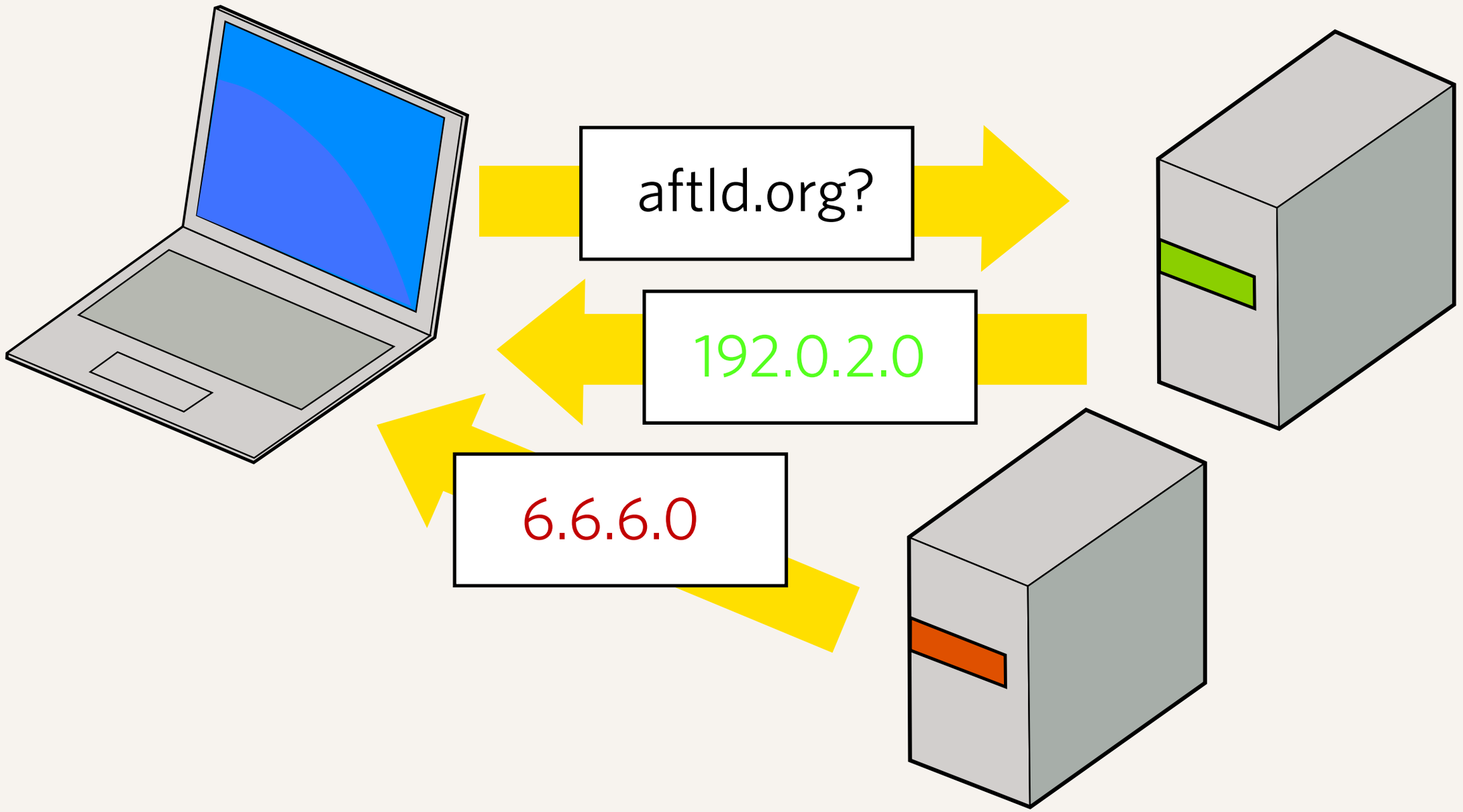
Receiving the wrong answer

- 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.

