Introduction to DNSSEC & DANE

Josh Kuo

josh@deepdivenetworking.com

Who Are We?

DEEPDIVE NETWORKING

– Company Info

DeepDive Networking possesses and delivers an incredible depth of knowledge related to DNS, DHCP, and core networking technologies. Our core specialties include, architecture, design, implementation services, training delivery, and training development for firms worldwide. DeepDive strives to exceed all expectations, and delivers master-level results to ensure ultimate, repeatable success.

http://www.deepdivenetworking.com

What Are We Talking About?

We are talking about 3 things basically:

1. What is DANE?
2. Why is DNSSEC necessary for us to use cool things like DANE?
3. How does DNSSEC work?

Everything I am about to talk about here is open standards, nothing proprietary, share it!

What is DANE?

DNS-based **A**uthentication of **N**amed **E**ntities

RFC 6698 (August 2012)

RFC 7218 (April 2014)

Basically, DANE allows us to store information about generic crypto objects such as a X.509 certificate (commonly known as SSL/TLS certs) in DNS as a TLSA record, it looks like this:

```
_443._tcp.www.mydnssecgood.org. 3600 IN   TLSA   3 0 1
85E4C96EA373020E6B558F657F61DD275E5FBD649280A3A7A0A848D4 ED8457C9
```

