DNS/DNSSEC

In conjunction with APRICOT2020

Champika Wijayatunga
Regional Technical Engagement Manager – Asia Pacific

12-16 Feb 2020, Melbourne – Australia

Agenda

- DNS Recap
- Setting up Authoritative and Recursive Servers
- DNS Security concepts
- DNS Security Extensions (DNSSEC)
- DNSSEC Key Management

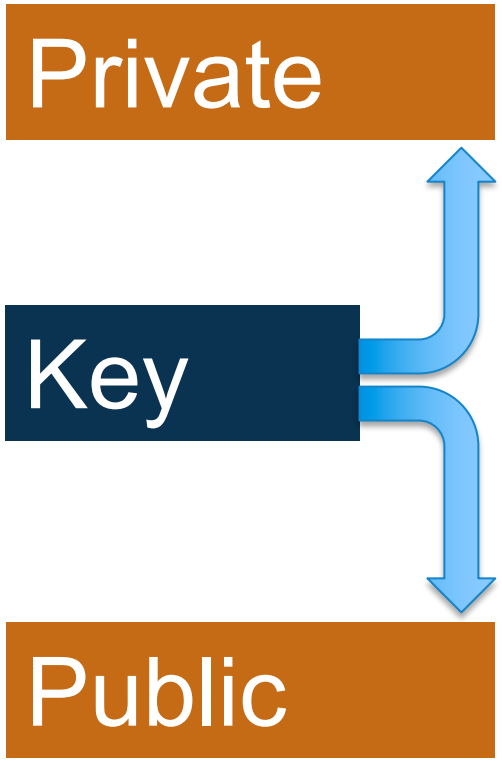
DNSSEC

Digital Signatures in Theory

Key

Digital Signatures in Theory

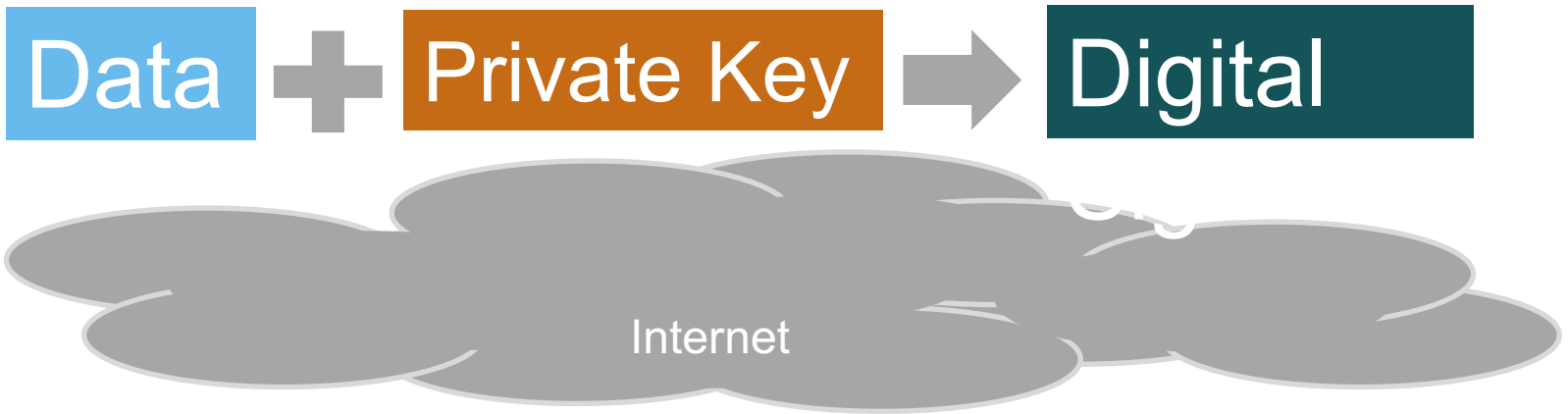
Caution: Cryptography



A pair of keys have a unique bond. If you can "verify" something with one, the other "signed" it.

If the public key of someone verifies it, that person's private key must have signed it.

Digital Signatures in Theory



Signing data...

