DNSSEC 101

Understanding DNSSEC

Paul Muchene

Joint ICANN/RIPE NCC Workshop

04 March 2021

ICANN

Today's Agenda

- ICANN: Who we are
- Overview of the DNS
- DNSSEC Signing
- DNSSEC Validation
- State of DNSSEC Deployment

ICANN: Who we are

ICANN's Mission

The mission of the Internet Corporation for Assigned Names and Numbers (ICANN) is to **ensure the stable and secure operation of the Internet's unique identifier systems.**

1. Coordinates the allocation and assignment of names in the root zone of the Domain Name System

2. Coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains (gTLDs)

3. Facilitates the coordination of the operation and evolution of the DNS root name server system

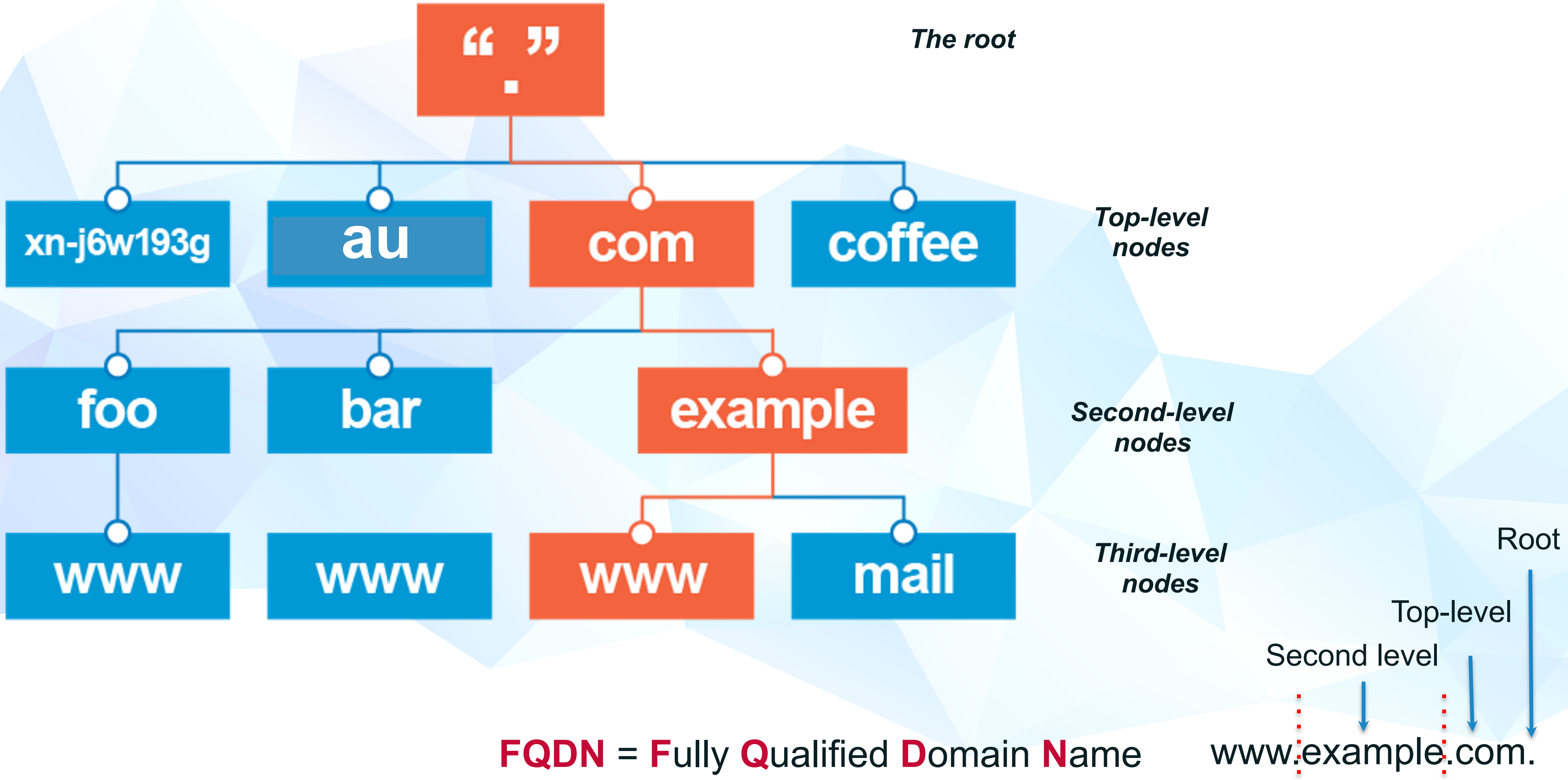
4. Coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers

5. Collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations

Overview of the DNS

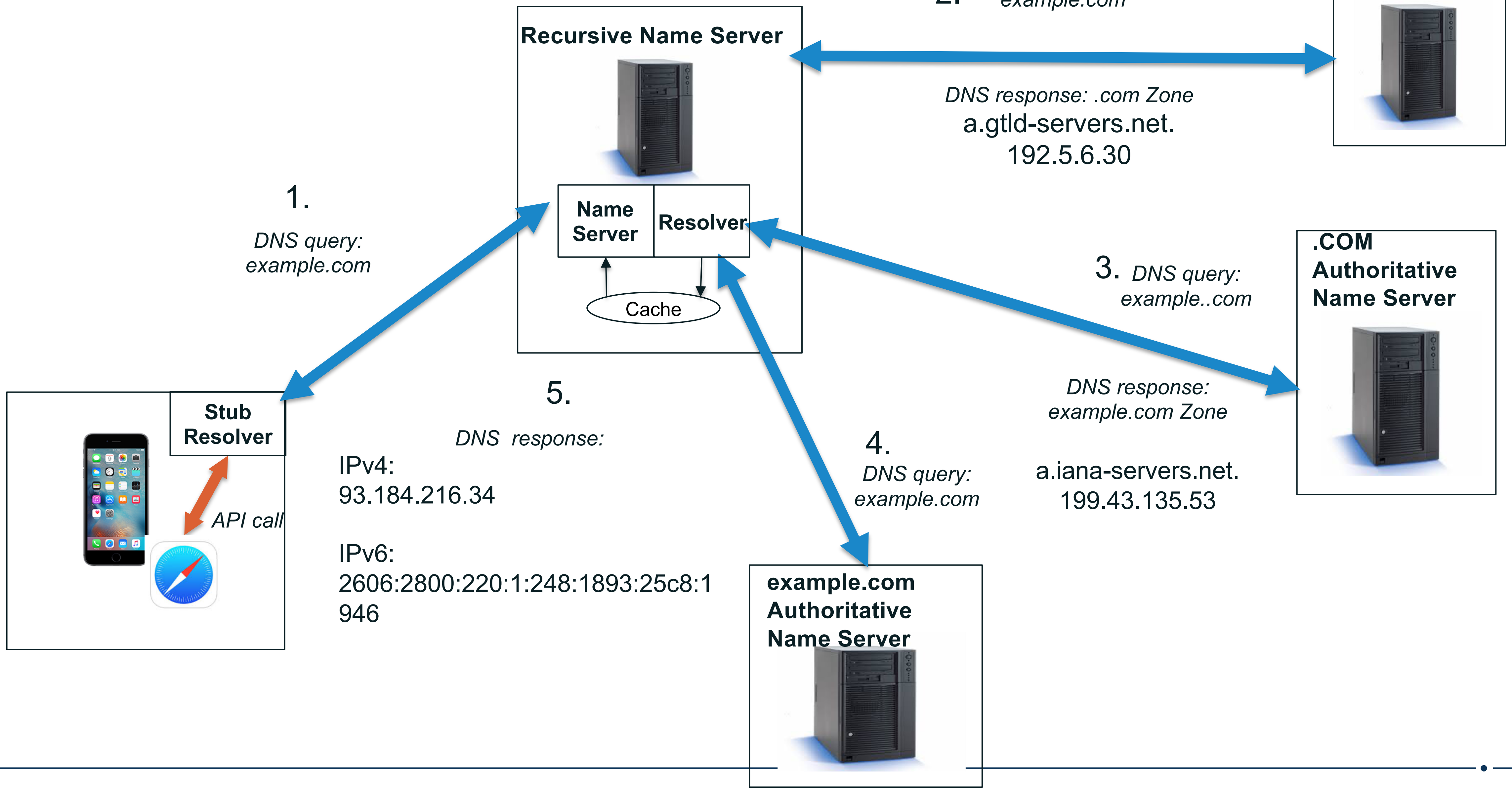
ICANN

The Domain Name System (DNS)