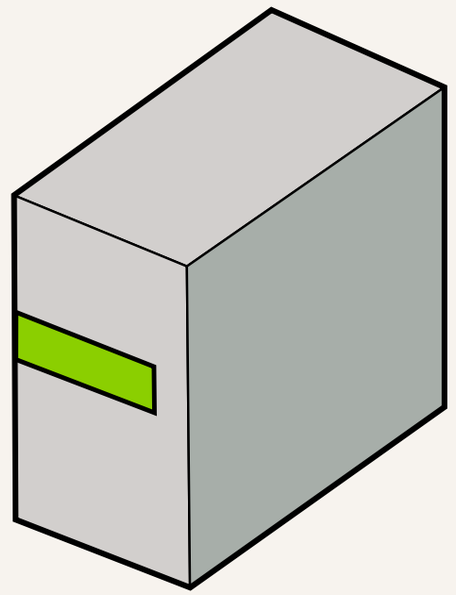


Receiving the wrong answer

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

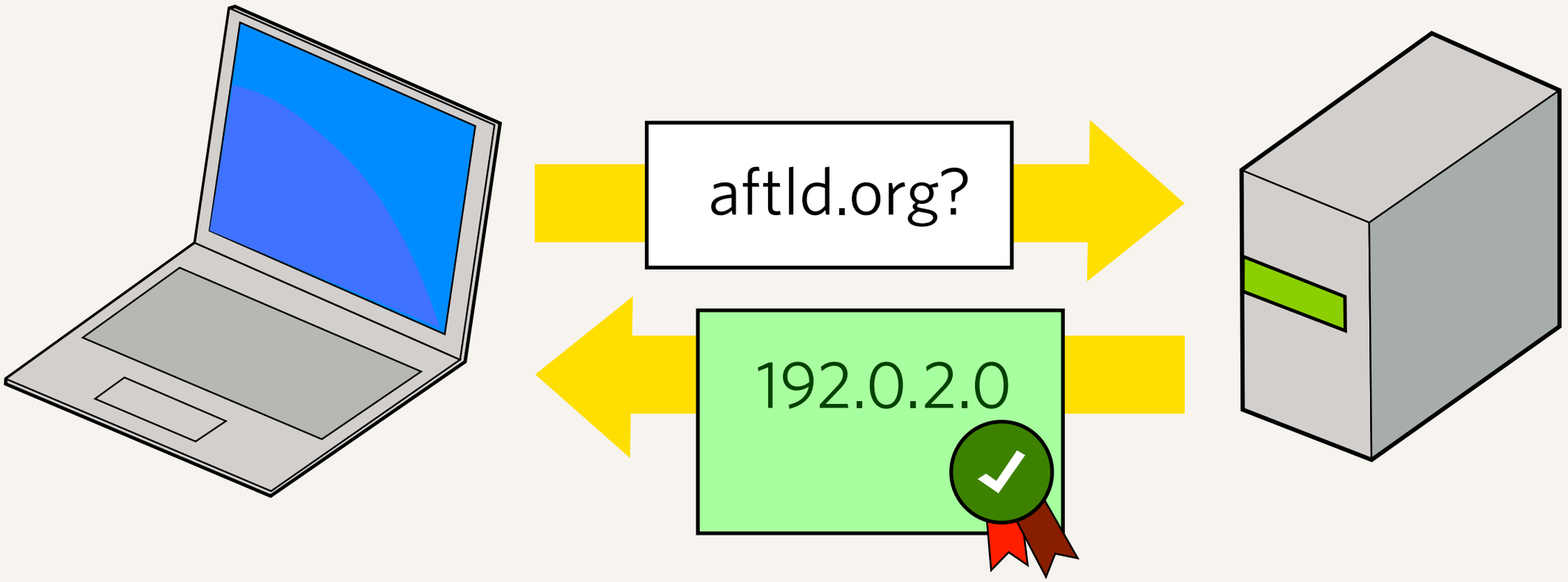
What DNSSEC provides

- 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

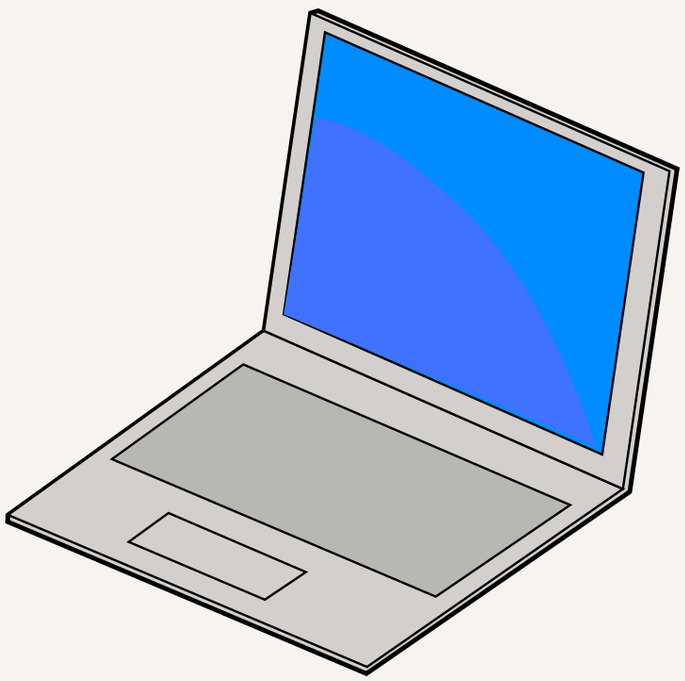
A DNSSEC secured transaction

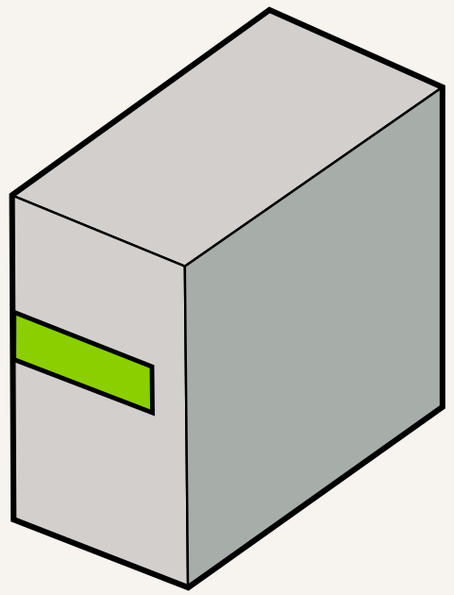


A DNSSEC secured transaction

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



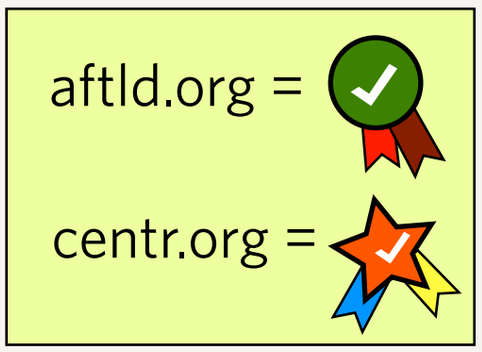


aftld.org =

centr.org =

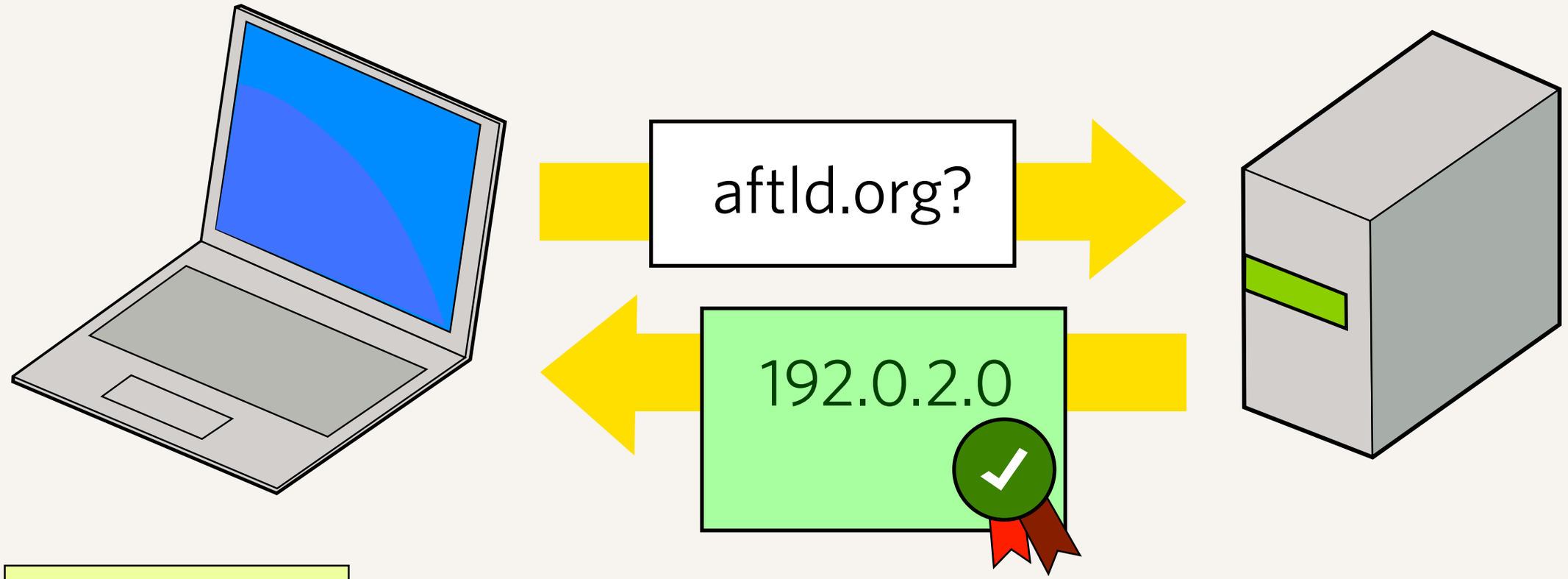
Verifying against a list of signatures

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