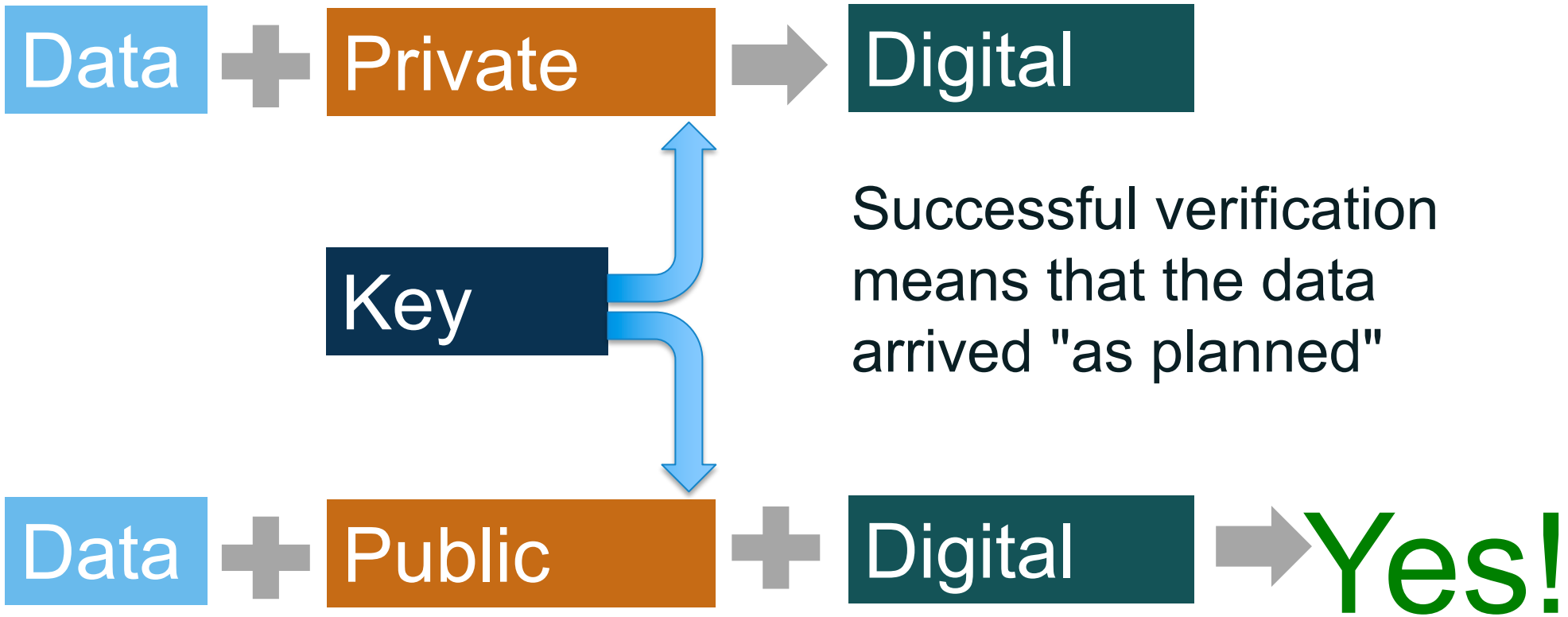
Digital Signatures in Theory

Digital Signatures in Theory

Verifying the data...

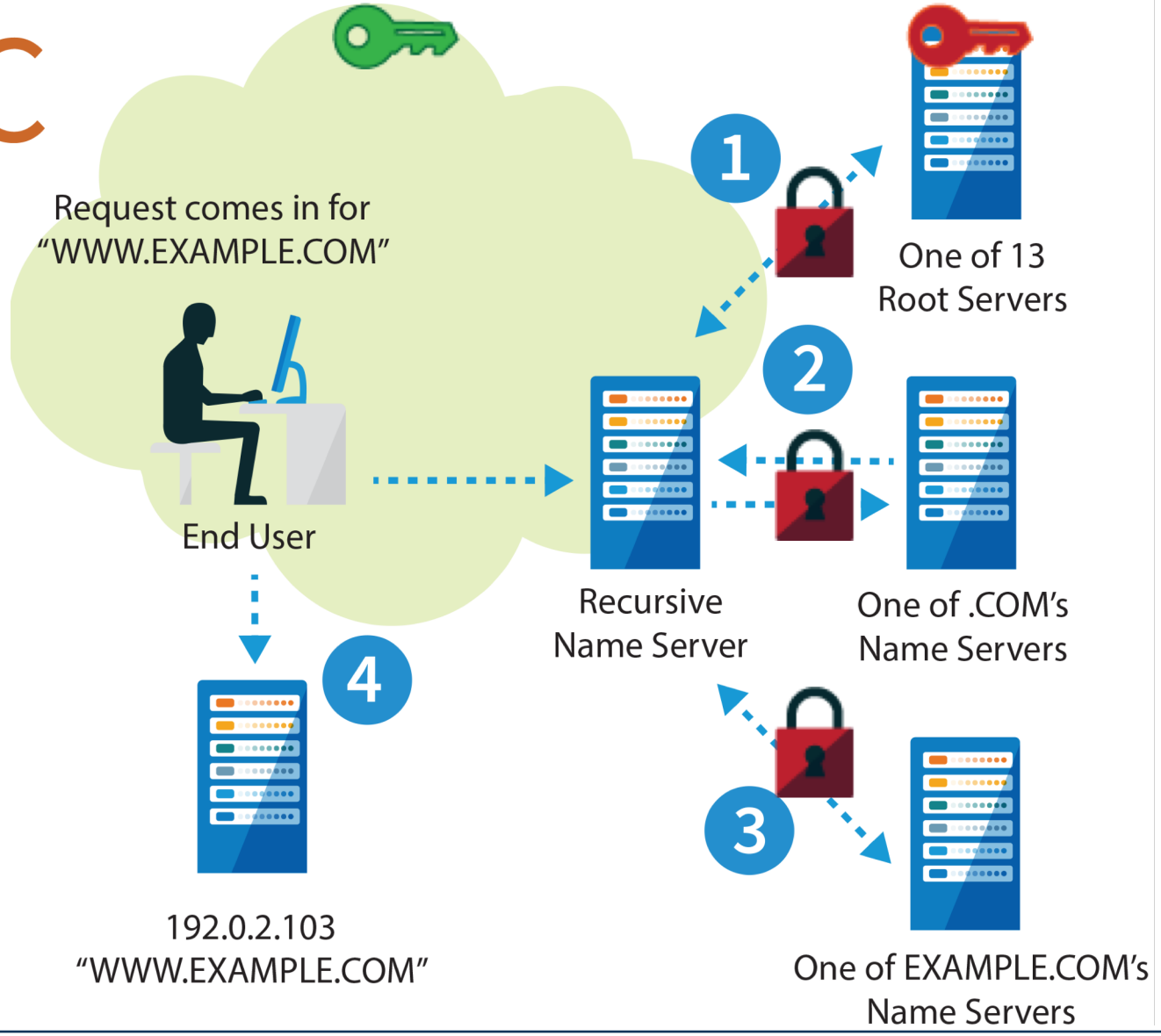
Data + Public + Digital → Yes! OR No!