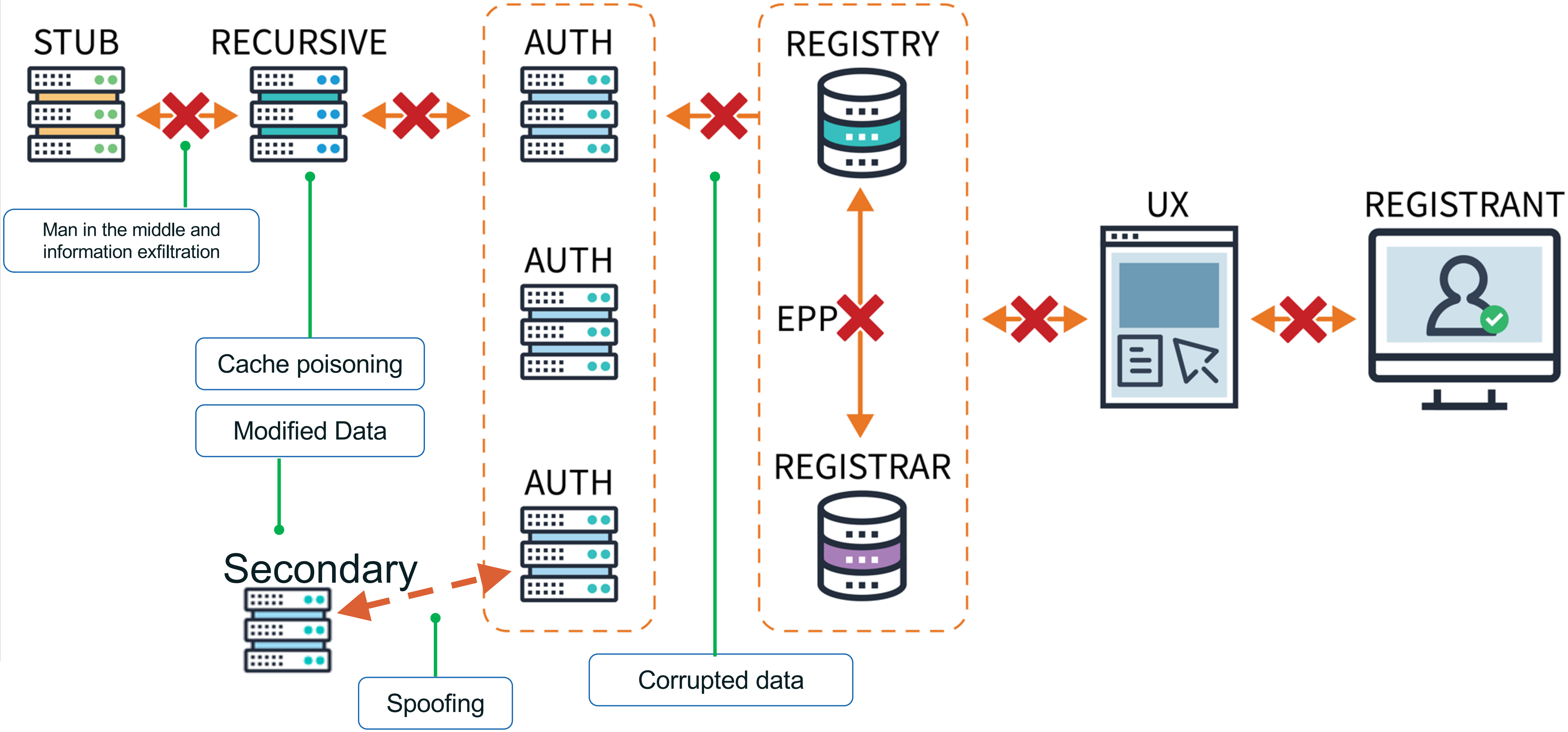


FQDN = **F**ully **Q**ualified **D**omain **N**ame

DNS Resolution Overview

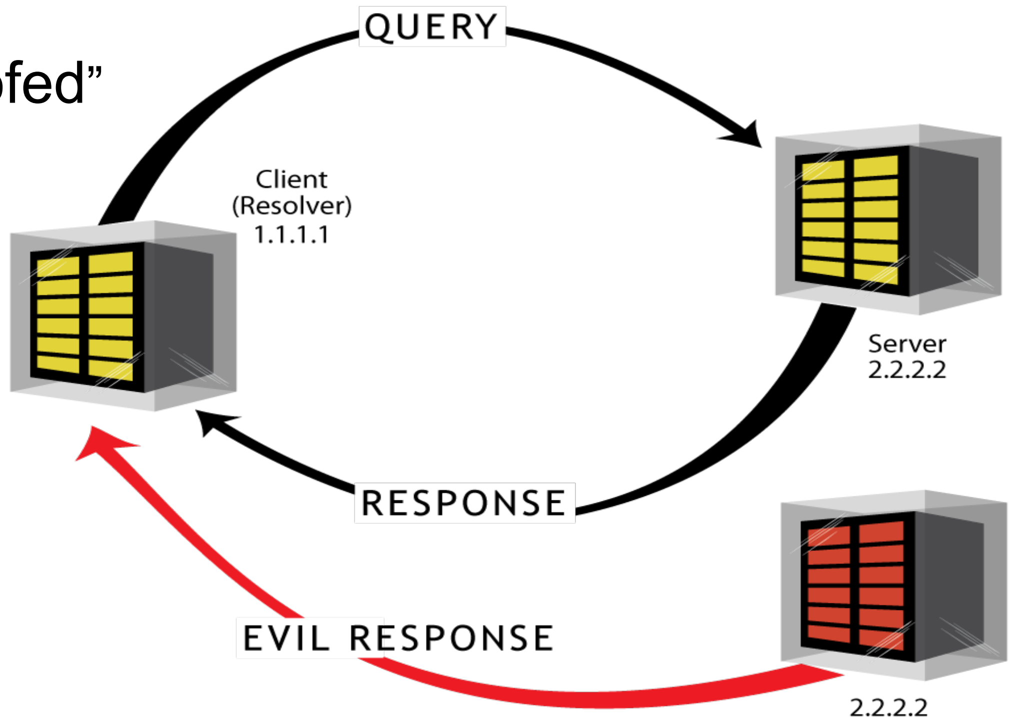


Some of the Potential Target Points of the DNS Ecosystem



Cache Poisoning

- Client has to trust the source address of the server
- But source addresses can be faked or “spoofed”