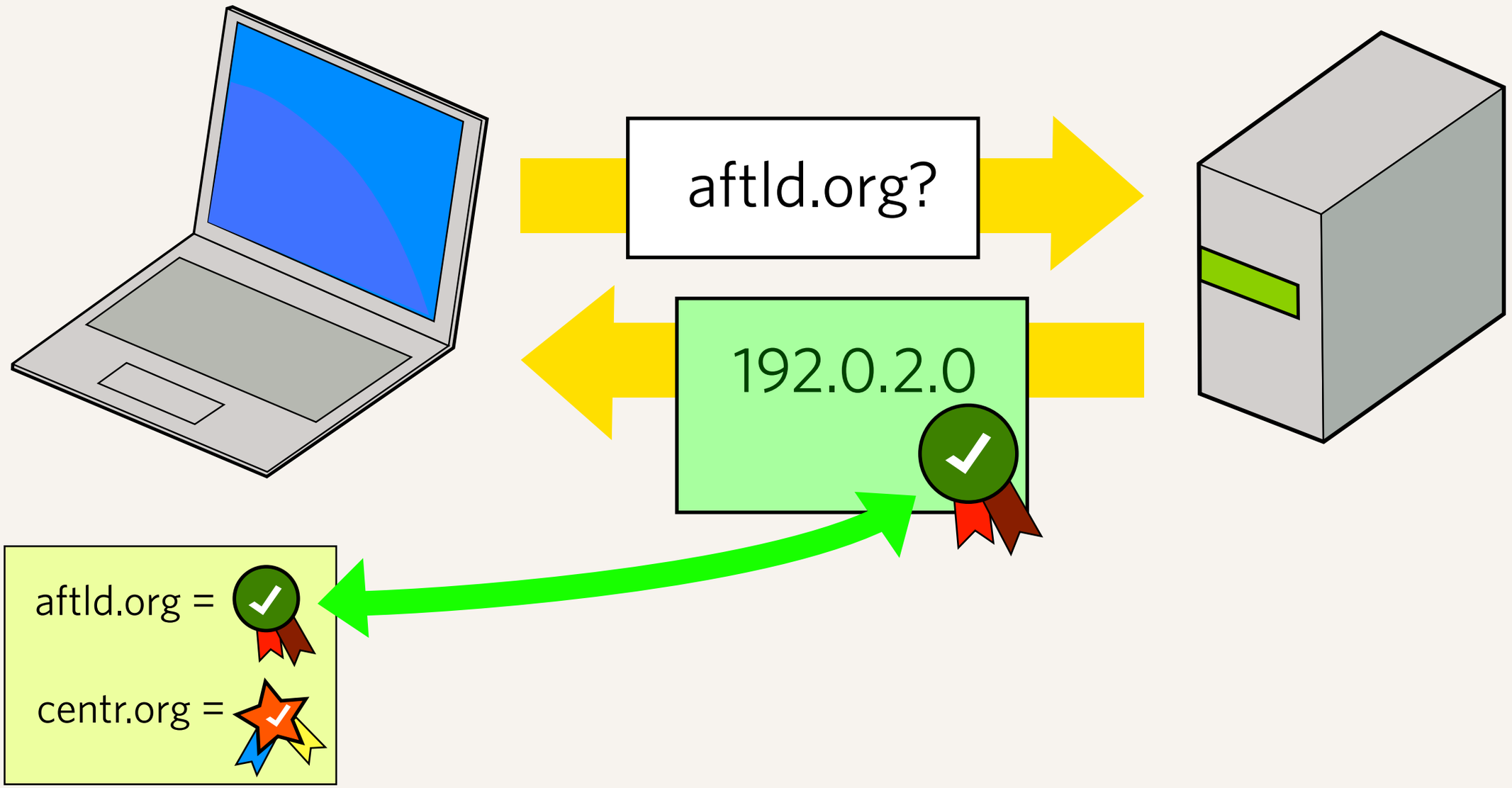
Verifying against a list of signatures

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



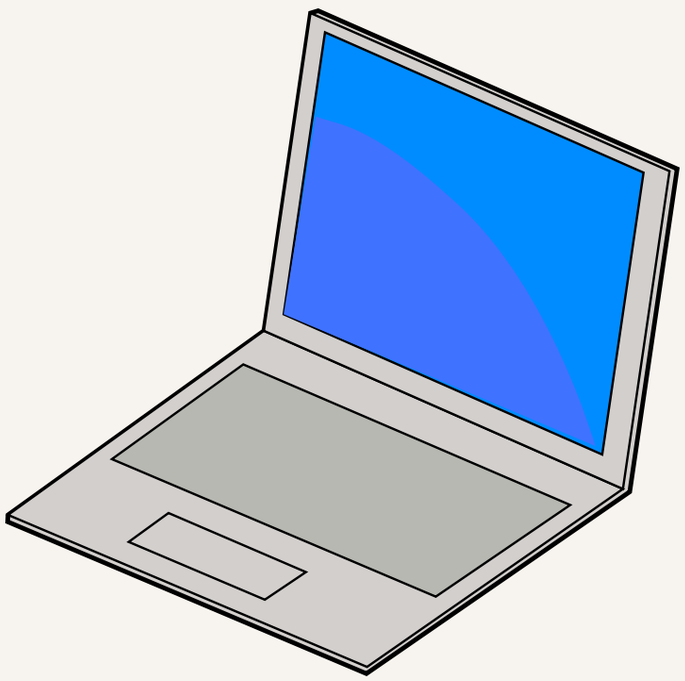
Verifying against a list of signatures

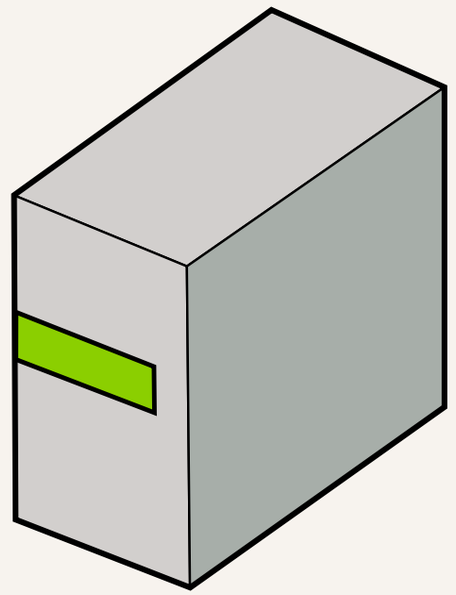
- Check against a known set of signatures, and if there is a match, is a valid answer.

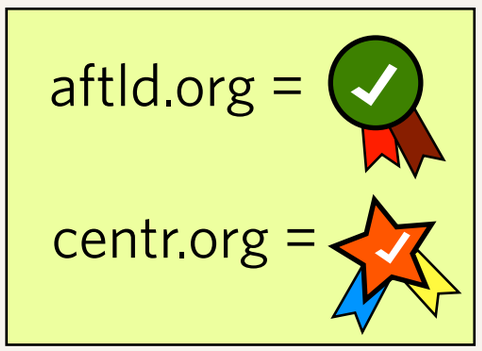


Verifying against a list of signatures

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







Verifying against a list of signatures

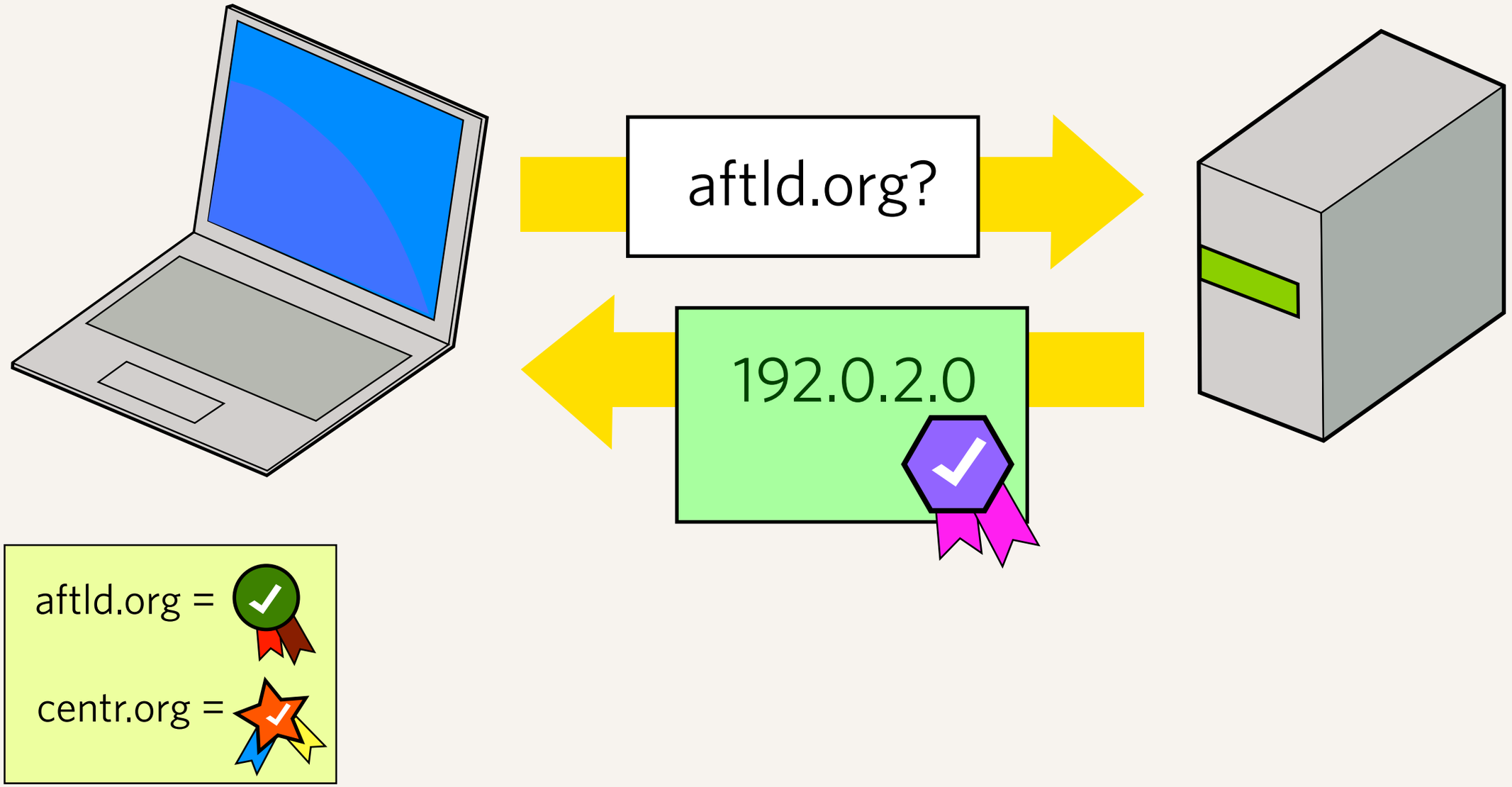
- Check against a list of known good signatures, if it fails, do not allow

