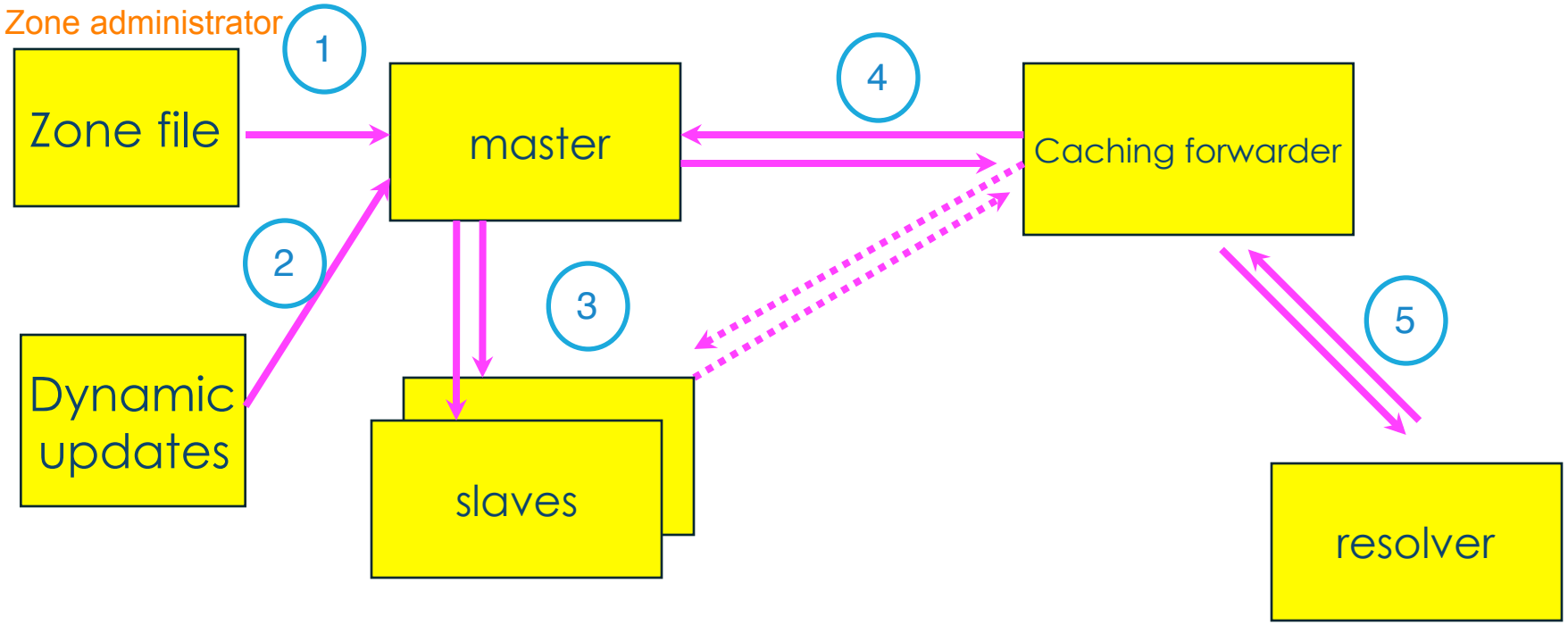
DNS Security and DNSSEC

Champika Wijayatunga | Mumbai - India | 10 August 2015

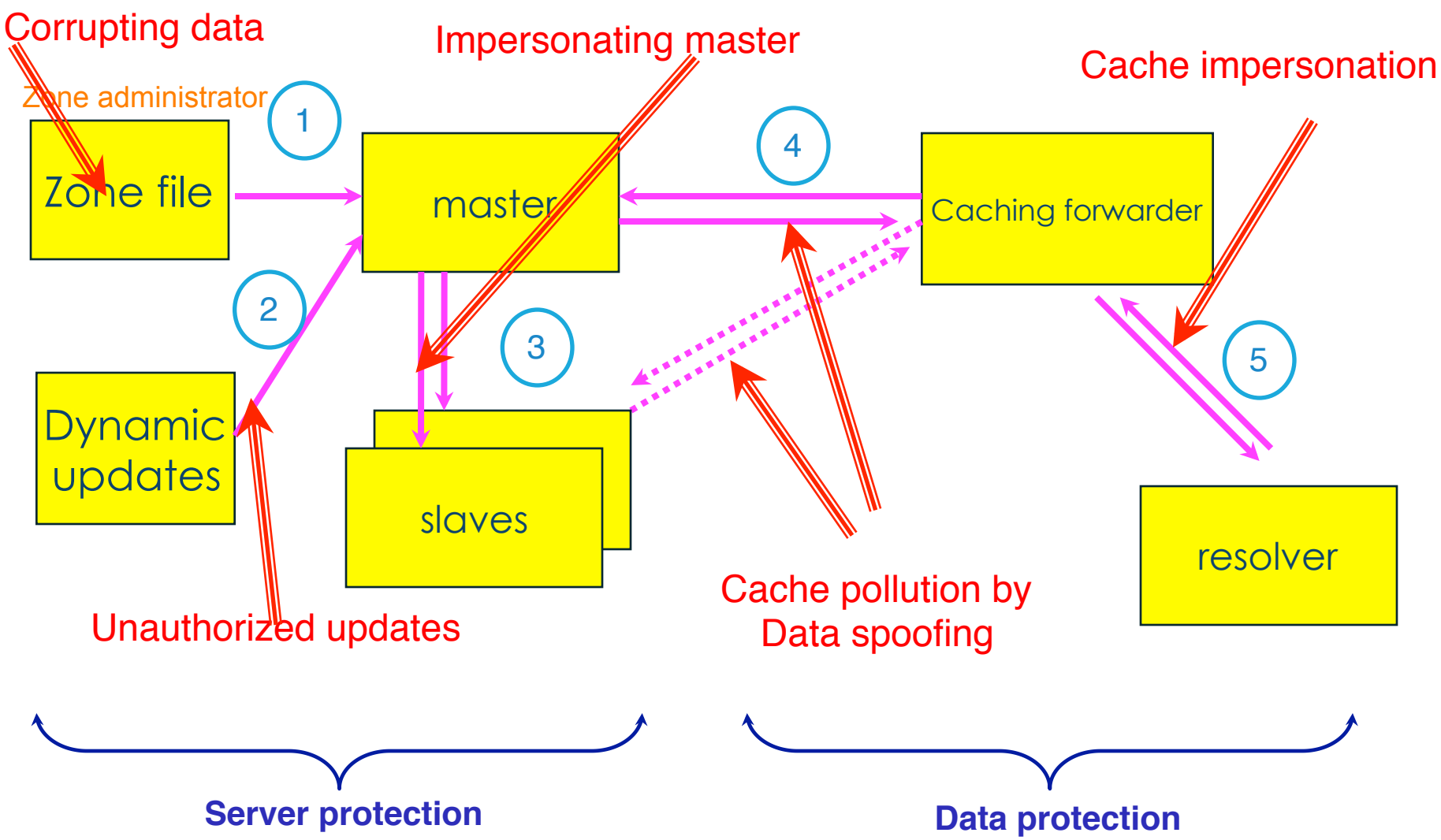
DNS Protocol Vulnerability

- DNS data can be spoofed and corrupted between master server and resolver or forwarder
- The DNS protocol does not allow you to check the validity of DNS data
  - Exploited by bugs in resolver implementation (predictable transaction ID)
  - Polluted caching forwarders can cause harm for quite some time (TTL)
  - Corrupted DNS data might end up in caches and stay there for a long time
- How does a slave (secondary) know it is talking to the proper master (primary)?