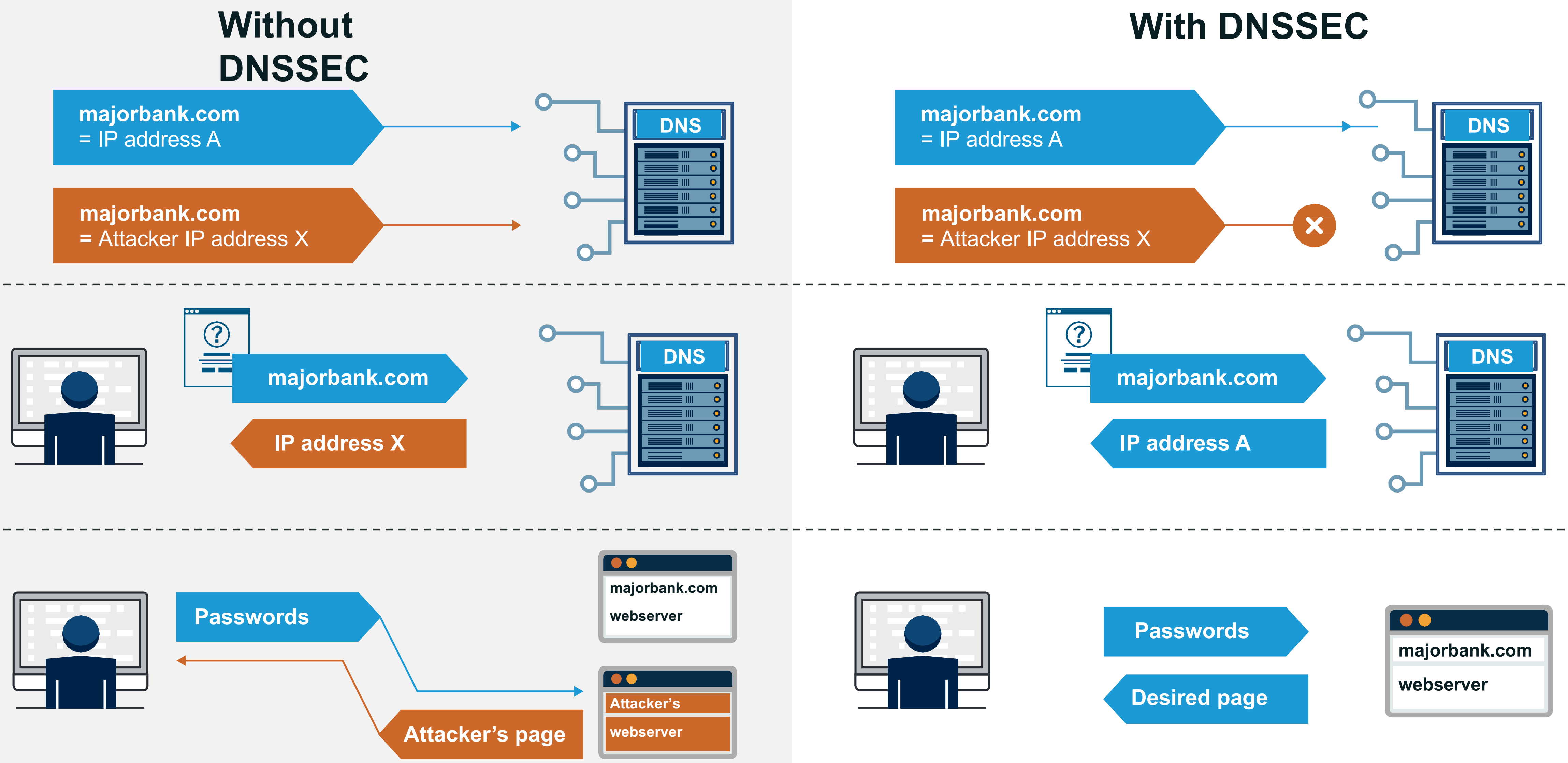


What Is DNSSEC?

DNSSEC stands for **Domain Name System (DNS) Security Extensions.**

- DNSSEC is a protocol that is currently being deployed to secure the DNS.
- DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names.
- DNSSEC is the result of over two decade of community-based, open standards development.
- Specified in RFCs 4033, 4034, 4035

Before and After Deploying DNSSEC



What DNSSEC Does

- DNSSEC uses public-key cryptography and digital signatures to provide:

  Data Origin Authenticity

  - "Did this response really come from the *example.com* zone?"

  Data Integrity

  - "Did an attacker (e.g., a man in the middle) modify the data in this response since the data was originally signed?"

- DNSSEC offers protection against spoofing of DNS data

What DNSSEC Doesn't Do

- Provide any confidentiality for DNS data:
  - ✓ No encryption
  - ✓ Man in the middle-attack
  - ✓ DNS over HTTPS (DoH- RFC 8484) and DNS over TLS (DoT – RFC 7858) – more suited