aftld.org =

centr.org =

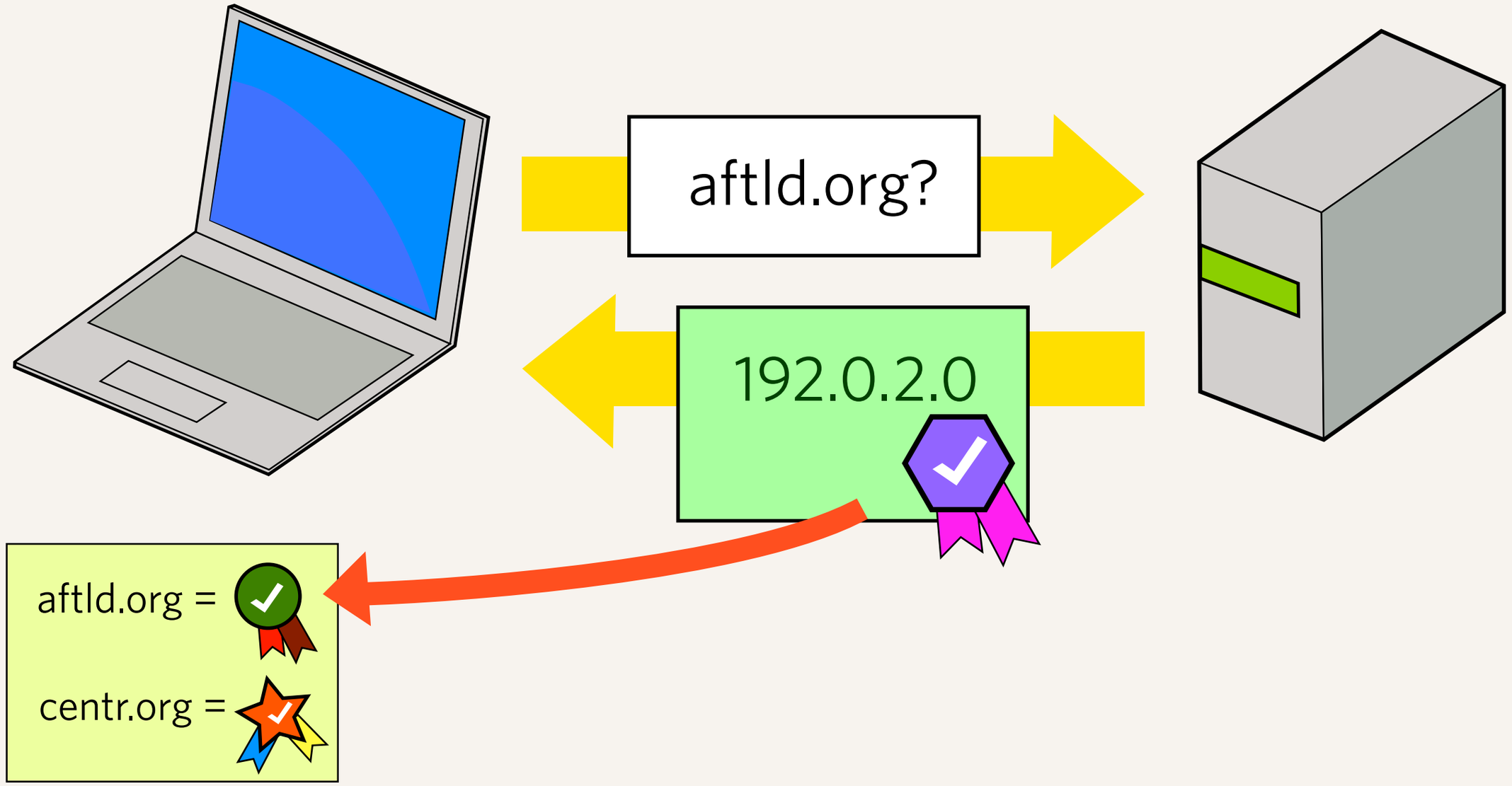
Verifying against a list of signatures

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



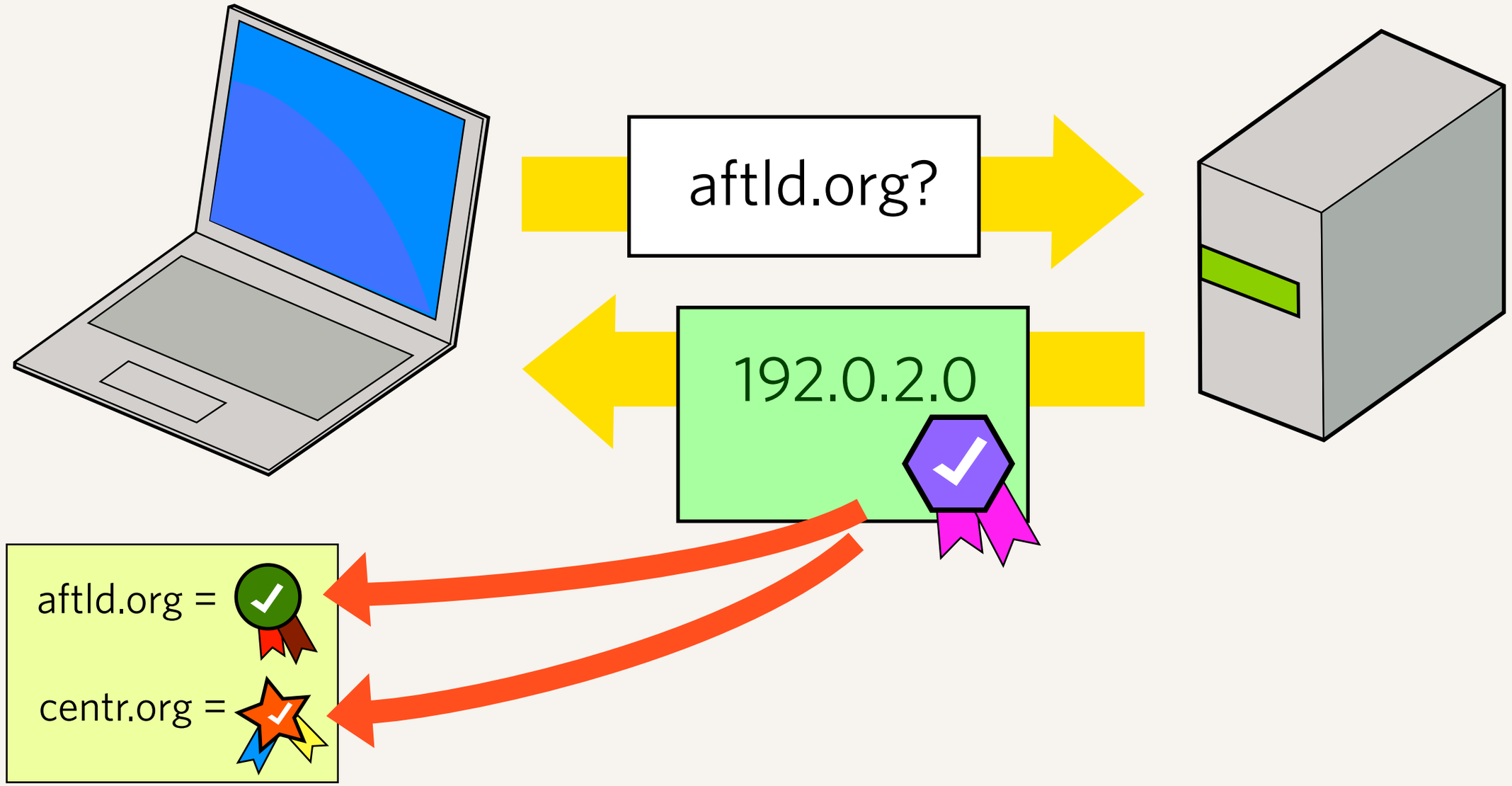
Verifying against a list of signatures

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



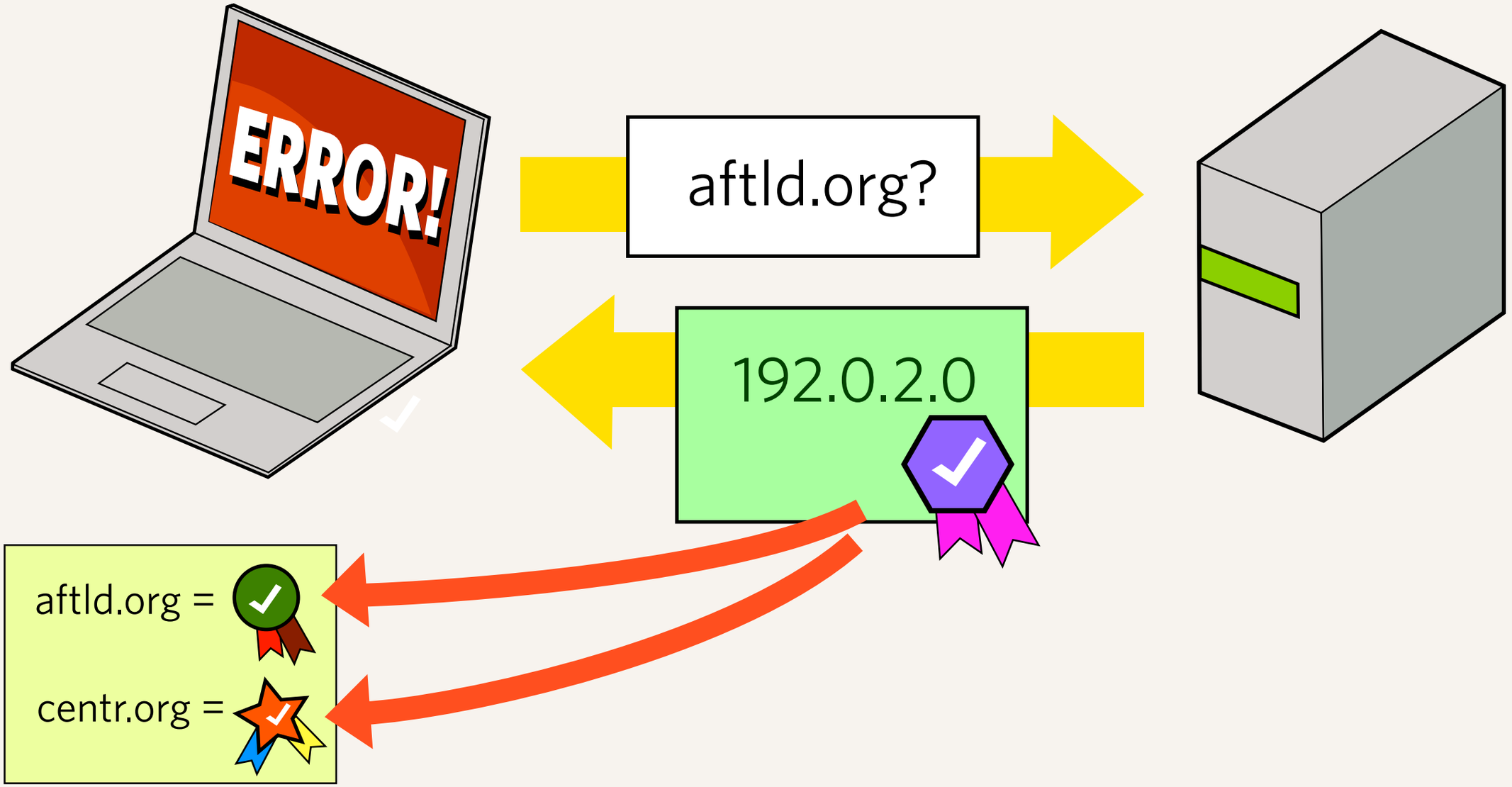
Verifying against a list of signatures

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



Verifying against a list of signatures

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

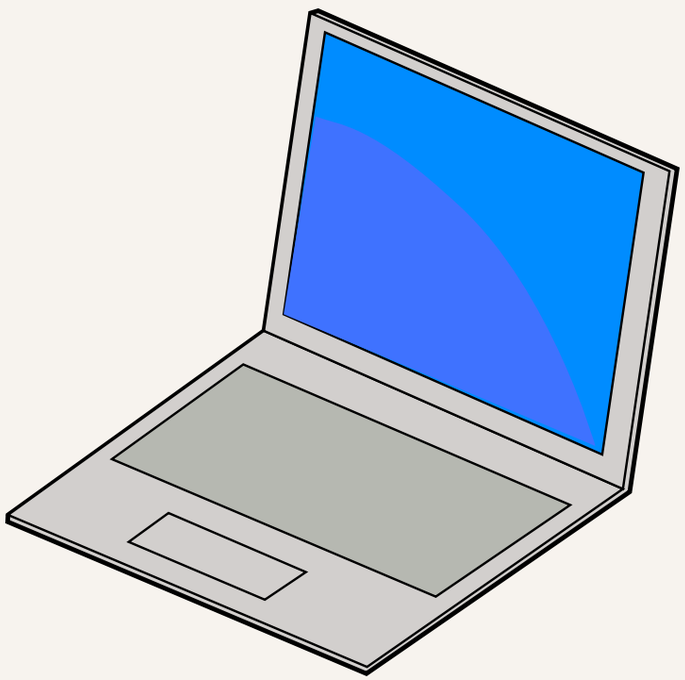


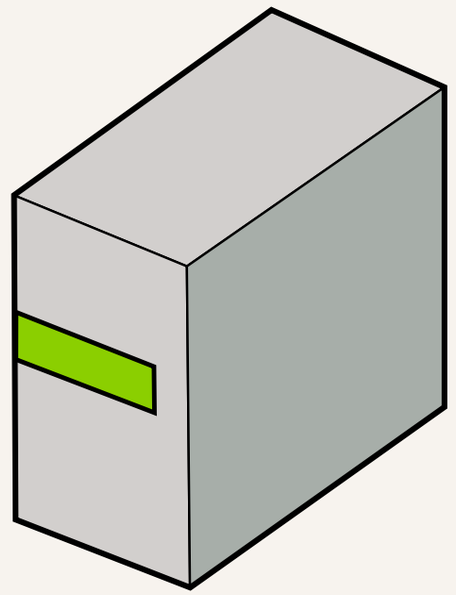
Verifying against a list of signatures

- 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?





aftld.org =

centr.org =

Verifying against a list of signatures

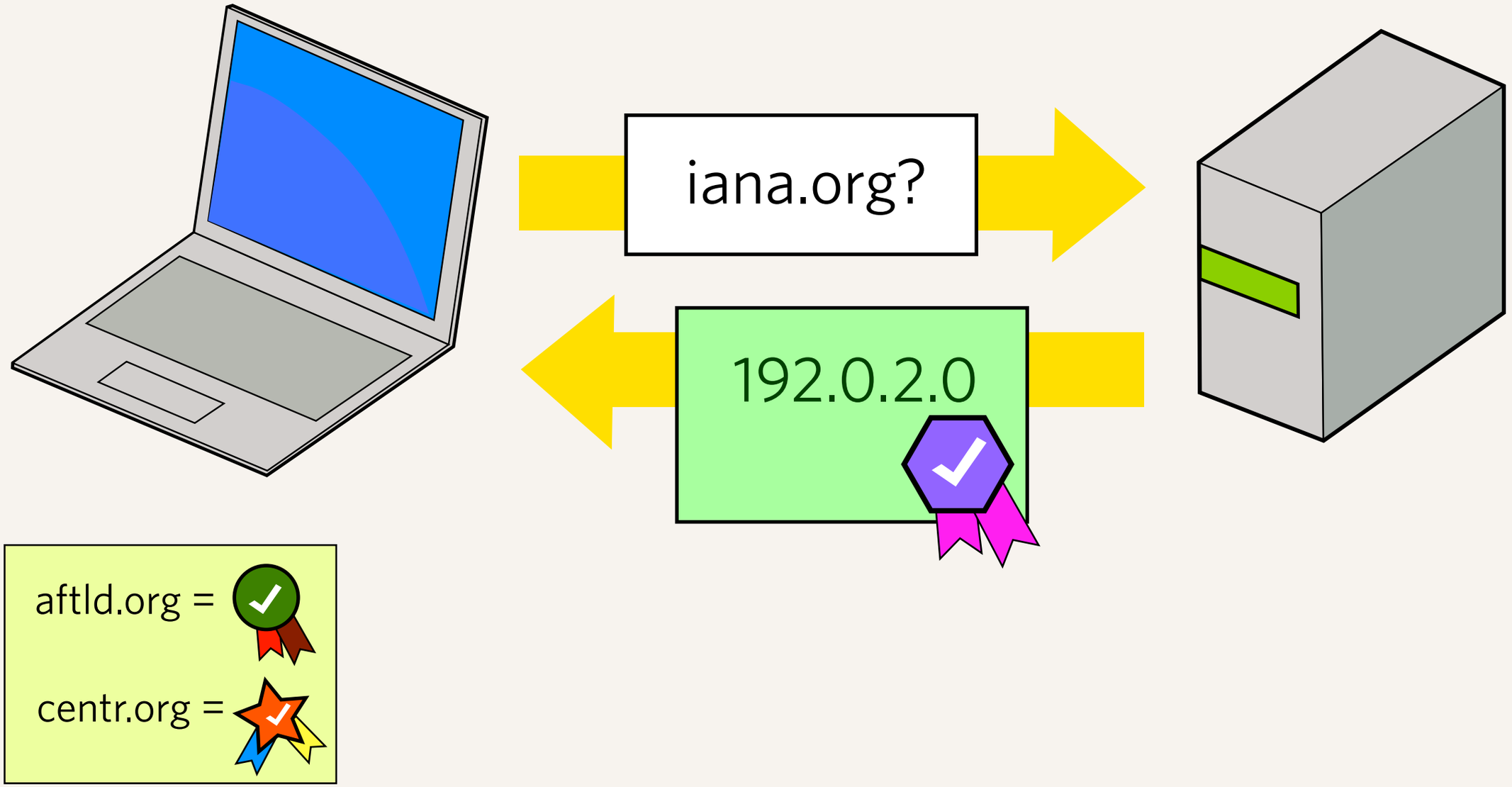
- What if it is not a domain you know about?

aftld.org =

centr.org =

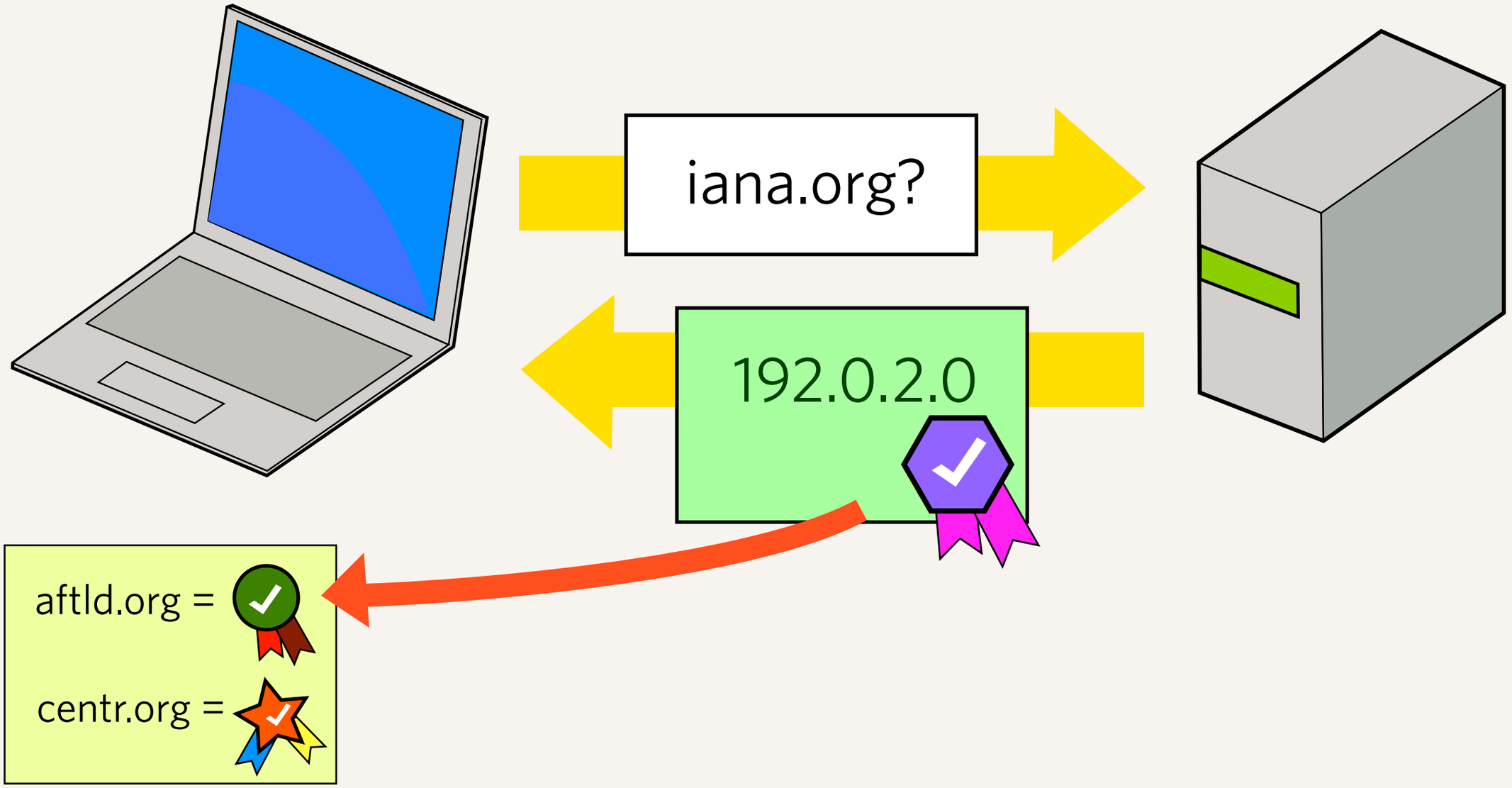
Verifying against a list of signatures

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



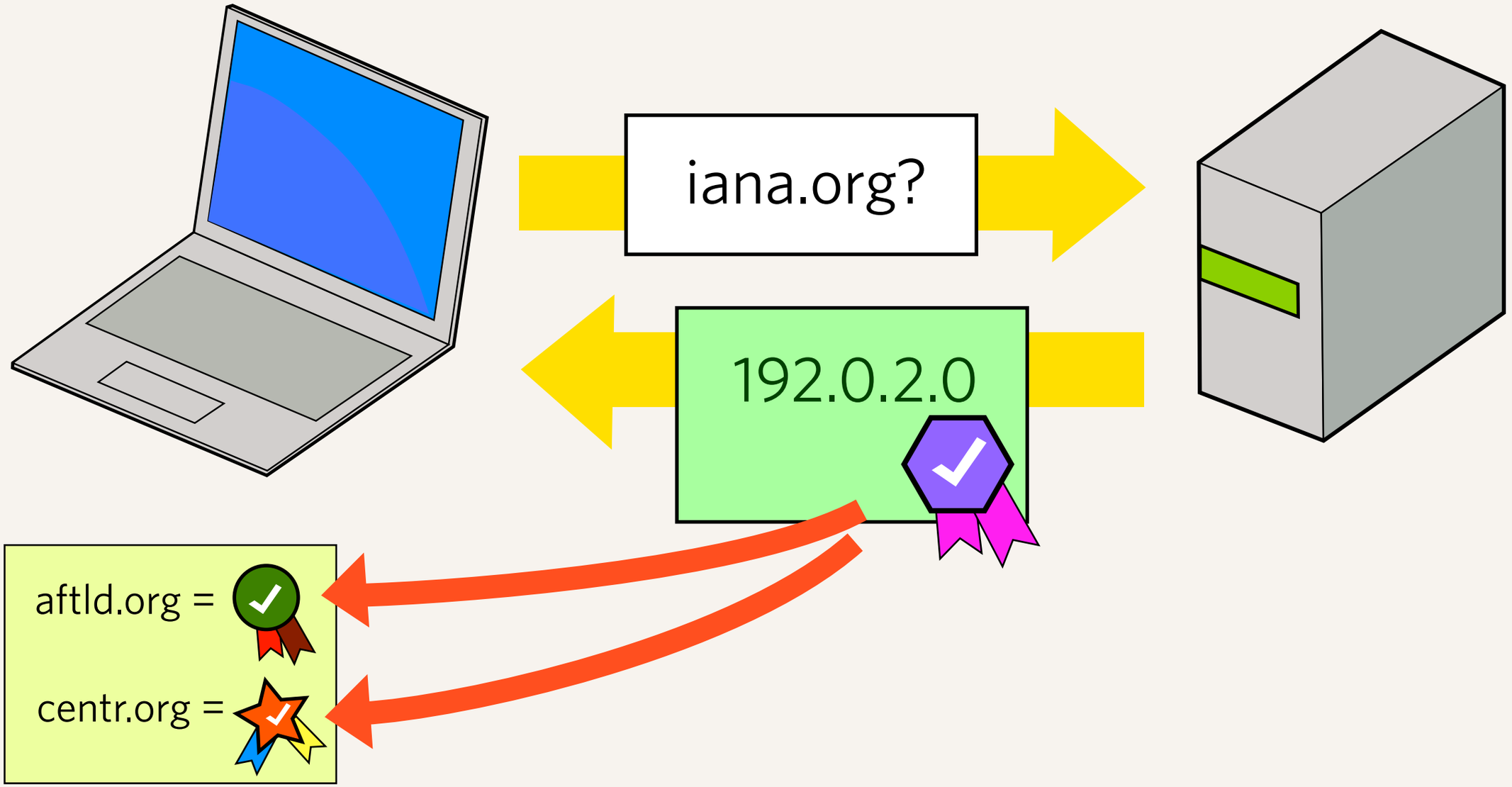
Verifying against a list of signatures

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



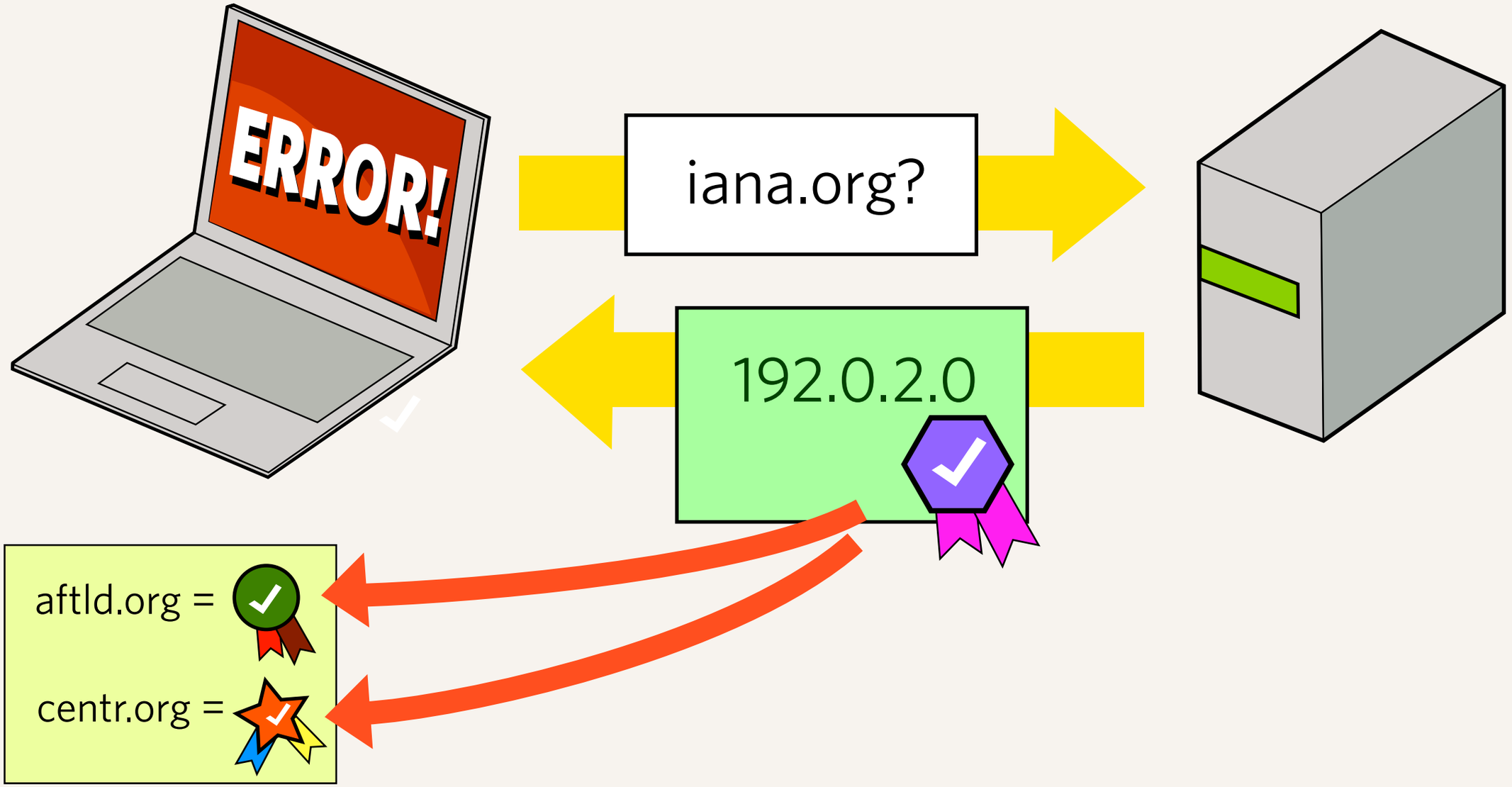
Verifying against a list of signatures

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



Verifying against a list of signatures

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



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...

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

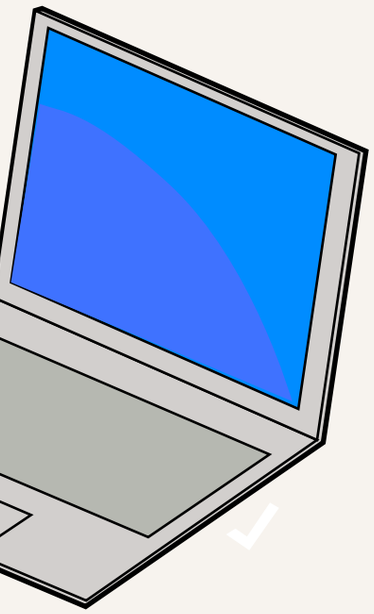
.org

iana.org =

Using a chain of trusted certificates

aftld.org =

centr.org =



iana.org?

192.0.2.0

root

.org =

.org

iana.org =

Using a chain of trusted certificates

aftld.org =

centr.org =

iana.org?

192.0.2.0

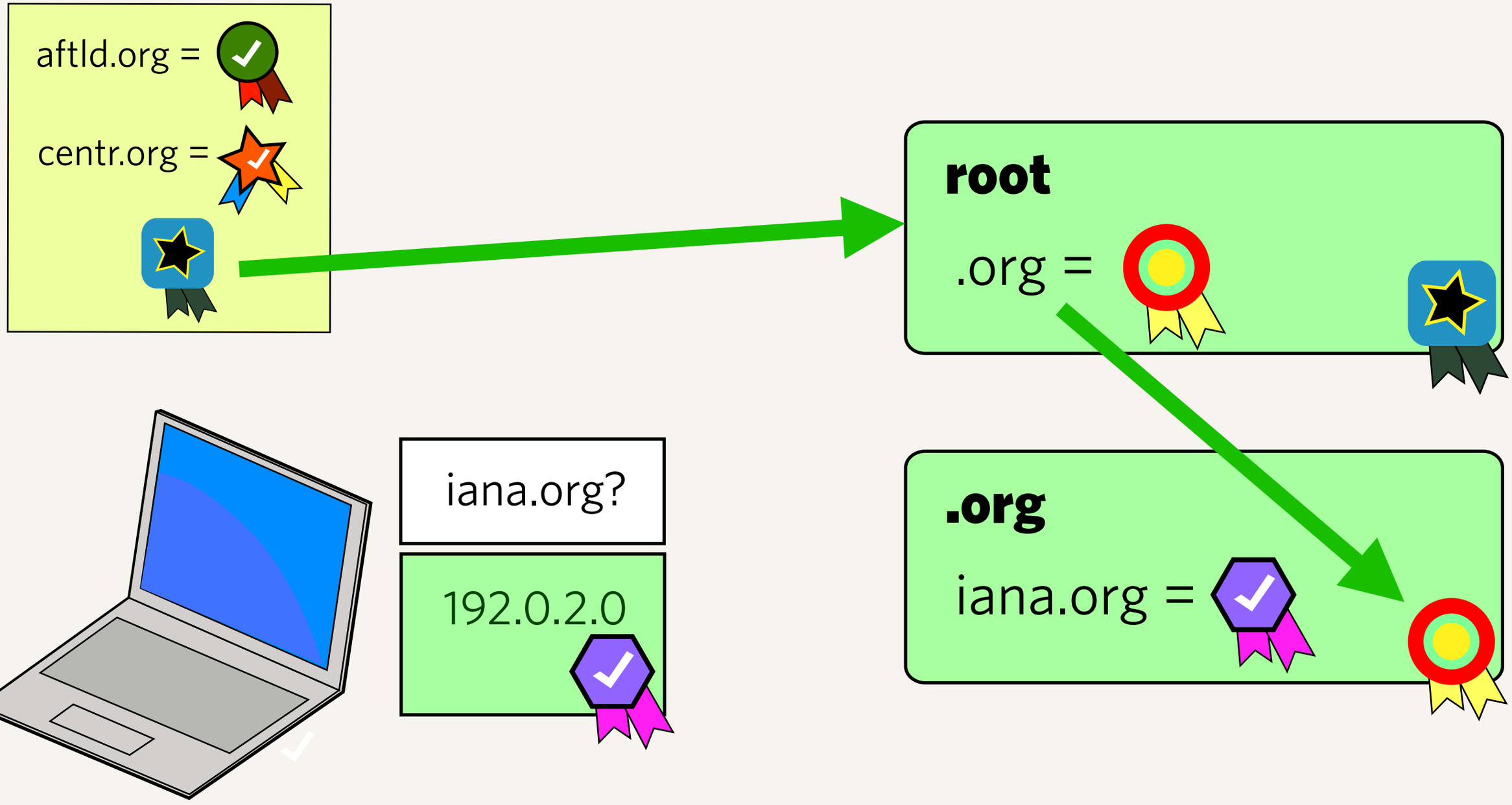
root

.org =

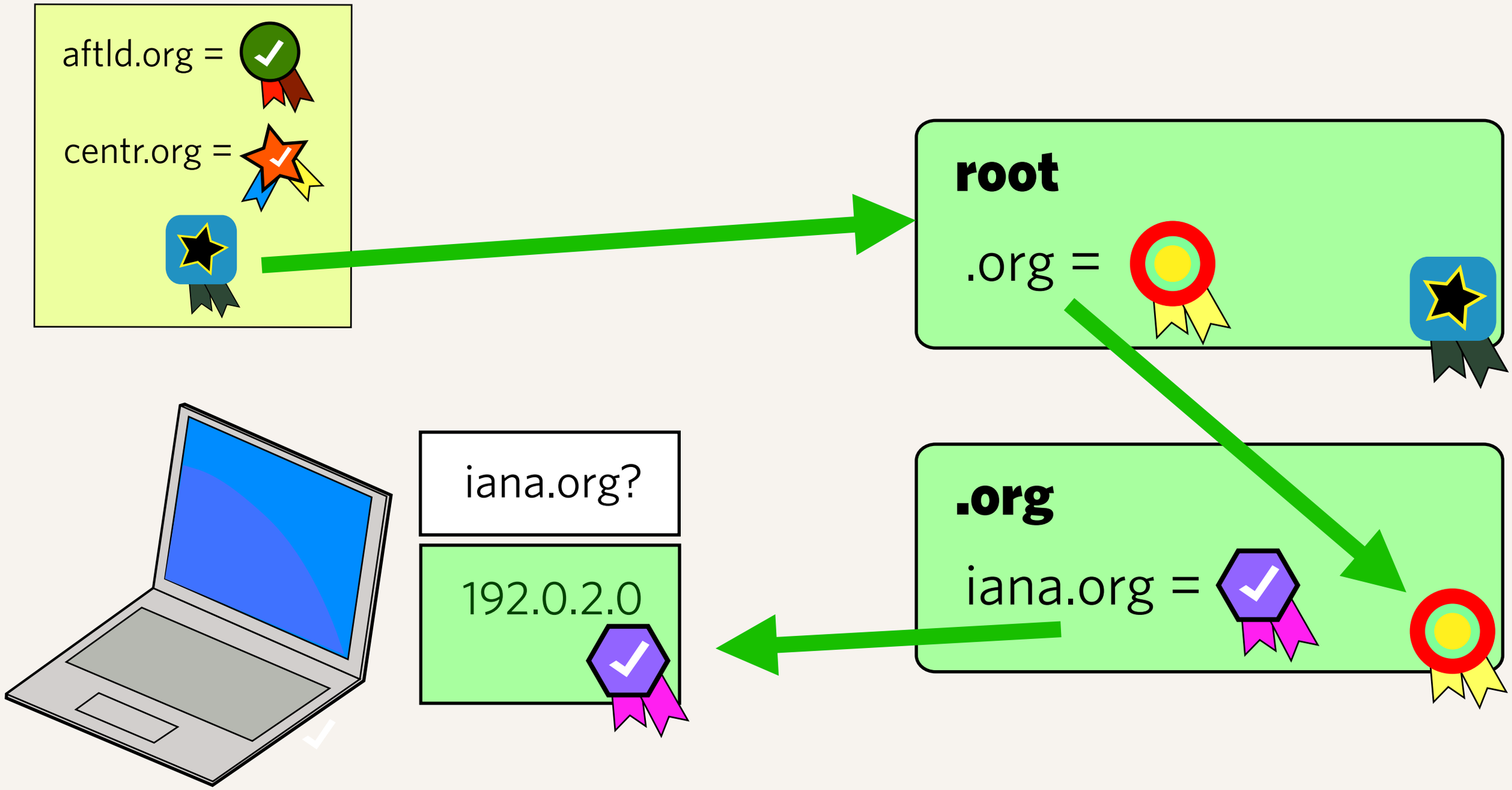
.org

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

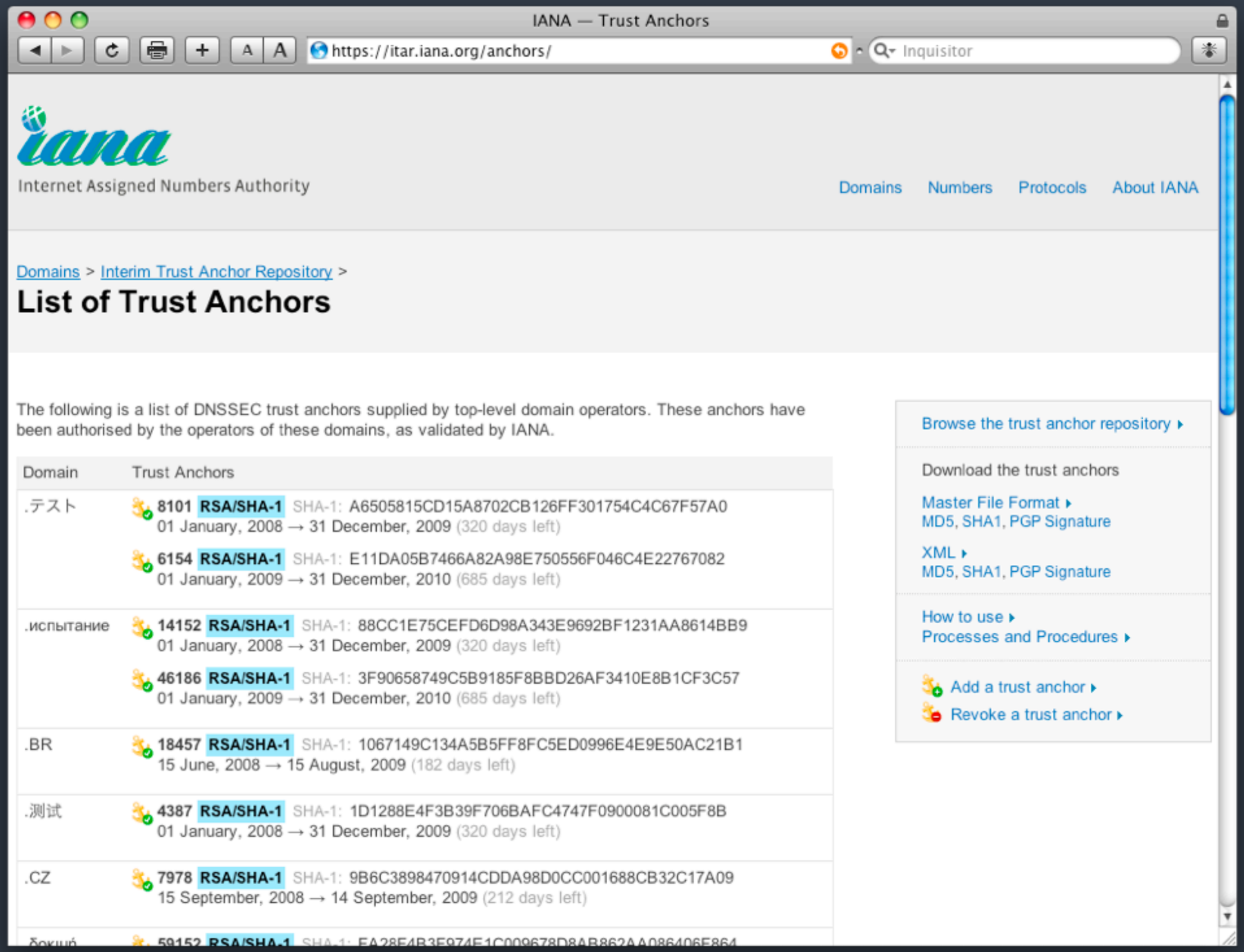
IANA has been asked to sign the root zone

- Several entities have formally asked ICANN to sign the root zone, including: RIPE, Registry for .SE, Nominet and APNIC
- A majority of respondents to the US DoC NTIA NoI favoured ICANN signing the root
- Signing the root allows a single signature to be used to verify any signed zone (theoretically)
- Zone data currently managed by IANA and edited by VeriSign

IANA's DNSSEC test bed

- Since 2007, IANA has run a DNSSEC signed root testbed
- https://ns.iana.org/dnssec/status.html
- The root zone on this testbed server is signed, as well as:
  - .ARPA and children (IN-ADDR/IP6/IRIS/URI/URN).ARPA
  - .INT
  - Everything in ITAR
- Served on ns.iana.org

Interim Trust Anchor Repository (ITAR)



DNSSEC outside the root zone

At IANA

- The Internet Architecture Board has asked IANA to sign the .ARPA zone
  - Currently published through a similar mechanism as the Root Zone (the root servers are authorities for .ARPA)
    - IANA is setting up a new set of authorities, to shift operations to allow it to sign .ARPA in production
- IANA has already begun signing all the test IDNs in the root zone.

Outside IANA

- More than a dozen TLDs sign their zones so far
  - https://itar.iana.org/anchors/
- RIPE NCC signs all of the zones it manages
- A collection of signed zones is published at http://secspider.cs.ucla.edu/
  - 16894 DNSSEC-enabled zones

How can a registry deploy DNSSEC?

To sign their own zone

- Generate a set of keys for signing their zone
- Modify their zone publication process to include the software process of signing the zone
- Review security procedures, to ensure the security of the “private key”
- If their parent zone supports DNSSEC, transmit their key to enable the chain of trust.

To allow their customers to sign their zone

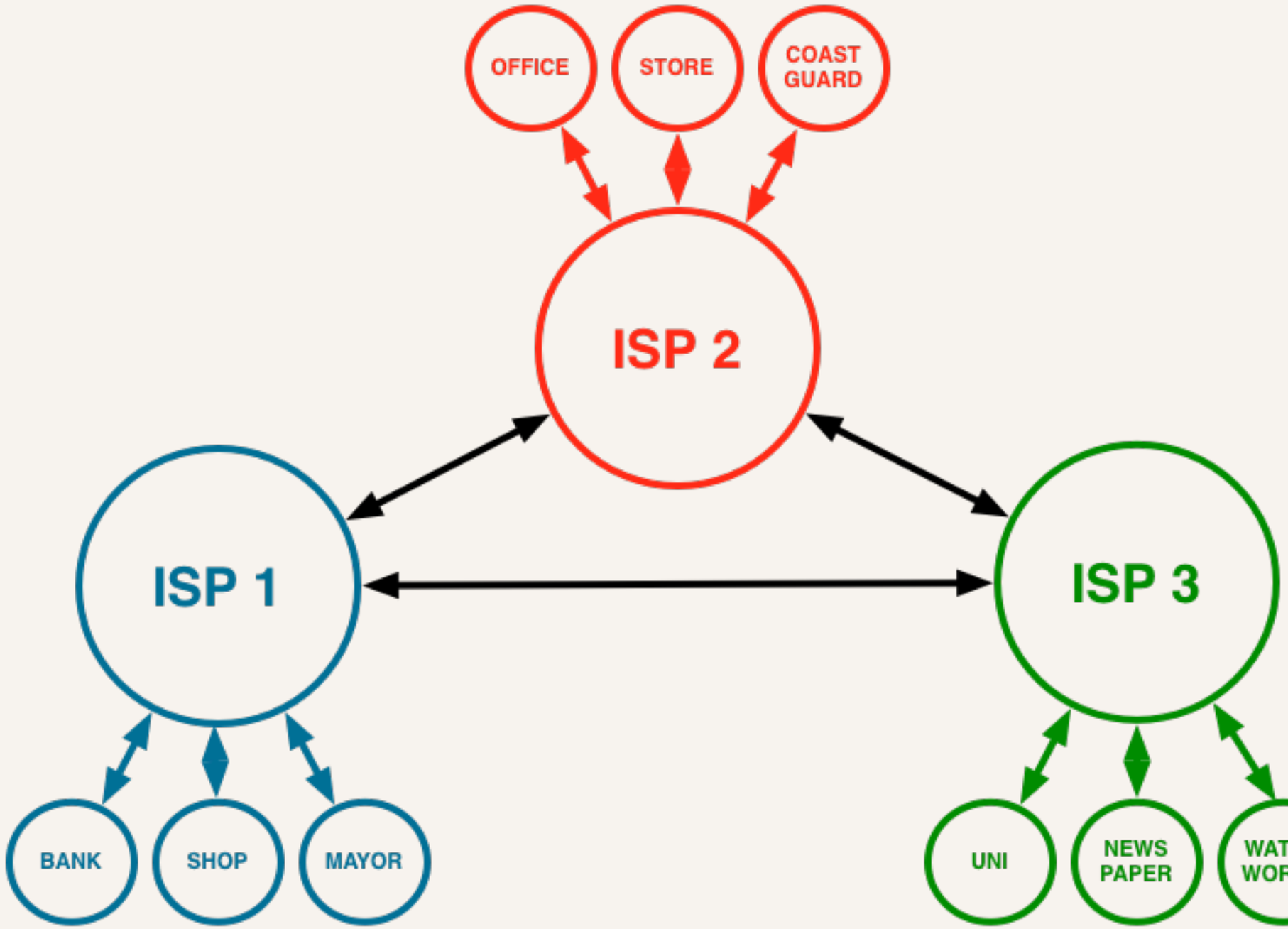
- Registries need to publish the signatures of their registrant's secure zones. This allows the chain of trust to work.
- They can be considered as a new piece of technical information that needs to be communicated to the registry.
- Registry interfaces need to add the ability for registrants to supply this information.
- A number of existing registries have examples on how they handle this.

What is BGP?

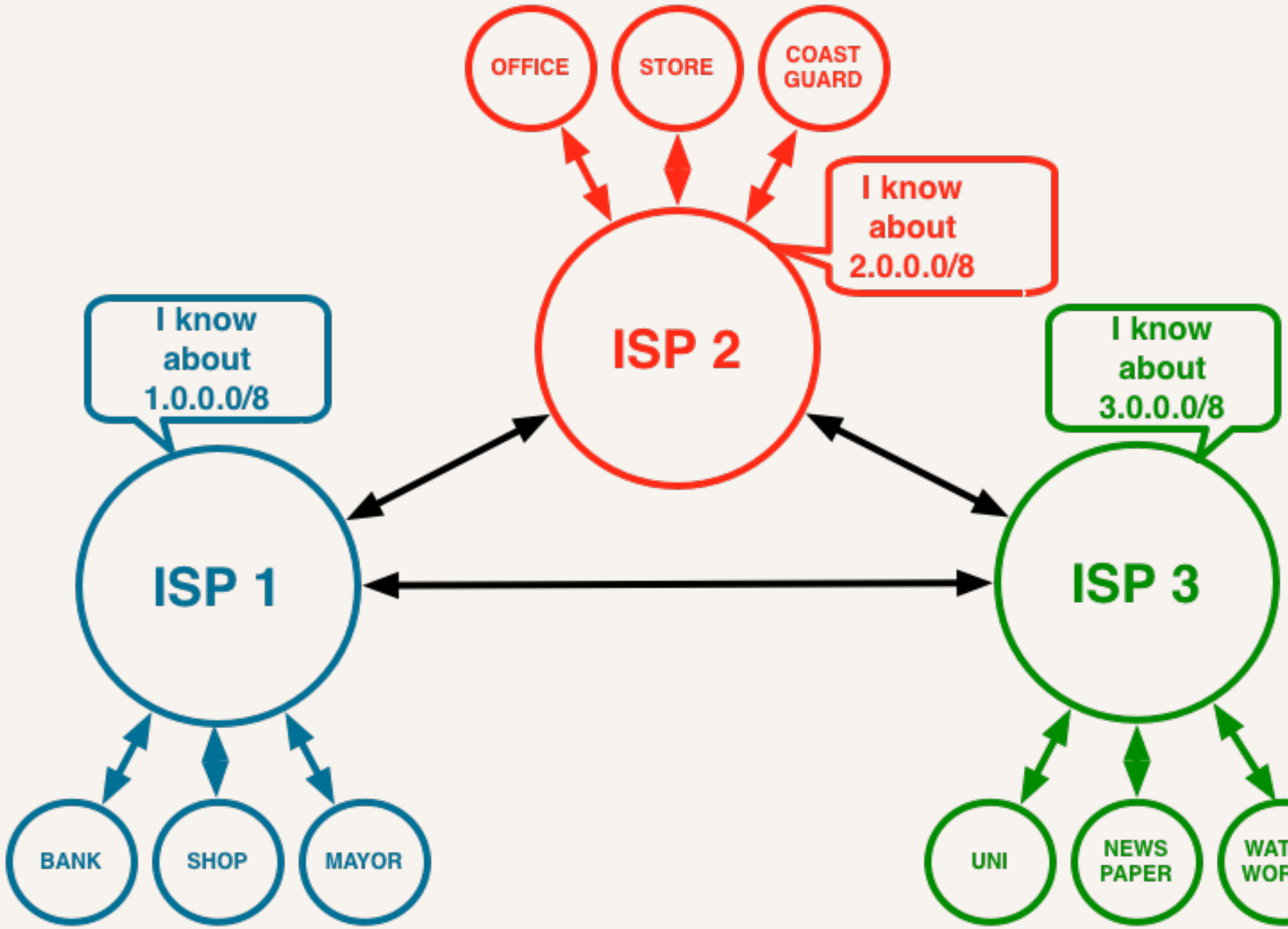
How does it work?

Inter-domain (ISP) routing is based on trust

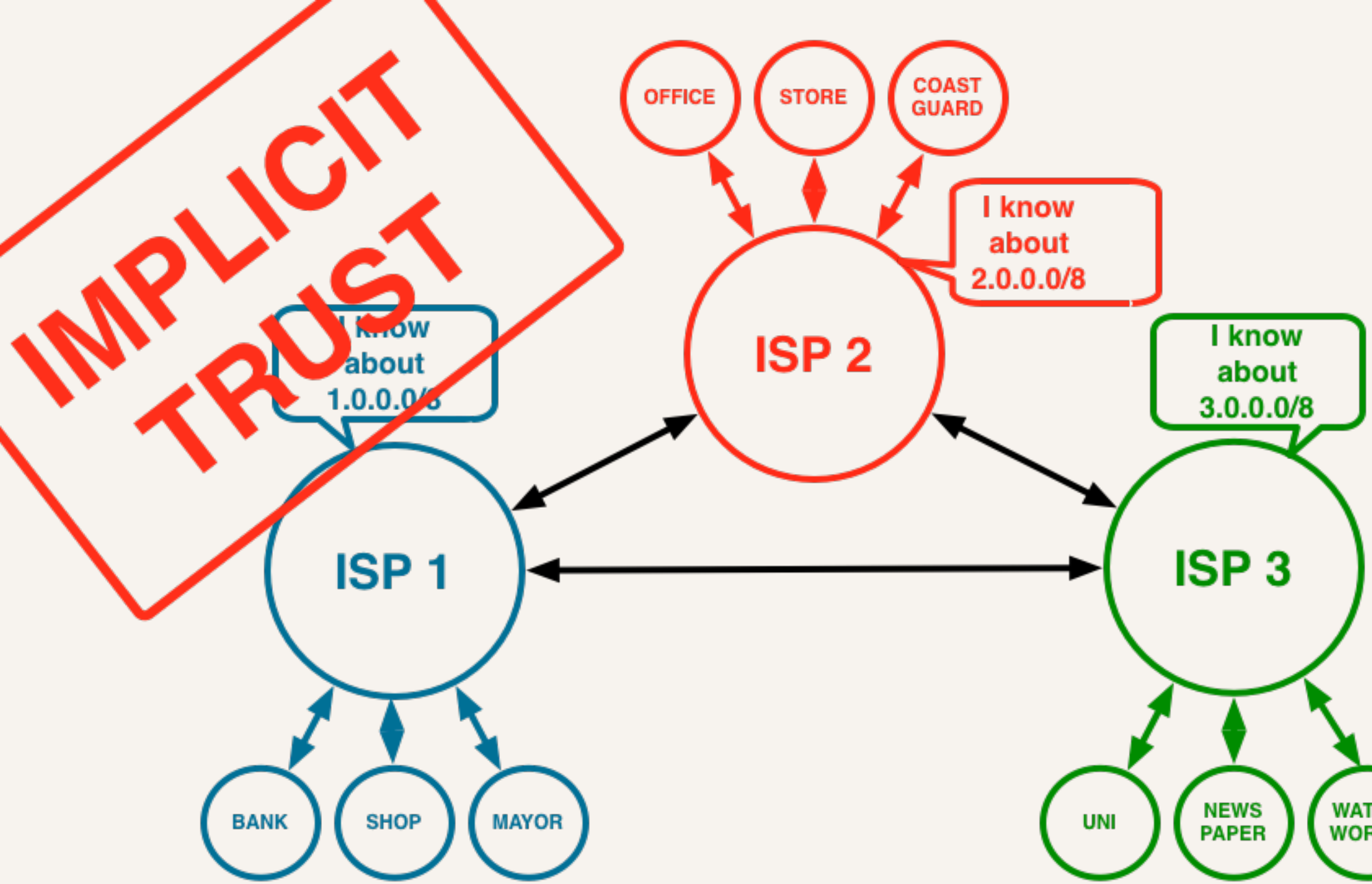
- A router announces the prefixes it knows how to get to
- Or the prefixes it claims it can get to
- A ISP network will get traffic for prefixes it has the shortest path to



Inter-ISP routing (1)

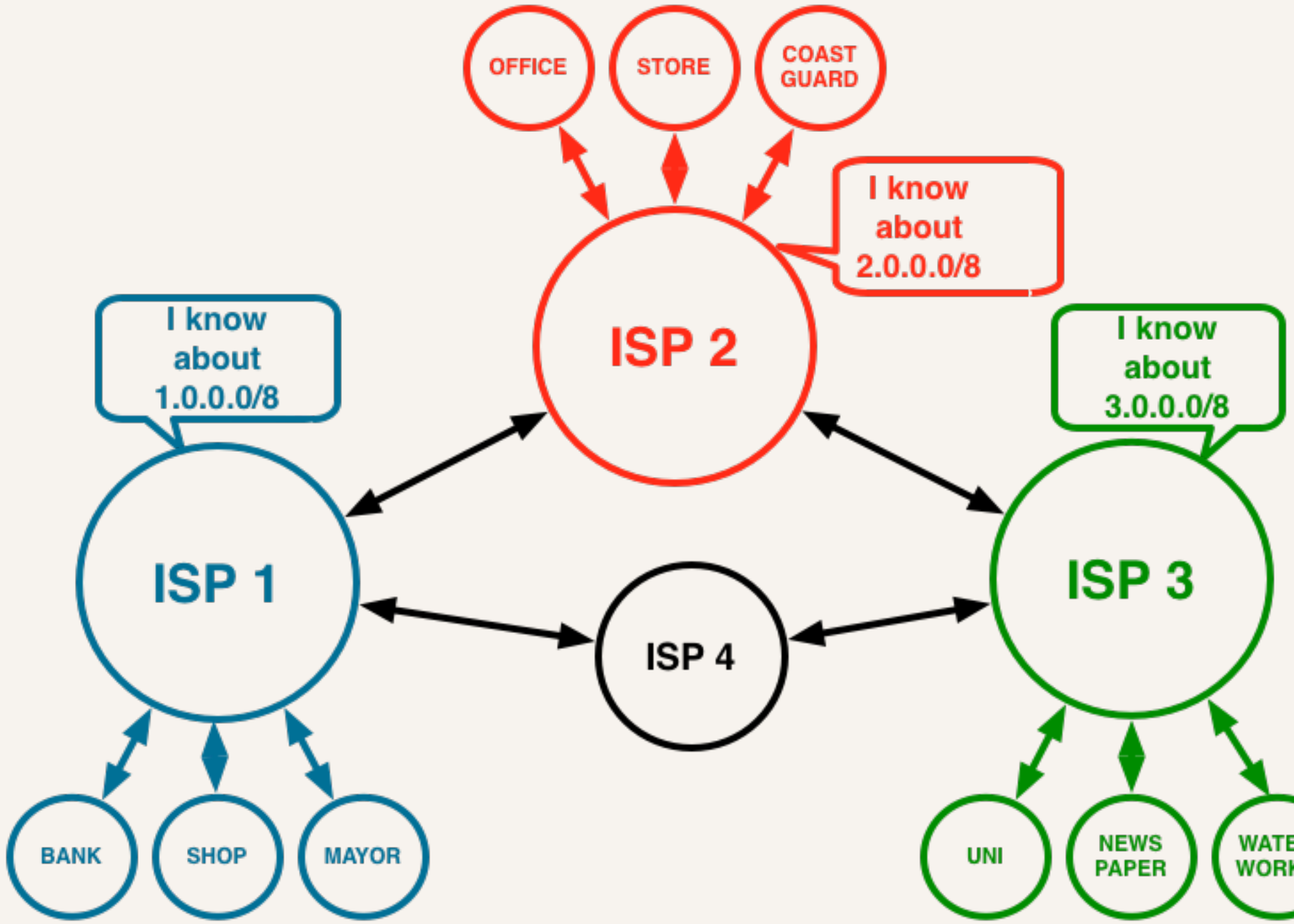


Inter-ISP routing (1)



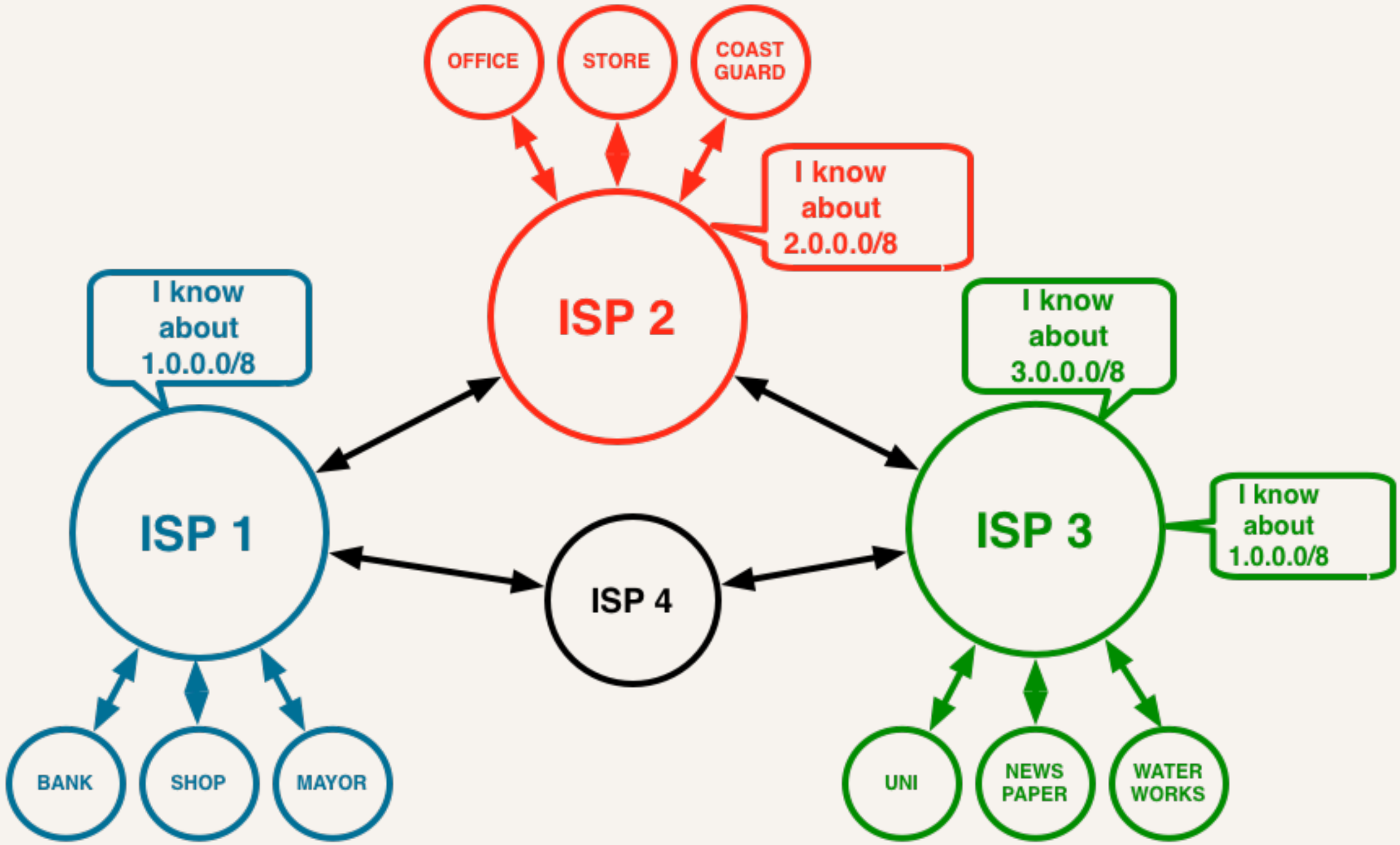
Inter-ISP routing (2)

- Feel the trust



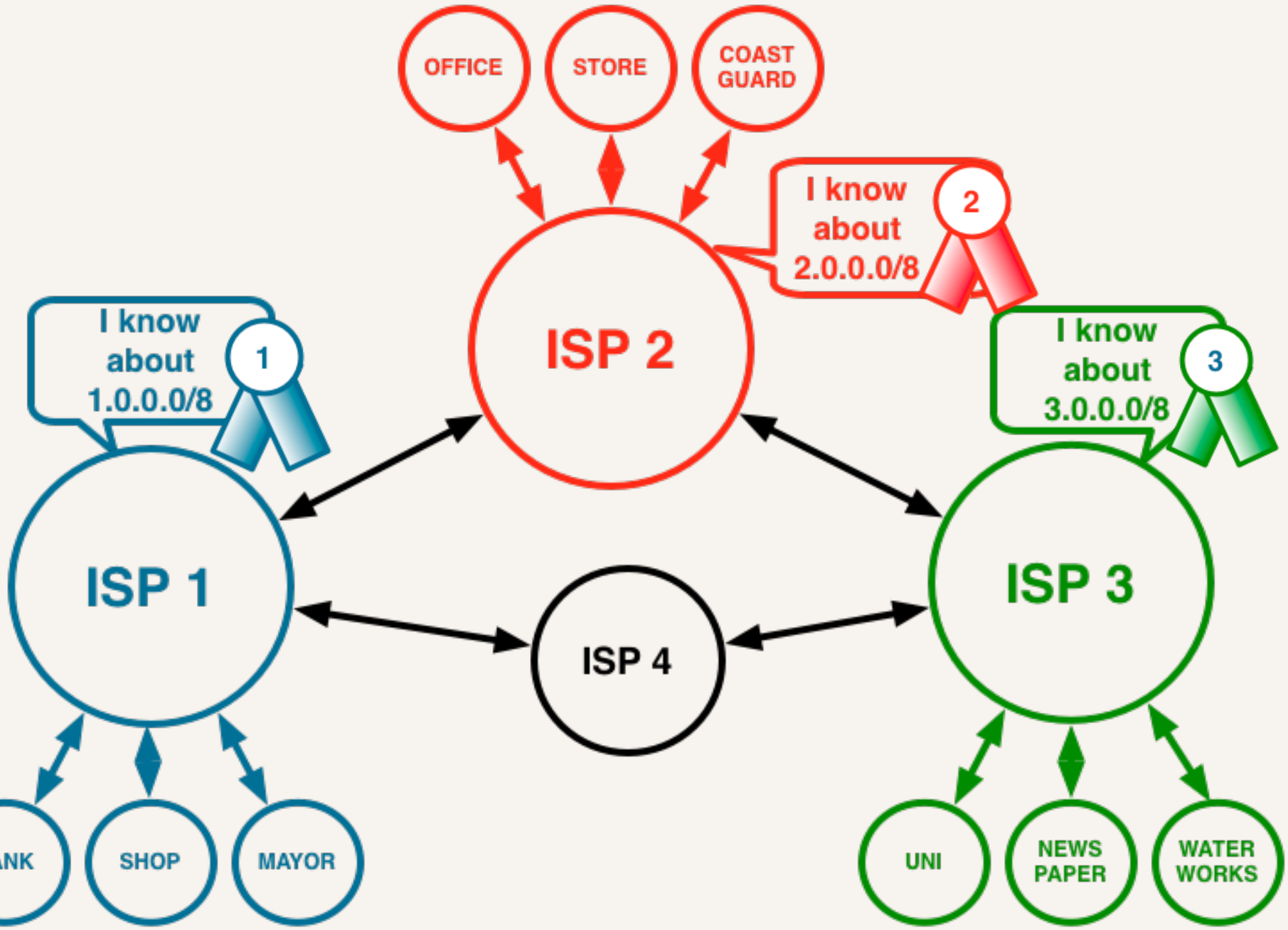
Inter-ISP routing (3)

- Whoops?

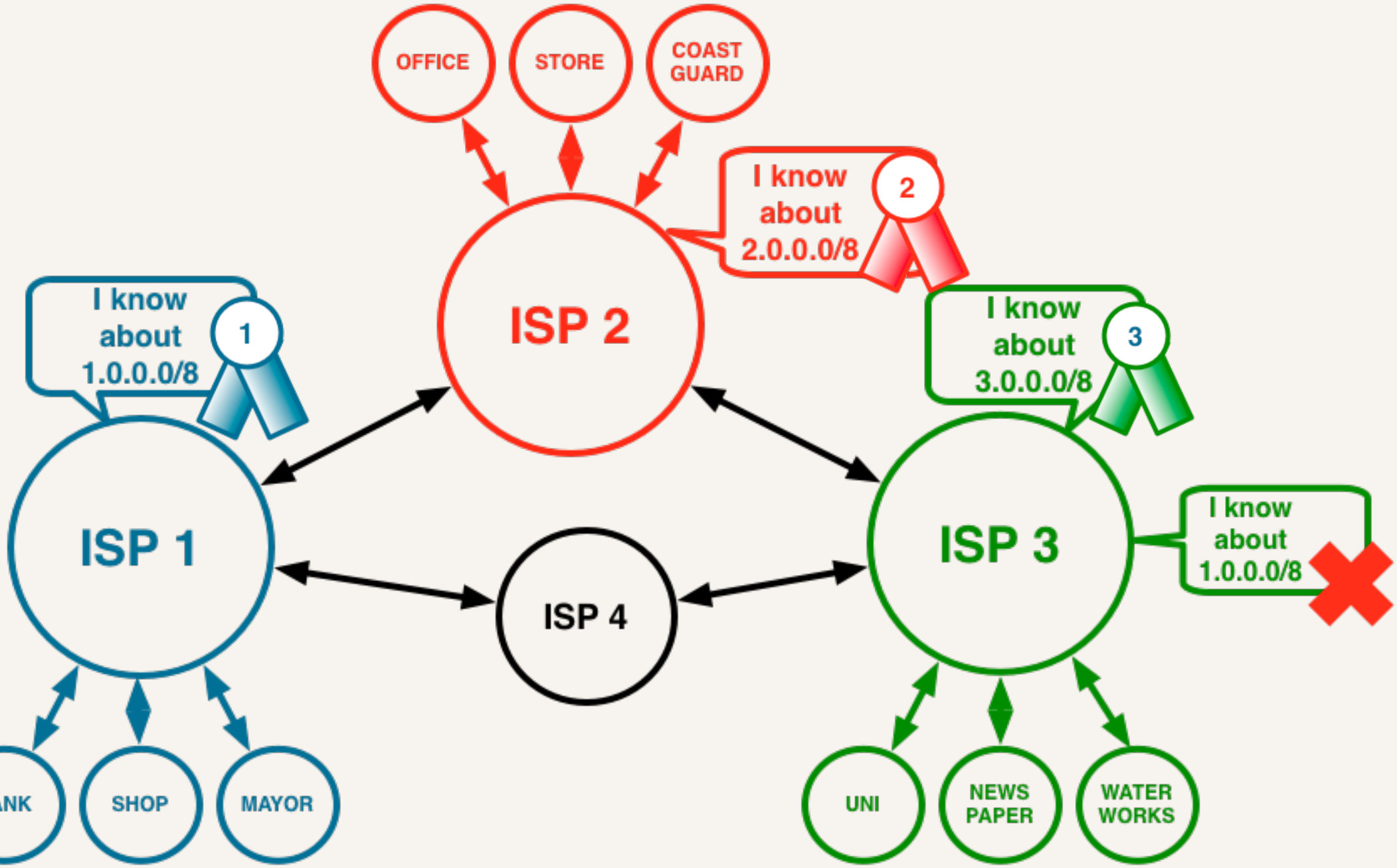


Inter-ISP routing (3)

- Whoops?



Certificates for IP address blocks are being developed to add security



Certificates for IP address blocks are being developed to add security

Real world examples

- ConEdison hijacked routes to Panix (among others) in January 2006
- YouTube's prefix was hijacked by Pakistan Telecom for about an hour in February 2008
- Alex Pilsov and Tony Kapela's demonstrated "man in the Middle" attack at Defcon 16 in August 2008
  - https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

Secure Inter-Domain Routing Status

- Protocol development in the IETF SIDR WG
  - http://www.ietf.org/html.charters/sidr-charter.html
- ICANN staff and RIR staff actively contribute
- Initial plans will allow out-of-band authentication of resource status
- Routing protocol changes to follow

What can be done now?

- BGP monitoring and notification services exist, including…
  - RIPE NCC MyASN
    - http://www.ris.ripe.net/myasn.html
  - BGPmon
    - http://bgpmon.net/
  - Reneys Routing Intelligence
    - http://www.renesys.com/products_services/routing_intelligence/

Thanks!

Leo Vegoda

leo.vegoda@icann.org