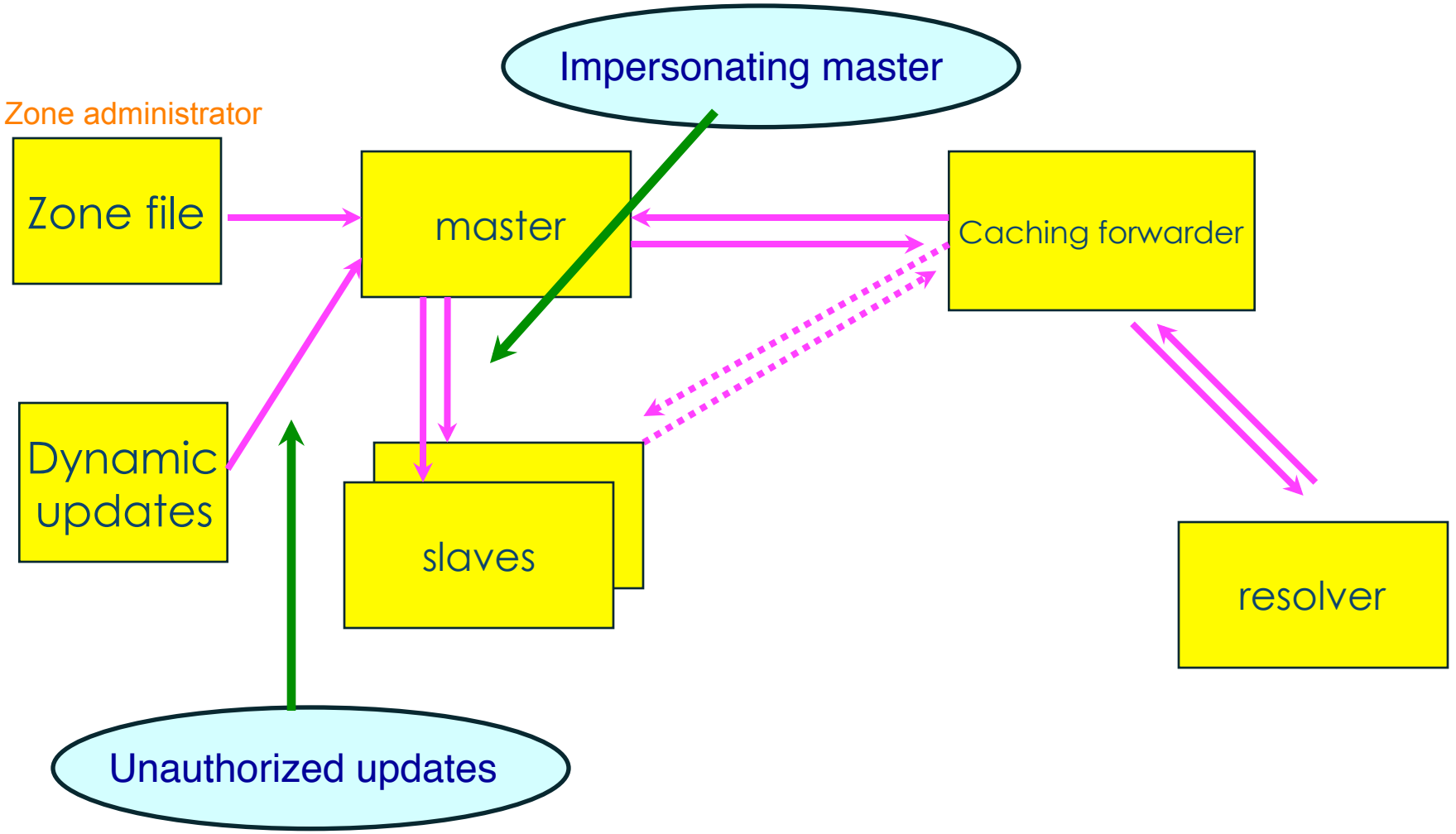
DNS Data Flow



DNS Data Flow



DNS Data Flow



What is TSIG - Transaction Signature?

- A mechanism for protecting a message from a primary to secondary and vice versa
- A keyed-hash is applied (like a digital signature) so recipient can verify the message
  - DNS question or answer
  - & the timestamp
- Based on a shared secret - both sender and receiver are configured with it
  - TSIG/TKEY uses DH, HMAC-MD5, HMAC-SHA1, HMAC-SHA224, HMAC-SHA512 among others

What is TSIG - Transaction Signature?

- TSIG (RFC 2845)
  - authorizing dynamic updates & zone transfers
  - authentication of caching forwarders
- Used in server configuration, not in zone file

TSIG Steps

1. Generate secret
2. Communicate secret
3. Configure servers
4. Test

TSIG - Names and Secrets

- TSIG name
  - A name is given to the key, the name is what is transmitted in the message (so receiver knows what key the sender used)
- TSIG secret value
  - A value determined during key generation
  - Usually seen in Base64 encoding

TSIG – Generating a Secret

- dnssec-keygen
  - Simple tool to generate keys
  - Used here to generate TSIG keys

```
> dnssec-keygen -a <algorithm> -b
  <bits> -n host <name of the key>
```

TSIG – Generating a Secret

- **Example**

```
> dnssec-keygen -a HMAC-MD5 -b 128 -n HOST ns1-
  ns2.pcx.net

This will generate the key
> Kns1-ns2.pcx.net.+157+15921

>ls
Kns1-ns2.pcx.net.+157+15921.key
Kns1-ns2.pcx.net.+157+15921.private
```

TSIG – Generating a Secret

- TSIG should never be put in zone files
  - might be confusing because it looks like RR:

```
ns1-ns2.pcx.net. IN KEY 128 3 157 nEfRX9…bbPn7lyQtE=
```

TSIG – Configuring Servers

- Configuring the key
  - in named.conf file, same syntax as for rndc
  - `key { algorithm ...; secret ...;}`
- Making use of the key
  - in named.conf file
  - `server x { key ...; }`
  - where 'x' is an IP number of the other server

Configuration Example – named.conf

Primary server 10.33.40.46

```
key ns1-ns2.pcx. net {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.50.35 {
    keys {ns1-ns2.pcx.net;};
};
zone "my.zone.test." {
    type master;
    file “db.myzone”;
    allow-transfer {
    key ns1-ns2.pcx.net ;};
};
```

Secondary server 10.33.50.35

```
key ns1-ns2.pcx.net {
    algorithm hmac-md5;
    secret "APlaceToBe";
};
server 10.33.40.46 {
  keys {ns1-ns2.pcx.net;};
};
zone "my.zone.test." {
    type slave;
    file “myzone.backup”;
    masters {10.33.40.46;};
};
```

You can save this in a file and refer to it in the named.conf using ‘include’ statement:

```
include “/var/named/master/tsig-key-ns1-ns2”;
```

TSIG Testing: dig

- You can use dig to check TSIG configuration
  - `dig @<server> <zone> AXFR -k <TSIG keyfile>`

```
$ dig @127.0.0.1 example.net AXFR \
    -k Kns1-ns2.pcx.net.+157+15921.key
```

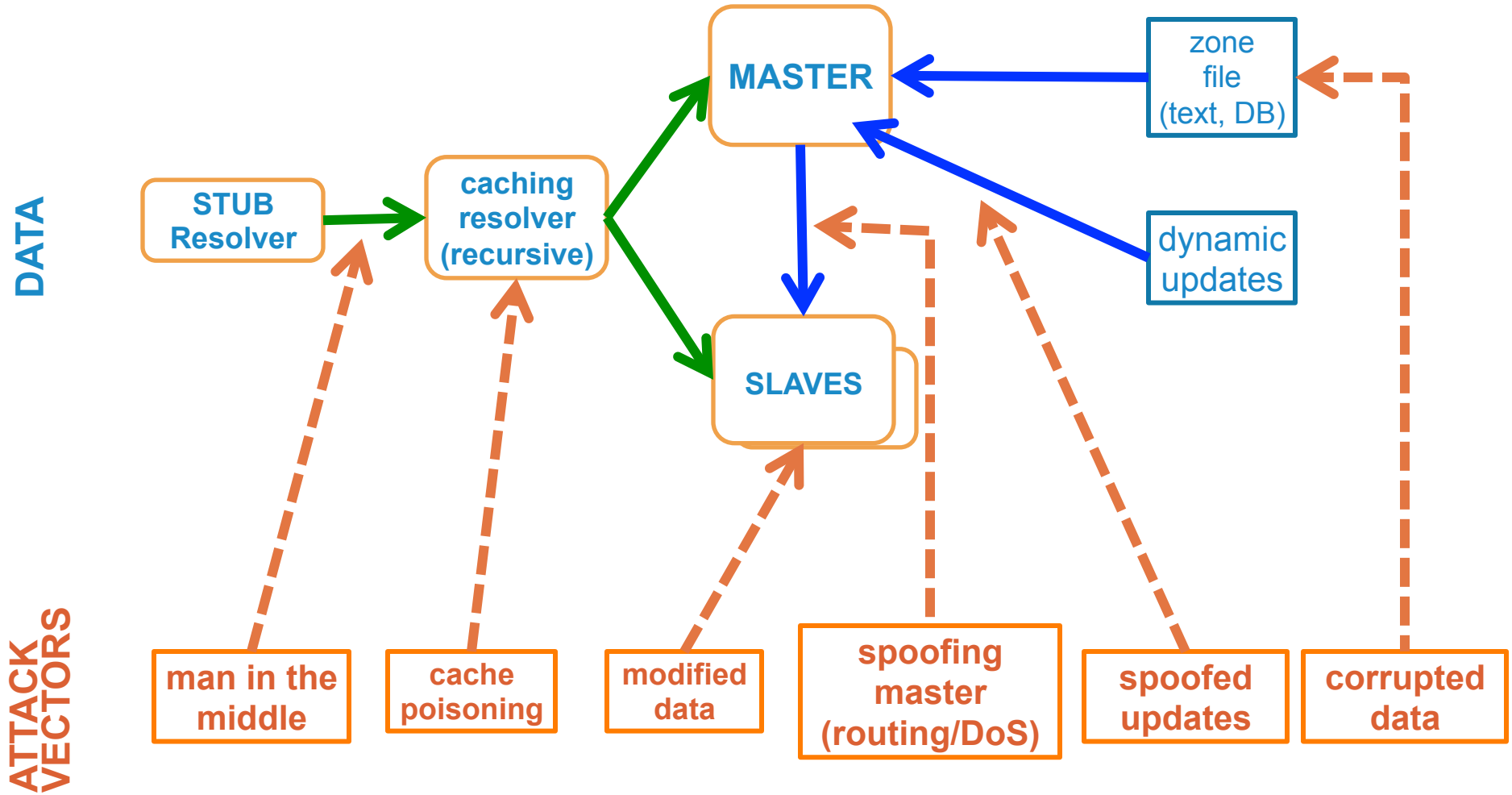
- Wrong key will give “Transfer failed” and on the server the security-category will log this.

TSIG Testing - TIME!

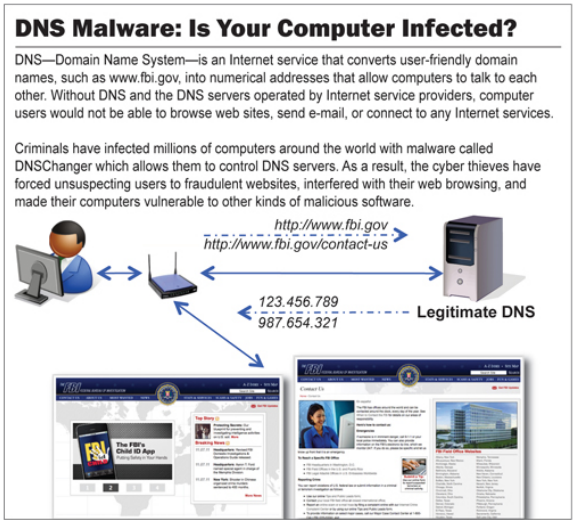
- TSIG is time sensitive - to stop replays
  - Message protection expires in 5 minutes
  - Make sure time is synchronized
  - For testing, set the time
  - In operations, (secure) NTP is needed


Why DNSSEC?

DNS Data Flow



The Bad



- DNSChanger*
  - Biggest Cybercriminal Takedown in History
  - 4M machines, 100 countries, $14M
- And many other DNS hijacks in recent times**
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

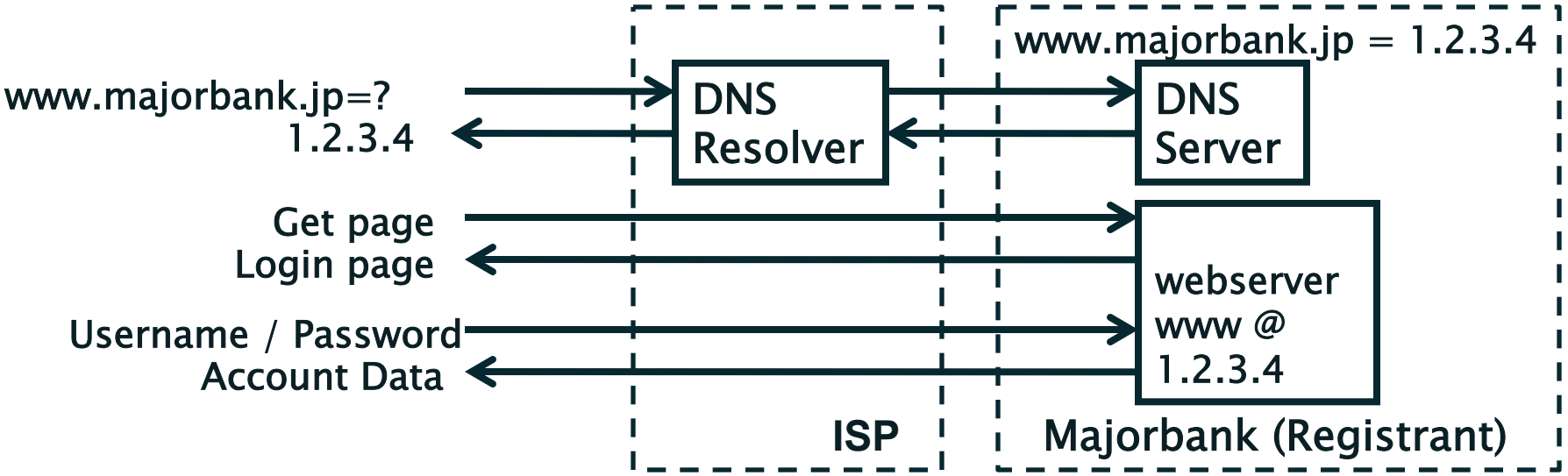
DigiNotar® A VASCO COMPANY

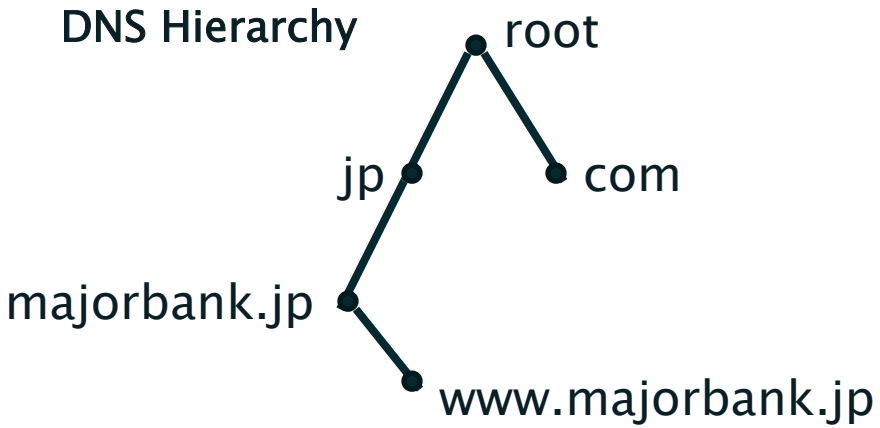
*** http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911**

End-2-end DNSSEC validation would have avoided the problems

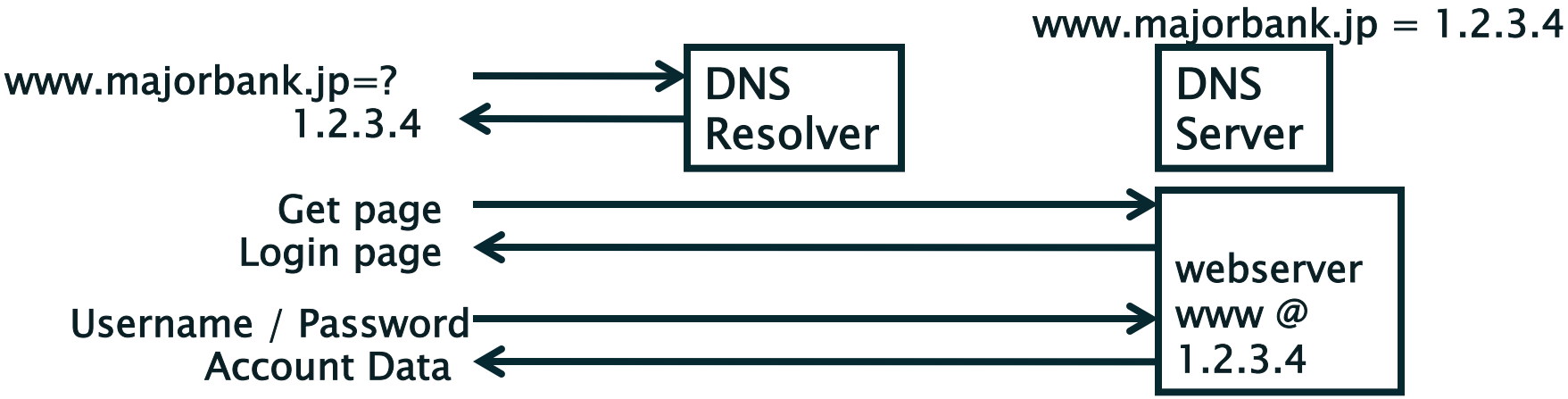
**** A Brief History of DNS Hijacking - Google**
http://costarica43.icann.org/meetings/sanjose2012/presentation-dns-hijackings-marquis-boire-12mar12-en.pdf

The Internet's Phone Book - Domain Name System

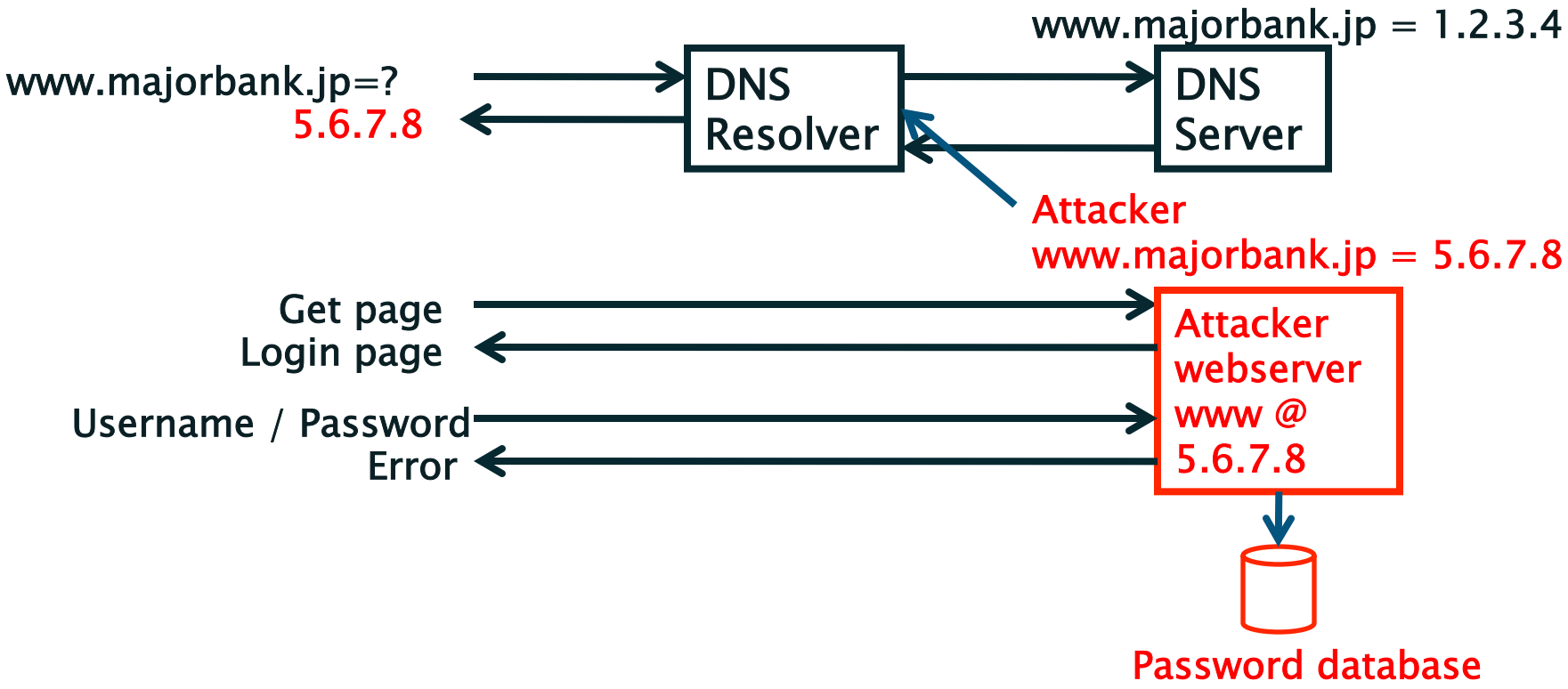




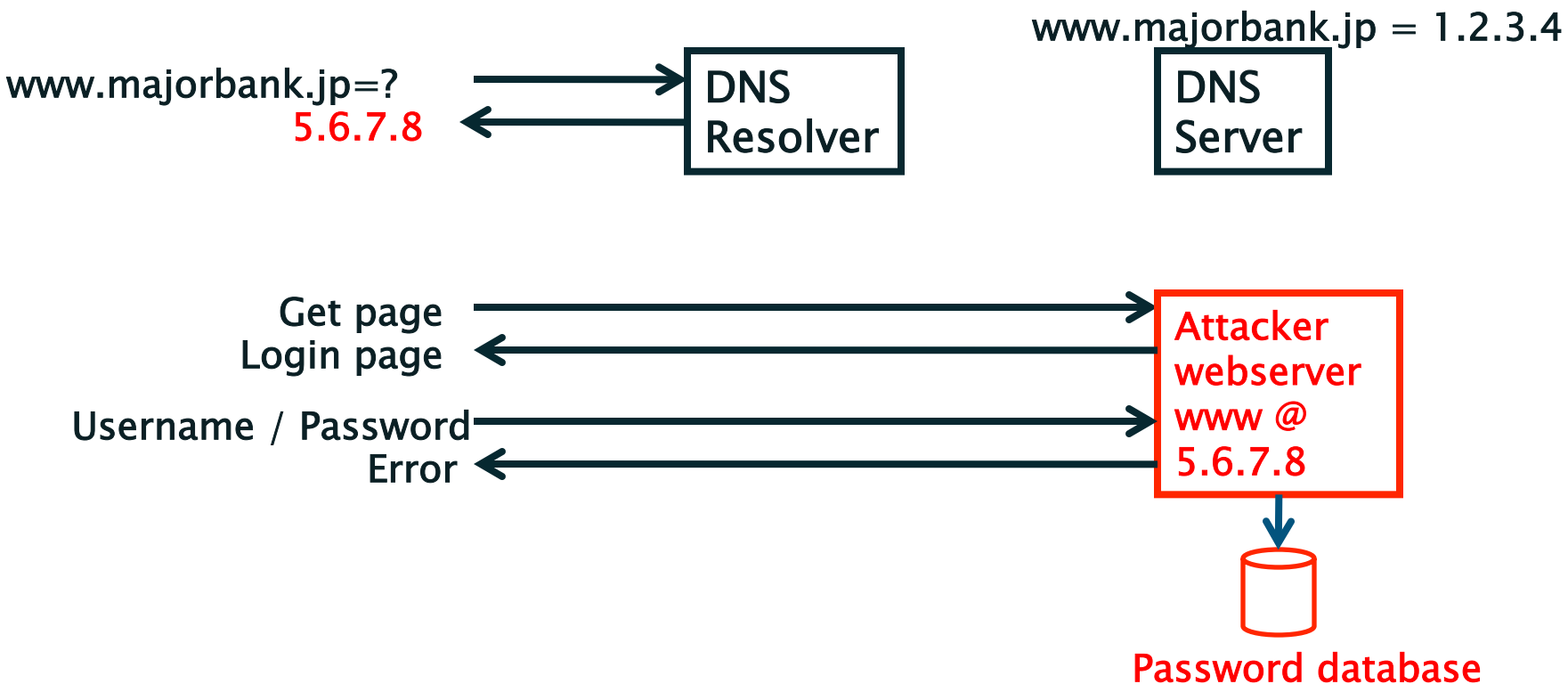
Caching Responses for Efficiency



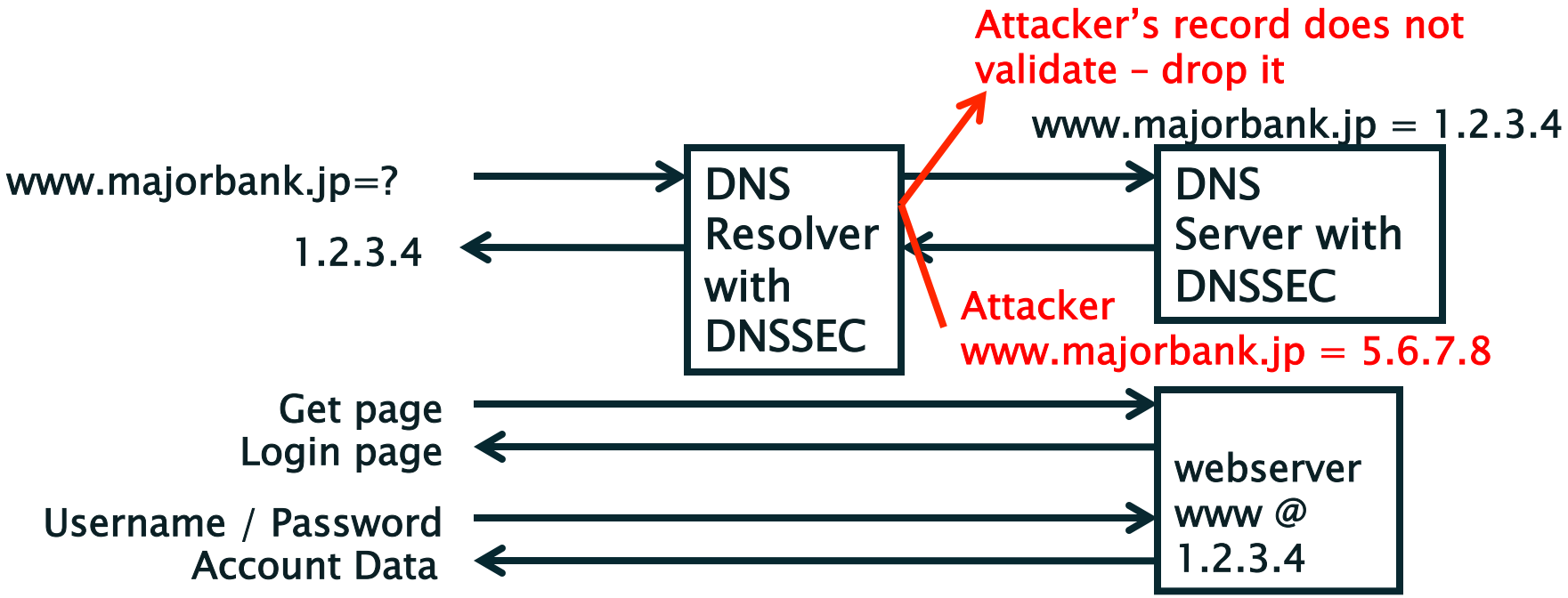
The Problem: DNS Cache Poisoning Attack



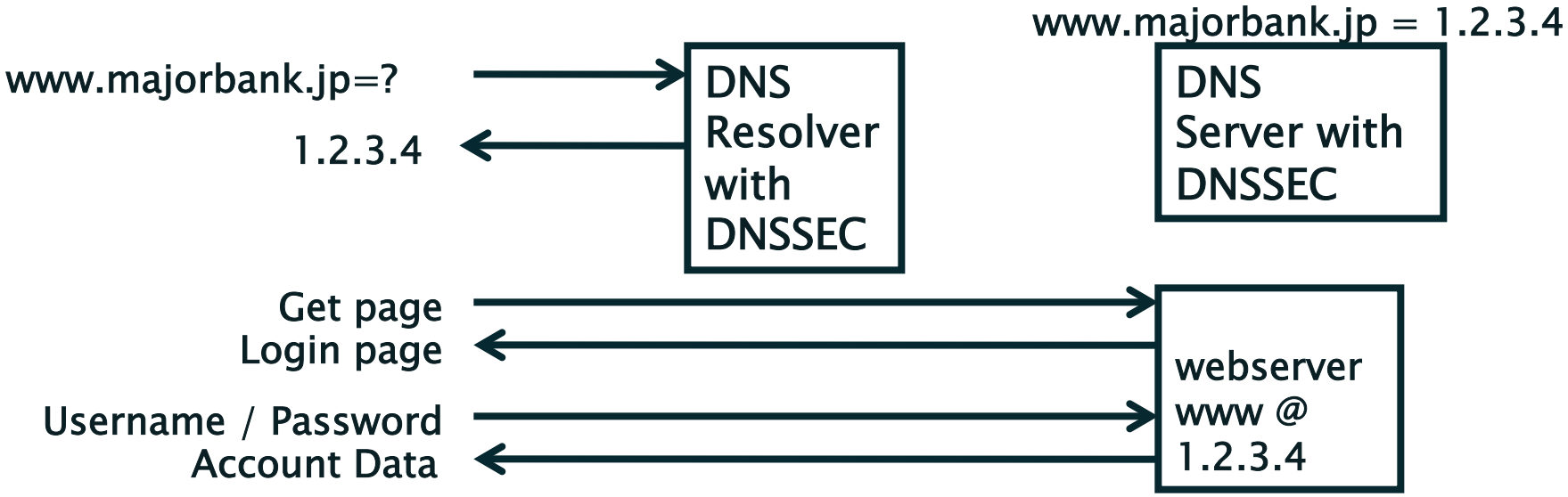
Now all ISP customers get sent to attacker…



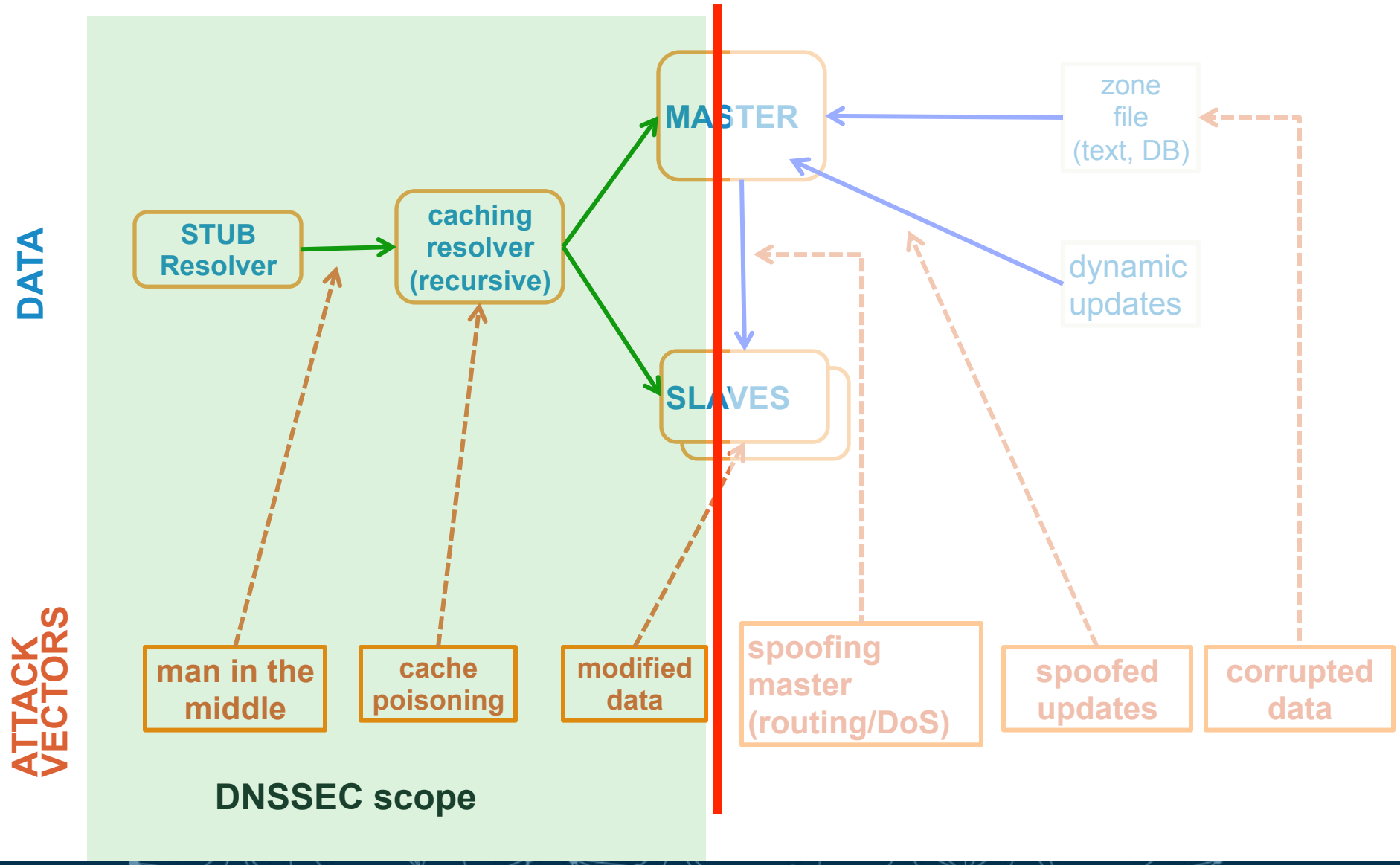
Securing The Phone Book - DNS Security Extensions (DNSSEC)



Resolver only caches validated records



What DNSSEC solves and what's not

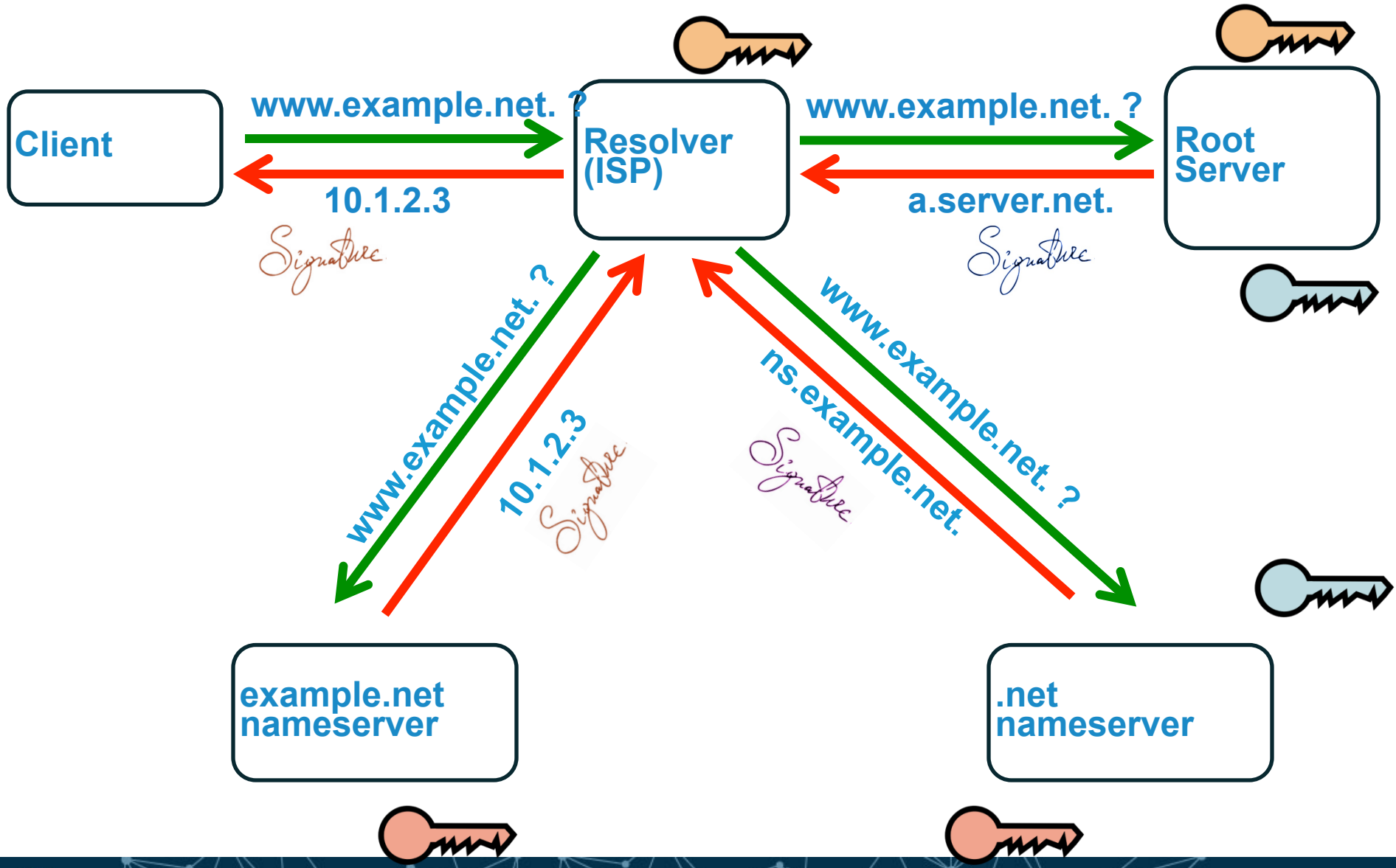


Brief reminder on Cryptography

- Nowadays most of our Security Services are based in one (or a combination) of the following areas:
  - One-way hash functions
  - Symmetric key crypto
  - Public-key crypto (or asymmetric)


How DNSSEC Works?

How DNSSEC Works



How DNSSEC Works

- Data authenticity and integrity by signing the Resource Records Sets with a private key
- Public DNSKEYs published, used to verify the RRSIGs
- Children sign their zones with their private key
  - Authenticity of that key established by parent signing hash (DS) of the child zone's key
- Repeat for parent…
- Not that difficult on paper
  - Operationally, it is a bit more complicated
  - $DS_{KEY} \rightarrow$ KEY –signs→ zone data

The Business Case for DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.

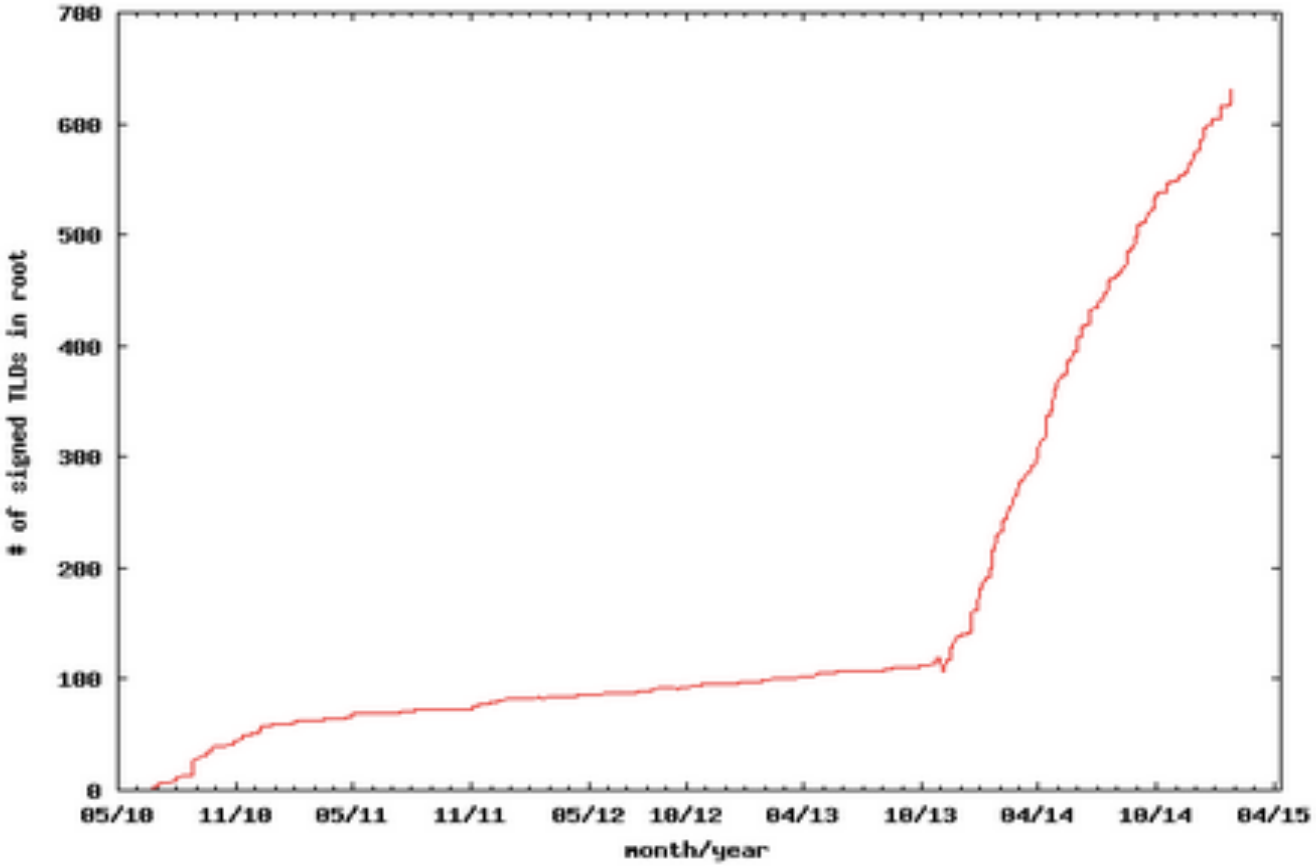
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

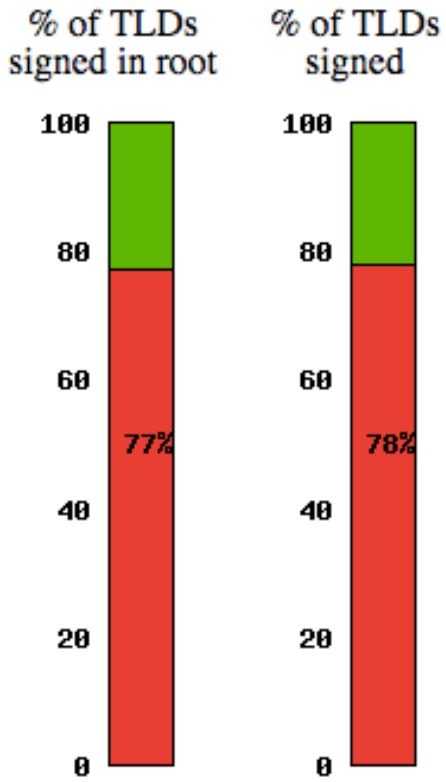
- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC ccTLD Map

https://rick.eng.br/dnssecstat/

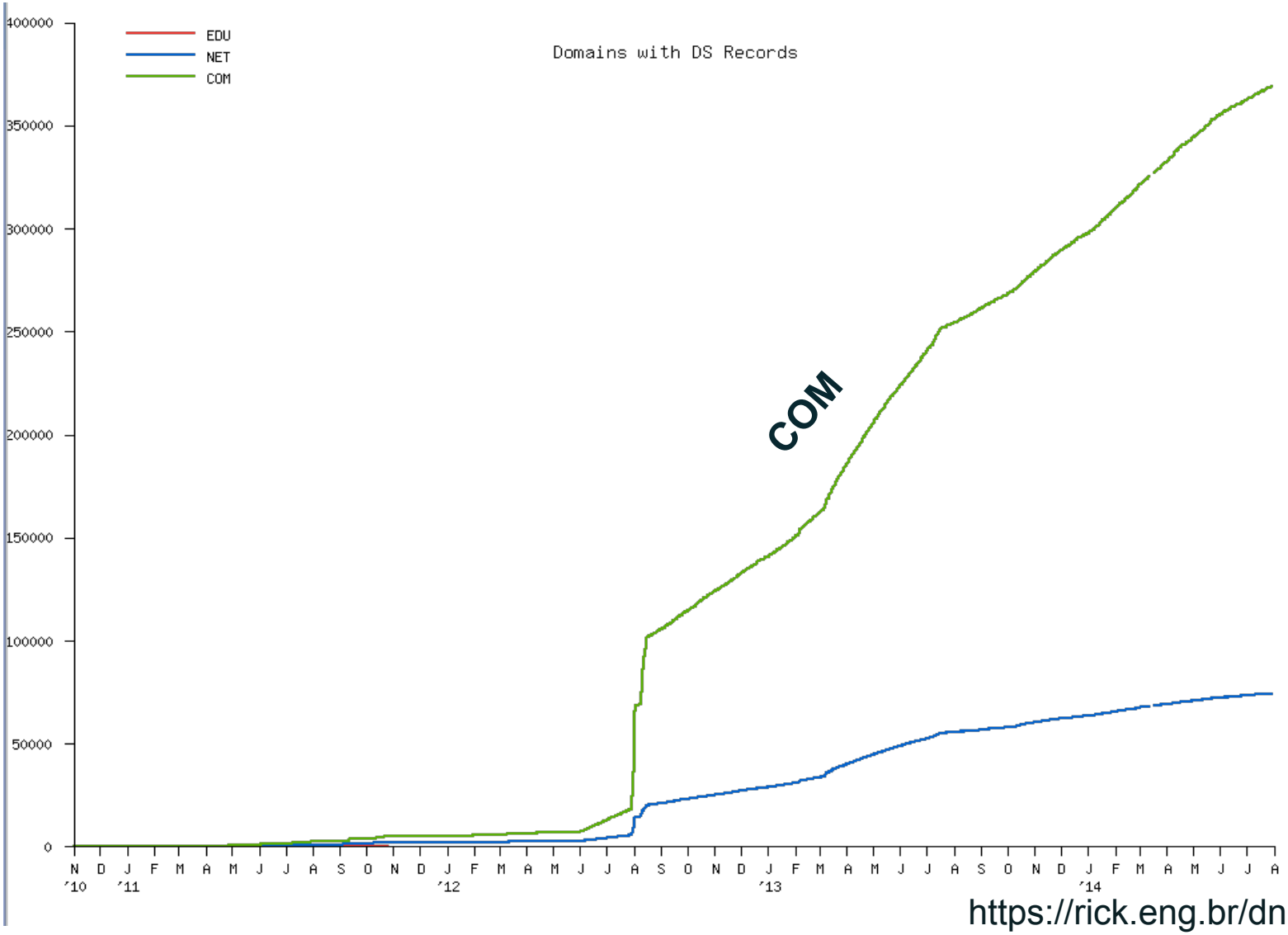
DNSSEC TLDs





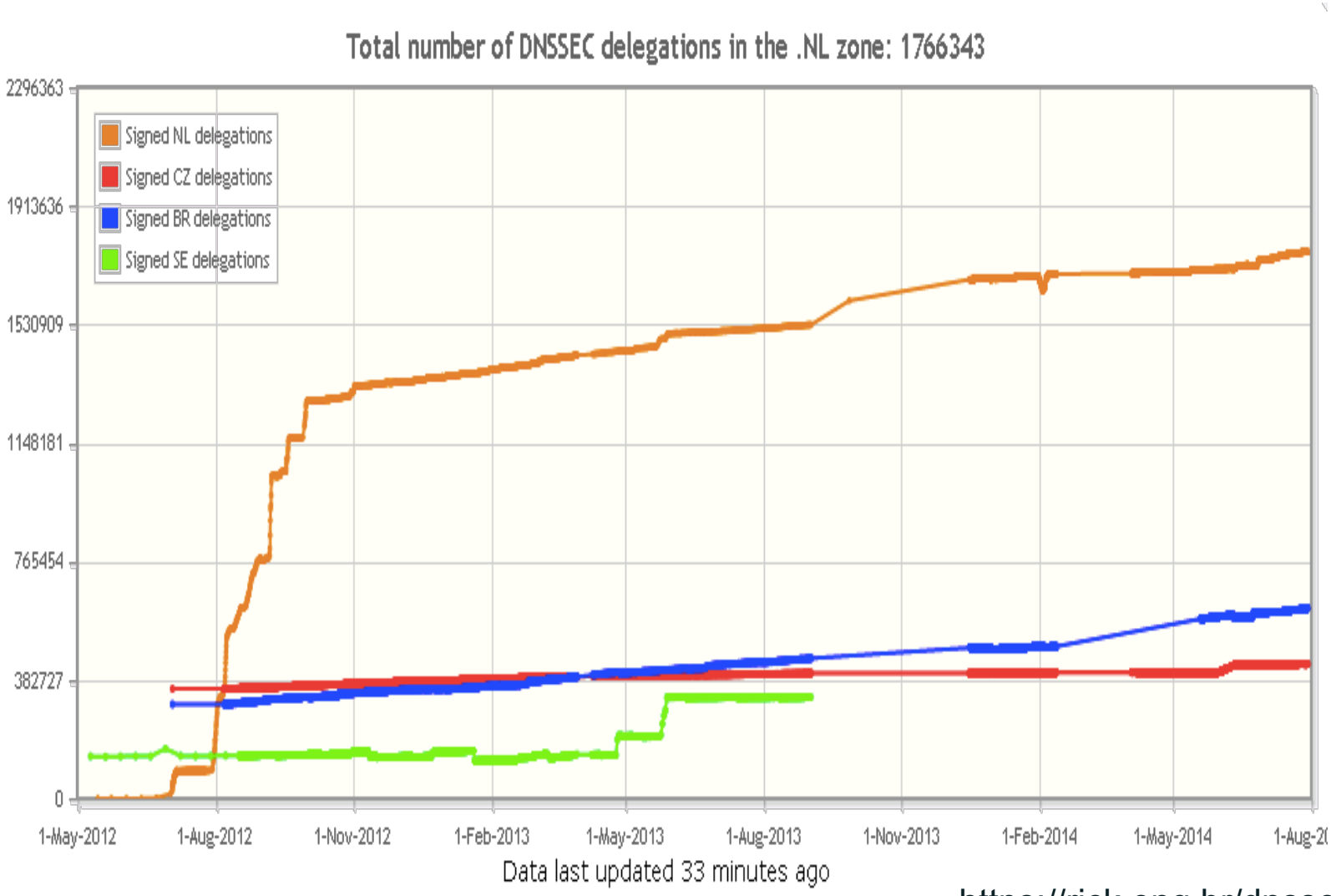
https://rick.eng.br/dnssecstat/

Domains with DS records



https://rick.eng.br/dnssecstat/

DNSSEC delegations in some ccTLD zones



https://rick.eng.br/dnssecstat/

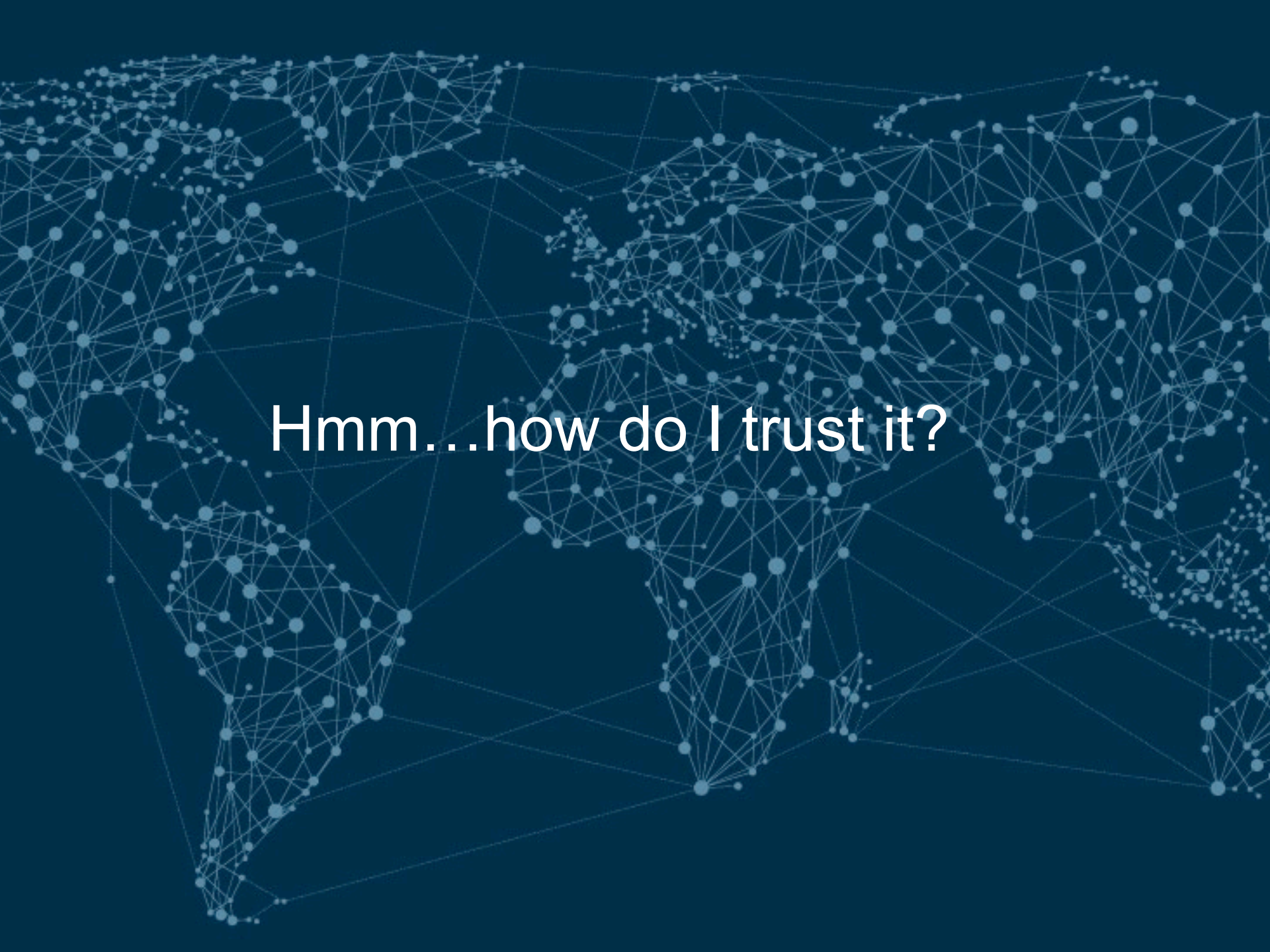
DNSSEC: So what's the problem?

- Not enough IT departments know about it or are too busy putting out other security fires.
- When they do look into it they hear old stories of FUD and lack of turnkey solutions.
- Registrars*/DNS providers see no demand leading to "chicken-and-egg" problems.

*but required by new ICANN registrar agreement

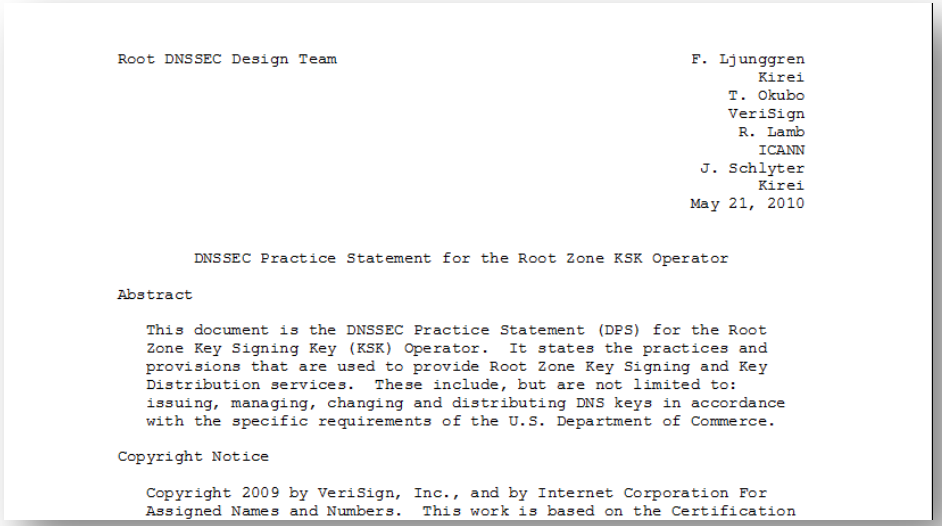
What you can do

- ***For Companies:***
  - Sign your corporate domain names
  - Just turn on validation on corporate DNS resolvers
- ***For Users:***
  - Ask ISP to turn on validation on their DNS resolvers
- ***For All:***
  - Take advantage of DNSSEC education and training


Hmm…how do I trust it?

ICANN DNSSEC Deployment @Root

- Multi-stakeholder, bottom-up trust model* /w 21 crypto officers from around the world
- Broadcast Key Ceremonies and public docs



Root DNSSEC Design Team

F. Ljunggren
Kirei
T. Okubo
VeriSign
R. Lamb
ICANN
J. Schlyter
Kirei
May 21, 2010

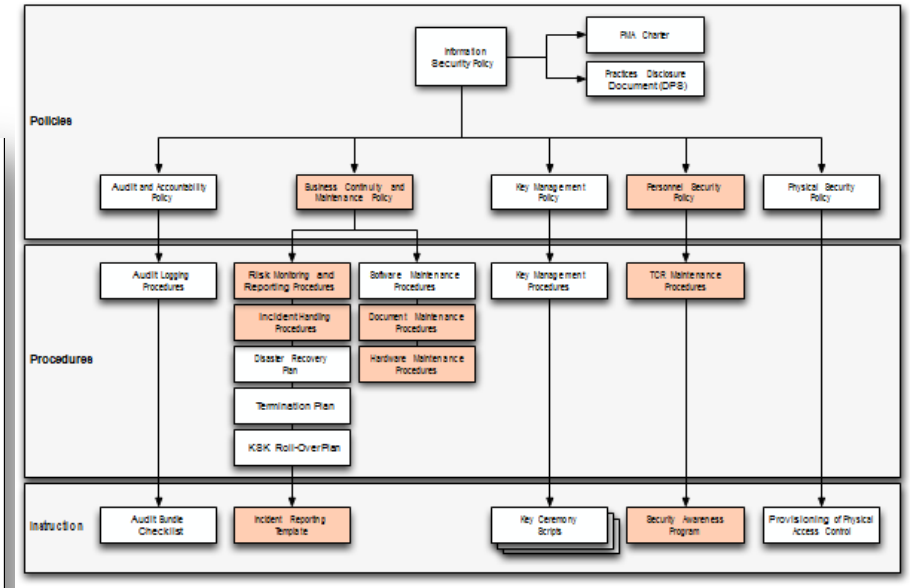
DNSSEC Practice Statement for the Root Zone KSK Operator

Abstract

This document is the DNSSEC Practice Statement (DPS) for the Root Zone Key Signing Key (KSK) Operator. It states the practices and provisions that are used to provide Root Zone Key Signing and Key Distribution services. These include, but are not limited to: issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. Department of Commerce.

Copyright Notice

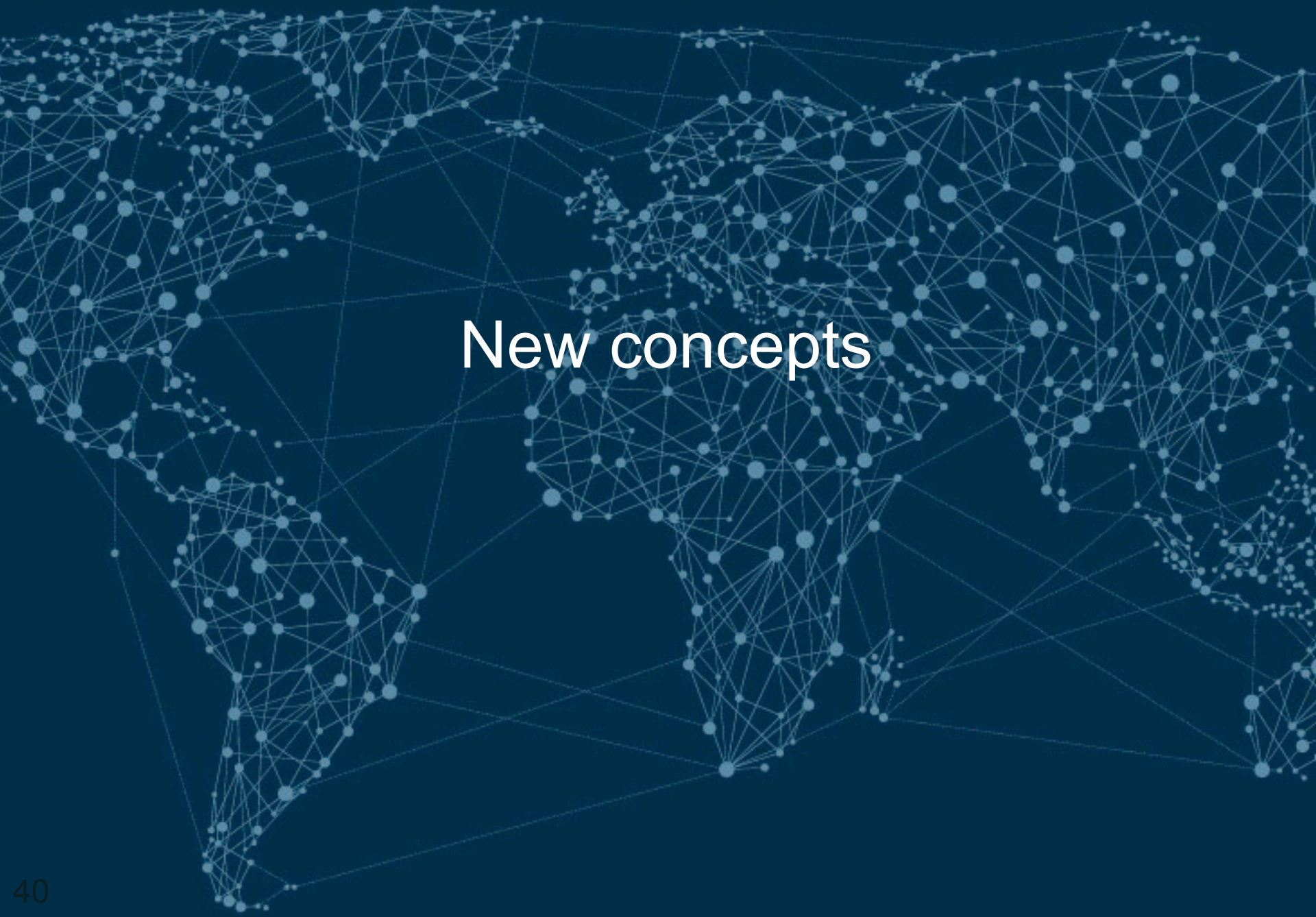
Copyright 2009 by VeriSign, Inc., and by Internet Corporation For Assigned Names and Numbers. This work is based on the Certification



Root DPS

DNSSEC Practice Statement

***Managed by technical community+ICANN**

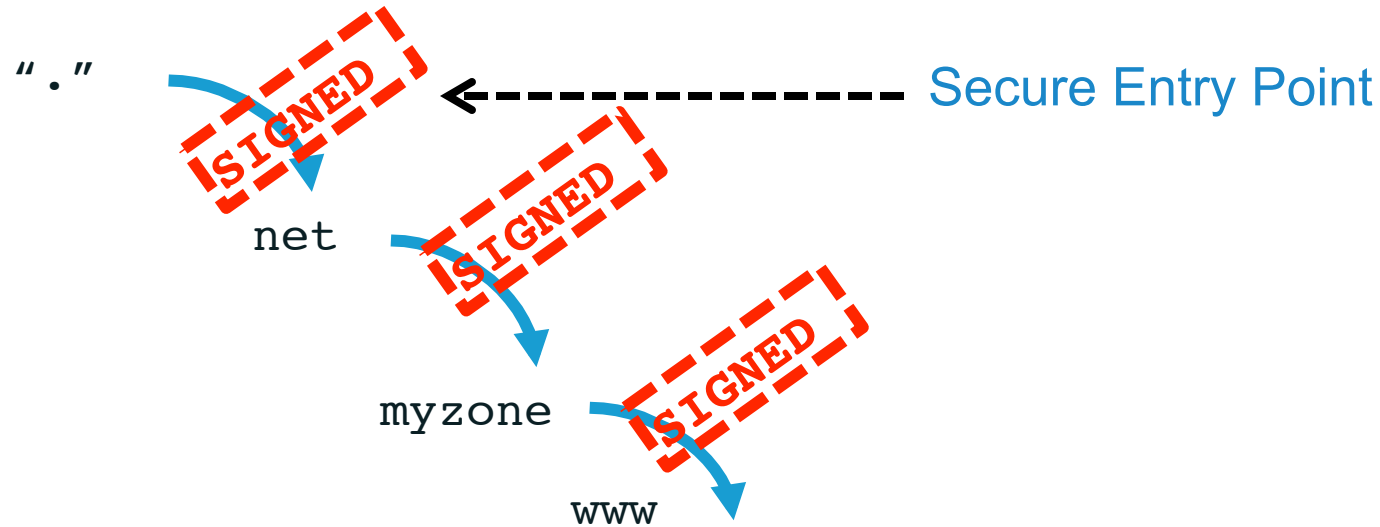

New concepts

New Concepts

- Secure Entry Point and Chain of Trust
  - Delegating Signing Authority
- New packet options (flags)
  - CD, AD, DO
- New RRs
  - DNSKEY, RRSIG, NSEC/NSEC3 and DS
- Signature expiration
- Key Rollovers

Chain of Trust and Secure Entry Point

- Using the existing delegation based model of distribution
- Don’t sign the entire zone, sign a RRset
- Parent **DOES NOT** sign the child zone. The parent signs a pointer (hash) to the key used to sign the data of the child zone (DS record)
- Example with **`www.myzone.net.`**



Steps

- Enable DNSSEC in the configuration file (named.conf)

```
dnssec-enable yes;
dnssec-validation yes;
```

- Create key pairs (KSK and ZSK)

```
dnssec-keygen -a rsasha1 -b 1024 -n zone myzone.net
dnssec-keygen -a rsasha1 -b 1400 -f KSK -n zone myzone.net
```

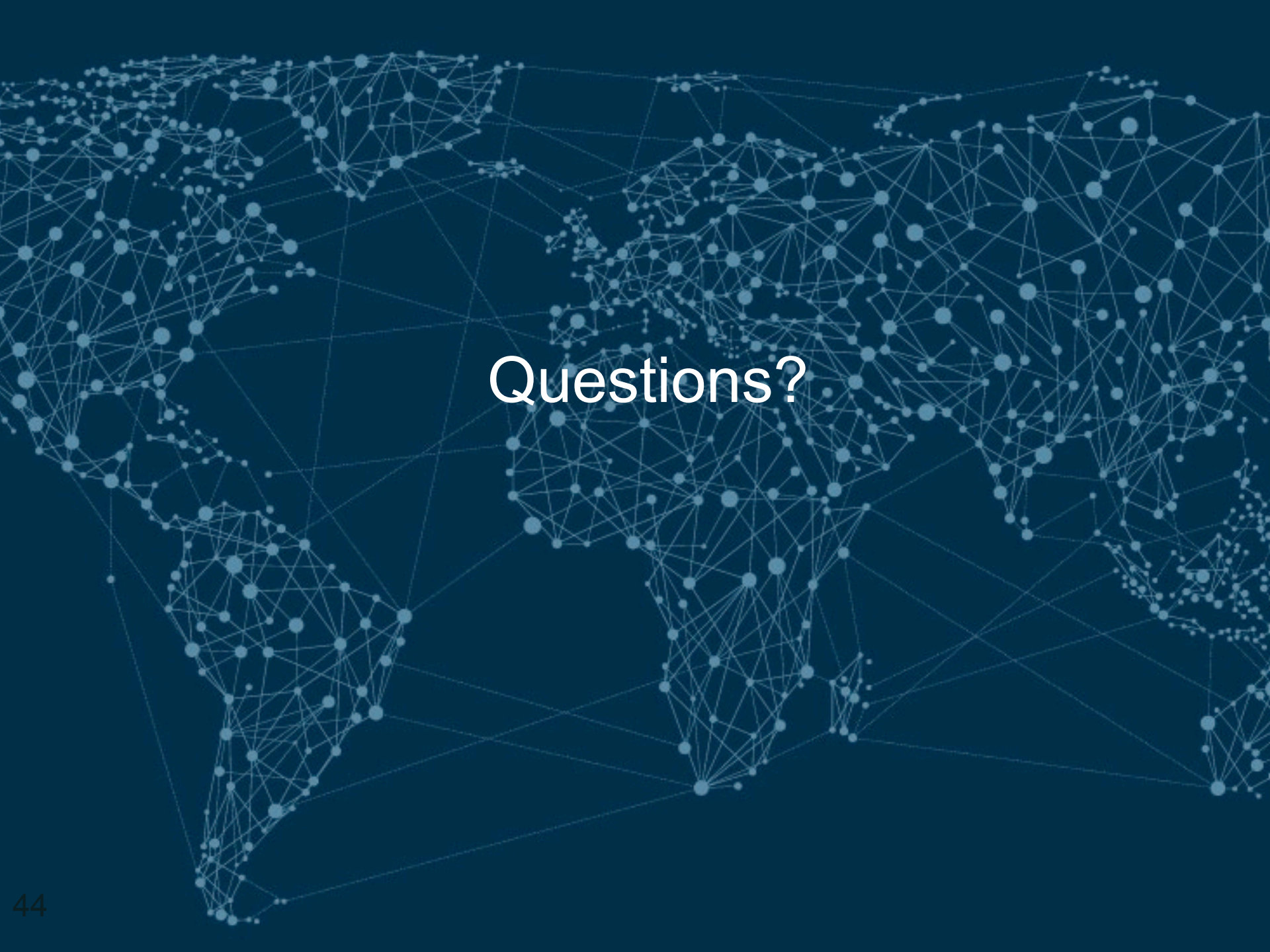
- Publish your public key

```
$INCLUDE /path/Kmyzone.net.+005+33633.key ; ZSK
$INCLUDE /path/Kmyzone.net.+005+00478.key ; KSK
```

- Signing the zone

```
dnssec-signzone –o myzone.net -t -k Kmyzone.net.+005+00478
db.myzone.net Kmyzone.net.+005+33633
```

- Update the config file
  - Modify the zone statement, replace with the signed zone file
- Test with dig


Questions?


Thank You!
<champika.wijayatunga@icann.org>