- Address attacks against DNS software:
  - ✓ DDoS
  - ✓ BCP38

DNSSEC Signing

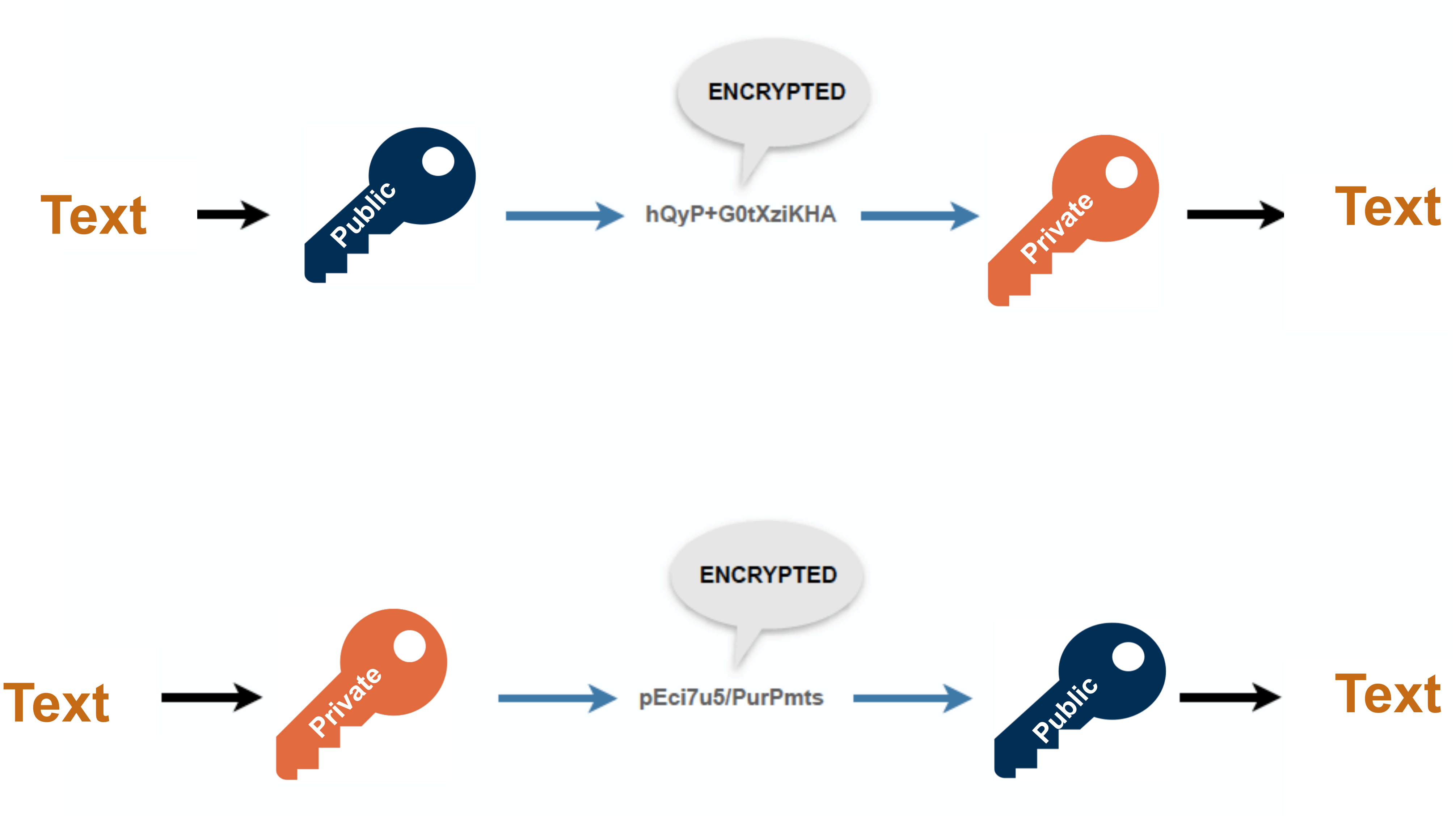
Signing a Zone

Cryptographic Basics

To provide this, we use

- Asymmetric cryptography
- Digital signatures

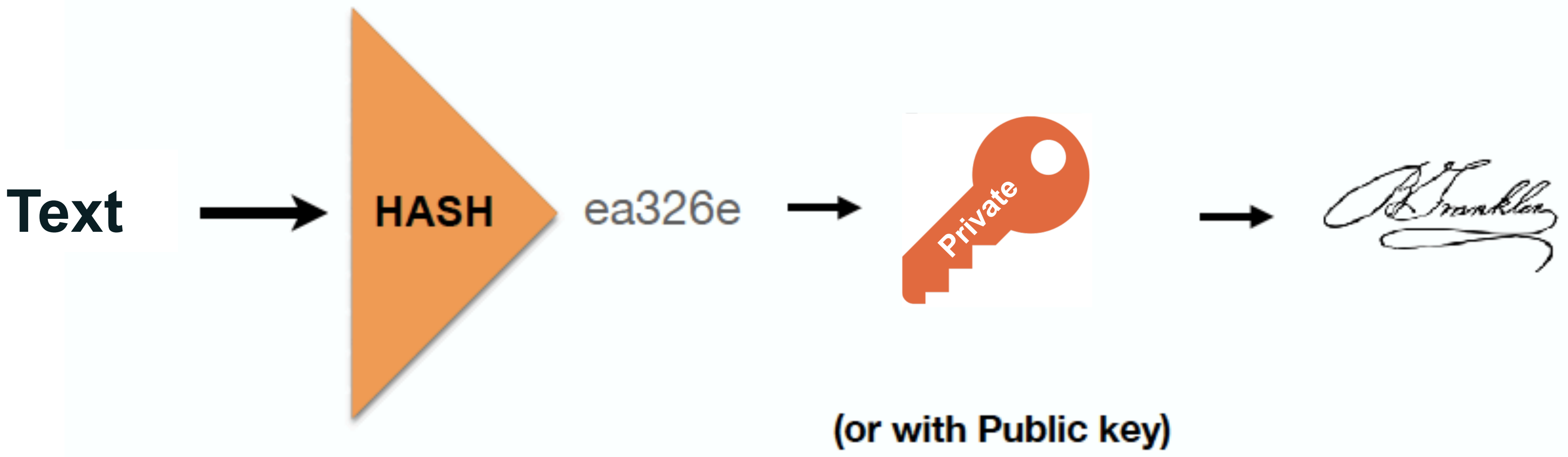
Private and Public Keys



Digital Signature

- We may combine *hash* with *private and public key*, to obtain a digital signature of any text

Hashing + Encrypt = Digital Signature



Two Keys: ZSK and KSK

- 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)

DNSSEC Changes To DNS

New resource record types created for DNSSEC

- DNSKEY – public portion of the cryptographic key
- RRSIG – Resource Record Signature
- DS – Delegation Signer – Pointer from Parent to Child Zone
- NSEC/NSEC3/NSEC5 – Proof of non-existence

DNSKEY– example.com

```
;; QUESTION SECTION:
;example.com.                   IN      DNSKEY

;; ANSWER SECTION:
example.com.            3476    IN      DNSKEY  256 3 8 AwEAAa79LdJaZfIxVzyjq4H7yB4VqT/rIreB+N0jija+4bWHzNrwhSiu D/SOtgvX+gXEgwAR6
tHGn9q9t65o85RfdHJrueORb0usa3x6LHM7qy6A r22P78UUn/rxa9jbi6yS4cVOzLnJ+OKO0w1Scly5XLDmmWPbIM2LvayR 2U4UAqZZ
example.com.            3476    IN      DNSKEY  257 3 8 AwEAAbOFAxl+Lkt0UMglZizKEC1AxUu8zlj65KYatR5wBWMrh18TYzK/ ig6Y1t5YTWCO68byn
orpNu9fqNFALX7bVl9/gybA0v0EhF+dgXmoUfRX 7ksMGgBvtfa2/Y9a3klXNLqkTszIQ4PEMVCjtryl19Be9/PkFeC9ITjg MRQsQhmB39eyMYnal+f3bUxKk4fq7cuEU
0dbRpue4H/N6jPucXWOwiMA kTJhghqgy+o9FfIp+tR/emKao94/wpVXDcPf5B18j7xz2SvTTxiuqCzC MtsxnikZHcoh1j4g+Y1B8zIMIvrEM+pZGhh/Yuf4RwCBgaYCi
9hpiMWV vS4WBzx0/lU=
example.com.            3476    IN      DNSKEY  257 3 8 AwEAAZ0aqu1rJ6orJynrRfNpPmayJZoAx9Ic2/Rl9VQWLMHyjxxem3VU SoNUIFXERQbj0A9Og
p0zDM9YIccKLRd6LmWiDCt7UJQxVdD+heb5Ec4q lqGmyX9MDabkvX2NvMwsUecbYBq8oXeTT9LRmCUt9KUt/WOi6DKECxoG /bWTykrXyBR8elD+SQY43OAVjlWrVltHx
gp4/rhBCvRbmdflunaPIgu2 7eE2U4myDSLT8a4A0rB5uHG4PkOa9dIRs9y00M2mWf4lyPee7vi5few2 dbayHXmieGcaAHrx76NGAABeY393xjlmDNcUkF1gpNWUla4fW
ZbbaYQz A93mLdrng+M=
```

RRSIG – example.com

```
;; QUESTION SECTION:
;example.com.            IN A

;; ANSWER SECTION:
example.com.             6714 IN A 93.184.216.34
example.com.             6714 IN RRSIG A 8 2 86400 (
                                 20210316192457 20210223165712 45150 example.com.
                                 K4fFznogZSz31RqPvWOJep7fh/gATg2i8bh4rj23aHFo
                                 NiVCAr4iY1+t2VYyv6KjYG/DzkIILQt4APLhcfJ8wCmO
                                 EmYZaac0ZkhnDXCaj6PvbHez+QLaF7+8b9Jy0EB02KHG
                                 rXq83JD6W1uZFwUChRJKJt/EK7hEU6N8QzJBpkw= )

;; AUTHORITY SECTION:
example.com.             23883 IN NS b.iana-servers.net.
example.com.             23883 IN NS a.iana-servers.net.
example.com.             23883 IN RRSIG NS 8 2 86400 (
                                 20210316152502 20210223165712 45150 example.com.
                                 T6OCLD1RWhv0nd+1atnk5EL2yNtbBW1A96pdWUPDwGK0
                                 UrR9gNp5JDBrpLJdmJzqiALFg6ggjrflUMP1Mt0yLeCa
                                 I9AbnwG494mAfJyqhZgwdY0d0RHMSVzsfB4/T+wolox3
                                 Xsw10iU4lVWv1SGaoCLR5ysR0p+pkFcEbevgkOw= )
```

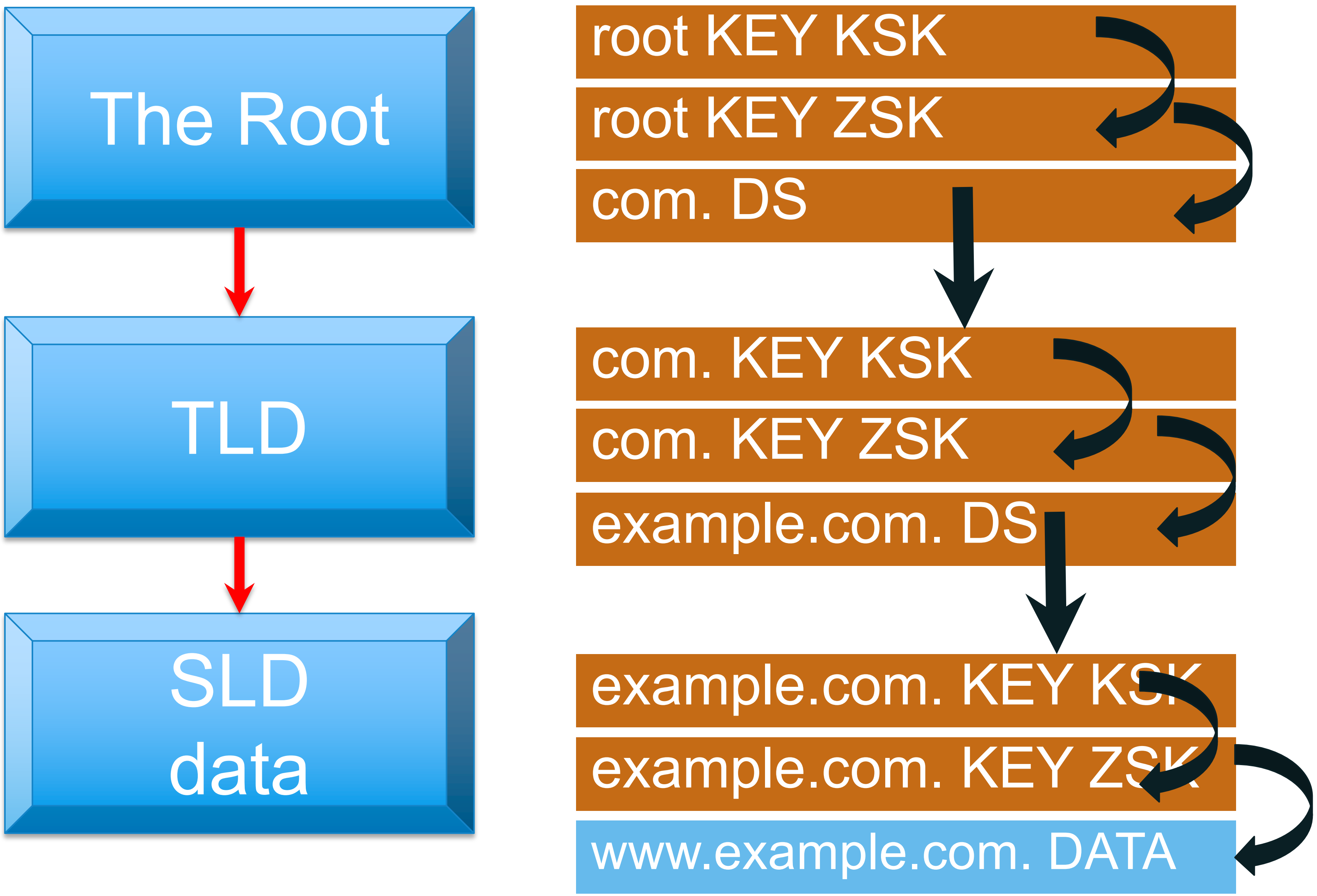
DS – example.com

```
;; QUESTION SECTION:
;example.com.                   IN      DS

;; ANSWER SECTION:
example.com.            6311    IN      DS      43547 8 1 B6225AB2CC613E0DCA7962BDC2342EA4F1B56083
example.com.            6311    IN      DS      31589 8 1 3490A6806D47F17A34C29E2CE80E8A999FFBE4BE
example.com.            6311    IN      DS      31406 8 2 F78CF3344F72137235098ECBBD08947C2C9001C7F6A085A17F518B5D 8F6B916D
example.com.            6311    IN      DS      43547 8 2 615A64233543F66F44D68933625B17497C89A70E858ED76A2145997E DF96A918
example.com.            6311    IN      DS      31589 8 2 CDE0D742D6998AA554A92D890F8184C698CFAC8A26FA59875A990C03 E576343C
example.com.            6311    IN      DS      31406 8 1 189968811E6EBA862DD6C209F75623D8D9ED9142
```

NSEC – example.com

```
;; QUESTION SECTION:
;example.com.                   IN      NSEC

;; ANSWER SECTION:
example.com.            3156    IN      NSEC    www.example.com. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
```

Signing Chain



Unsigned Zone vs Signed Zone: example.com

```
example.com.        SOA   <SOA stuff>
example.com.        NS    ns1.secure-hoster.net.
example.com.        NS    ns2.secure-hoster.net.
example.com.        A     192.45.56.67
example.com.        MX    10 mail.example.com.
mail.example.com.   A     192.45.56.68
www.example.com.    A     192.45.56.67
```

```
example.com.                 SOA          <SOA stuff>
example.com.                 RRSIG        SOA <RRSIG stuff>
example.com.                 NS           ns1.example.com.
example.com.                 NS           ns2.example.com.
example.com.                 RRSIG        NS <RRSIG stuff>
example.com.                 A            192.0.2.1
example.com.                 RRSIG        A <RRSIG stuff>
example.com.                 MX           10
mail.example.com.
example.com.                 RRSIG        MX <RRSIG stuff>
example.com.                 DNSKEY       <Key that signs the
example.com DNSKEY RRset>       ; KSK
example.com.                 DNSKEY       <Key that signs the
rest of the example.com zone> ; ZSK
example.com.                 RRSIG        DNSKEY <RRSIG
stuff>
example.com.                 NSEC         mail.example.com.
SOA A MX DNSKEY RRSIG NSEC
```

DNSSEC Validation

DNSSEC enabled - resolvers in action

DNSSEC Validation

- DNSSEC validation is the process of checking the signatures on DNSSEC data
- Validation can occur in applications, stub resolvers or recursive resolvers
- Most validation today occurs in recursive resolvers
- Trust Anchor: To perform DNSSEC validation, you have to trust somebody (some zone's key). **Root Zone KSK is the most important trust Anchor**
- What happens when validation fails?
  - Overloaded signaling mechanism from recursive resolver to stub resolvers
    - SERVFAIL error, which has other meanings
  - No signaling mechanism from stub resolver to application
    - Most resolver APIs not rich enough to pass validation status

Digital Signatures - Verification

Hash of Data + Private → Digital Signature

Key

Successful verification means that the data arrived "as planned"

Hash of Data + Public + Digital Signature → Yes!

Chain of Trust

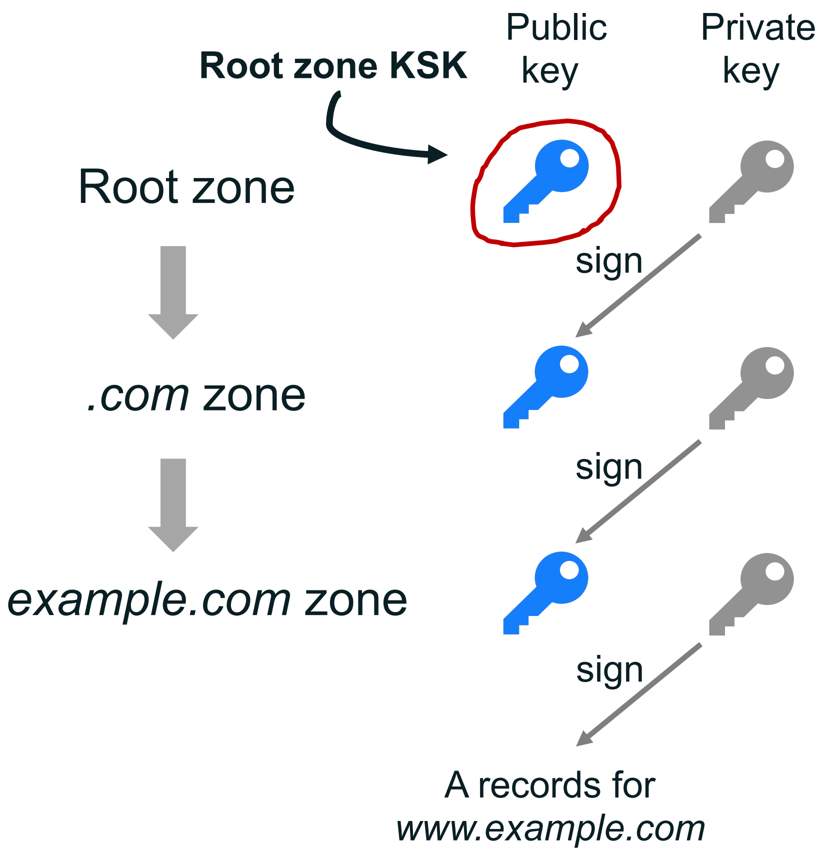
Finally, how do we trust DS record?

Well, we just sign DS record like we did with other RRsets, creating a corresponding RRSIG for the DS record in the parent.

We repeat the validation process and get to the parents public KSK... And again must go to that parent's DS record to verify… on and on up to the DNS root.

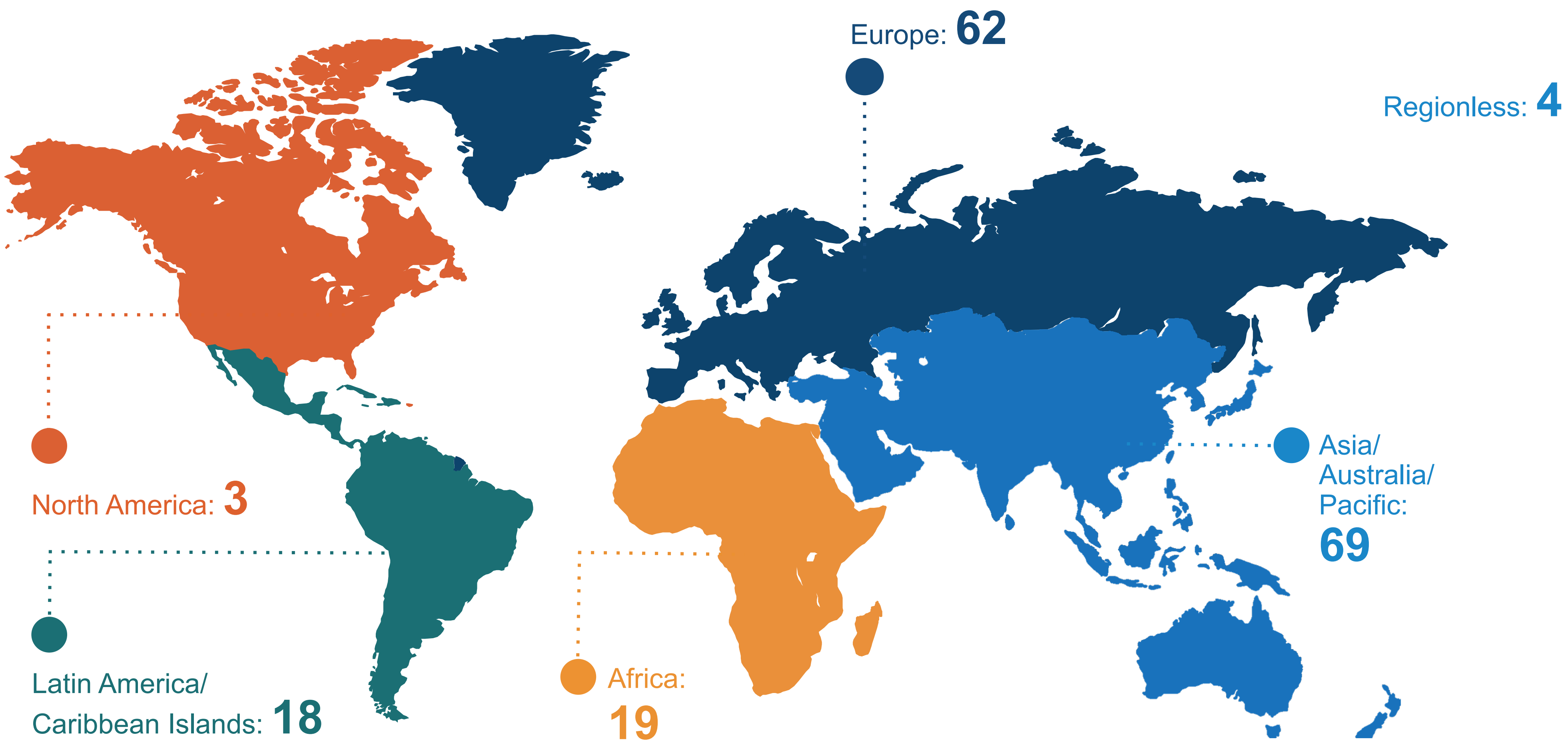
Eventually, we get to the root and there's nothing up there (sadly no parent)… and so we must come with a solution to create a trust anchor for the root, a "one key to rule them all" (*sorry, can't resist quoting LOTR again*)… and here it comes a solution implemented since 2010 called:

The Root Signing Ceremony



State of DNSSEC Deployment

State of DNSSEC Deployment in ccTLDs – (November 2020)



Based on ICANN Geographic Regions: https://meetings.icann.org/en/regions

State of DNSSEC Validation

- Most validation today occurs in recursive resolvers
- **Bad News:**
  25% of DNS responses are validated according to APNIC Labs*
  Too many resolvers do not validate DNS answers
  . . And not enough domains are signed
- ICANN has a mandate in our strategic plan for 2021-2025 to significantly increase DNSSEC adoption, including convincing DNS resolver vendors to ship their software with DNSSEC validation turned-on by default

State of DNSSEC Validation– (February 2021)

Code	Region	DNSSEC Validates	Partial Validates	Samples	Weight	Weighted Samples
XA	World	24.88%	10.00%	8,974,483	1	8,974,483
XF	Oceania	37.97%	6.46%	36,589	1.77	64,935
XE	Europe	30.85%	7.01%	1,718,347	0.77	1,325,288
XC	Americas	28.22%	5.67%	2,157,096	0.74	1,602,788
XD	Asia	23.38%	10.31%	4,353,851	1.17	5,102,891
XB	Africa	17.59%	20.91%	708,599	1.24	878,388
XG	Unclassified	0	0	64	3.08	196

Source: APNIC Labs: https://stats.labs.apnic.net/dnssec/XA

Questions, Comments and Feedback

octo@icann.org

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann