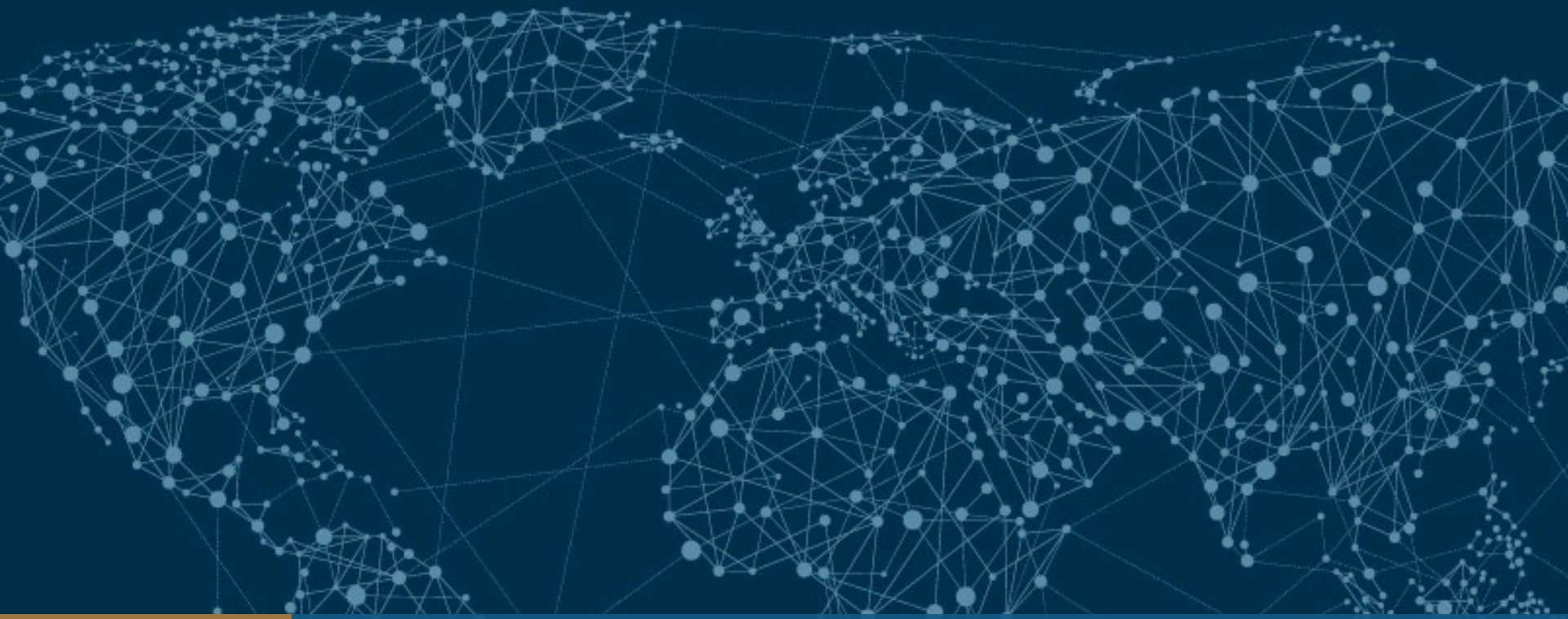


Understanding and Deploying DNSSEC

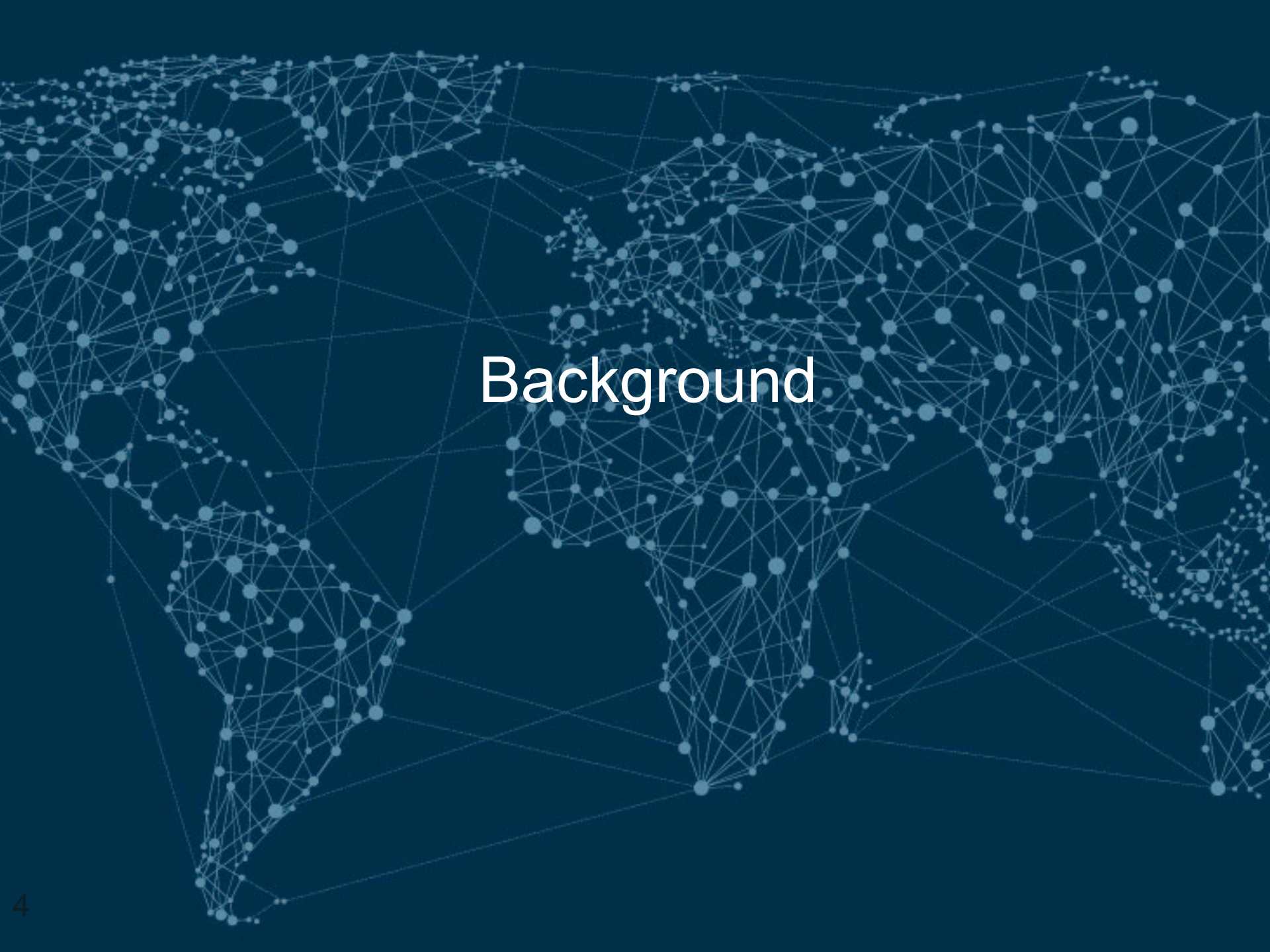
Champika Wijayatunga | SANOG28 Mumbai – India | Aug 1-9 2016

Acknowledgements

- Rick Lamb
  - Sr. Program Manager DNSSEC - ICANN

Agenda

1. Background
2. Why DNSSEC?
3. How it Works?
4. Signatures and Key Rollovers
5. DNSSEC Demo


Background

DNS in a Nutshell

- DNS is a distributed database
- Types of DNS servers
  - DNS Authoritative
    - Master
    - Slaves
  - DNS Resolver
    - Recursive
    - Cache
    - Stub resolver

+1-202-7
VoIP

HealthCare.gov

US-NSTIC effort

DNS is a part of all IT ecosystems

Google

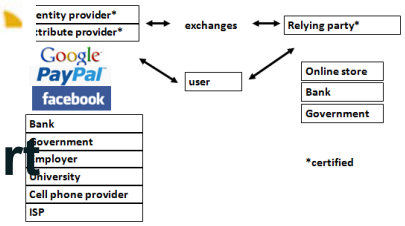
OpenID

facebook

eBay

AADHAAR

PayPal

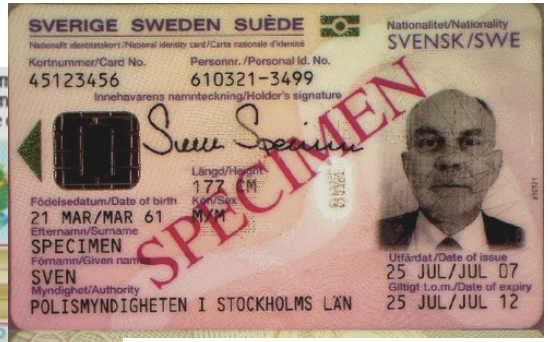


OECS ID effort

amazon Prime

e-Passport symbol

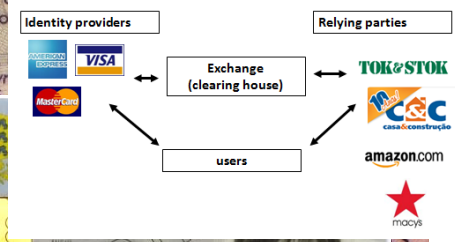
ICP Brasil
O Brasil na era da certificação digital



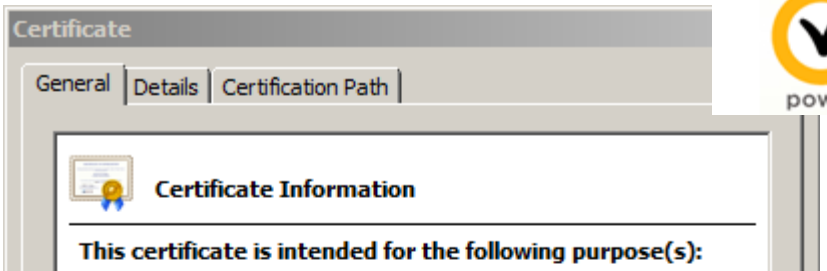
DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

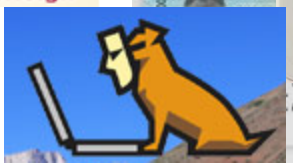
Trust frameworks are not new



Smart Electrical Grid



Norton SECURED
powered by VeriSign

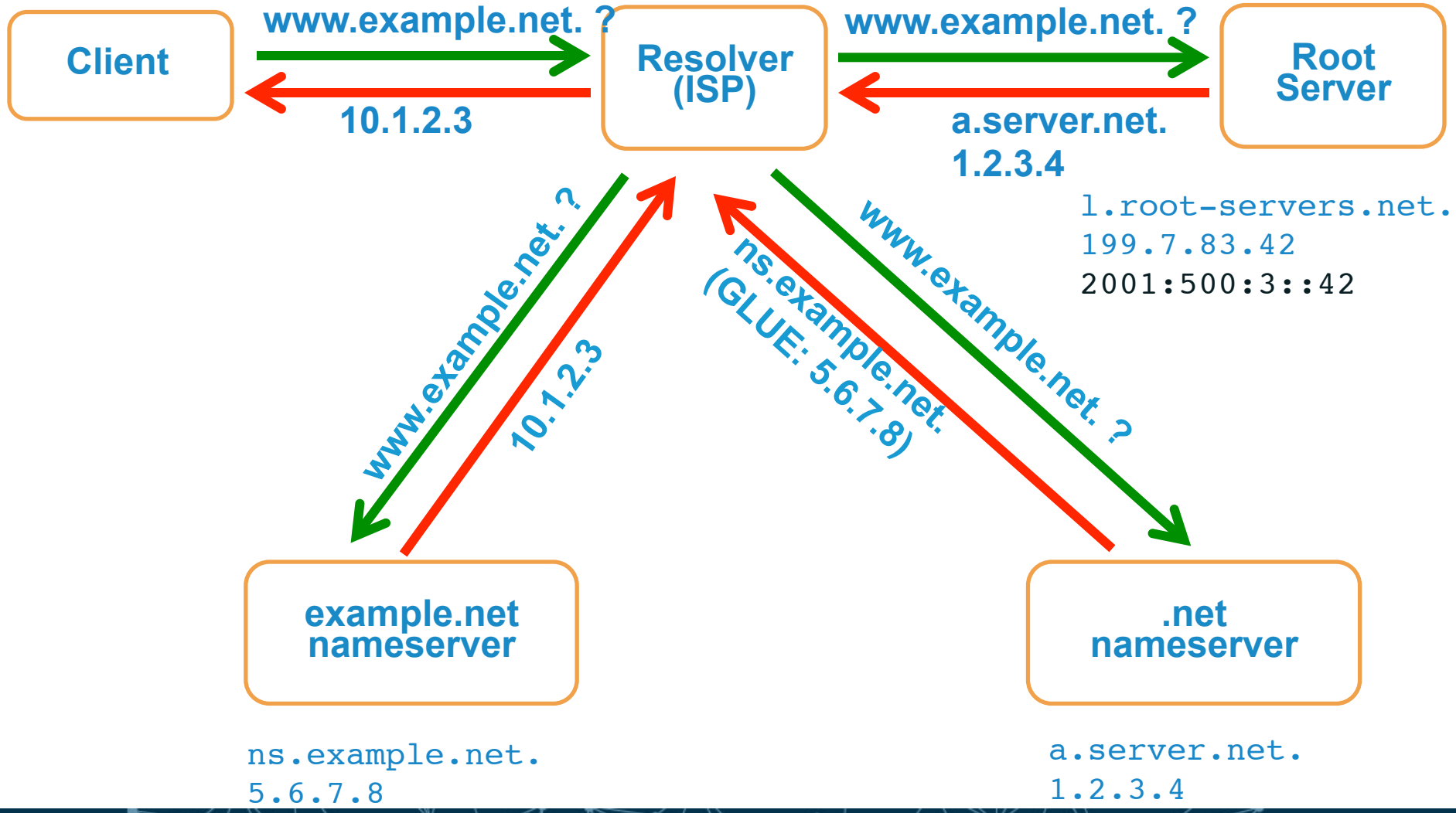


lamb@xtcn.co
m

[CANN

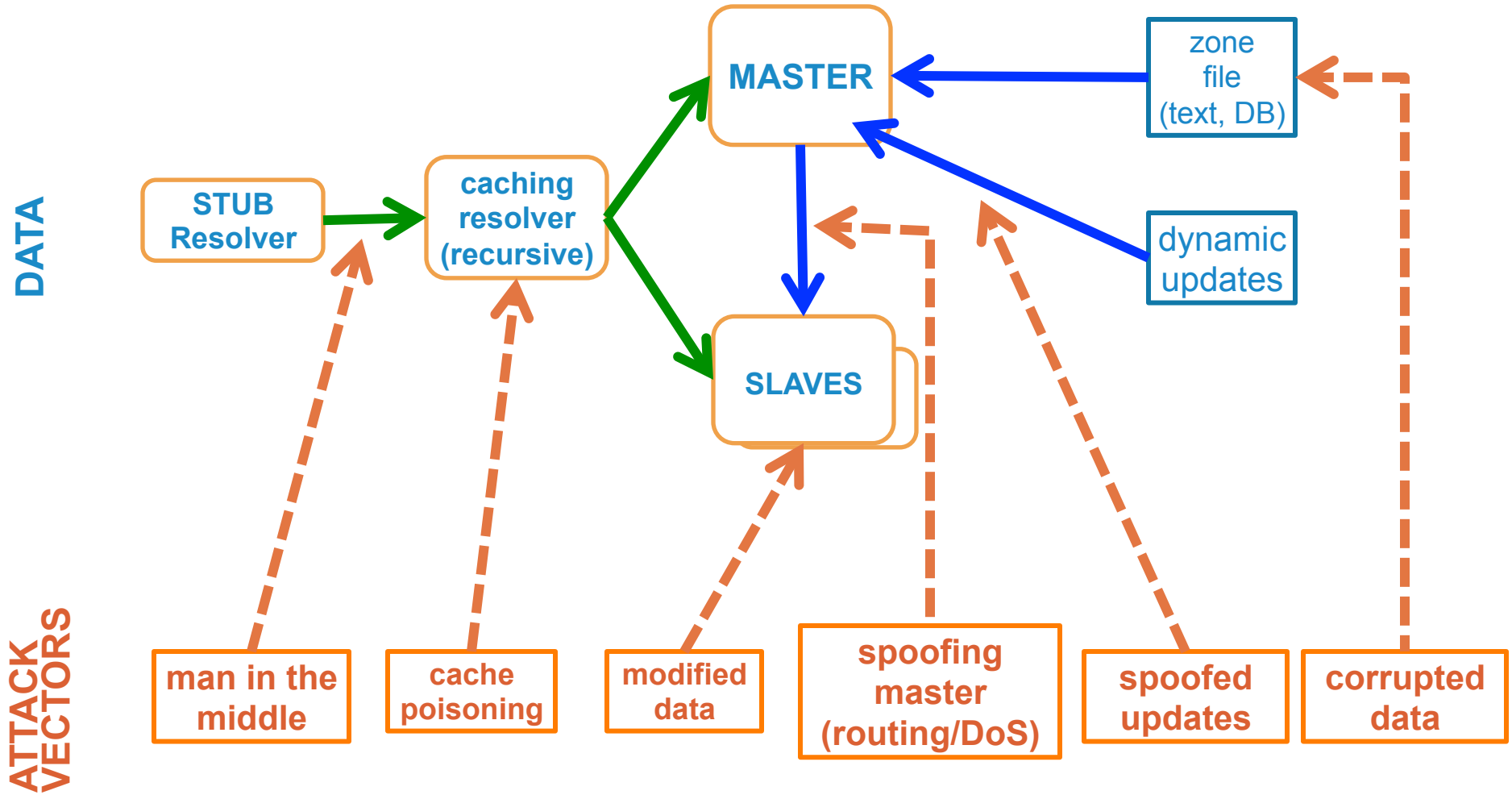
mydomainname.co

DNS Resolution

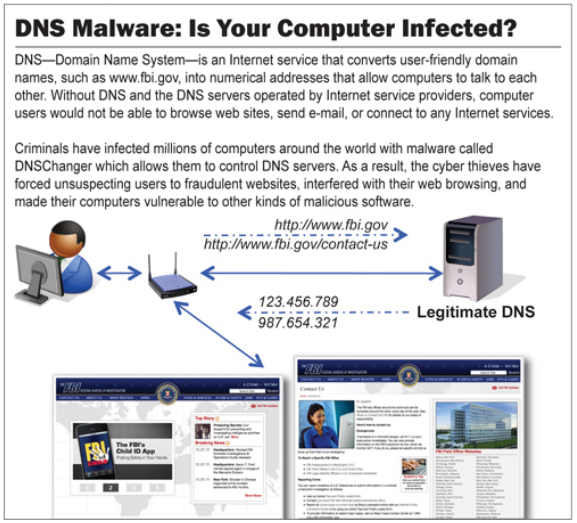



Why DNSSEC?

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

Basic Cache Poisoning

Attacker

- Launches a spam campaign where spam message contains http://loseweightfastnow.com
- Attacker's name server will respond to a DNS query for loseweightnow.com with malicious data about ebay.com
- Vulnerable resolvers add malicious data to local caches
- The malicious data will send victims to an eBay phishing site for the lifetime of the cached entry

My Mac

What is the IPv4 address for loseweightfastnow.com

I'll cache this response… and update www.ebay.com

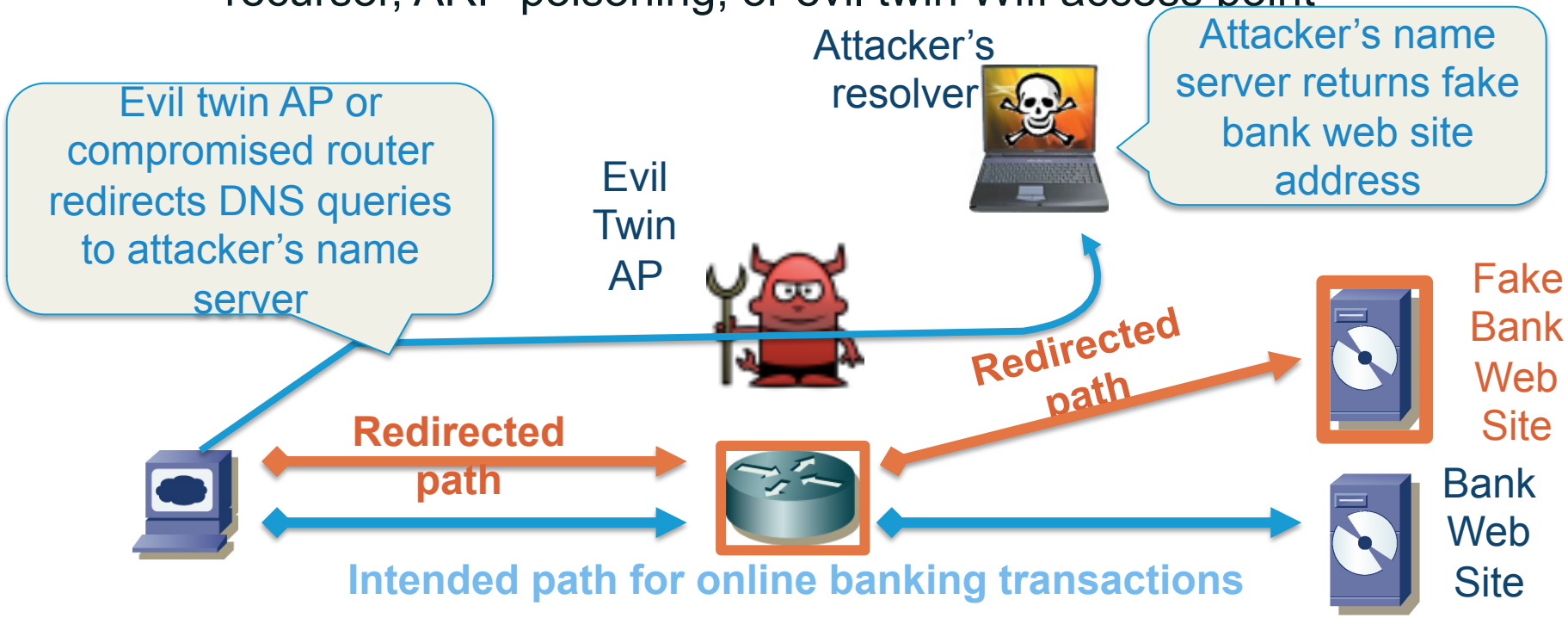
My local resolver

loseweightfastnow.com IPv4 address is 192.168.1.1
ALSO *www.ebay.com is at 192.168.1.2*

ecrime name server

Query Interception (DNS Hijacking)

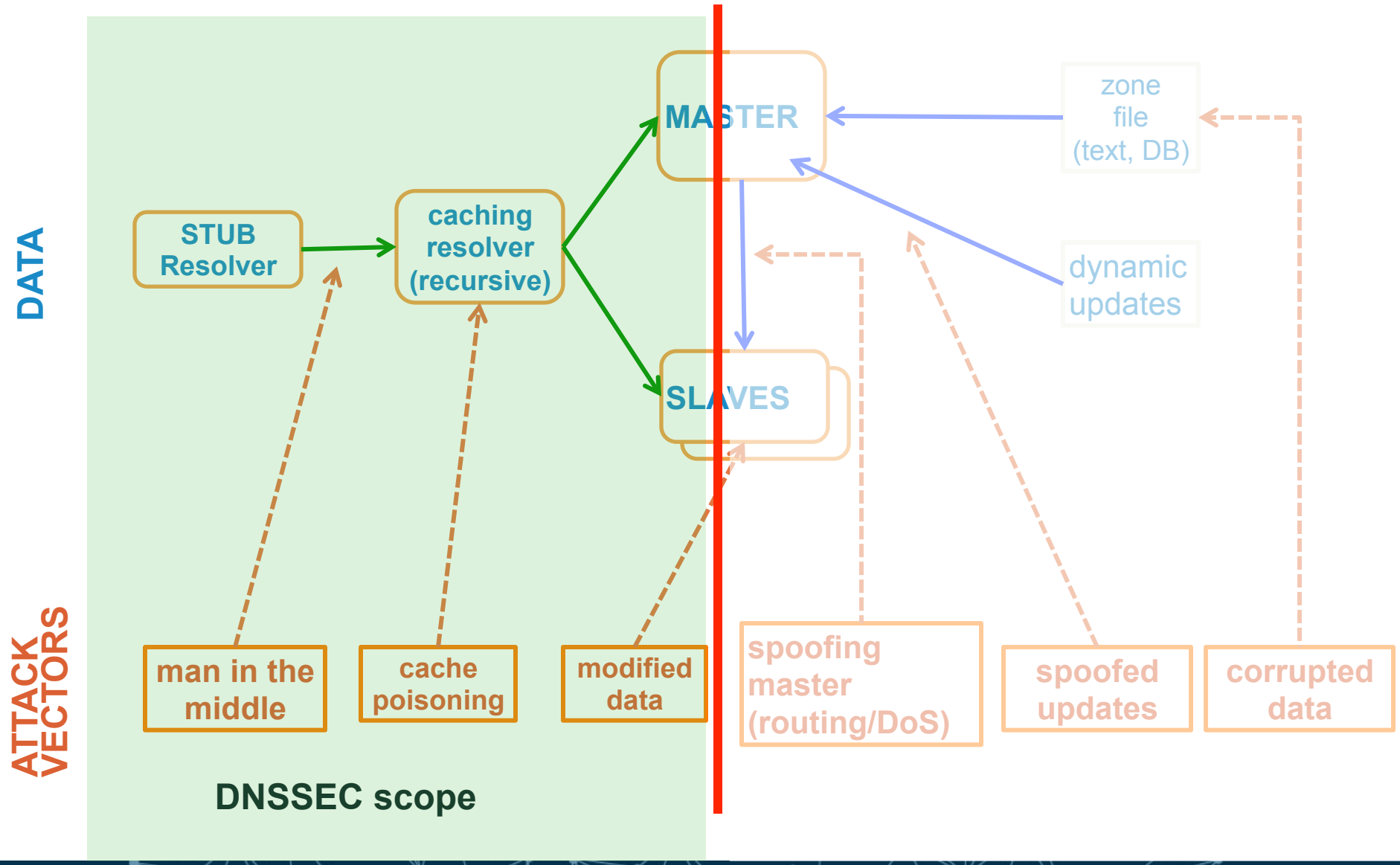
- A man in the middle (MITM) or spoofing attack forwards DNS queries to a name server that returns forge responses
  - Can be done using a DNS proxy, compromised access router or recursor, ARP poisoning, or evil twin Wifi access point



Where DNSSEC fits in

- CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
- DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents
- With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)

What DNSSEC solves and what's not

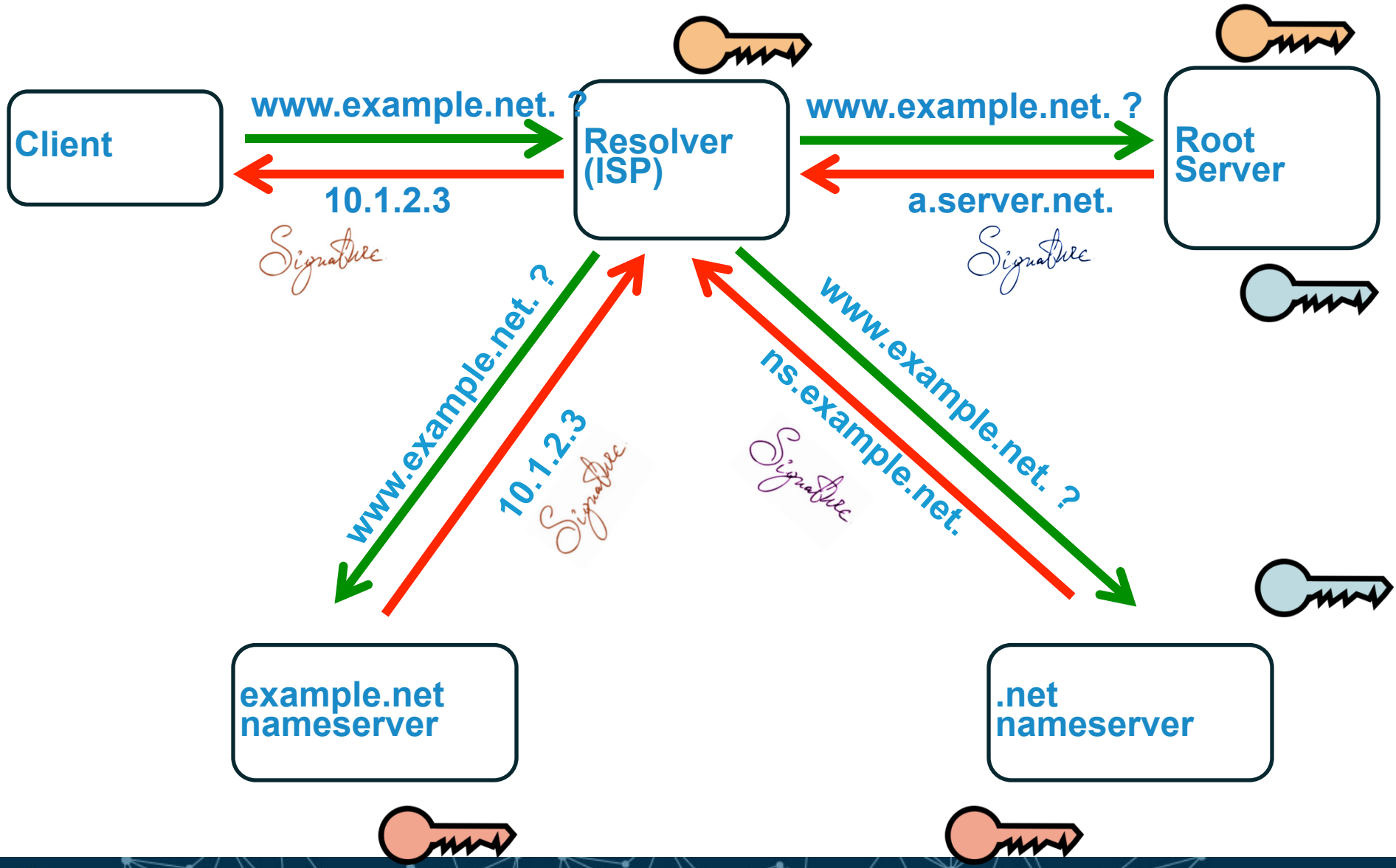


Brief reminder on Cryptography

- 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.

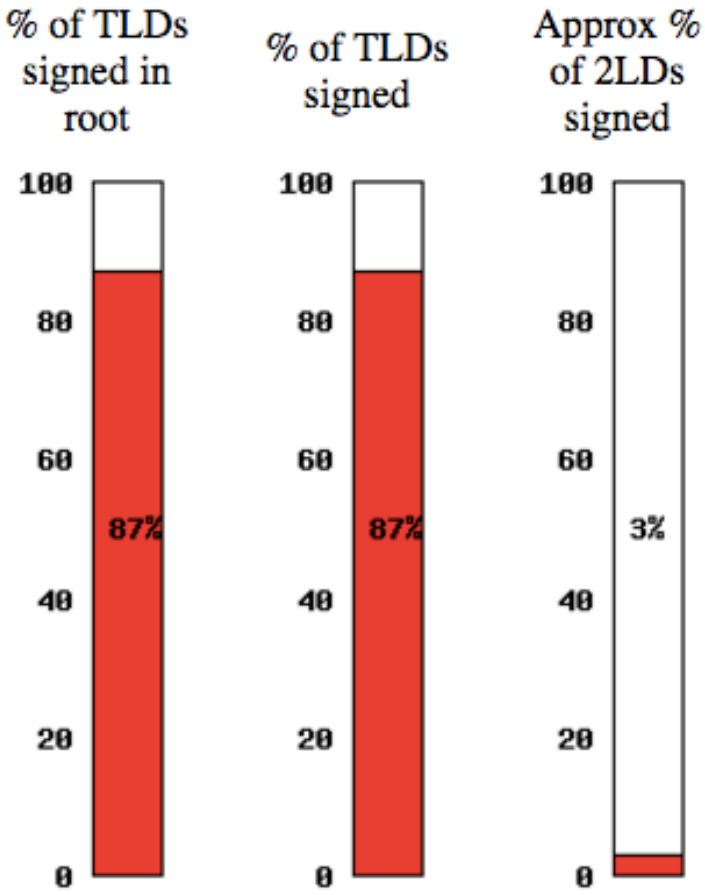
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).

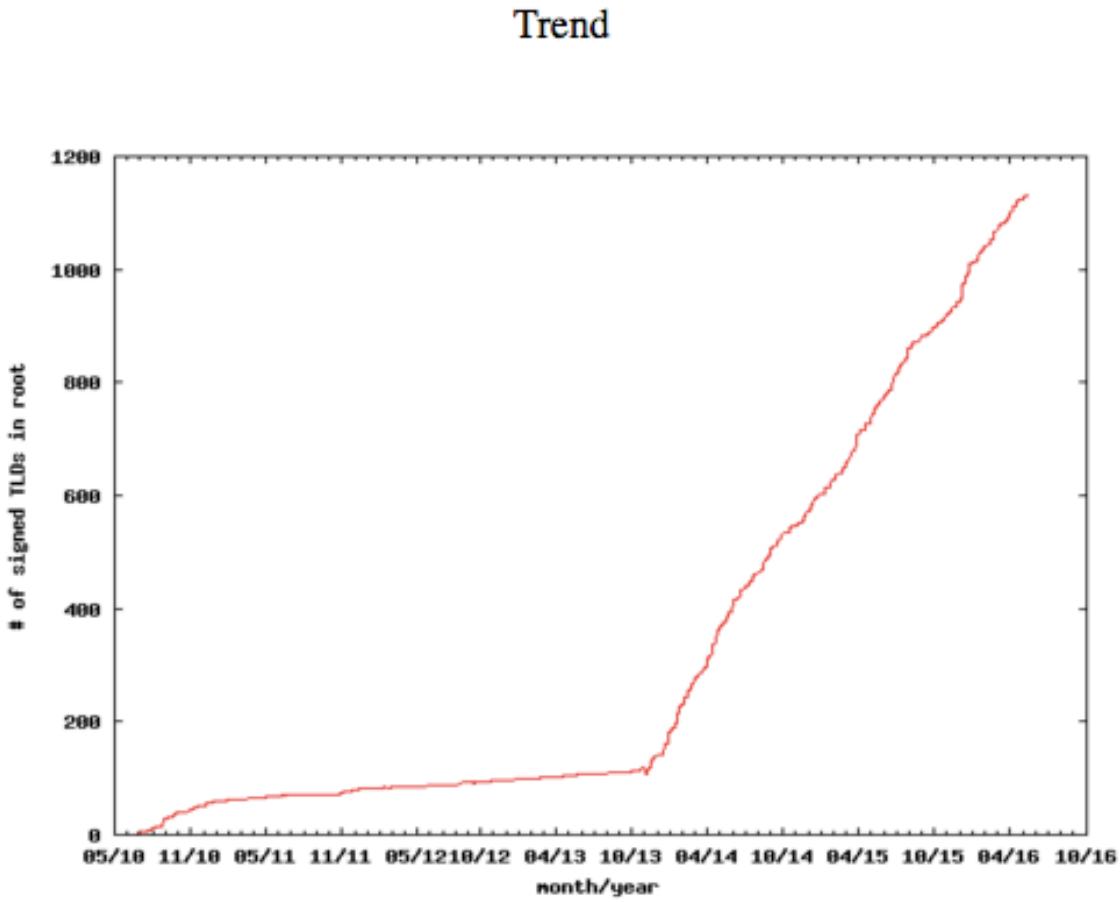
- DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.

DNSSEC ccTLD Map

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

DNSSEC Deployment – Where we are?





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

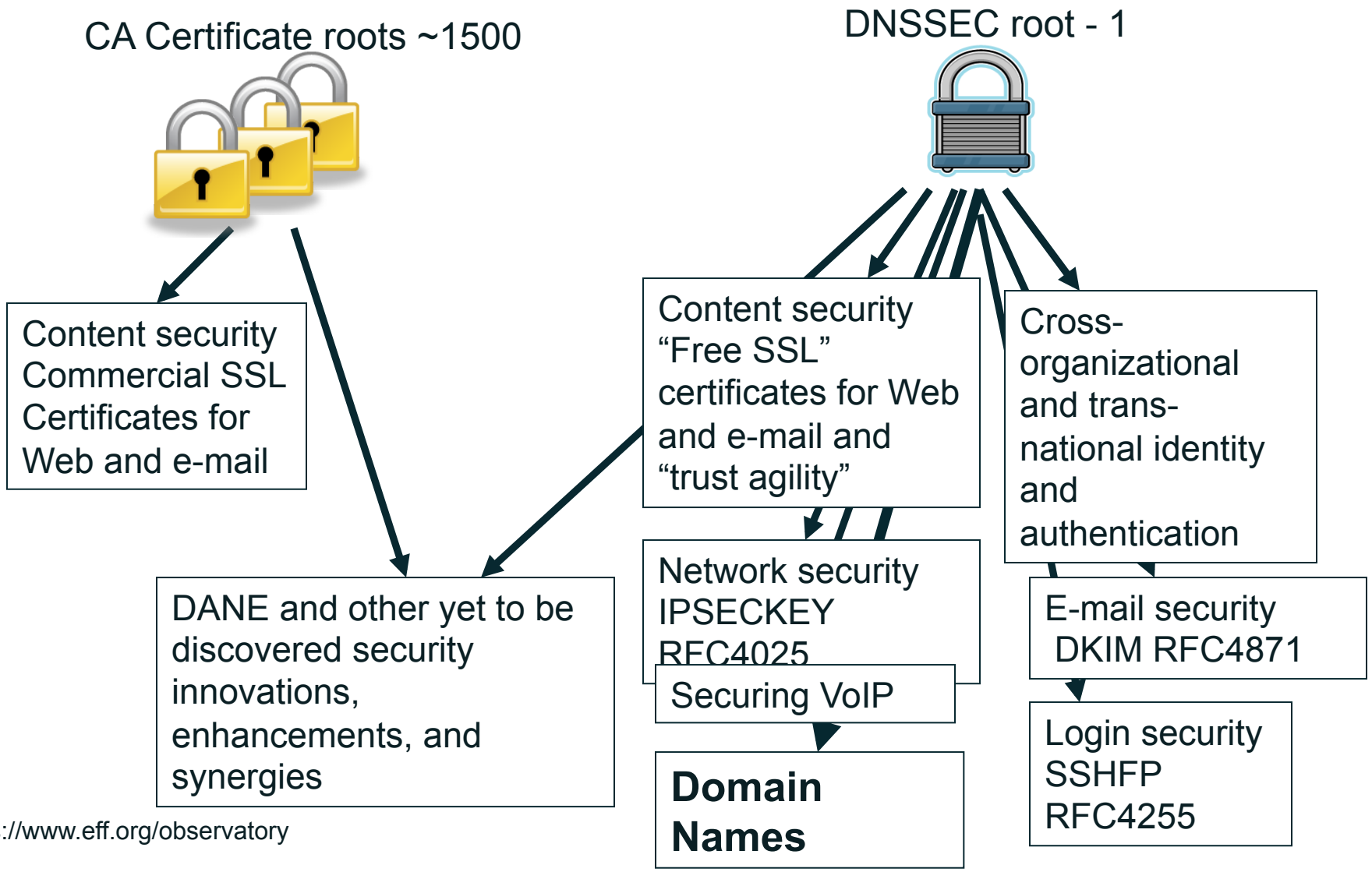
What you can do

- ***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

Game changing Internet Core Infrastructure Upgrade

“More has happened here today than meets the eye. An infrastructure has been created for a hierarchical security system, which can be purposed and re-purposed in a number of different ways. ..” – Vint Cerf (June 2010)

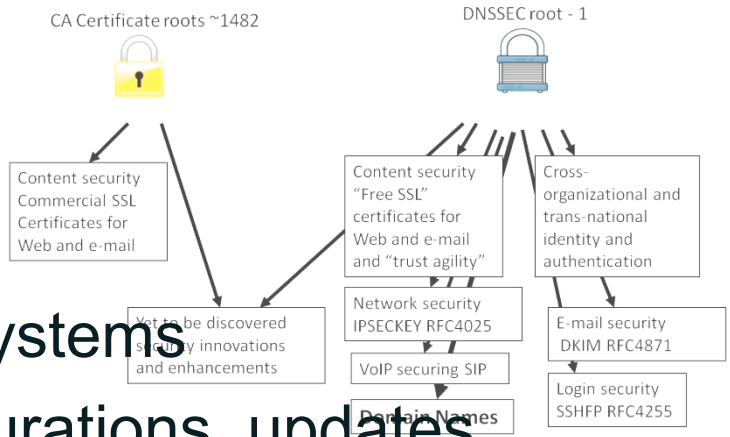
Too many CAs. Which one can we trust?



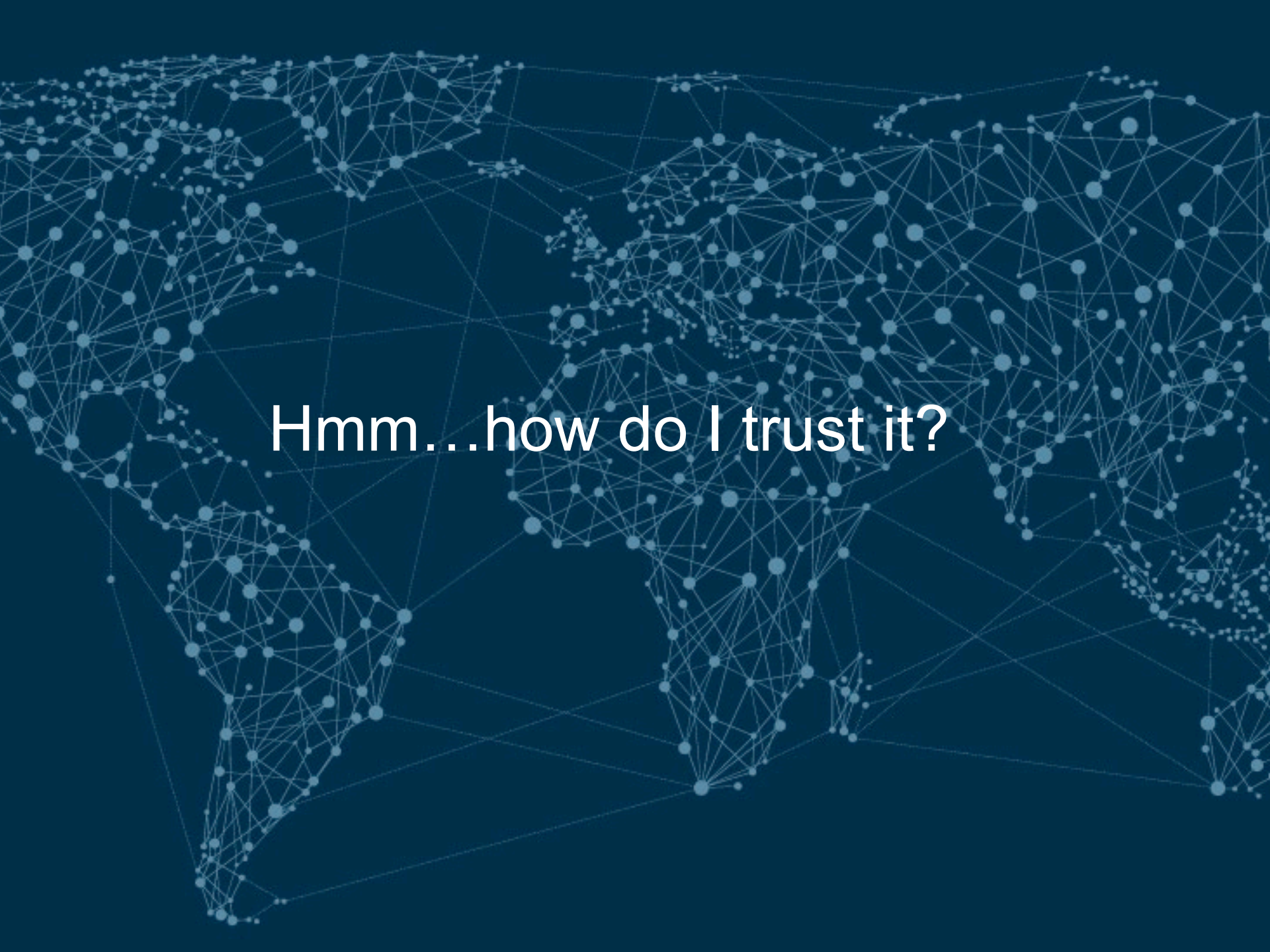
https://www.eff.org/observatory

Opportunity: New Security Solutions

- Improved Web SSL and certificates for all
- Secured e-mail (S/MIME) for all
- Validated remote login SSH, IPSEC
- Securing VoIP
- Cross organizational digital identity systems
- Secured content delivery (e.g. configurations, updates, keys)
- Securing Smart Grid efforts
- First global FREE PKI
- Increasing trust in e-commerce

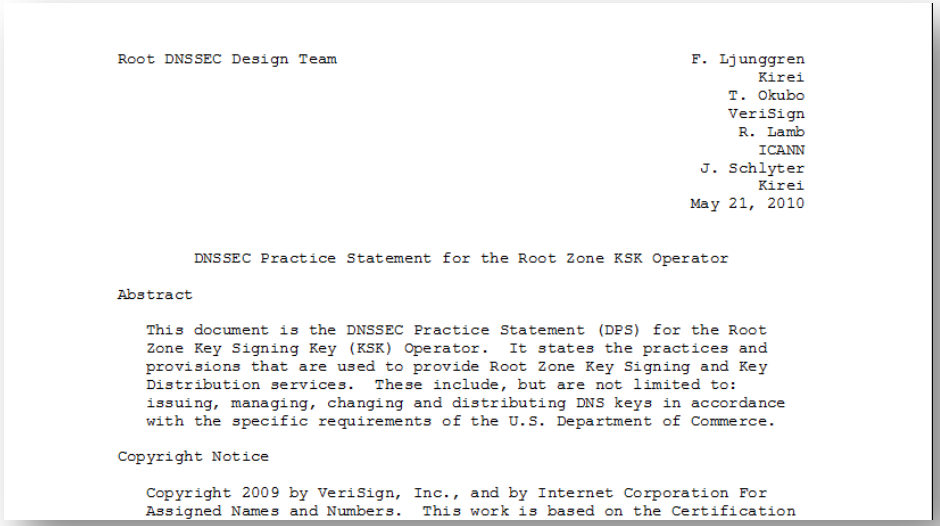



DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.


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
- SysTrust audited
- FIPS 140-2 level 4 HSMs



Root DNSSEC Design Team

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

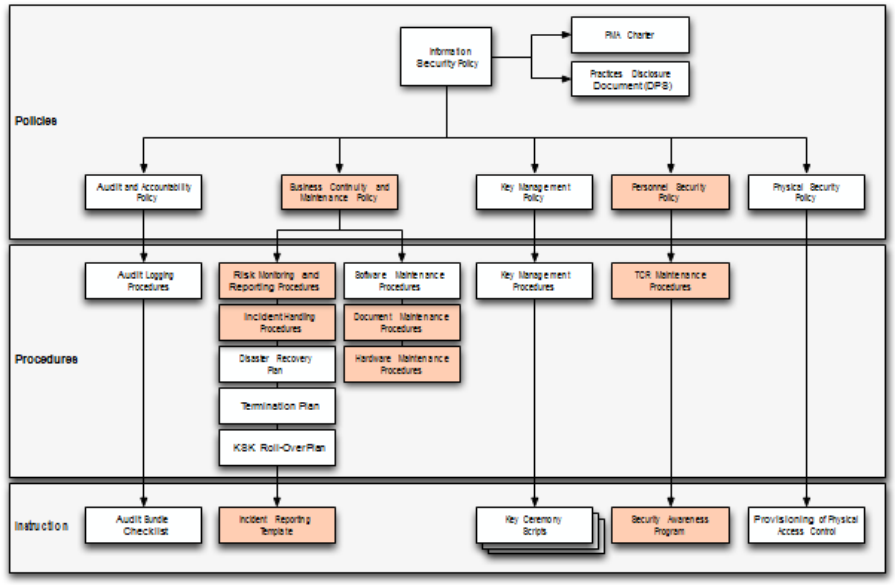
DNSSEC Practice Statement for the Root Zone KSK Operator

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**

ICANN DNSSEC Deployment @Root (and elsewhere)

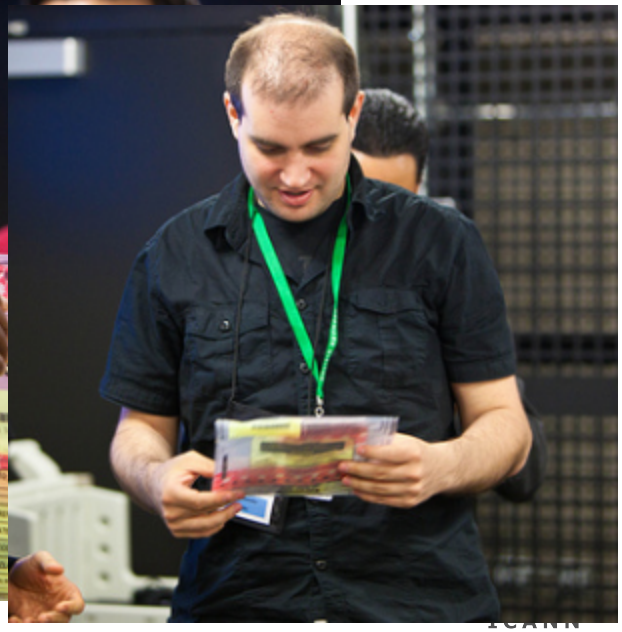
FIPS 140-2
level 4

DCID 6/9

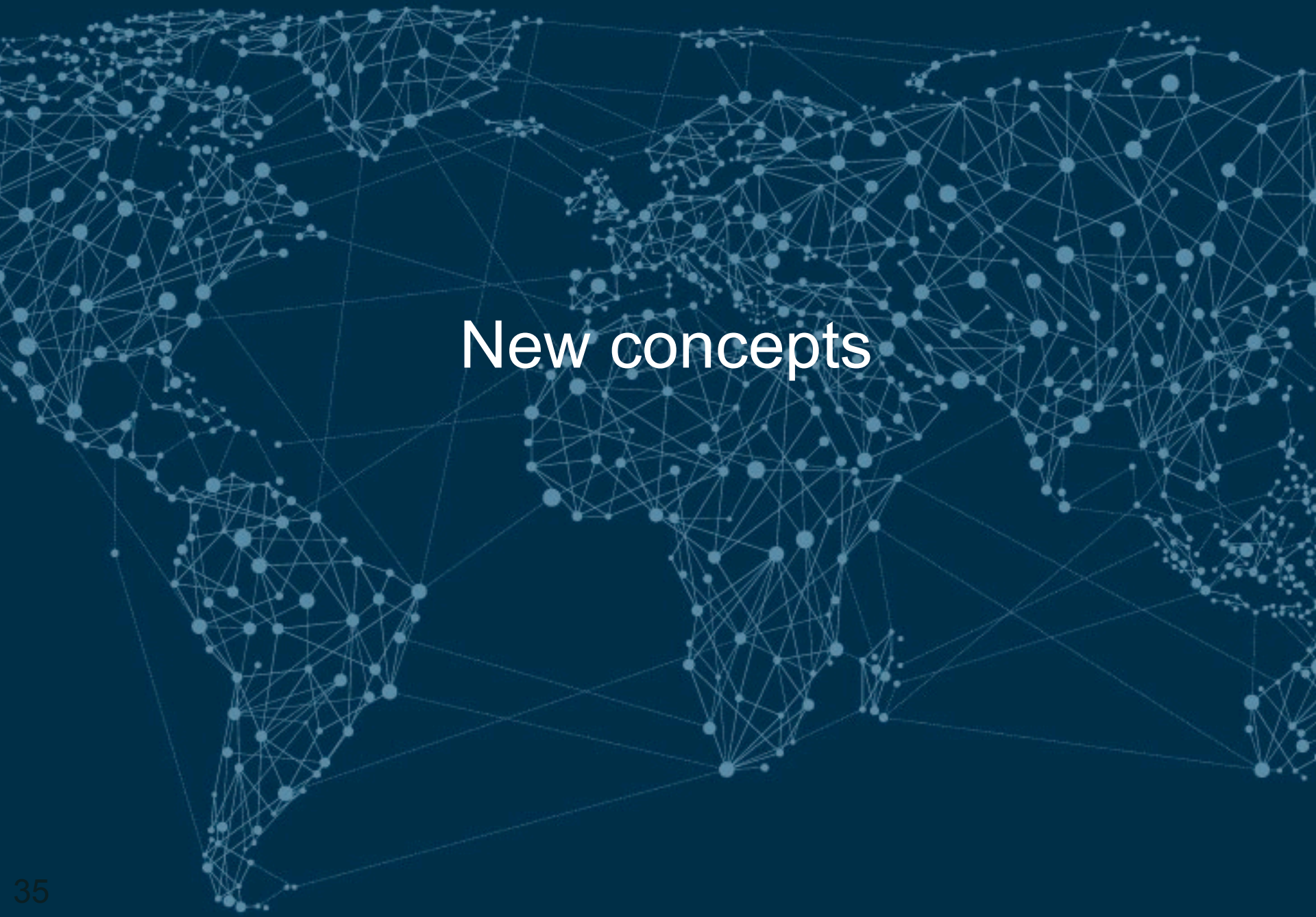
Photos: Kim Davies


January 27, 2010


ICAN



Photos: Kim Davies

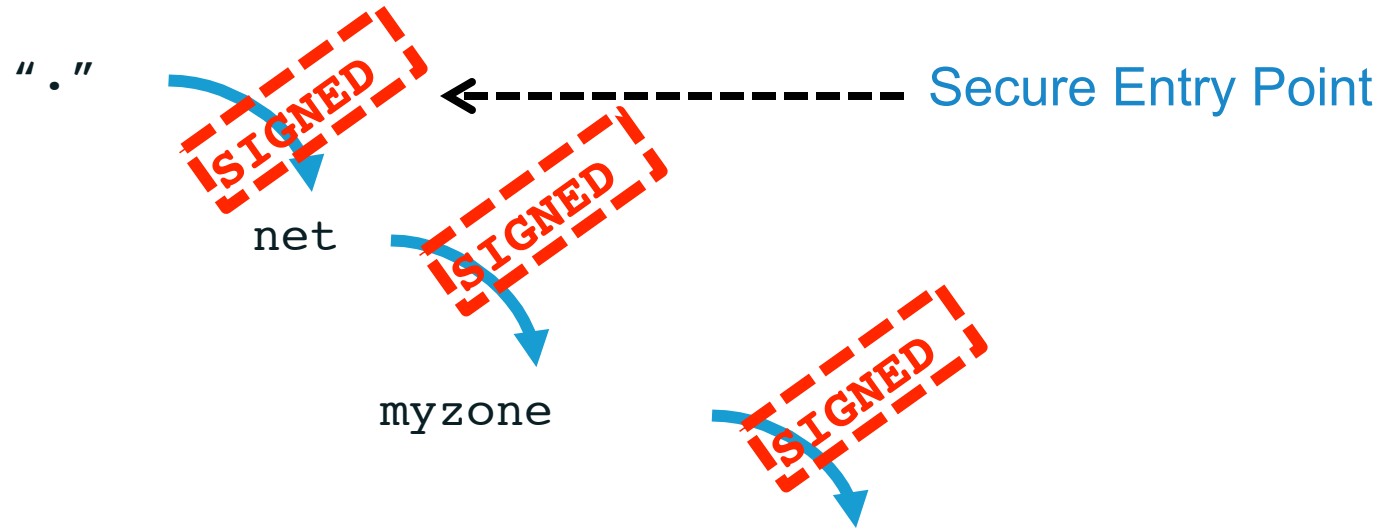

New concepts

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.`**



New Fields and Flags

- DNSSEC Updates DNS protocol at the packet level

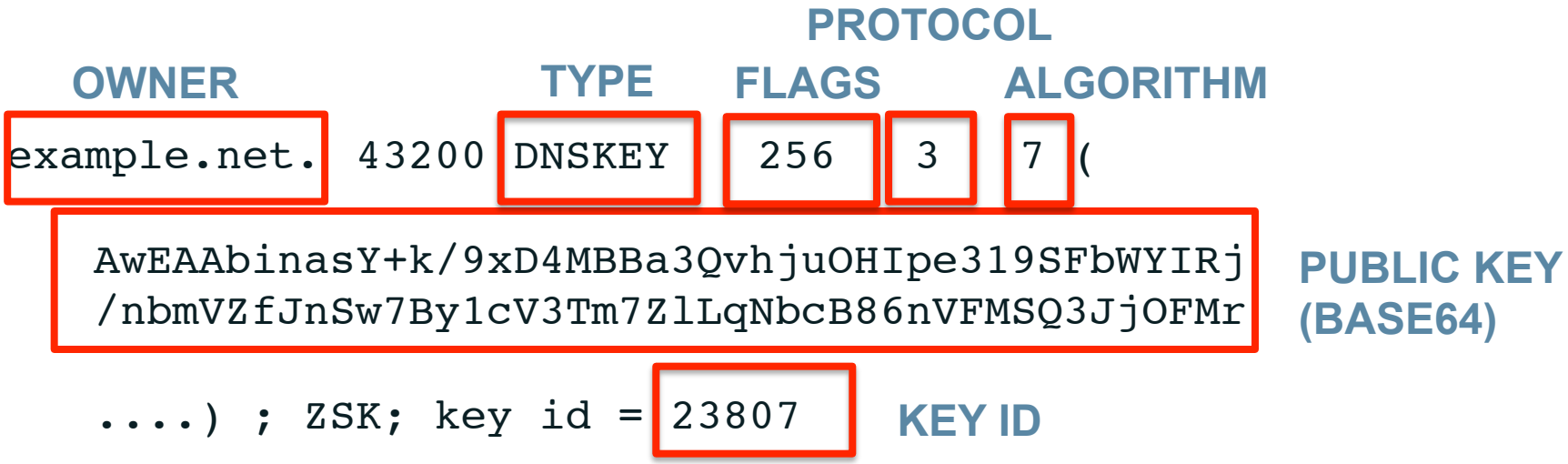
- Non-compliant DNS recursive servers ***should*** ignore these:
  - **CD**: **C**hecking **D**isabled (ask recursing server to not perform validation, even if DNSSEC signatures are available and verifiable, i.e.: a SEP can be found)
  - **AD**: **A**uthenticated **D**ata, set on the answer by the validating server if the answer could be validated, and the client requested validation
  - **DO**: **D**NSSEC **O**K. A new EDNS0 option to indicate that client supports DNSSEC options


New Resource Records

New RRs

- Adds five new DNS Resource Records:
  1. **DNSKEY**: Public key used in zone signing operations.
  2. **RRSIG**: RRset signature
  3. **NSEC** &
  4. **NSEC3**: Returned as verifiable evidence that the name and/or RR type does not exist
  5. **DS**: Delegation Signer. Contains the hash of the public key used to sign the key which itself will be used to sign the zone data. Follow DS RR's until a ”trusted” zone is reached (ideally the root).

New RR: DNSKEY



- FLAGS determines the usage of the key
- PROTOCOL is always 3 (DNSSEC)
- ALGORITHM can be (3: DSA/SHA-1, 5: RSA/SHA1, 8: RSA/SHA-256, 12: ECC-GOST)
  - http://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xml

DNSKEY: Two Keys, not one…

- There are in practice at least **two** DNSKEY pairs for every zone
- Originally, **one** key-pair (public, private) defined for the zone
  - **private**: key used to sign the zone data (RRsets)
  - **public**: key published (DNSKEY) in the zone
- DNSSEC works fine with a single key pair
- Problem with using a single key:
  - Every time the key is updated, the DS record must be updated on the parent zone as well
  - Introduction of **K**ey **S**igning **K**ey (flags=257)

KSK and ZSK

- Key Signing Key (KSK)
  - Pointed to by parent zone in the form of DS (Delegation Signer). Also called Secure Entry Point.
  - Used to sign the Zone Signing Key
  - Flags: 257
- Zone Signing Key (ZSK)
  - Signed by the KSK
  - Used to sign the zone data RRsets
  - Flags: 256
- This decoupling allows for independent updating of the ZSK without having to update the KSK, and involve the parents (i.e. less administrative interaction)

New RR: RRSIG (Resource Record Signature)

```
example.net.   600   A   192.168.10.10
example.net.   600   A   192.168.23.45
```

OWNER	TYPE	TYPE COVERED	ALG	#LABELS	TTL	
example.net.	600	RRSIG	A	7	2	600 (

SIG. EXPIRATION	SIG. INCEPTION	KEY ID	SIGNER NAME
20150115154303	20141017154303	23807	example.net.

SIGNATURE

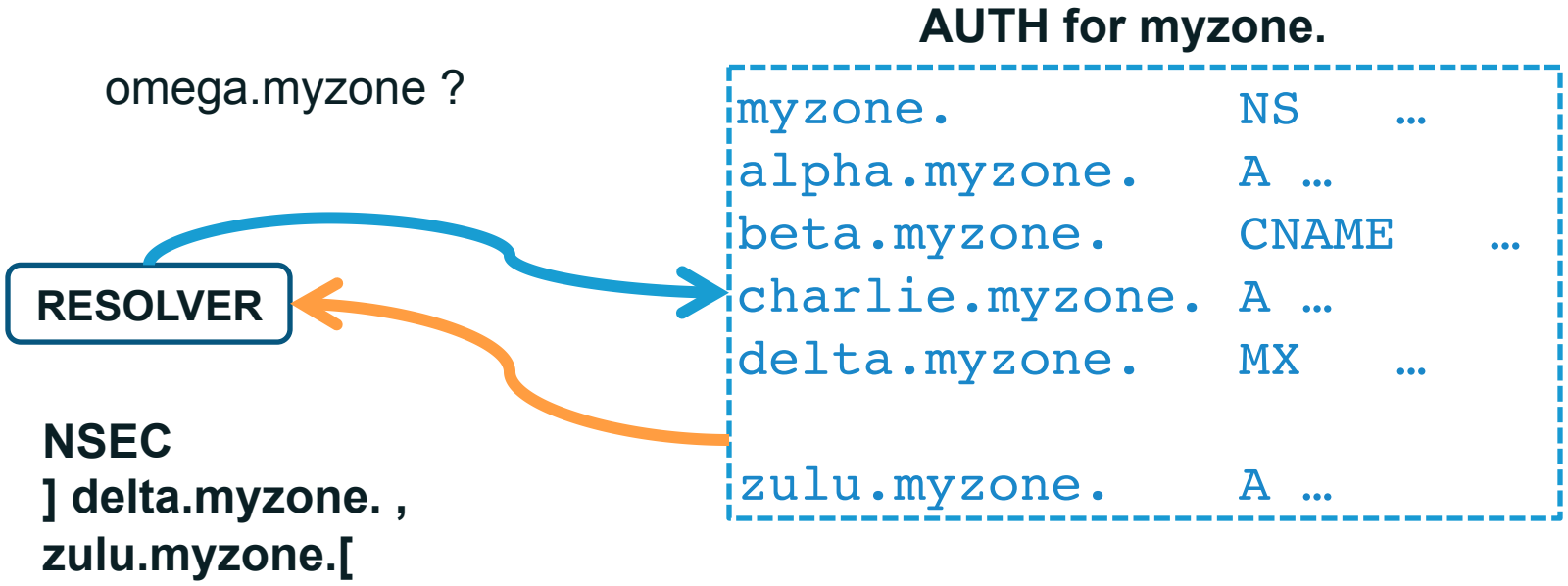
```
CoYkYPqE8Jv6UaVJgRrh7u16m/cEFGtFM8TArbJdaiPu
W77wZhrvonoBEyqYbhQ1yDaS74u9whECEe08gfoe1FGg
. . .
)
```

RRSIG

- Typical default values
  - Signature inception time is 1 hour before.
  - Signature expiration is 30 from now
  - Proper timekeeping (NTP) is required
- What happens when signatures run out?
  - SERVFAIL
  - Domain effectively disappears from the Internet for validating resolvers
- Note that *keys* do **not** expire
- No all RRSets need to be resigned at the same time

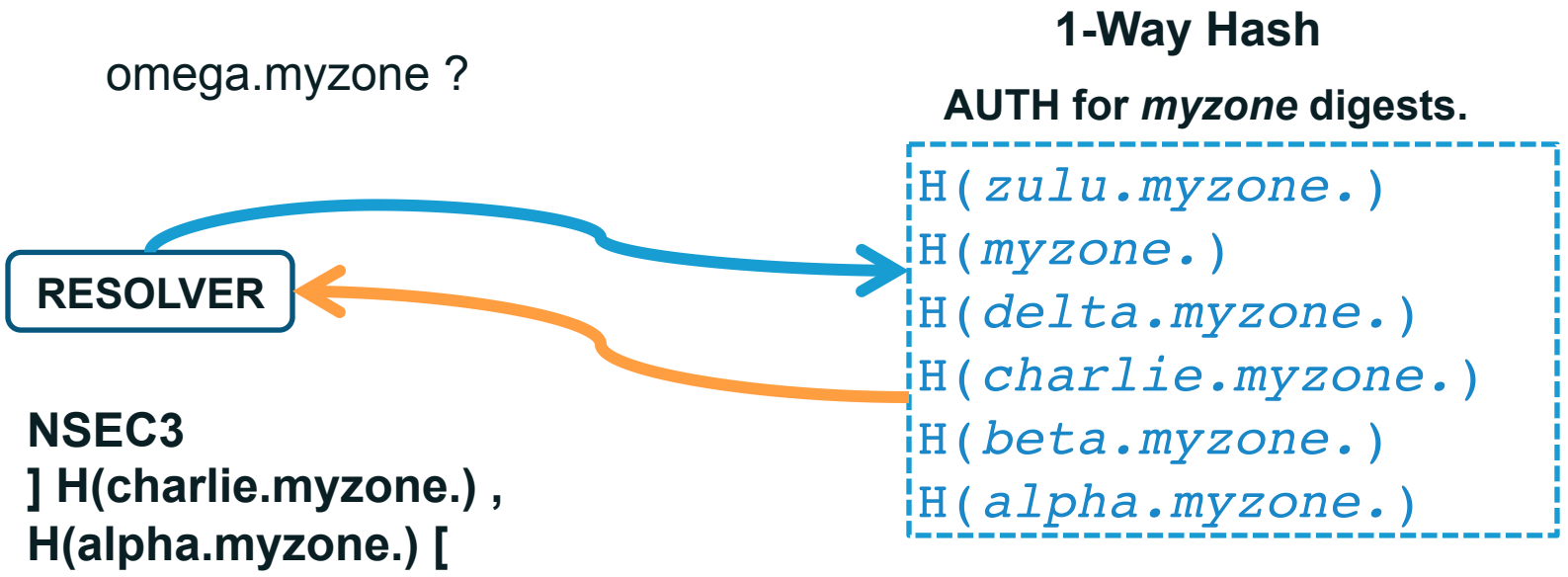
New RR: NSEC

- NXDomains also must be verified
- NSEC provides a pointer to the **N**ext **SEC**ure record in the chain of records.



New RR: NSEC3

- To avoid concerns about “zone enumeration”
- To avoid large zone-files: opt-out concept



New RR: DS (Delegation Signer)

- Hash of the KSK of the child zone
- Stored in the parent zone, together with the NS RRs indicating a delegation of the child zone.
- The DS record for the child zone is signed together with the rest of the parent zone data
- NS records are NOT signed (they are a hint/pointer)

Security Status of Data

- **Secure**
  - Resolver is able to build a chain of signed DNSKEY and DS RRs from a trusted security anchor to the RRset
- **Insecure**
  - Resolver knows that it has no chain of signed DNSKEY and DS RRs from any trusted starting point to the RRset
- **Bogus**
  - Resolver believes that it ought to be able to establish a chain of trust but for which it is unable to do so
  - May indicate an attack but may also indicate a configuration error or some form of data corruption
- **Indeterminate**
  - No trust anchor to indicate if the zone and children should be secure.
  - Resolver is not able to determine whether the RRset should be signed.


Signatures expiration and
Key Rollovers

Signature Expiration

- Signatures are per default 30 days (BIND)
- Need for regular resigning:
  - To maintain a constant window of validity for the signatures of the existing RRset
  - To sign new and updated Rrsets
  - Use of jitter to avoid having to resign all expiring RRsets at the same time
- The keys themselves do NOT expire…
- But they may need to be rolled over...

Key Rollovers

- Try to minimise impact
  - Short validity of signatures
  - Regular key rollover
- Remember: DNSKEYs do not have timestamps
  - the RRSIG over the DNSKEY has the timestamp
- Key rollover involves second party or parties:
  - State to be maintained during rollover
  - Operationally expensive

Key Rollovers

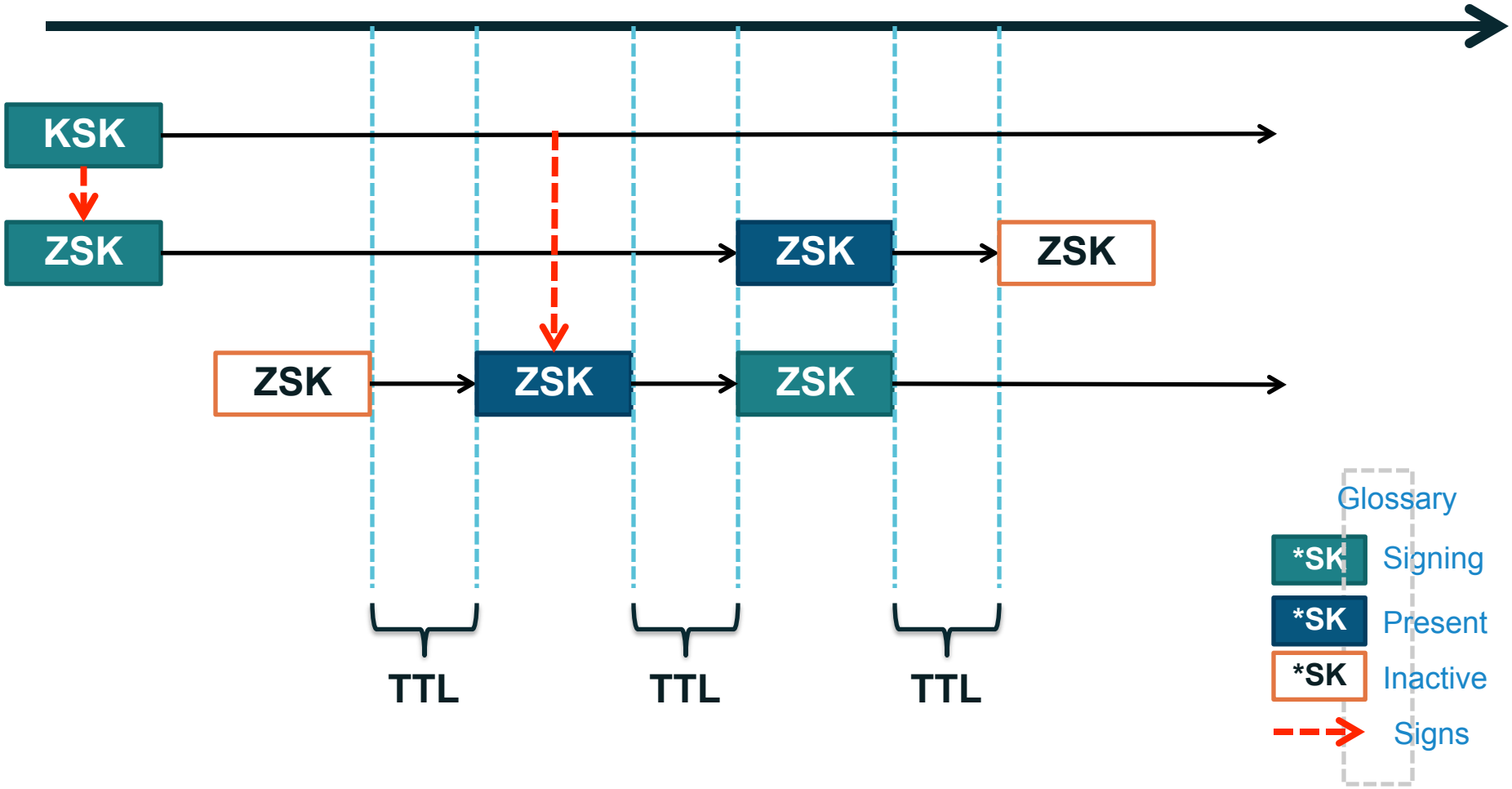
- Two methods for doing key rollover
  - Pre-Publish
  - Double Signature

- KSK and ZSK rollover use different methods.
  - Remember that KSK needs to interact with parent zone to update DS record.

Key Rollovers: Pre-Publish method

- ZSK Rollover using the pre-publish method
  1. Wait for old zone data to expire from caches (TTL)
  2. Sign the zone with the KSK and published ZSK
  3. Wait for old zone data to expire from caches
  4. Adjust Key list and sign the zone with new ZSK

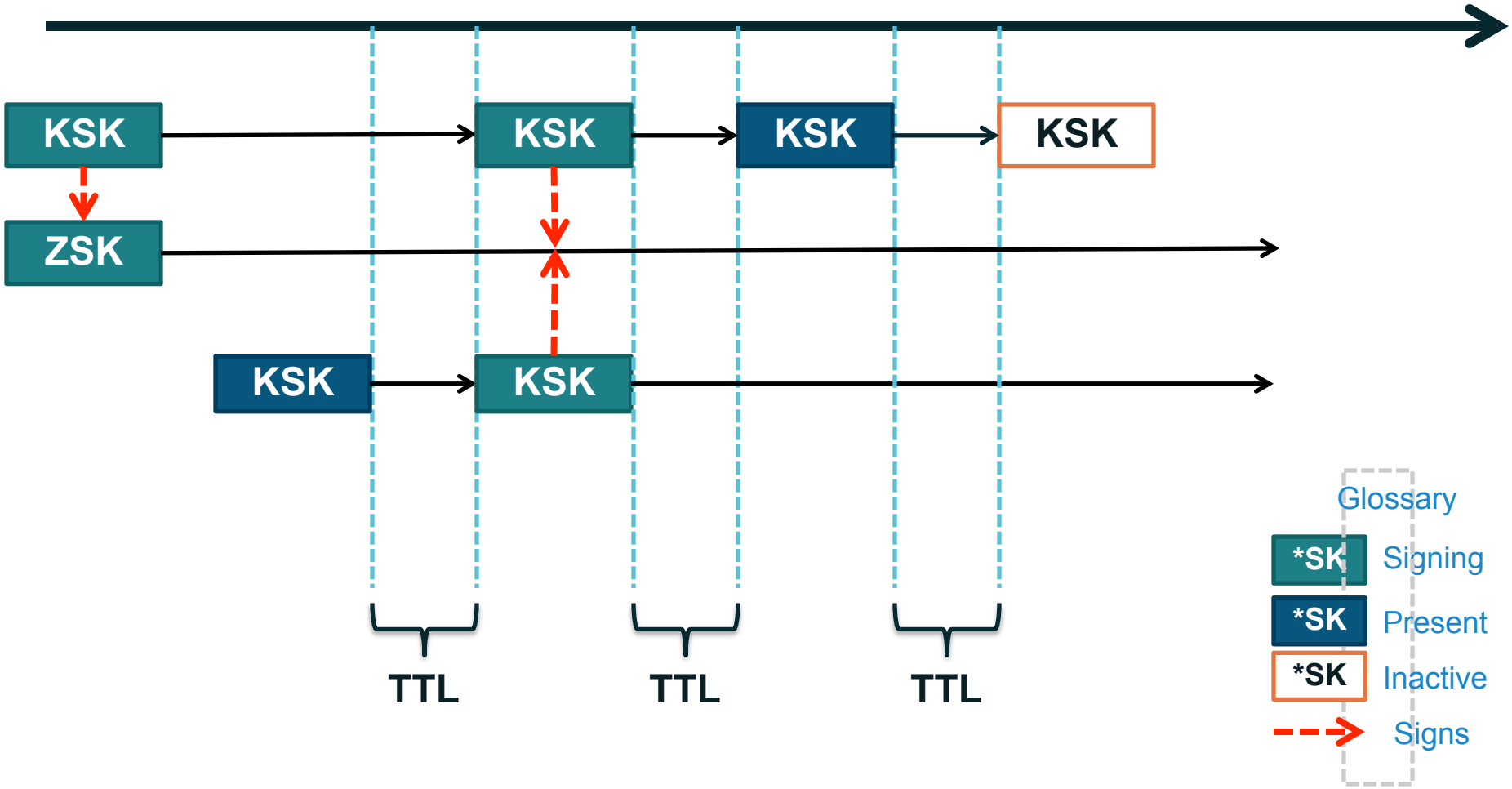
Key Rollovers: Pre-Publish method



Key Rollovers: Double Signature

- KSK Rollover using the Double Signature method
  1. Wait for old zone data to expire from caches
  2. generate a new (published) KSK
  3. Wait for the old DNSKEY RRset to expire from caches
  4. roll the KSKs
  5. Transfer new DS keyset to the parent
  6. Wait for parent to publish the new DS record
  7. Reload the zone
- It is also possible to use dual DS in the parent zone

Key Rollovers: Double Signature




Setting Up a Secure Zone - Demo

Steps

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

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

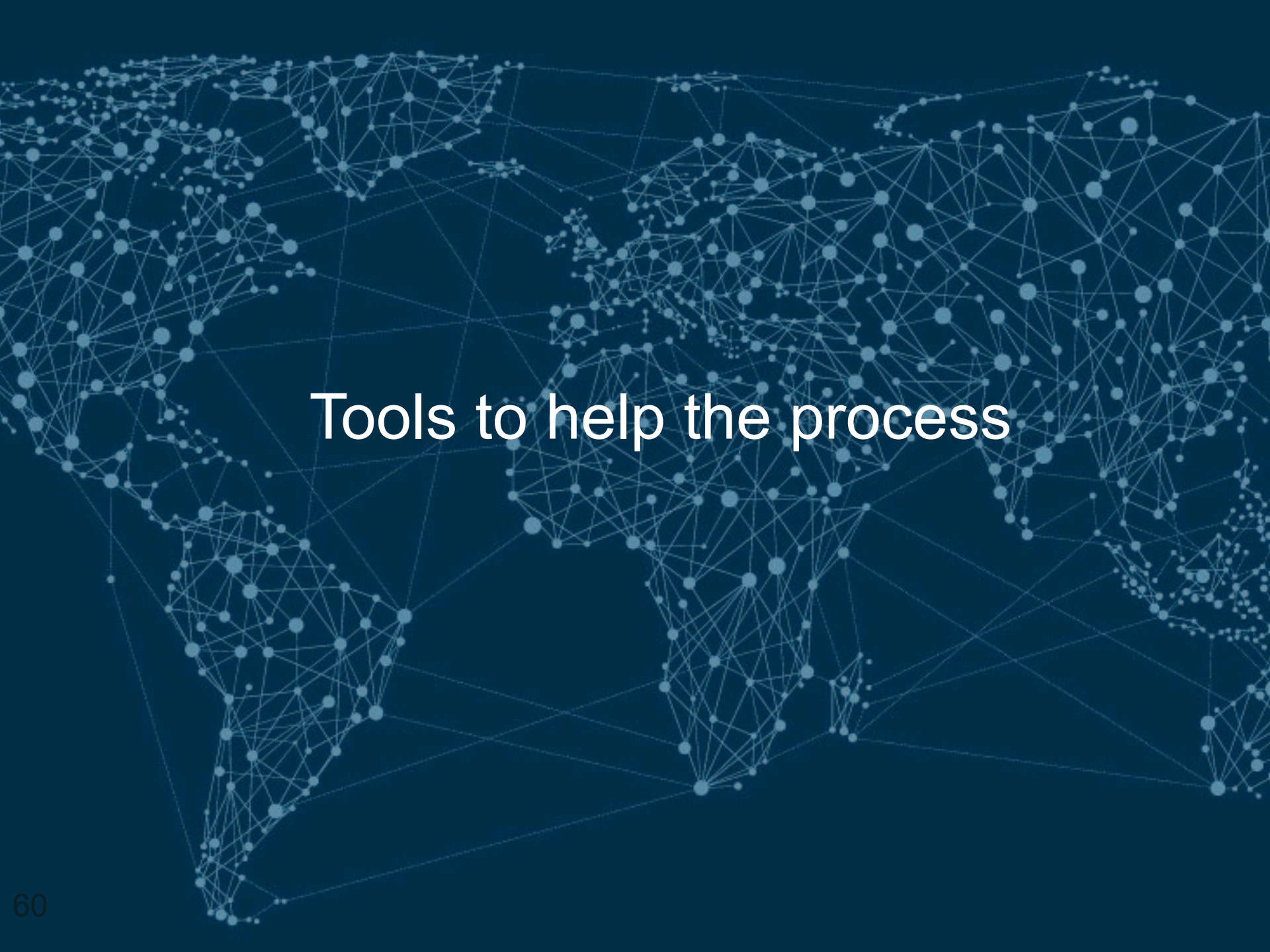
- Create key pairs (KSK and ZSK)

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


Tools to help the process

Tools to use in DNSSEC

- Authoritative Servers that support DNSSEC
  - NSD (by NLNetLabs)
  - Knot (by CZ NIC Labs)
  - BIND (by ISC)
  - Vantio (by Nominum)
  - YADIFA (by EURid)
  - MS DNS Server (by Microsoft)
  - TinyDNSSEC (based on tinydns by D.J. Bernstein)

Tools to use in DNSSEC

- Resolvers that support DNSSEC
  - Unbound (by NLNetLabs)
  - BIND (by ISC)
  - MS Windows Server (by Microsoft)

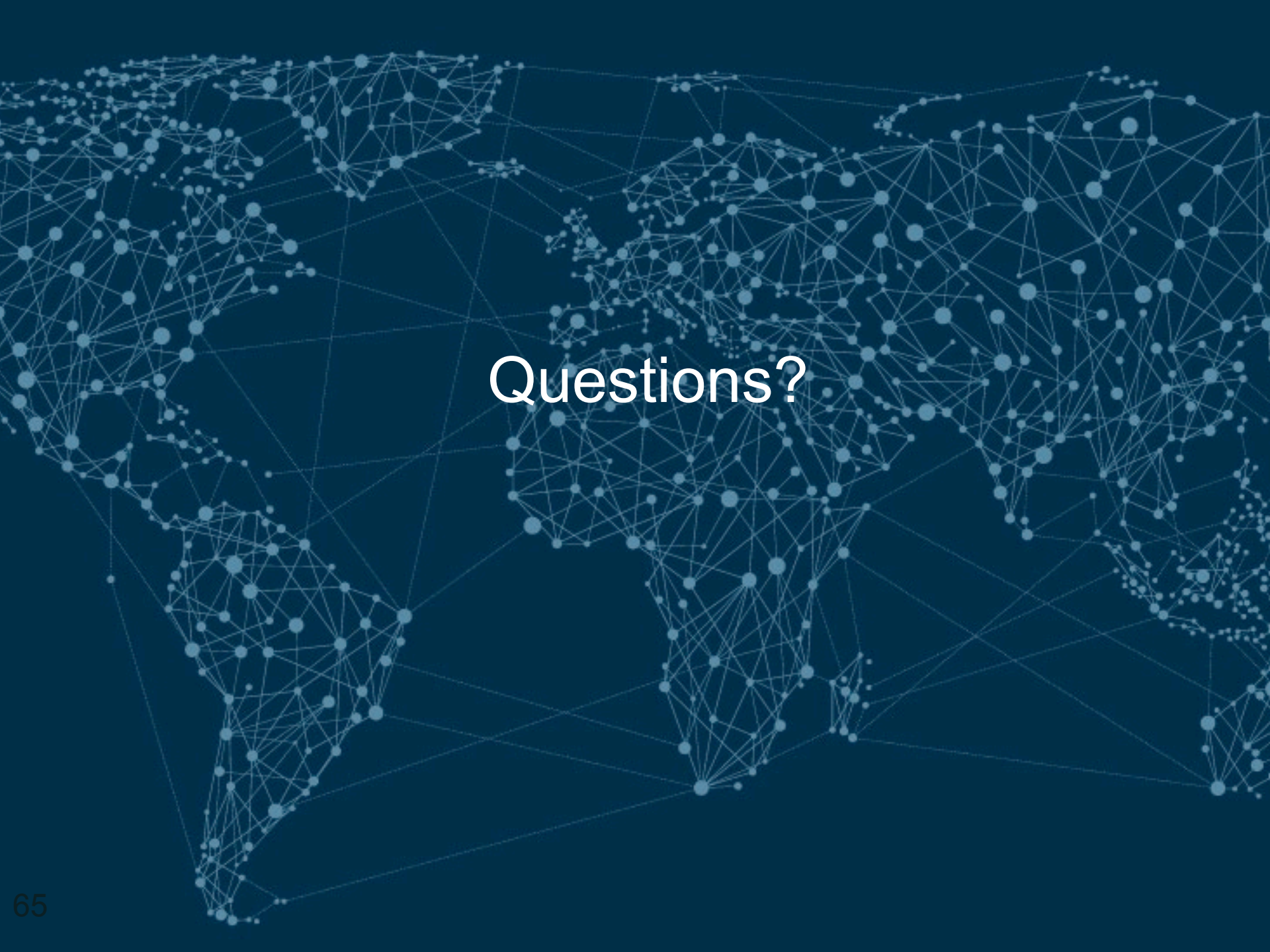
- Tools to automate DNSSEC
  - OpenDNSSEC (by NLnetLabs, .SE, Nominet…et al)
  - DNSSEC-Tools (by Sparta)
  - BIND (by ISC)

Useful links

- https://www.dnssec-deployment.org
- http://www.internetsociety.org/deploy360/dnssec
- http://dnssec-debugger.verisignlabs.com
- http://dnsviz.net
- http://www.dnssec-failed.org

Summary

1. Background
2. Why DNSSEC?
3. How it Works?
4. Signatures and Key Rollovers
5. DNSSEC Demo


Questions?


DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.


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