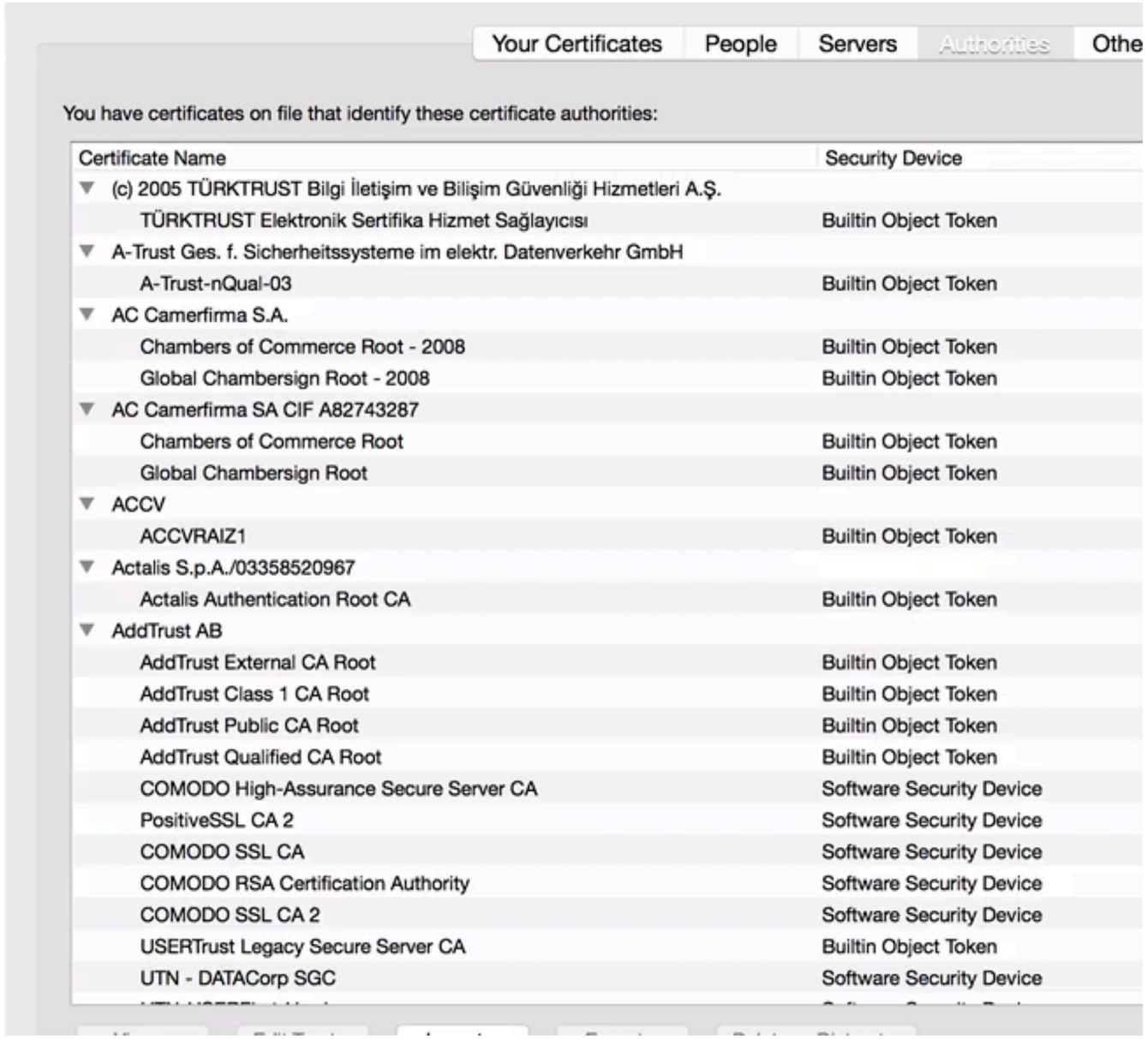
Uses of DANE

1. Use DANE as a verification mechanism to verify SSL/TLS certificates received over HTTPS for added security
2. Store self-signed X.509 certificates, bypass having to pay a third party*
3. Integrate with Mail Transfer Agents (MTA) to provide seamless, end-to-end email encryption

* Requires smarter applications

Why Verify Certs?

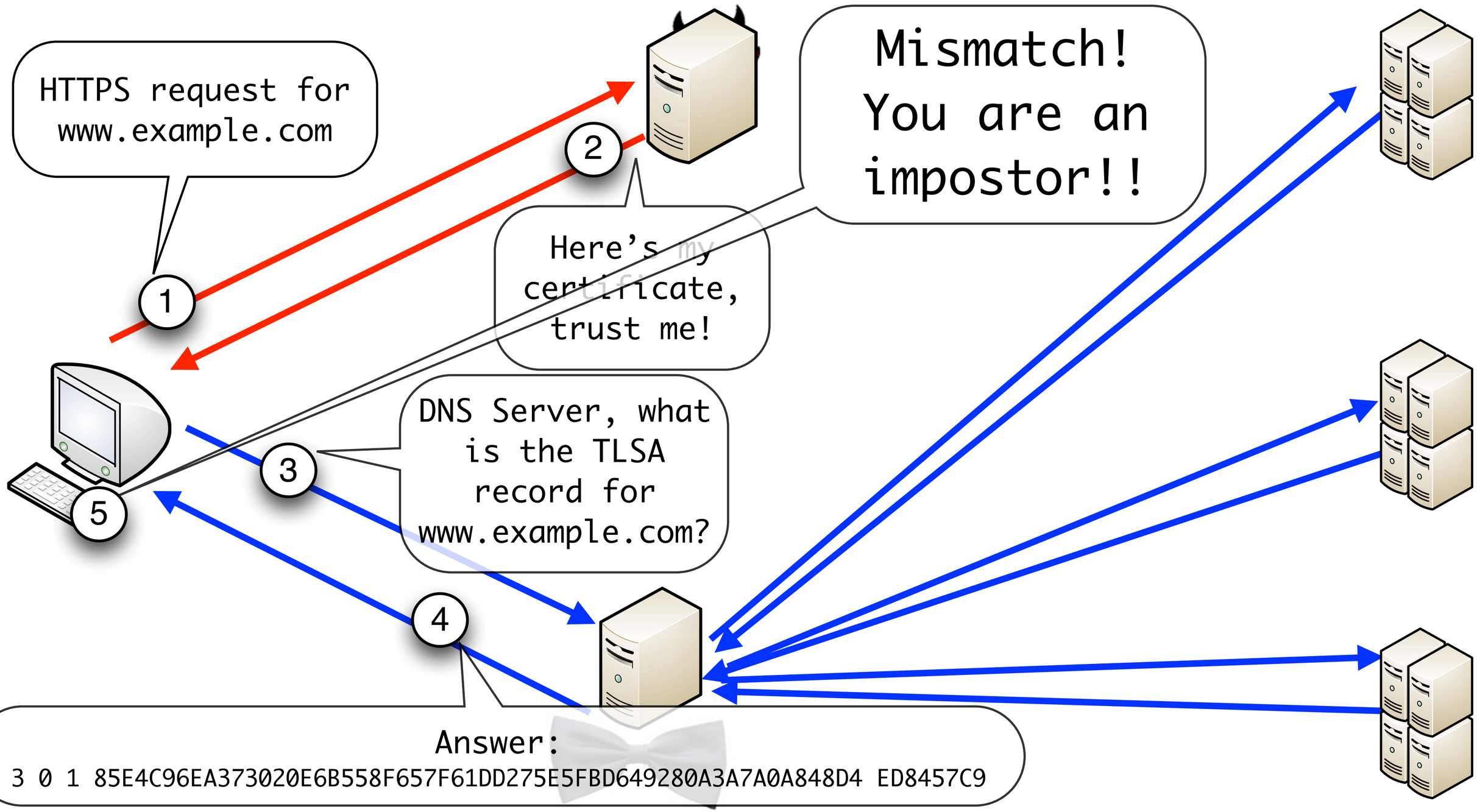
Don’t we trust Certificate Authorities (CA)?



Why Verify Certs?

But if a certificate is “known bad”, we can revoke it, right? Surely our browsers will check that for us, right? Right?

DANE Verification Overview



Self-Signing Certificate with DANE

Limited support today:

- Firefox with a plugin
- Bloodhound Browser (Mozilla)

Resources:

http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html#recipes-tlsa

http://dane.verisignlabs.com

https://www.dnssec-validator.cz/

http://www.ietf.org/mail-archive/web/dane/current/pdfk2DbQF0Oxs.pdf

Automatic Email Encryption with DANE

- Leveraging DANE, MTA (email server) can encrypt an email before it is sent on the wire
- Postfix 2.11.1 supports opportunistic encryption using OpenPGP keys published in DNS as TLSA records
- Still in draft status

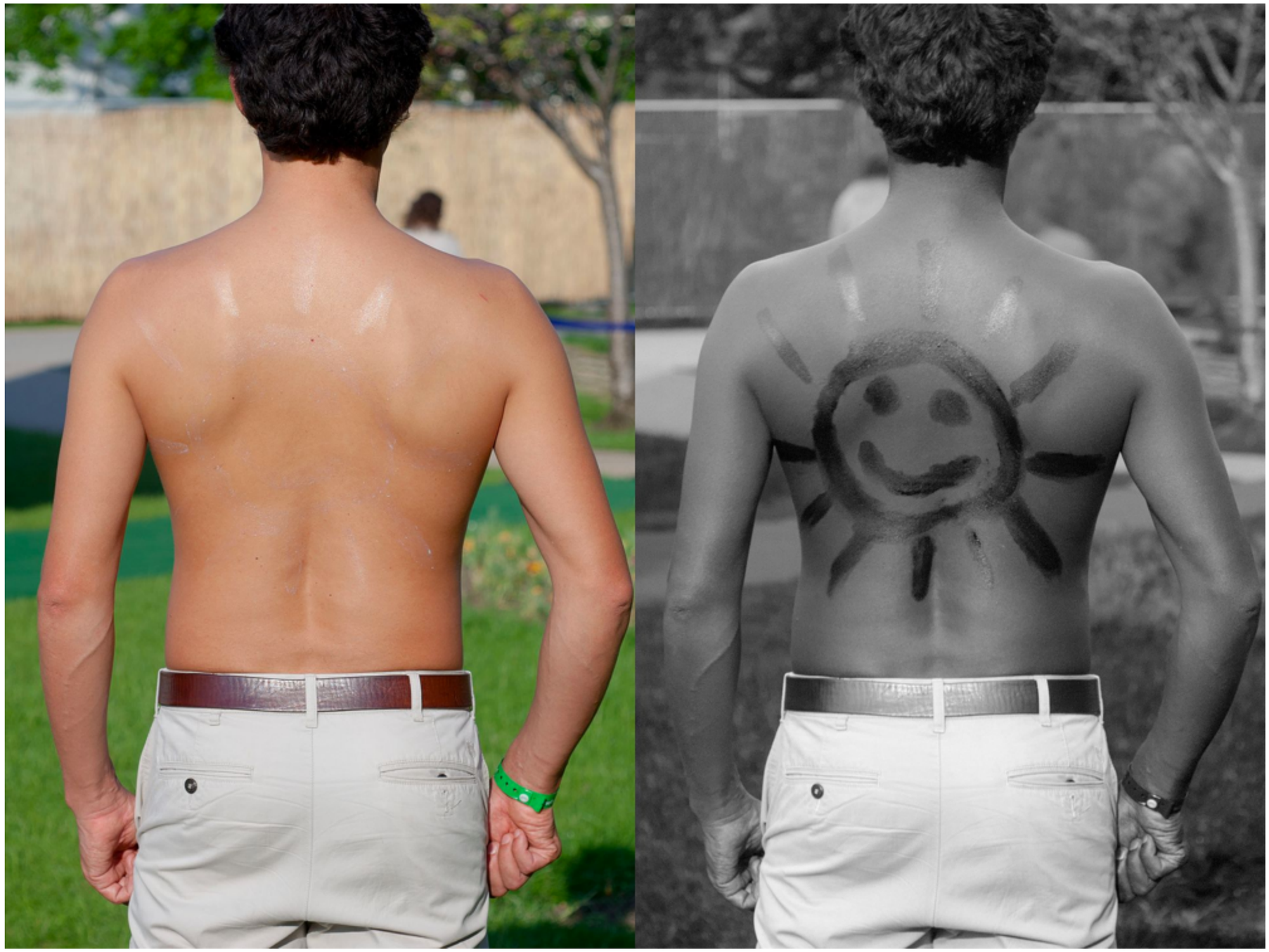
  https://tools.ietf.org/html/draft-wouters-dane-openpgp-02

Other Similar Record Types

Other DNS Resource Records that work similarly to DANE (TLSA):

1. SSHFP (RFC 4255)
2. IPSECKEY (RFC 4025)
3. TXT Record (Spam Detection):
    1. SPF (http://www.openspf.org/)
    2. DKIM (http://www.opendkim.org/)
    3. DMARC (http://dmarc.org)

SPF Example



SPF Example

```
example.com.  3600  IN  TXT  "v=spf1 mx ip4:45.0.0.0/15 -all”
```

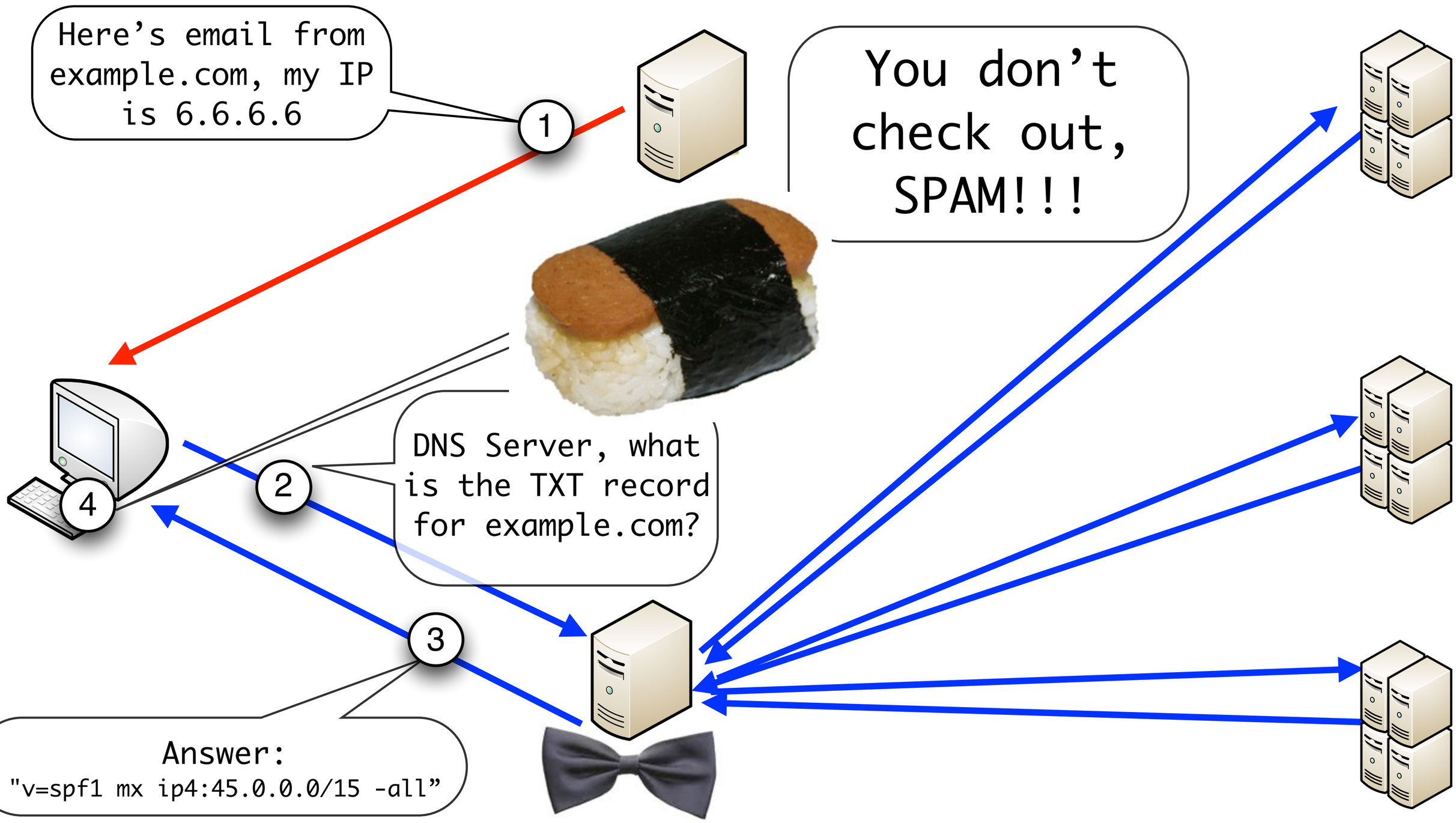
spf1 = SPF version

mx = whatever I have listed in my MX records

ip4:45.0.0.0/15 = email from this network is ok

-all = fail everyone else

SPF Example

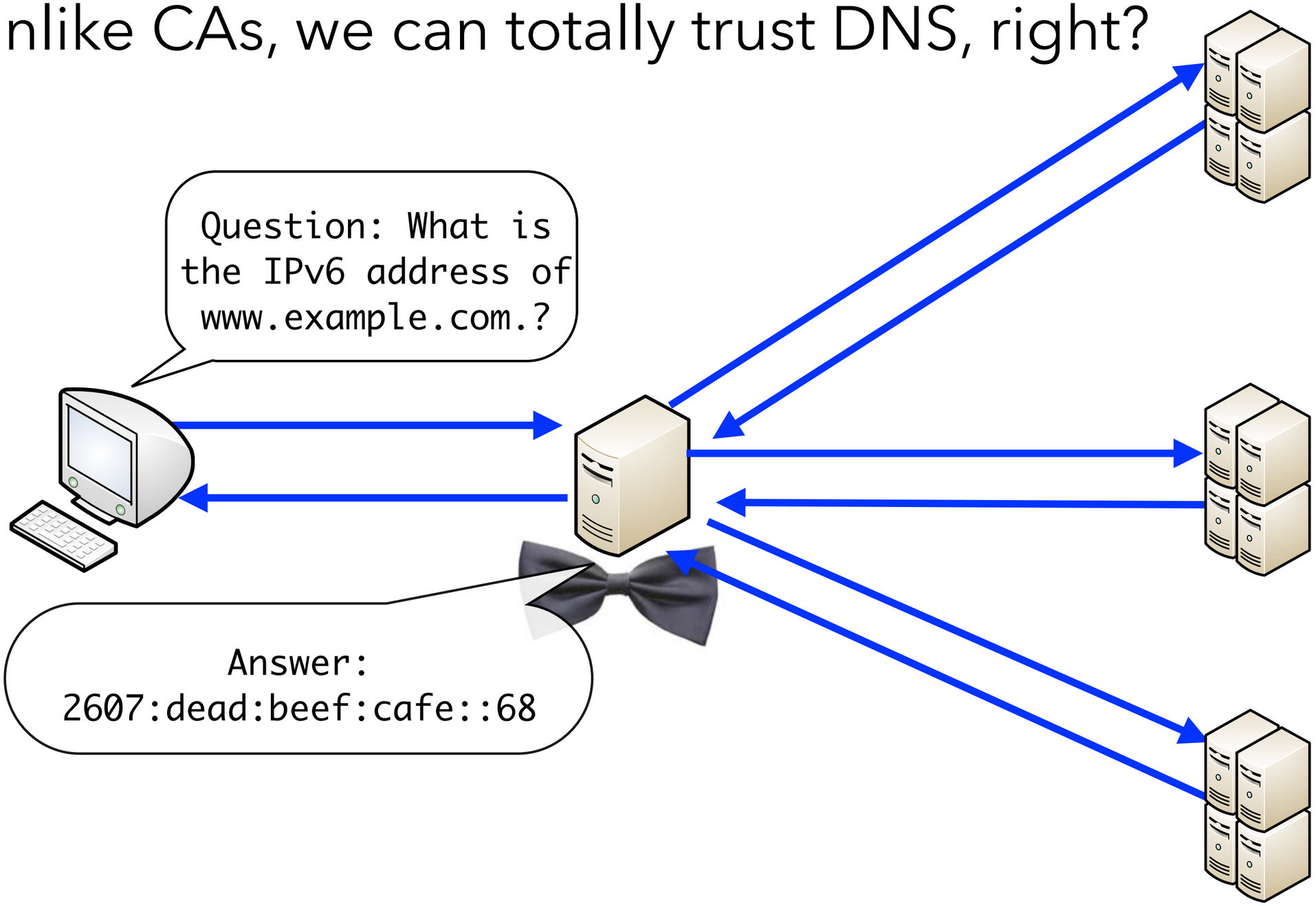

Here's email from example.com, my IP is 6.6.6.6
1
You don't check out, SPAM!!!
DNS Server, what is the TXT record for example.com?
2
3
4
Answer:
"v=spf1 mx ip4:45.0.0.0/15 -all"

Hey, I can store that in…

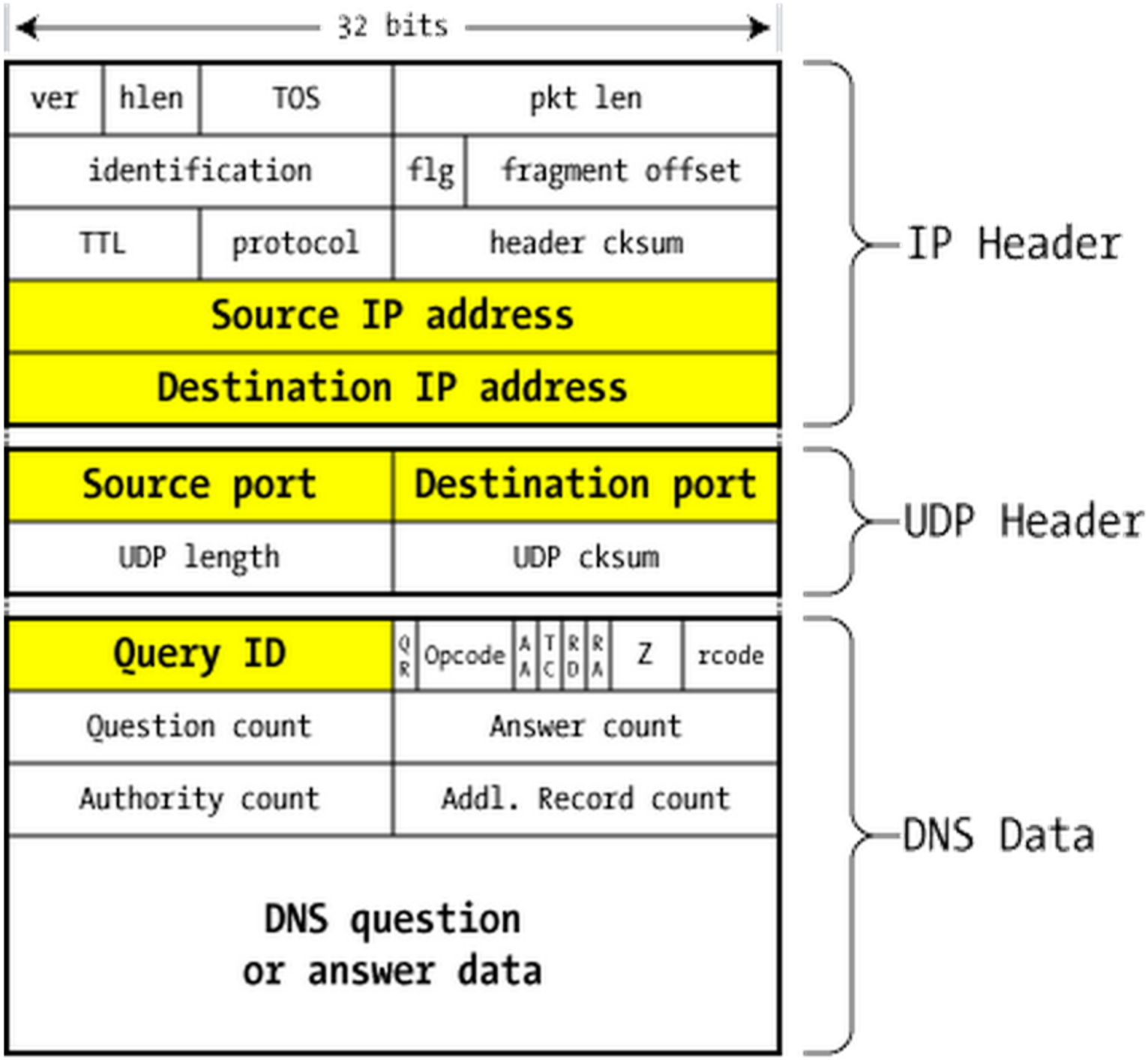
F**k it, it's in DNS now.

Trusting DNS

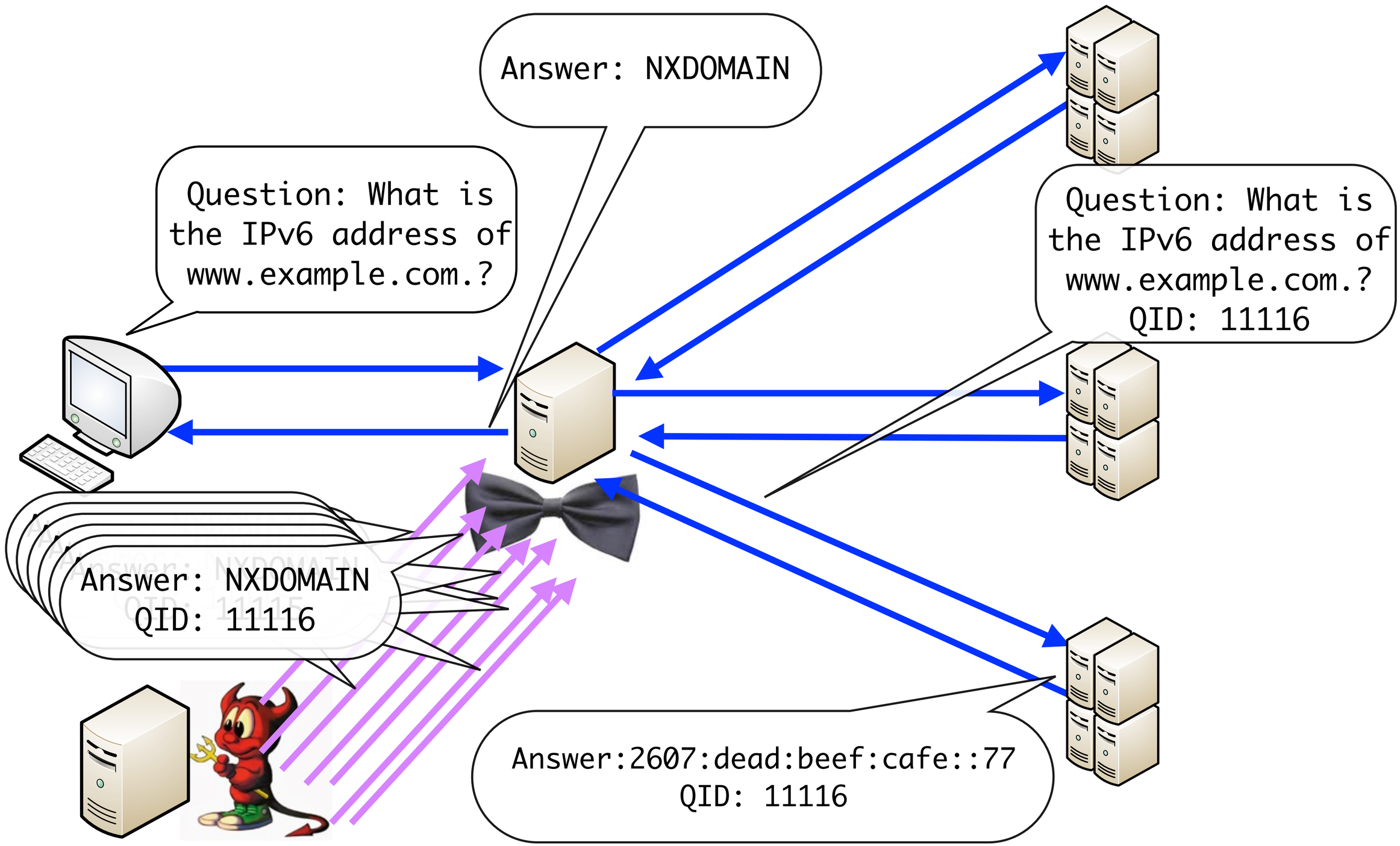
But unlike CAs, we can totally trust DNS, right?



Trusting DNS



Trusting DNS



DNSSEC provides:

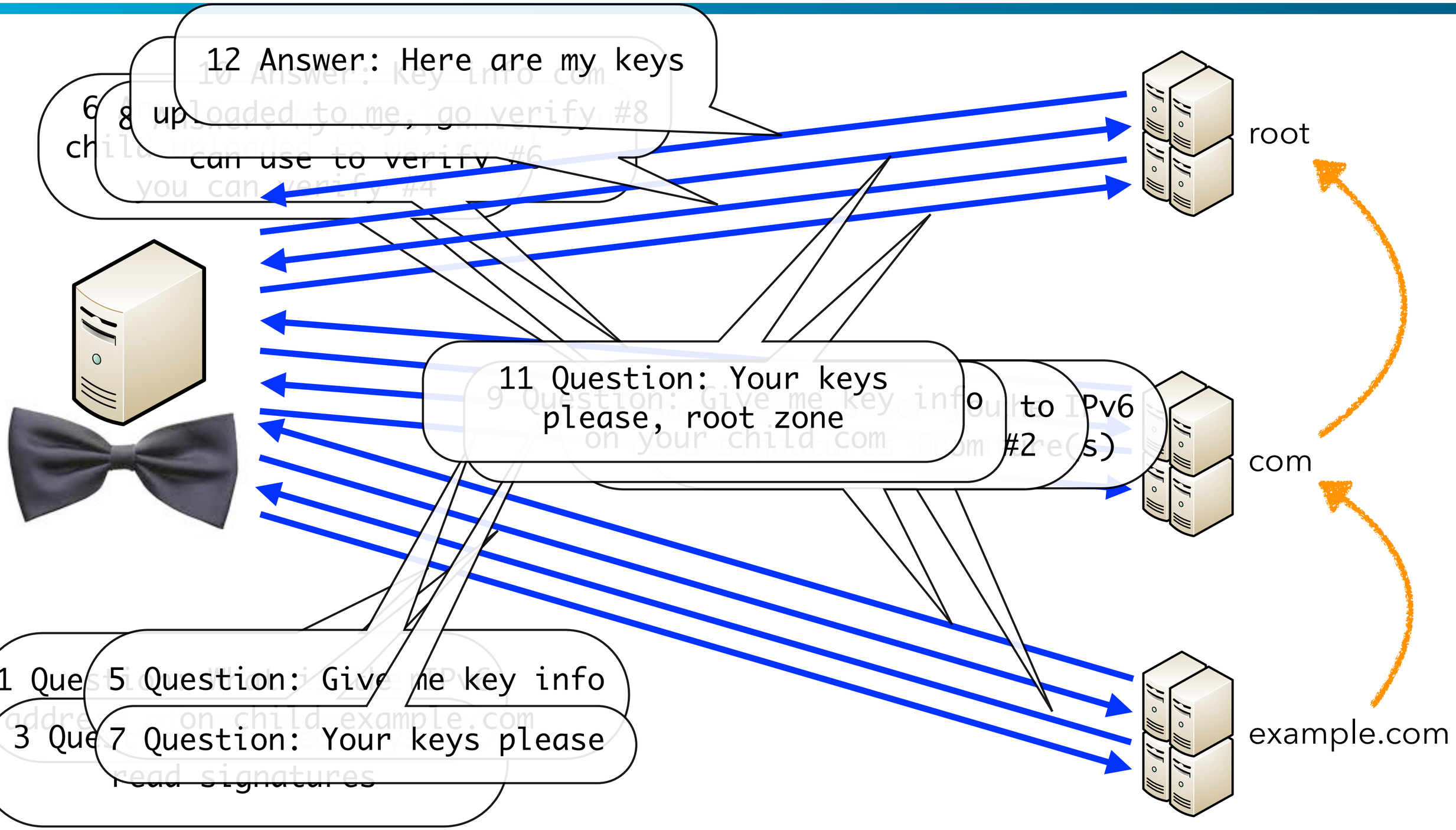
1. Authentication
2. Data Integrity
3. Proof of non-existence

RFC 4034, 4034, and 4035 outline the basics

Uses public key crypto and digital signatures

But not data privacy, no encryption!

DNSSEC 12-Step Program



Network Requirements for DNSSEC

- DNS server supports EDNS0 (large UDP packets)
- Network gear *not* drop large DNS packets (larger than 1500 bytes typically)
- Network is aware of DNS over TCP

How Do I Know I Have DNSSEC?

- Recursive servers, look for **`ad`** flag in returned header (ad = authenticated data)

```
dig @4.2.2.2 www.isc.org. A
dig @8.8.8.8 www.isc.org. A
```

- Authoritative servers, use **`dig +dnssec`**

```
dig enet.interop.net. SOA +dnssec
```

That's right, Google has been providing DNSSEC validation since 2013.

Challenges of DNSSEC

- Perception: it's DNS with crypto, it's hard!
- It will break lookups! (8.8.8.8)
- Does not solve last mile problem (yet)
- No incentives, maybe PCIDSS will fix that
- We need to reach critical mass like .gov

Work in Progress

- DANE working group

  https://datatracker.ietf.org/wg/dane/

- DNS Private Exchange working group

  http://datatracker.ietf.org/wg/dprive/