Digital Signatures in Theory

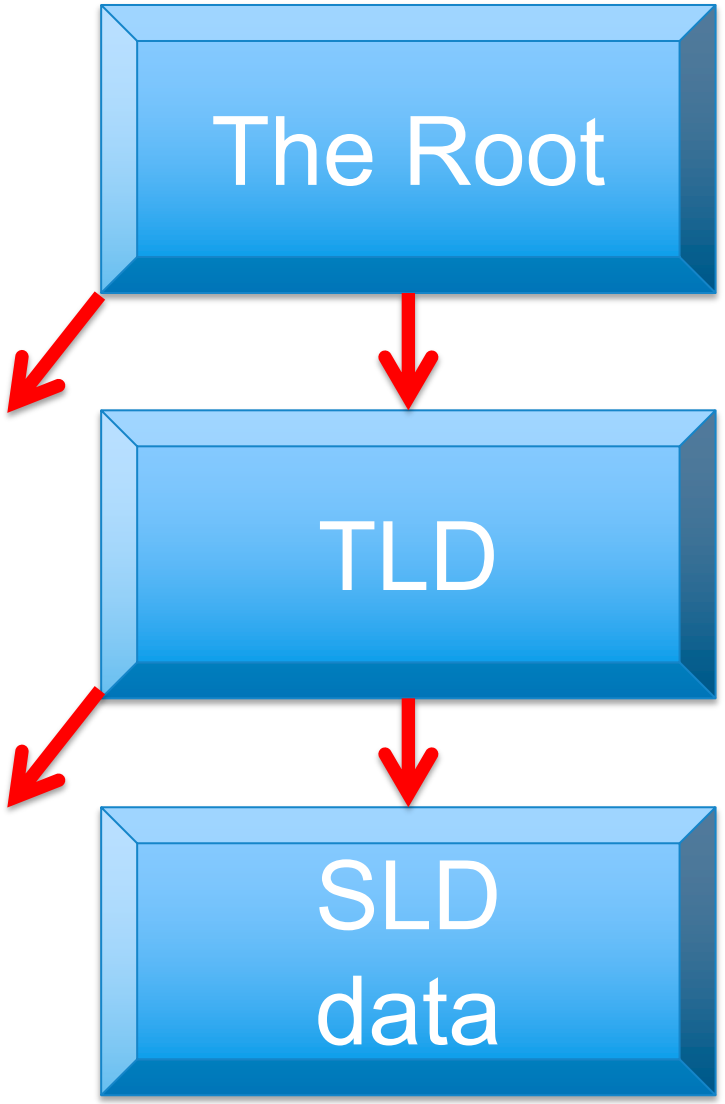


How DNSSEC Works

DNSSEC

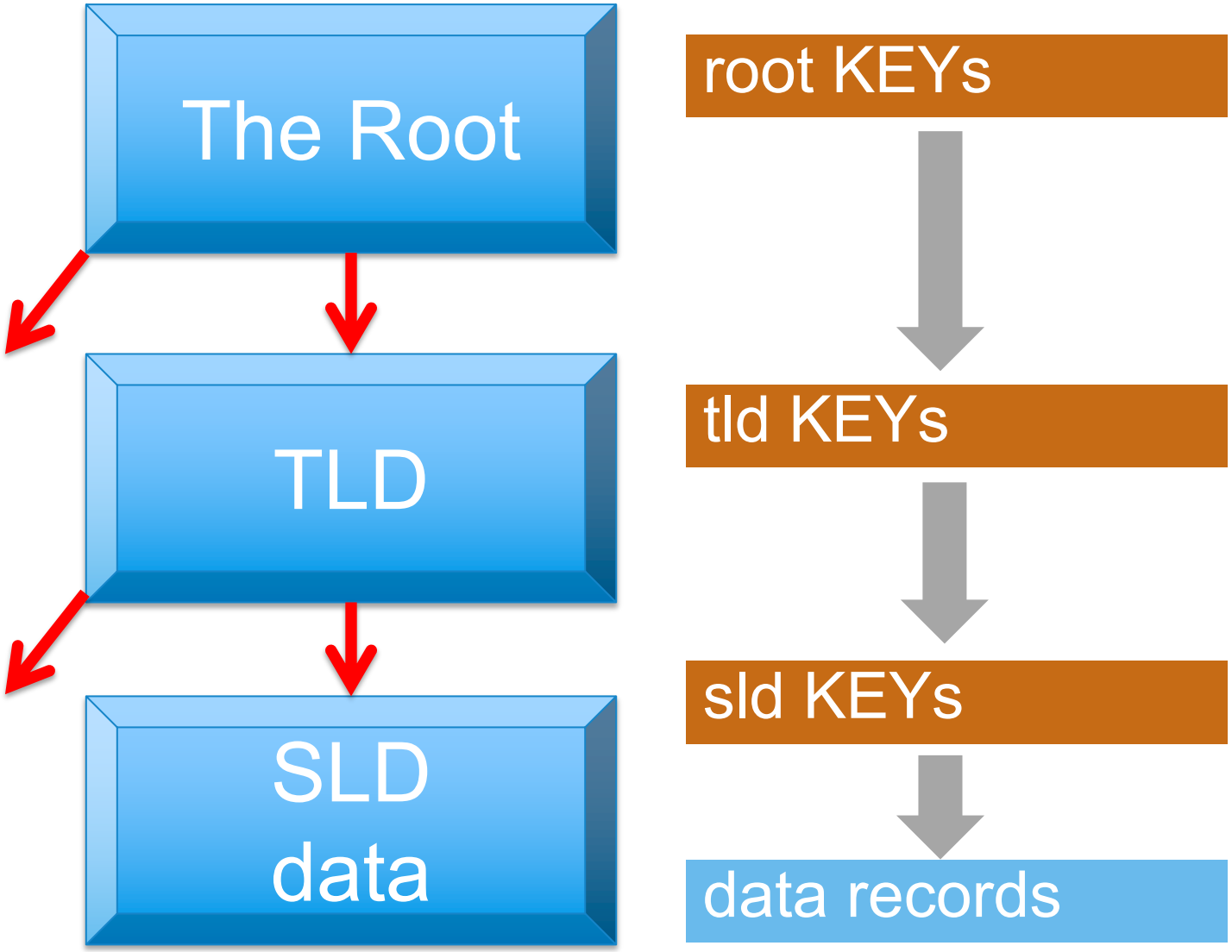


DNS's Data Organization



- The DNS is a federation of owners (registrants) of information
  - Each owner signs their own data with their own key
  - That's a lot of keys
- Hierarchy to the rescue!

DNSSEC Chain of Keys In Theory



Making A Chain

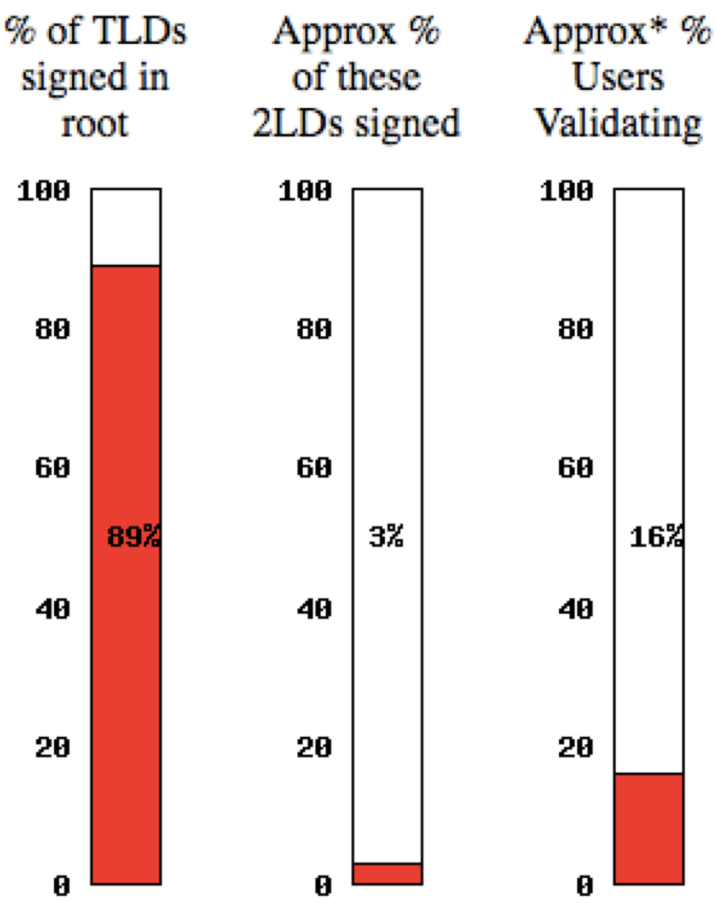
- The root zone signs TLD keys
- A TLD (administrator) signs registrant keys
- A DNS zone administrator (registrant) signs their own data

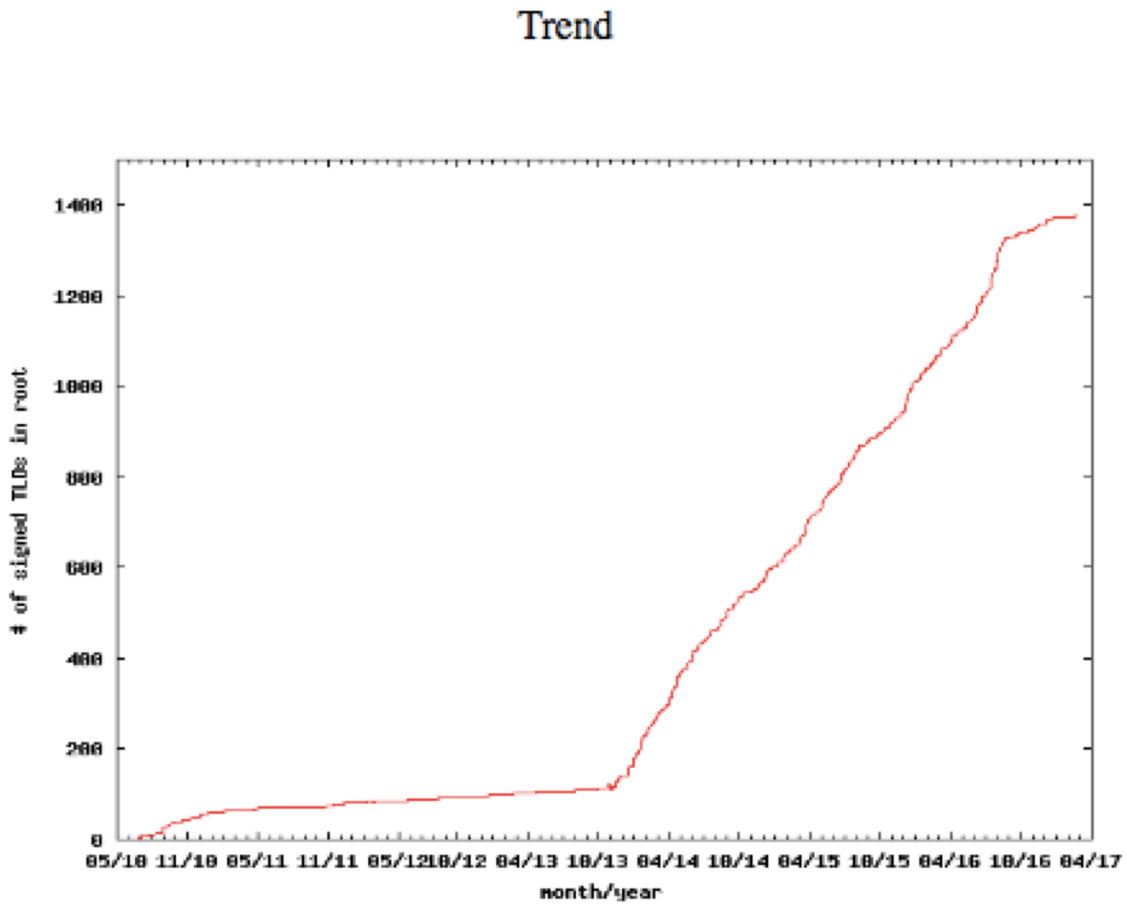
This creates a "chain" used in validation

DNSSEC ccTLD Map

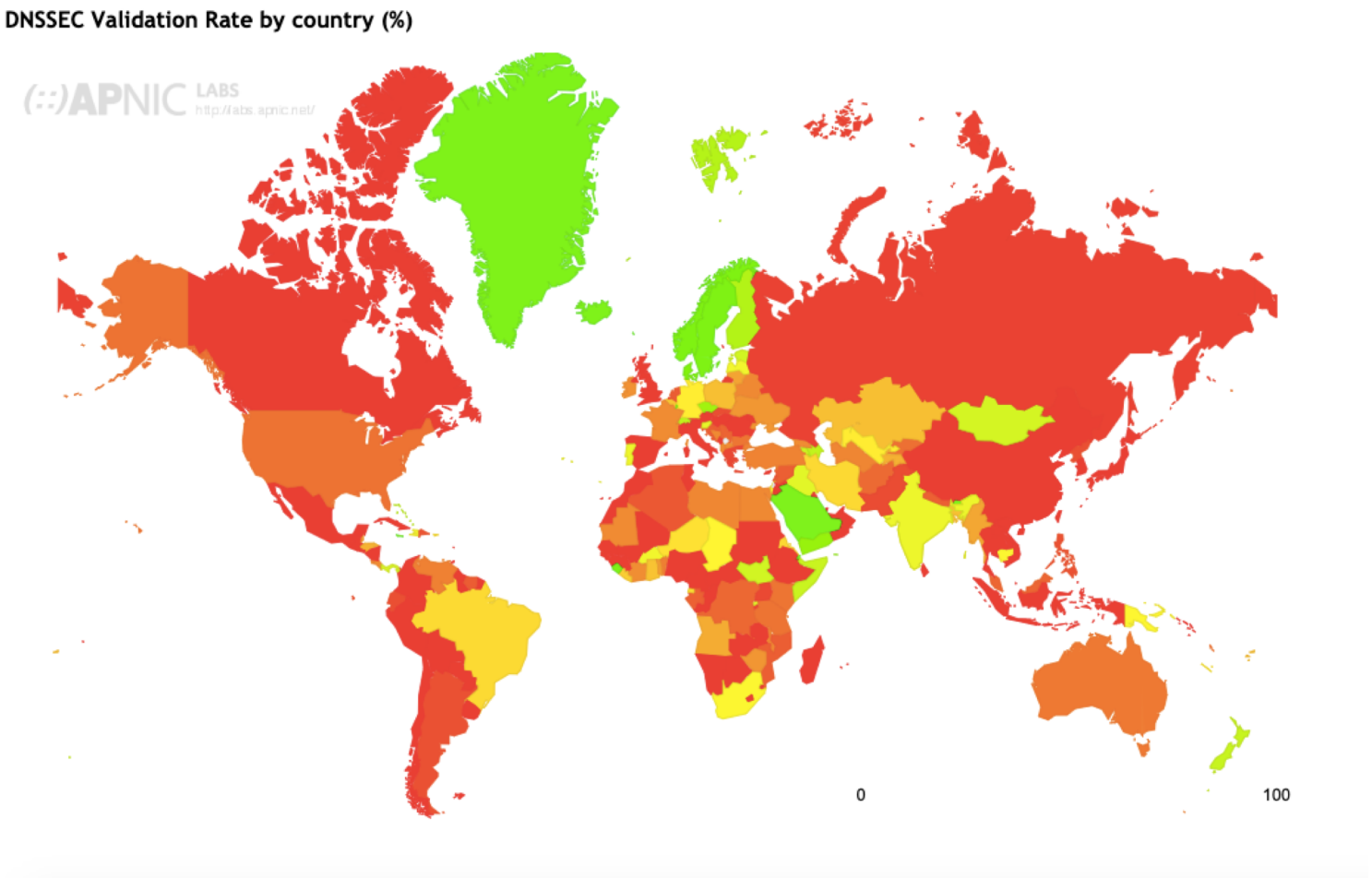
DNSSEC

DNSSEC Deployment





DNSSEC Validations



Region	DNSSEC Validates
World	24.09%
Oceania	32.70%
Europe	26.62%
Americas	24.16%
Asia	23.74%
Africa	21.10%

Country	DNSSEC Validates
Kiribati	95.12%
Iceland	92.34%
Greenland	90.11%
Sweden	83.37%
Finland	76.35%
India	54.06%
Singapore	41.51%
Australia	24.72%
United States	23.75%
United Kingdom	9.70%
Japan	8.71%
China	0.96%

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

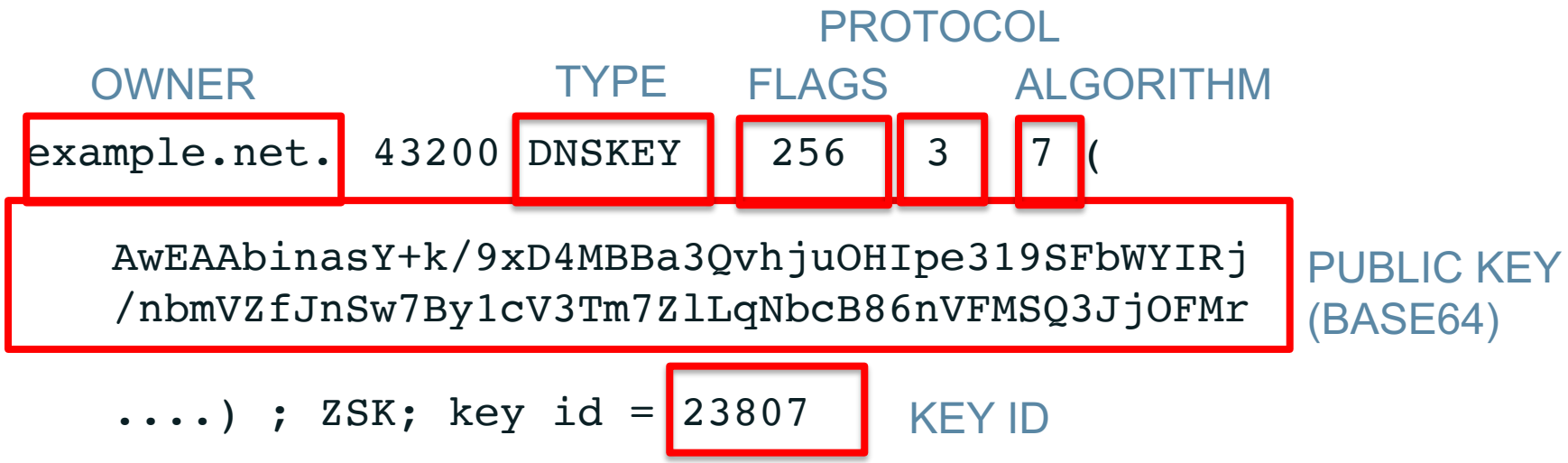
What you can do

- 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

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

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 Key Signing Key (flags=257)

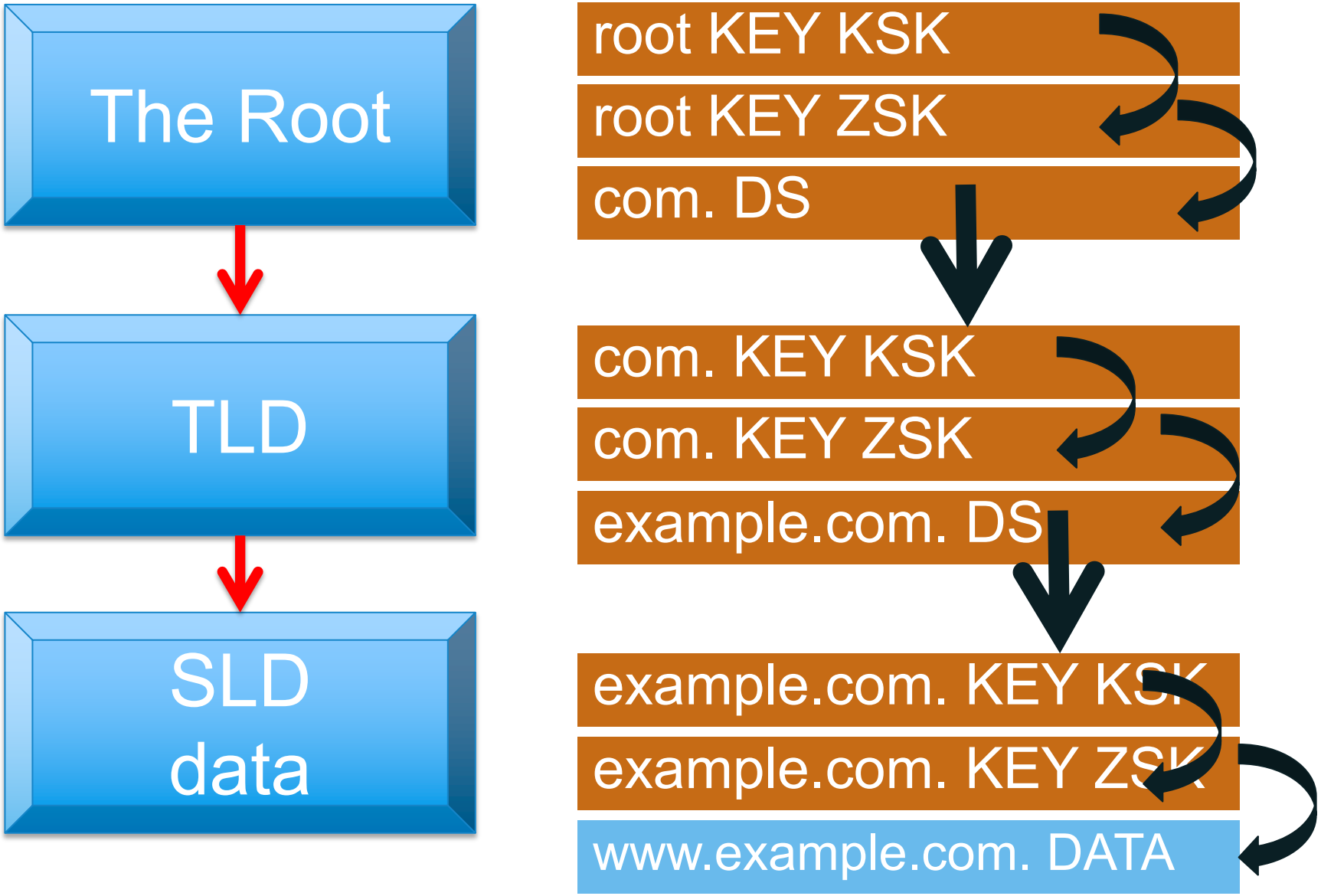
KSK and ZSK

- 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)

Roles (Jobs) of Keys

- A key that is a "ZSK" will sign information
  - Changed frequently and easily
- A key that is a "KSK" will sign the keys
  - Changed rarely and carefully
- The "DS" record
  - Delegation Signer

Signing Chain



New RR: RRSIG (Resource Record Signature)

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

TYPE COVERED #LABELS

OWNER | TYPE | ALG | TTL

```
example.net.  600  RRSIG  A  7  2  600  (
```

SIG. EXPIRATION | SIG. INCEPTION | KEY ID | SIGNER NAME

```
20150115154303  20141017154303  23807  example.net.
```

SIGNATURE

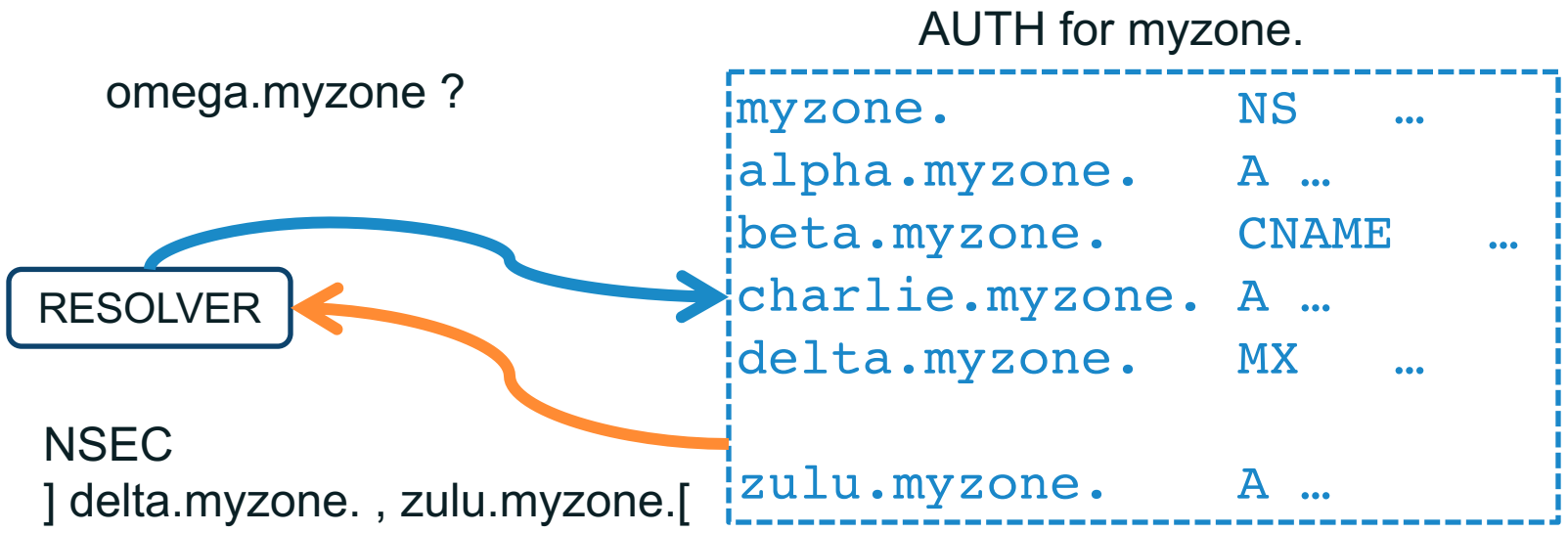
```
CoYkYPqE8Jv6UaVJgRrh7u16m/cEFGtFM8TArbJdaiPu
W77wZhrvonoBEyqYbhQ1yDaS74u9whECEe08gfoe1FGg
. . .
)
```

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

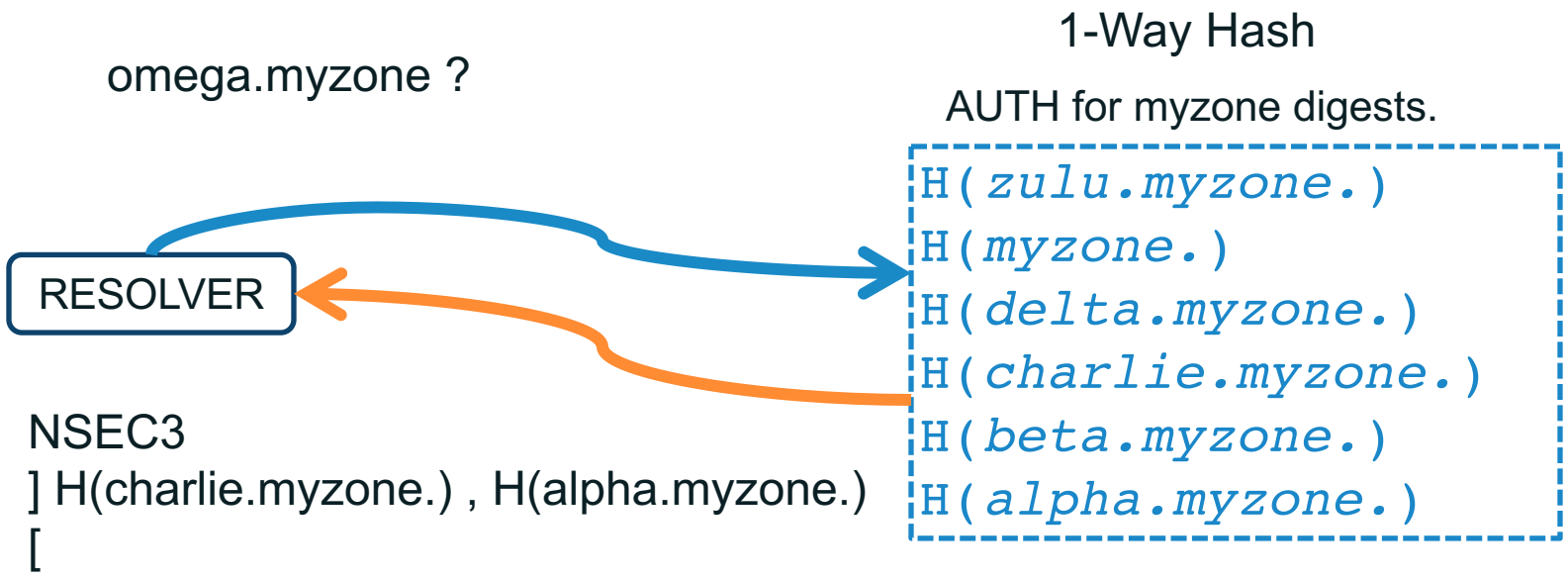
New RR: NSEC

- NXDomains also must be verified
- NSEC provides a pointer to the Next SECure record in the chain of records.



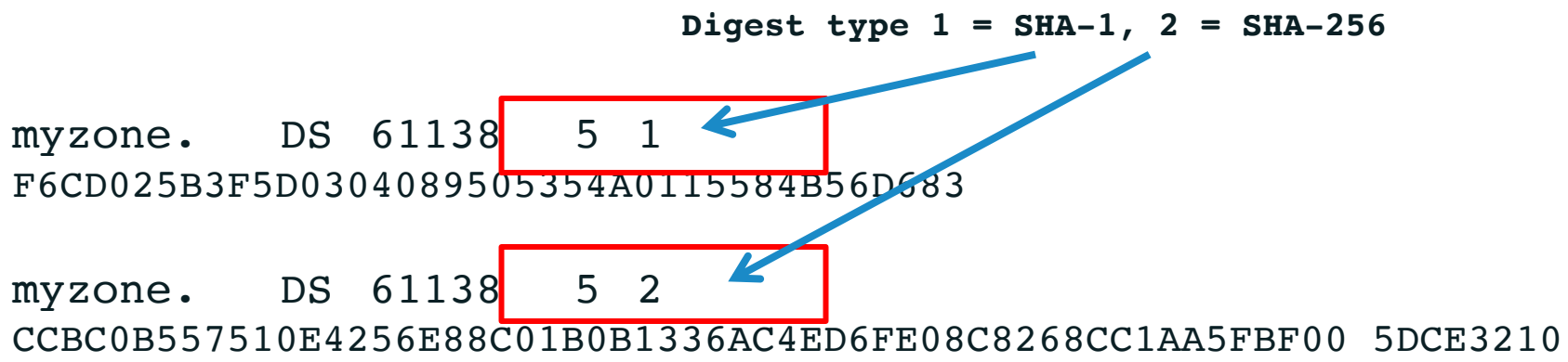
New RR: NSEC3

- 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)



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

Labs
Setting up DNSSEC and Securing Zones

Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

Email: champika.wijayatunga@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann