Domain Name System Security

Moritz Müller

SIDN LABS

SIDN and SIDN Labs

- *Stichting Internet Domeinregistratie Nederland* (SIDN)

- Critical infrastructure services
  - Lookup IP address of a domain name (almost every interaction)
  - Registration of all .nl domain names
  - Manage fault-tolerant and distributed infrastructure

- Labs = research department
- www.sidnlabs.nl

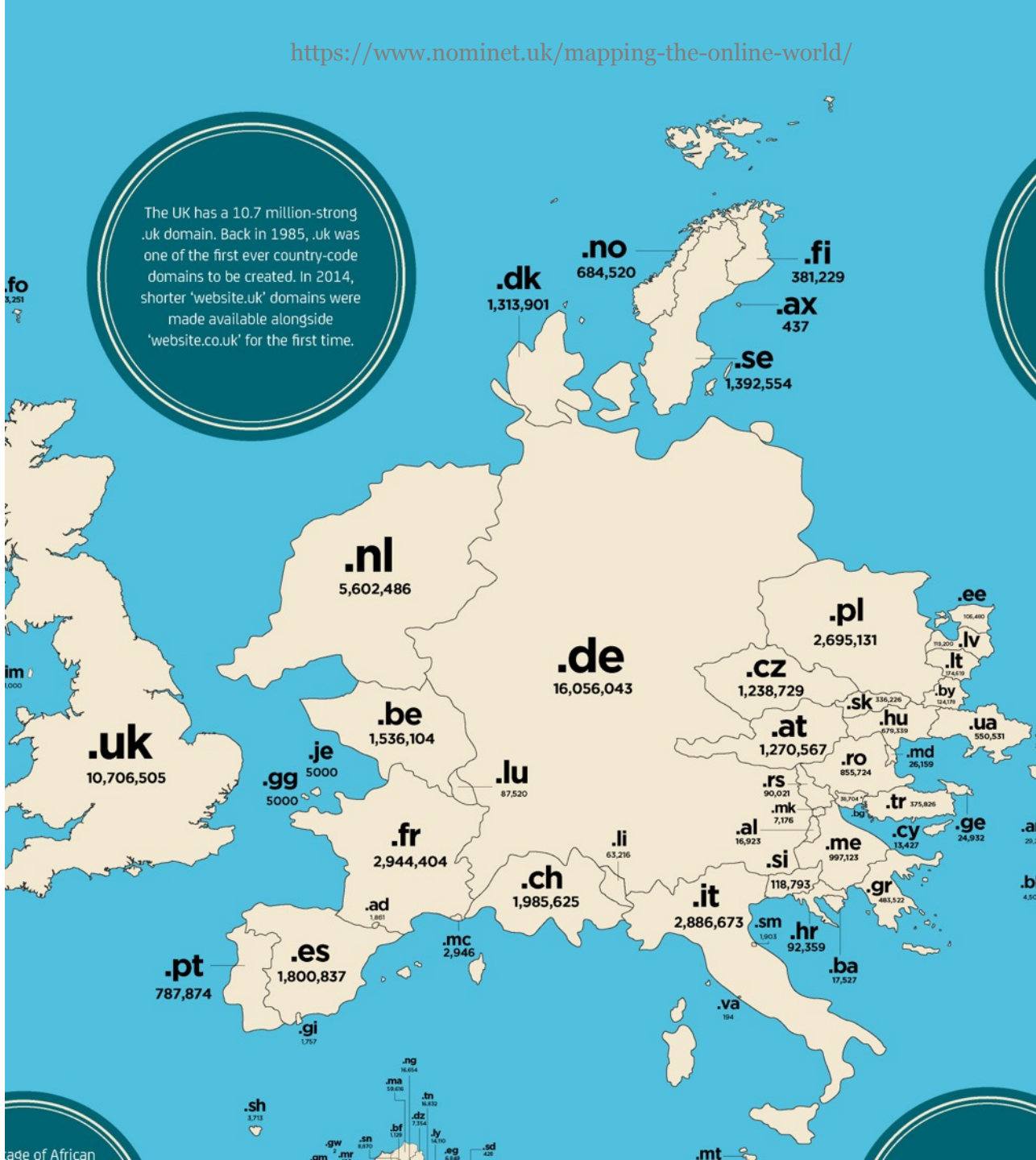
.nl = the Netherlands
17M inhabitants
6.0M domain names
3.3M DNSSEC-signed
2.5B DNS queries/day

Agenda

- Introduction to the DNS
- Attacks on the DNS
- DNSSEC to the rescue
- Other challenges to the DNS

Photo by Kelli Tungay on Unsplash

The Domain Name System



The Basics

- Since 1983
- Most known for translating domain names to IP addresses
- Precedes almost any connection setup on the Internet
- Also other information stored in the DNS
  - Text: TXT
  - Mail servers: MX
  - SPF/DKIM/ DANE
  - many more…

The DNS components

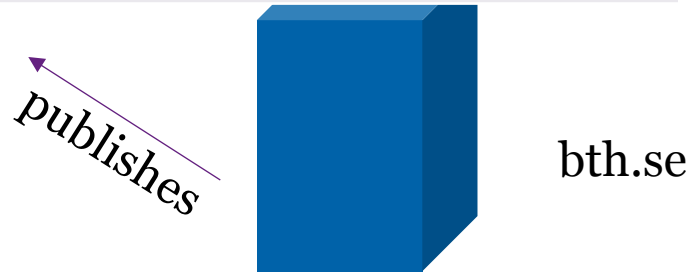
Would like to visit www.bth.se.

bth.se

Authoritative Name Server

Zone file of: **bth.se**

domain name	TTL	class	type	value
@	86400	IN	SOA	netsrv10.bth.se. hostmaster.litnet.se. (2015101478 ; serial ... 900 ; minimum (15 minutes))
	86400	IN	NS	sunic.sunet.se.
	86400	IN	NS	netsrv10.bth.se.
	86400	IN	NS	ns3.ltblekinge.se.
www	86400	IN	A	213.52.129.125
www	86400	IN	AAAA	2a01:7e00::f03c:91ff:fe18:15af



The DNS components

Recursive
Resolver

bth.se

Authoritative Name Server

Recursive resolver usually provided by:

- your Internet Service Provider (ISP)
- your local network (e.g. university, coffee shop, …)
- a cloud provider (e.g. Google [8.8.8.8], Cloudflare [1.1.1.1])

SDN LABS

The DNS lookup

What is the IP address of www.bth.se.

Recursive Resolver

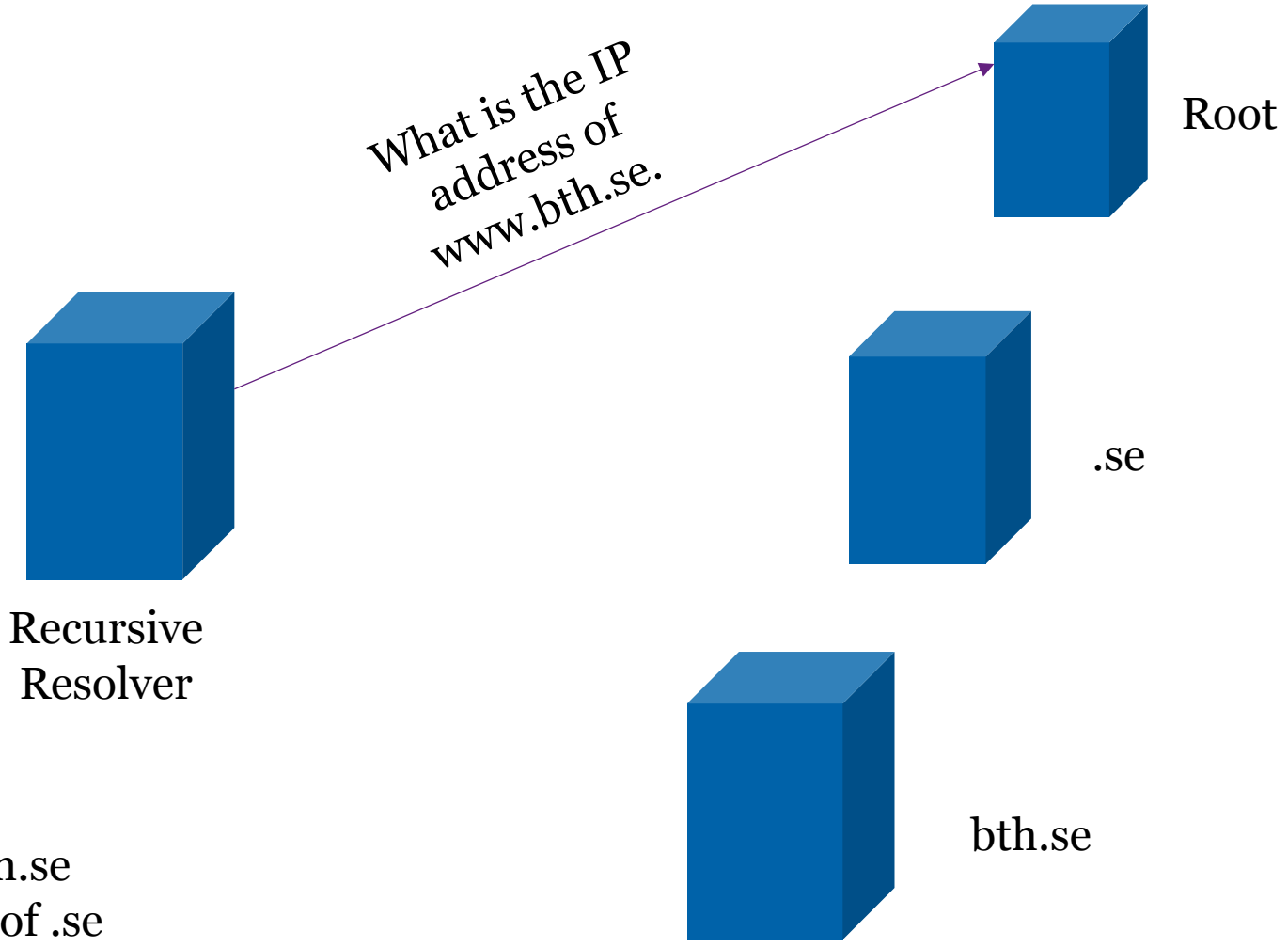
Root

.se

bth.se

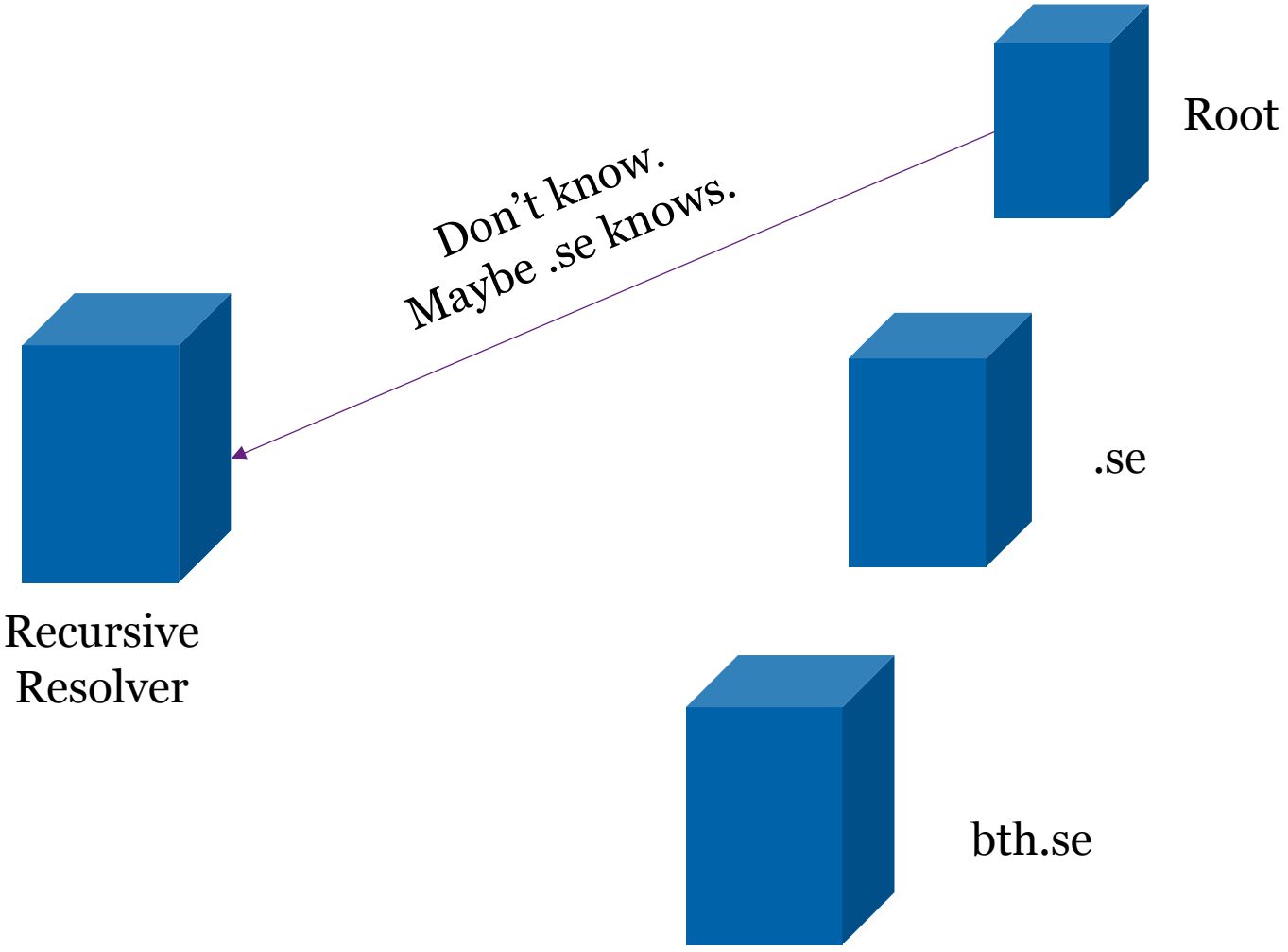
Authoritative Name Server

The DNS lookup



- .se is the “parent” of bth.se
- Root (.) is the “parent" of .se

The DNS lookup



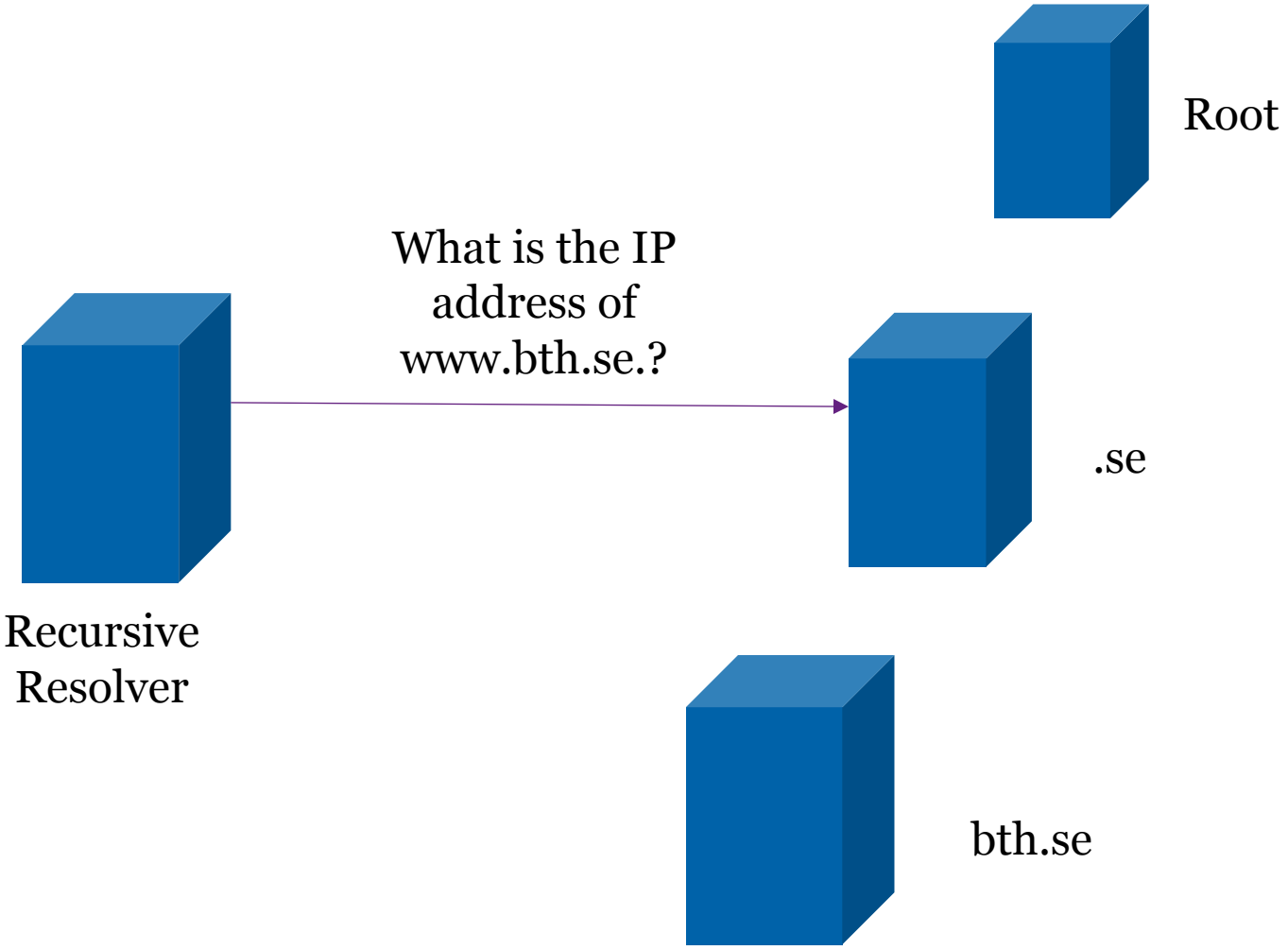
Response of the root

domain name	TTL	class	type	value
Answer Section				
-				
Authority Section				
se.	172800	IN	NS	a.ns.se.
se.	172800	IN	NS	b.ns.se.
				…
Additional Section				
a.ns.se.	172800	IN	A	192.36.144.107
b.ns.se.	172800	IN	A	192.36.133.107
				…

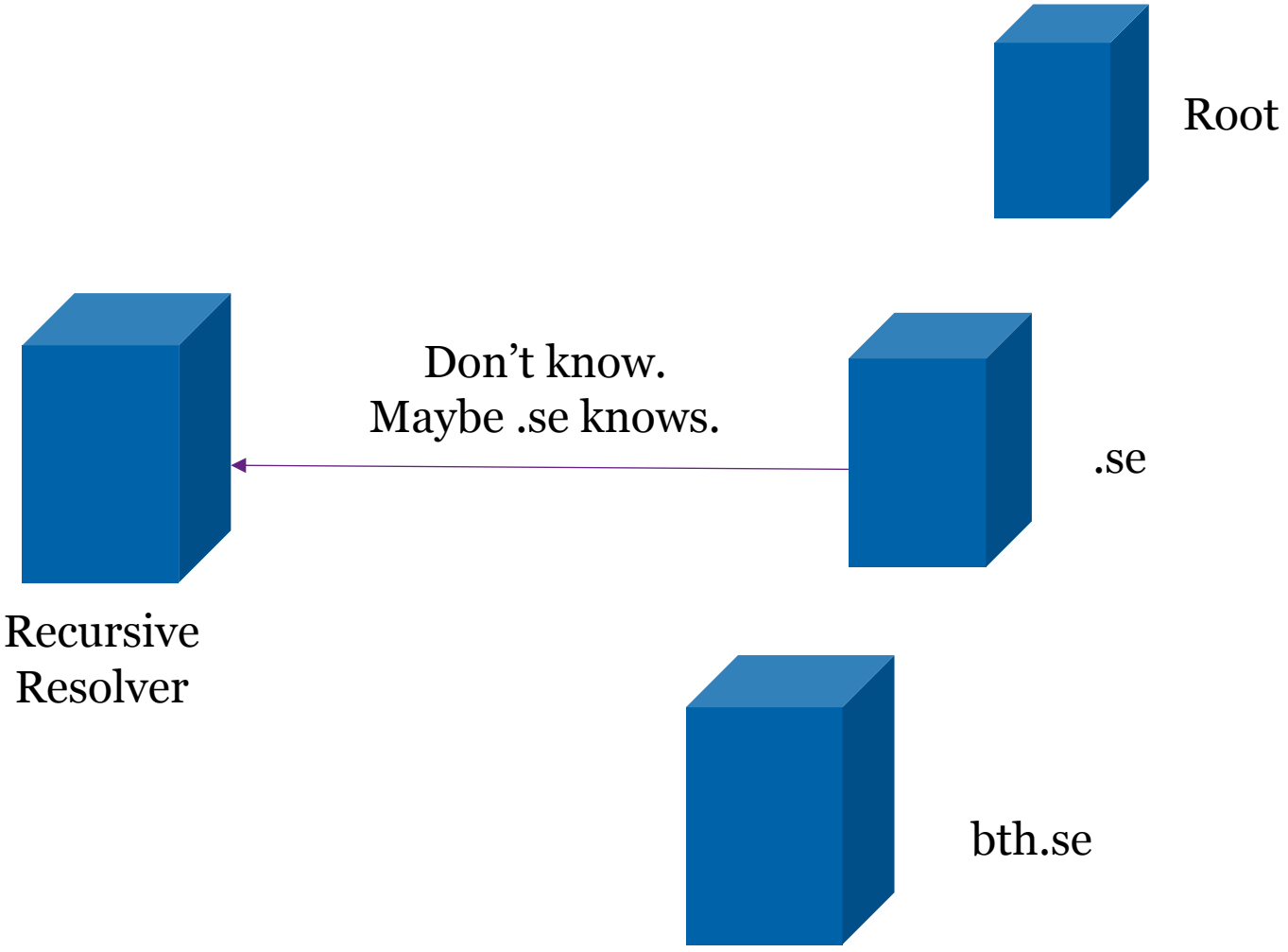
Root

```
dig +multiline @a.root-servers.net www.bth.se
```

The DNS lookup



The DNS lookup



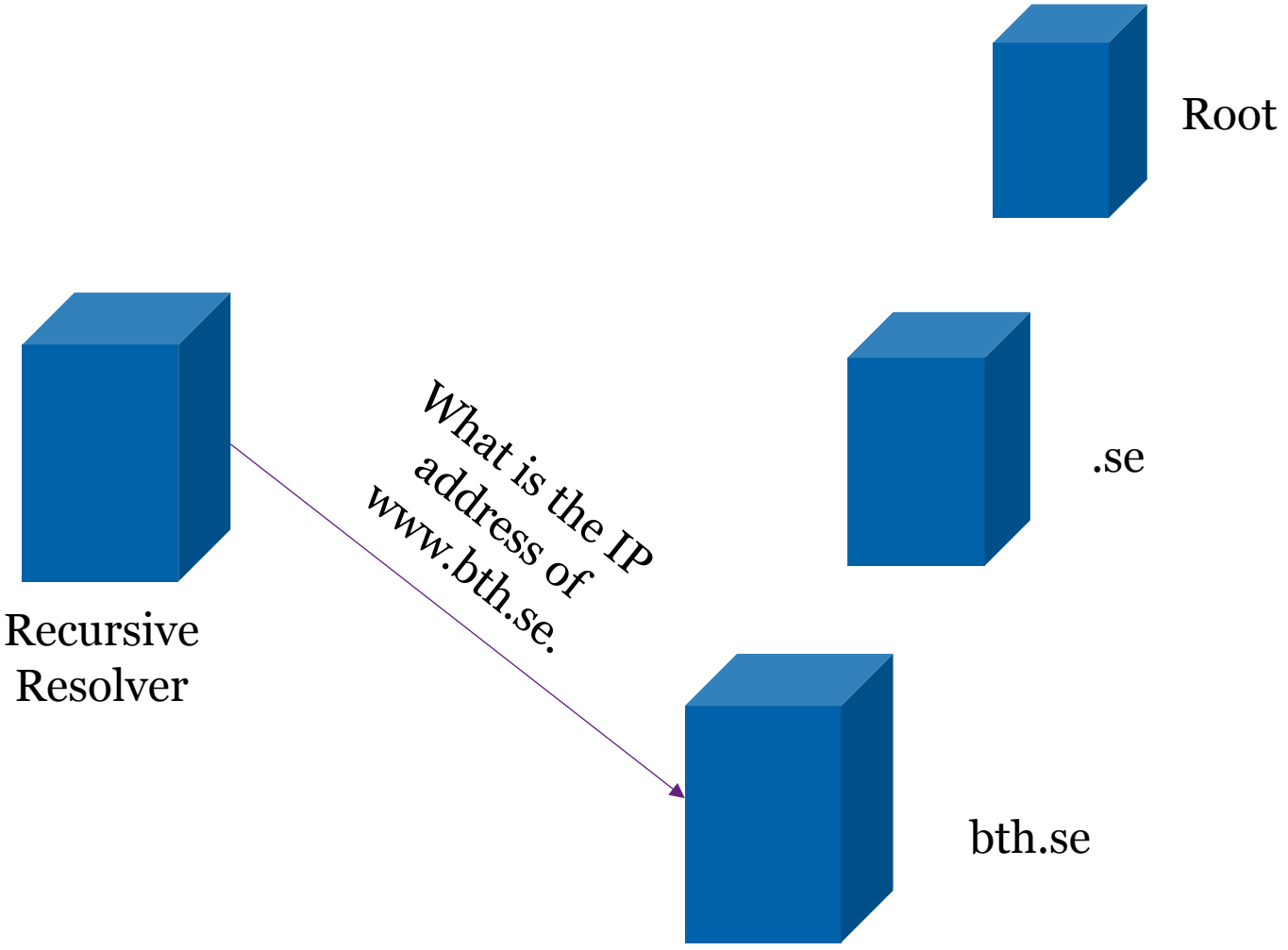
Response of .se

domain name	TTL	class	type	value
Answer Section				
-				
Authority Section				
bth.se.	86400	IN	NS	sunic.sunet.se.
bth.se.	86400	IN	NS	netsrv10.bth.se.
				…
Additional Section				
netsrv10.bth.se.	86400	IN	A	194.47.129.10
sunic.sunet.se.	86400	IN	A	192.36.125.2
				…

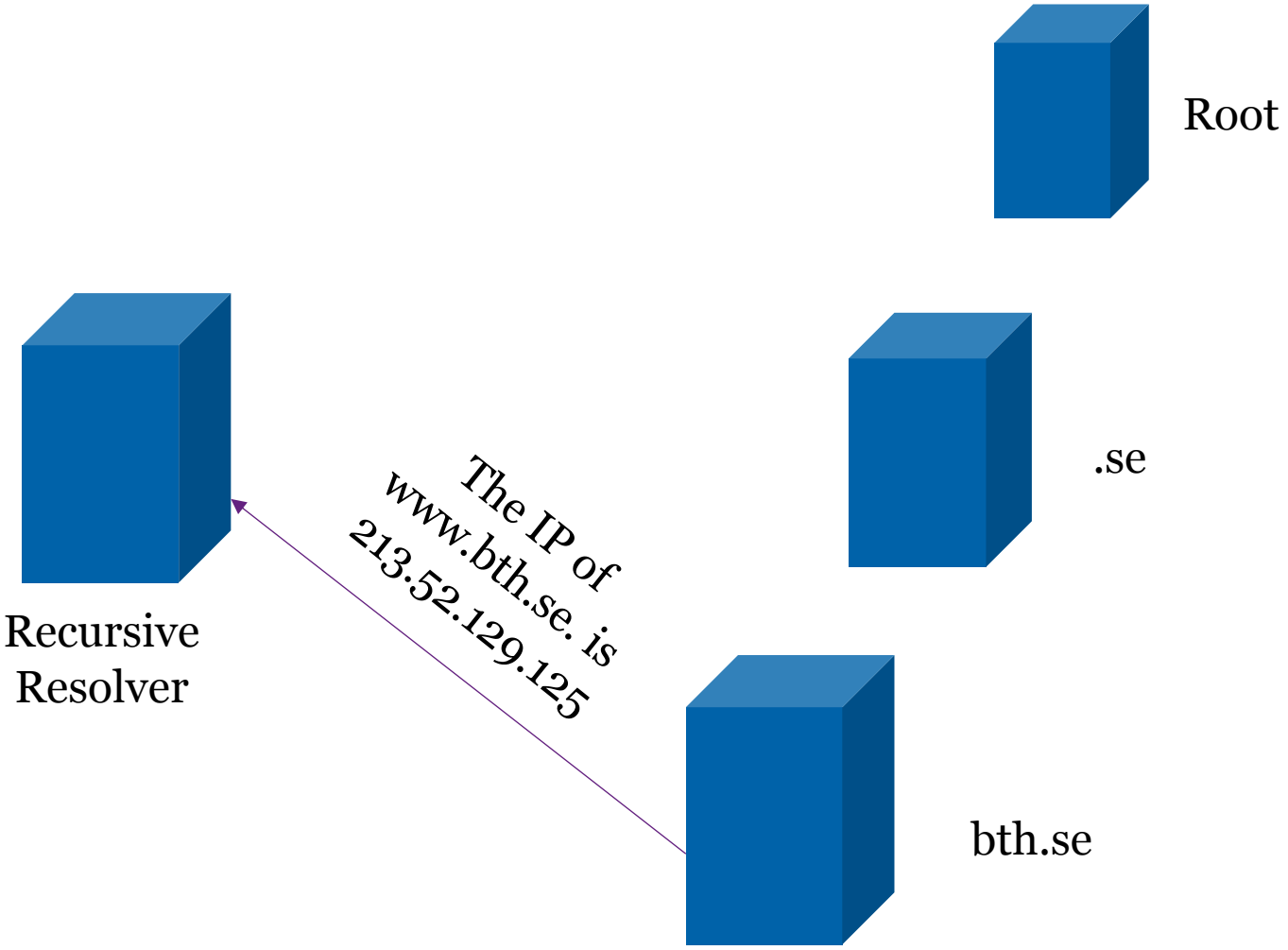
Root

```
dig +multiline @a.ns.se www.bth.se
```

The DNS lookup



The DNS lookup



The DNS lookup

The IP of
www.bth.se. is
213.52.129.125

Recursive
Resolver

Root

.se

bth.se

The DNS lookup

Webserver
213.52.129.125

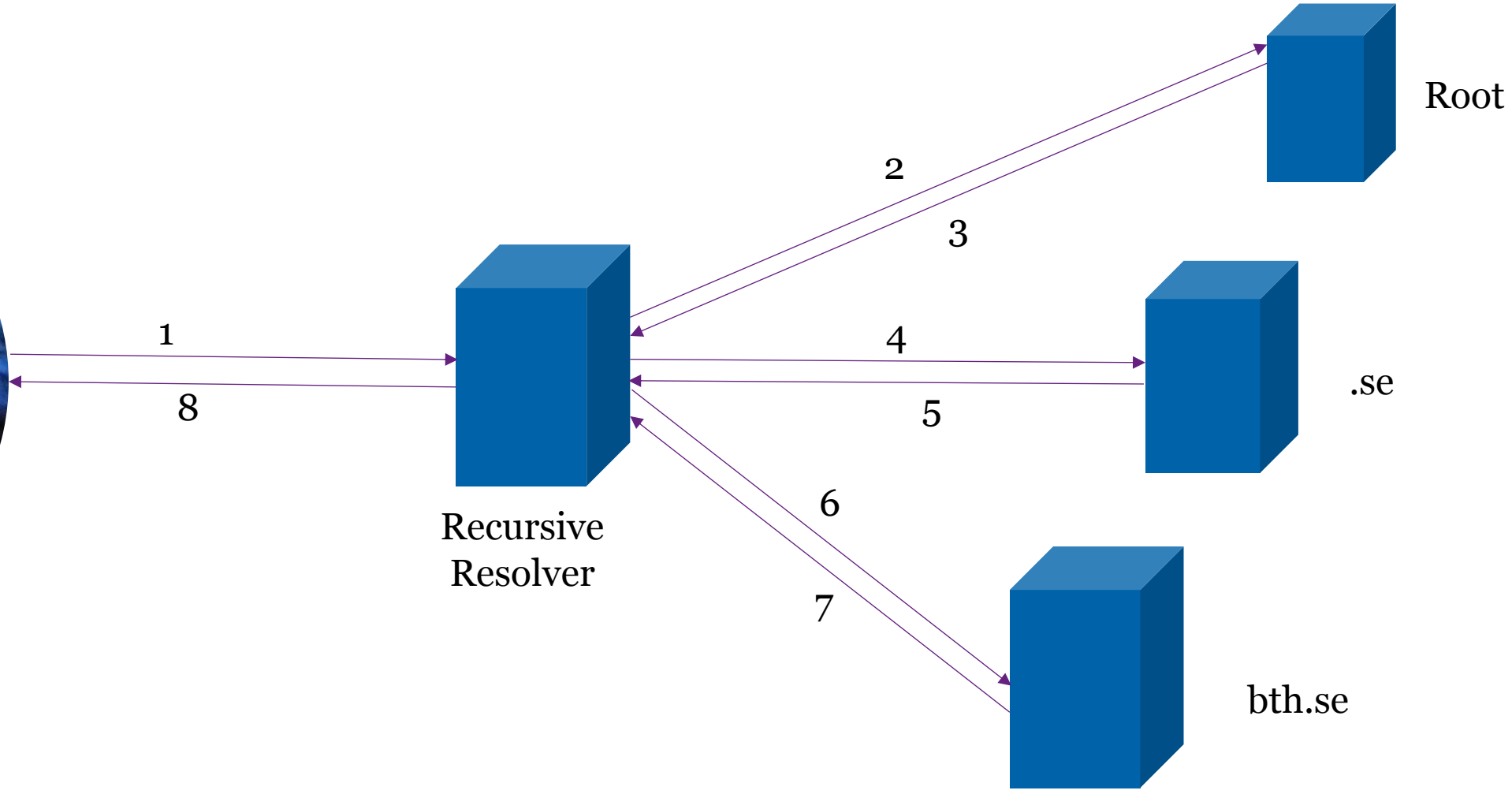
Recursive
Resolver

Root

.se

bth.se

The DNS lookup



Attacks against the Domain Name System

DNS Cache Poisoning

- Goal: Directing users to malicious websites
- Approach: Convincing a resolver that a domain name has a different IP
- Demonstrated by Dan Kaminsky in 2008
- Similar vulnerabilities found, e.g. by Herzberg et al. (2013) and Man et al. (2020)

Source: https://en.wikipedia.org/wiki/Dan_Kaminsky

Cache Poisoning

6.6.6.6

Recursive
Resolver

194.47.129.10

bth.se

Cache Poisoning

What is the IP address of www.bth.se.?

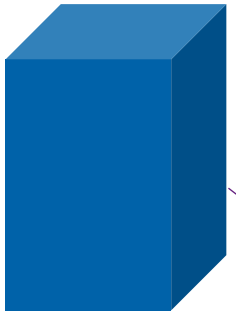
Recursive Resolver

bth.se

194.47.129.10

SDN LABS

Cache Poisoning



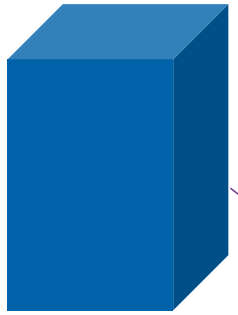
Recursive Resolver

What is the IP address of www.bth.se.?	
Source Port	553
Query ID	54375

194.47.129.10

bth.se

Cache Poisoning



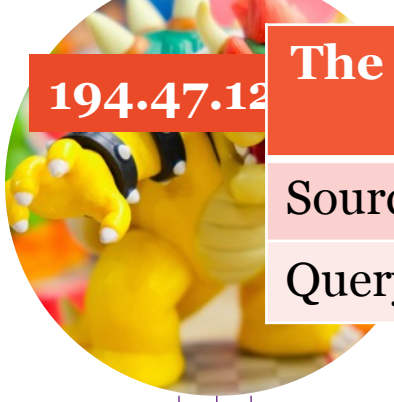
What is the IP address of www.bth.se.?	
Source Port	553
Query ID	54375

Recursive Resolver

bth.se

194.47.129.10

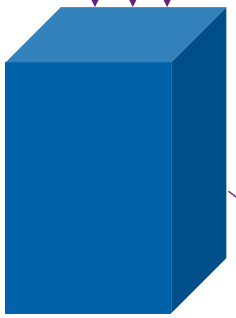
Cache Poisoning



The IP address of www.bth.se. is 6.6.6.6	
Source Port	553
Query ID	54375

Query ID	543754

Query ID	54373



Recursive Resolver

What is the IP address of www.bth.se.?	
Source Port	553
Query ID	54375

bth.se

194.47.129.10

Cache Poisoning

6.6.6.6

The IP of
www.bth.se. is
6.6.6.6

Recursive
Resolver

The IP of
www.bth.se. is
213.52.129.125

194.47.129.10

bth.se

DNS Cache Poisoning

- Proposed solutions:
  - Randomize source port (adds another 2^16 possibilities)
  - Randomize query name (Www.BTh.sE)
- Only one real solution:
  - DNSSEC

The DNS Security Extensions

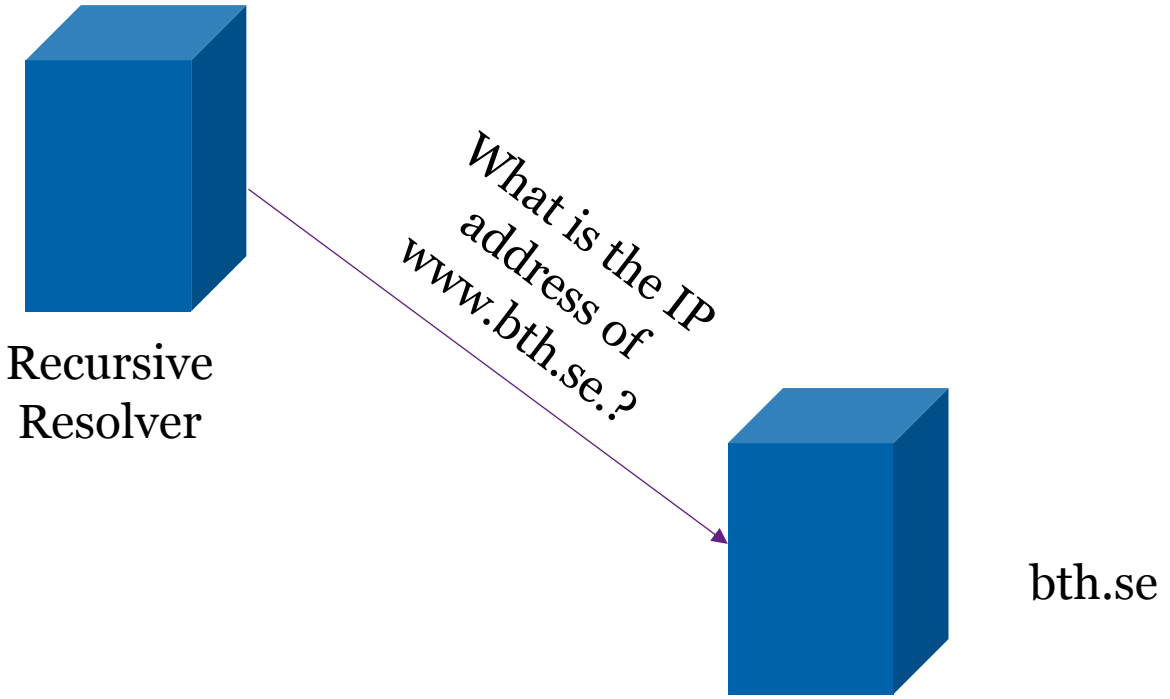
DNSSEC

- Adds integrity and authenticity to DNS
- Published as RFCs in 2005
- Gained more traction after Kaminsky Attack
- Allows zone operators to **sign their records** using **public key cryptography**
- Allows recursive resolvers to **validate the signatures**

DNSSEC

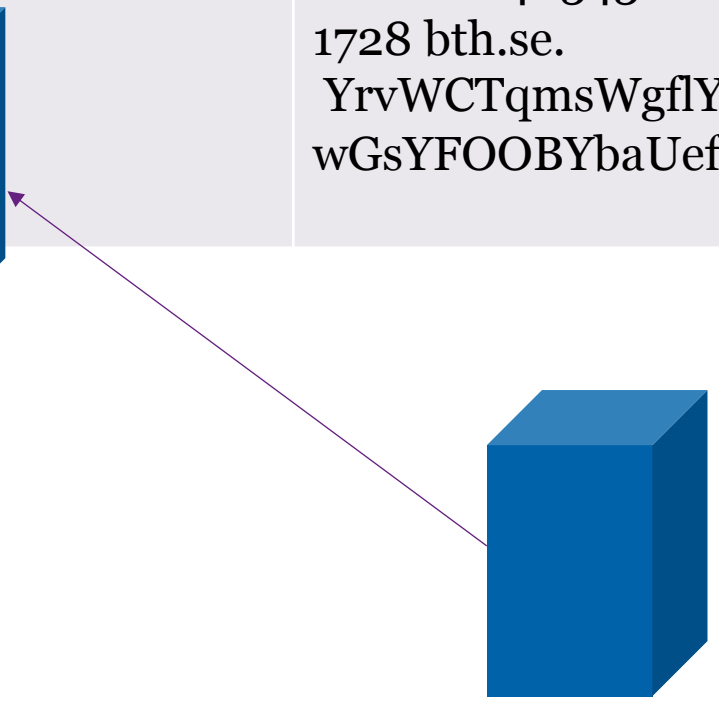
- Adds keys (DNSKEY resource record)
  - Public key and private key
- Adds signatures (RRSIG resource record)
- Adds proof of non-existence (NSEC resource record)

DNSSEC Lookup



DNSSEC Lookup

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fCwGsYFOOBYbaUefqcP …



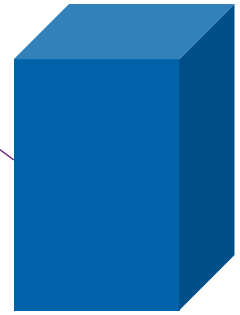

```
dig +multiline @a.ns.se www.bth.se +dnssec
```

DNSSEC Lookup

Resource Record Type covered

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fCwGsYFOOBYbaUefqcP …

Recursive Resolver



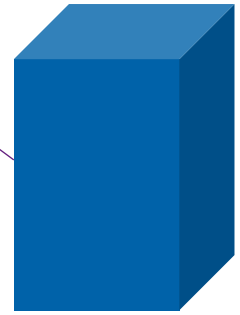
bth.se

DNSSEC Lookup

Cryptographic Algorithm

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fCwGsYFOOBYbaUefqcP …

Recursive Resolver



bth.se

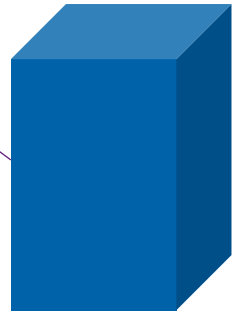
Algorithm 8: RSA/SHA-256
Full list here

DNSSEC Lookup

Time to live of covered record

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fCwGsYFOOBYbaUefqcP …

Recursive Resolver



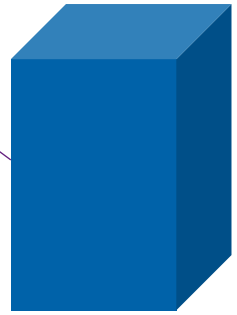
bth.se

DNSSEC Lookup

Inception and validity of signature

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fC wGsYFOOBYbaUefqcP …

Recursive Resolver



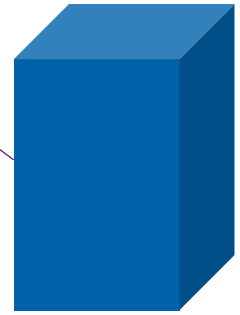
bth.se

DNSSEC Lookup

Key identifier

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fCwGsYFOOBYbaUefqcP …

Recursive Resolver



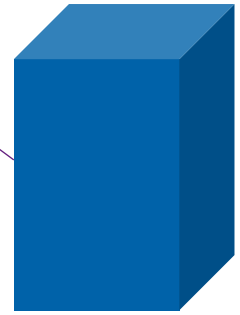
bth.se

DNSSEC Lookup

Key “owner”

The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWYZ1fC wGsYFOOBYbaUefqcP …

Recursive Resolver



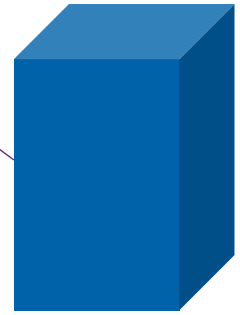
bth.se

DNSSEC Lookup

The Signature

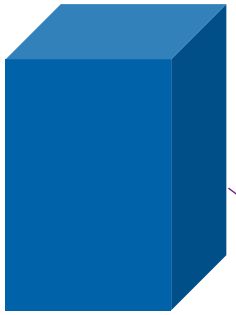
The IP address of www.bth.se. is	
A	213.52.129.125
RRSIG	RRSIG A 8 3 86400 20201214034302 20201207034013 1728 bth.se. YrvWCTqmsWgflYFALlZwUWY Z1fCwGsYFOOBYbaUefqcP …

Recursive Resolver



bth.se

DNSSEC Lookup



Recursive
Resolver

What is the public key of bth.se.?

bth.se

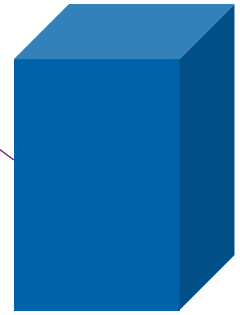
Cached	
A	www.bth.se
RRSIG	www.bth.se

DNSSEC Lookup

```
dig +multiline @a.ns.se bth.se DNSKEY +dnssec
```

The key of bth.se. is	
DNSKEY	DNSKEY 256 3 8 AwEAAb3i8bDp5rhukbsz2PKTO3/9B kV9fpfgbXWKS3Rx … (ZSK; key id = 1728;)

Recursive Resolver

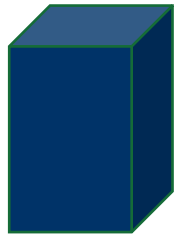


bth.se

Cached	
A	www.bth.se
RRSIG	www.bth.se
DNSKEY	bth.se.

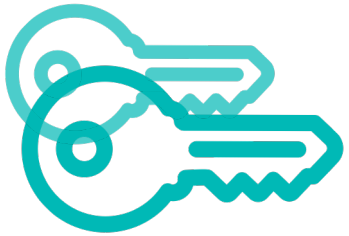
Trust in DNSSEC

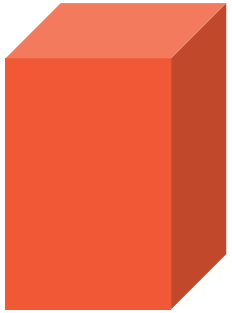
Recursive Resolver



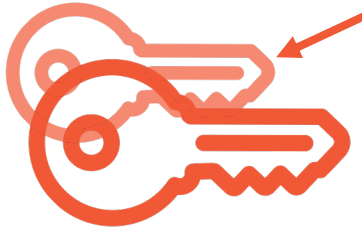
Root

.se





public key



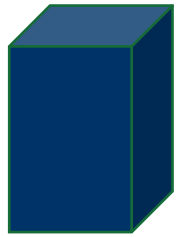
bth.se

private key

A

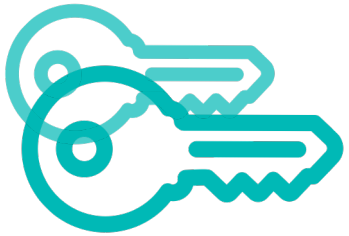
Trust in DNSSEC

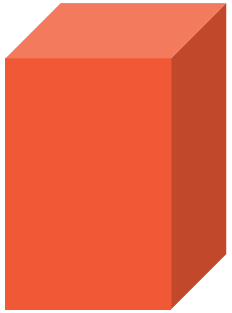
Recursive Resolver



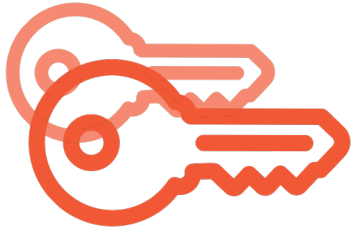
Root

.se



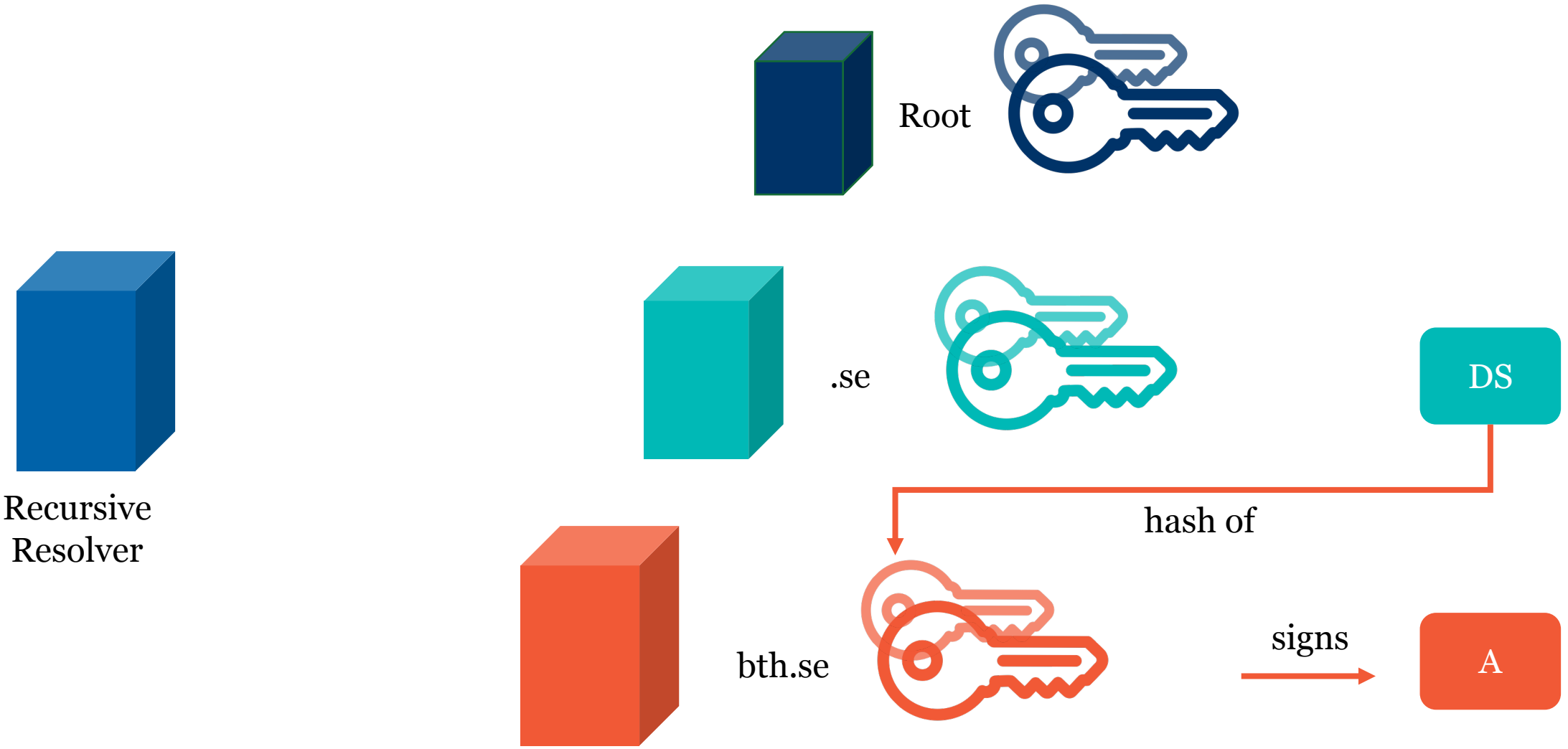


bth.se

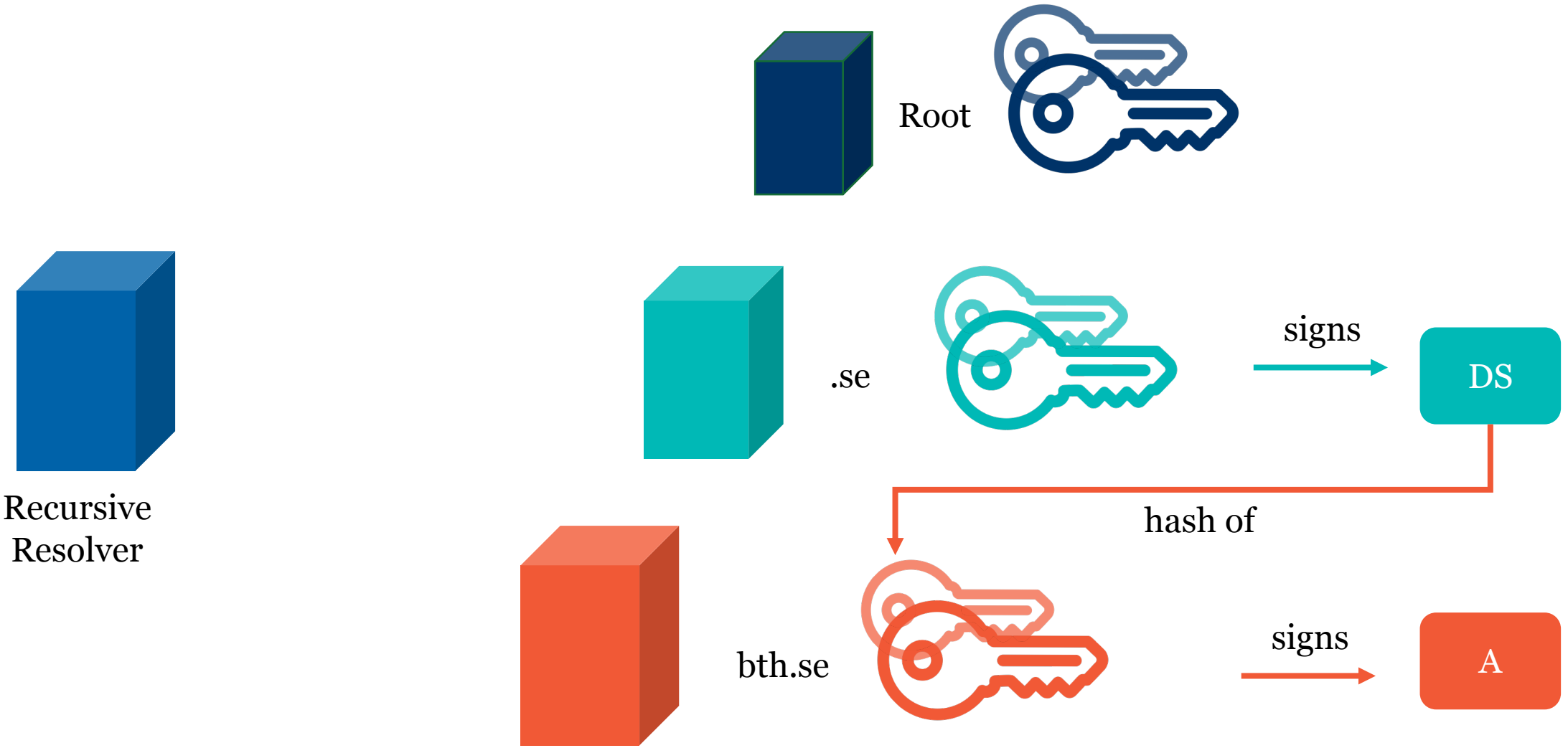


signs

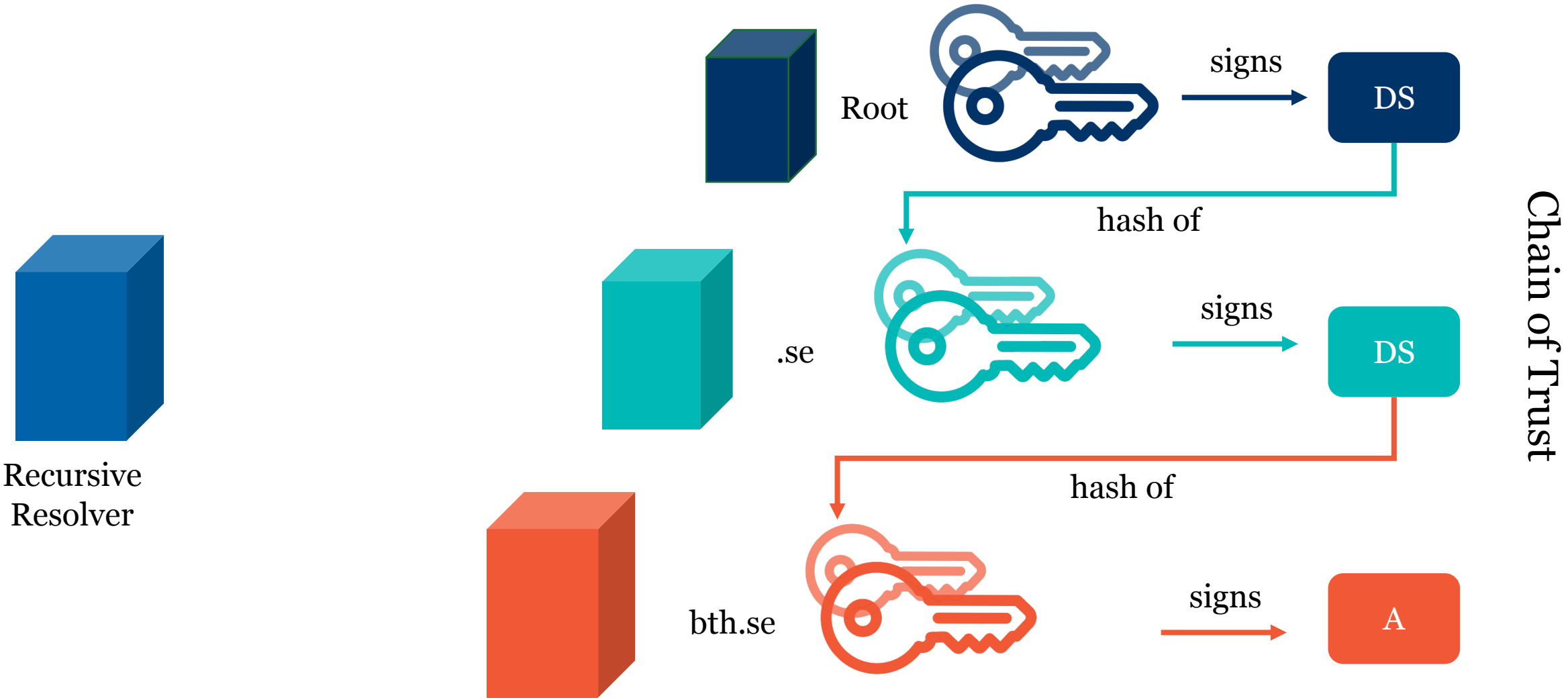
Trust in DNSSEC



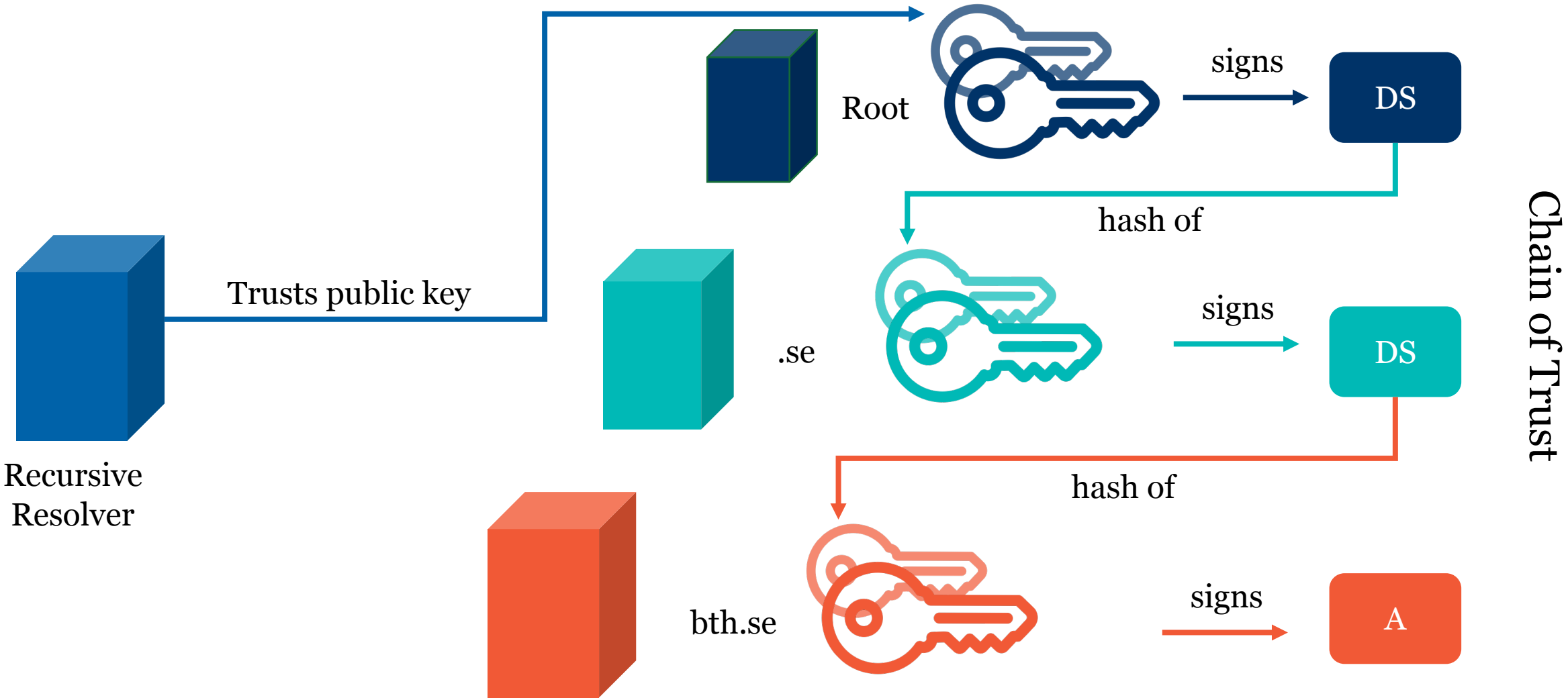
Trust in DNSSEC



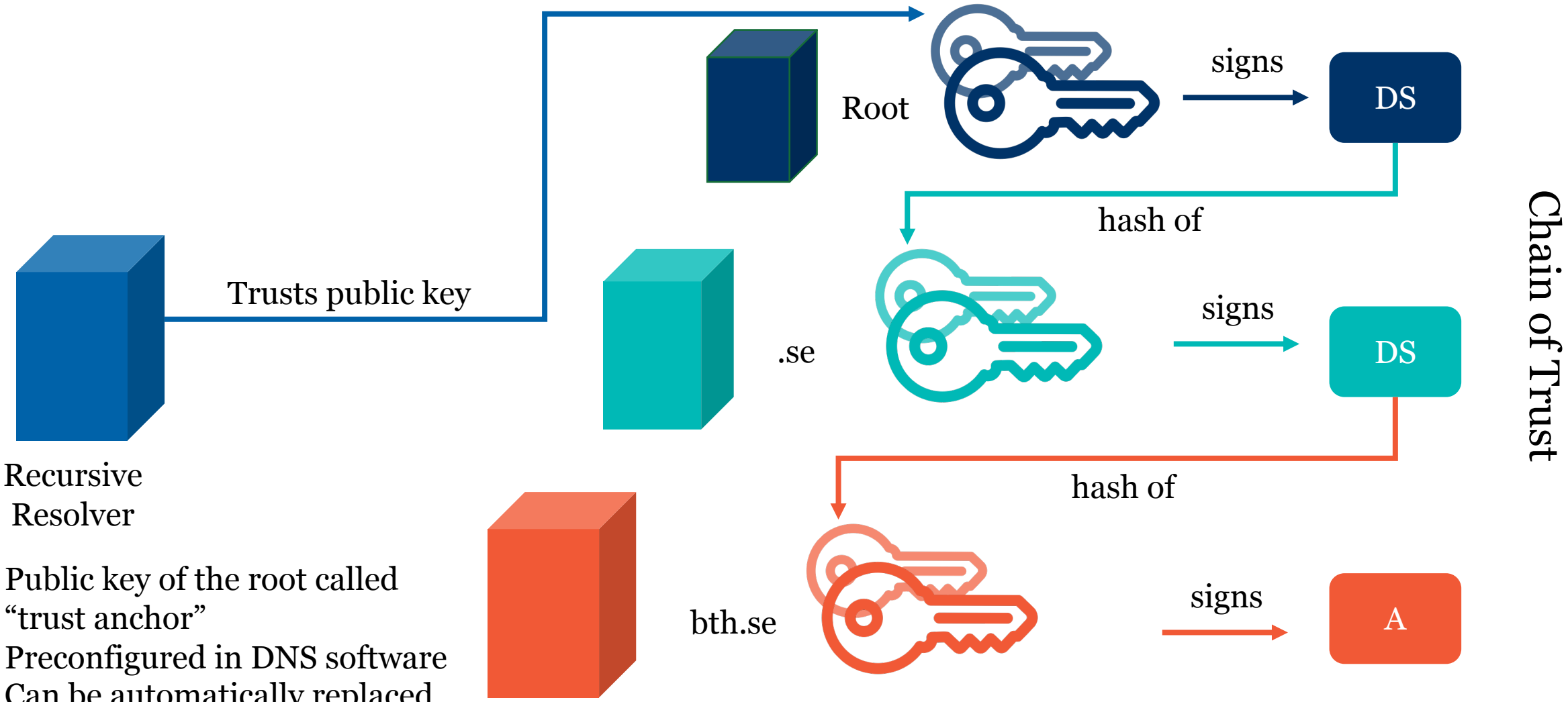
Trust in DNSSEC



Trust in DNSSEC



Trust in DNSSEC

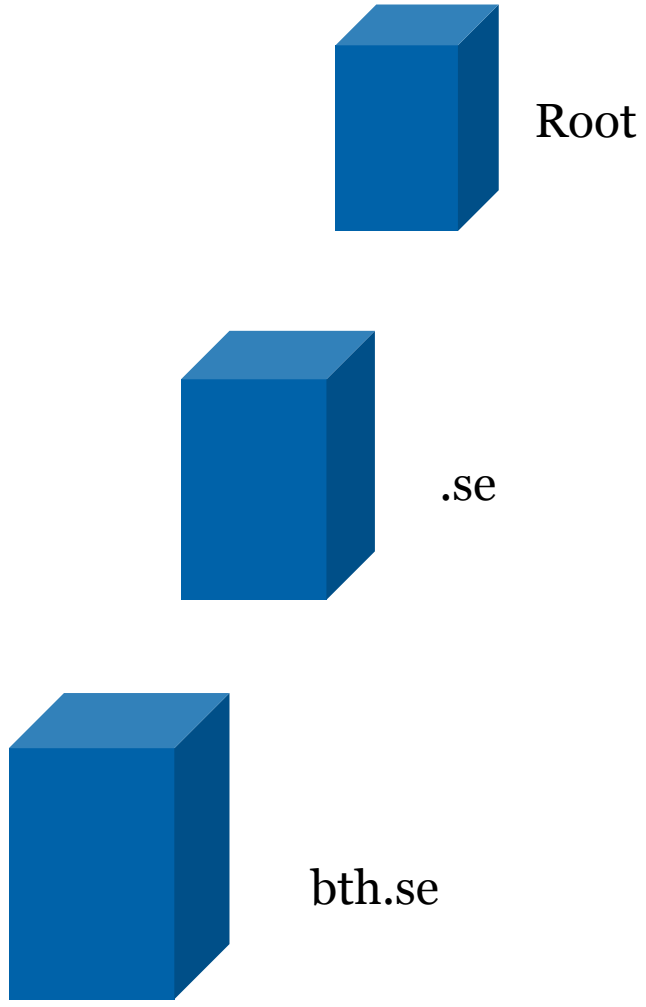


- Public key of the root called "trust anchor"
- Preconfigured in DNS software
- Can be automatically replaced (RFC 5011)

DNSSEC Lookup

Recursive Resolver

Cached	
A	www.bth.se
RRSIG	www.bth.se
DNSKEY	bth.se.
DS	DNSKEY bth.se
DNSKEY	.se
DS	DNSKEY se.
DNSKEY	. (root)



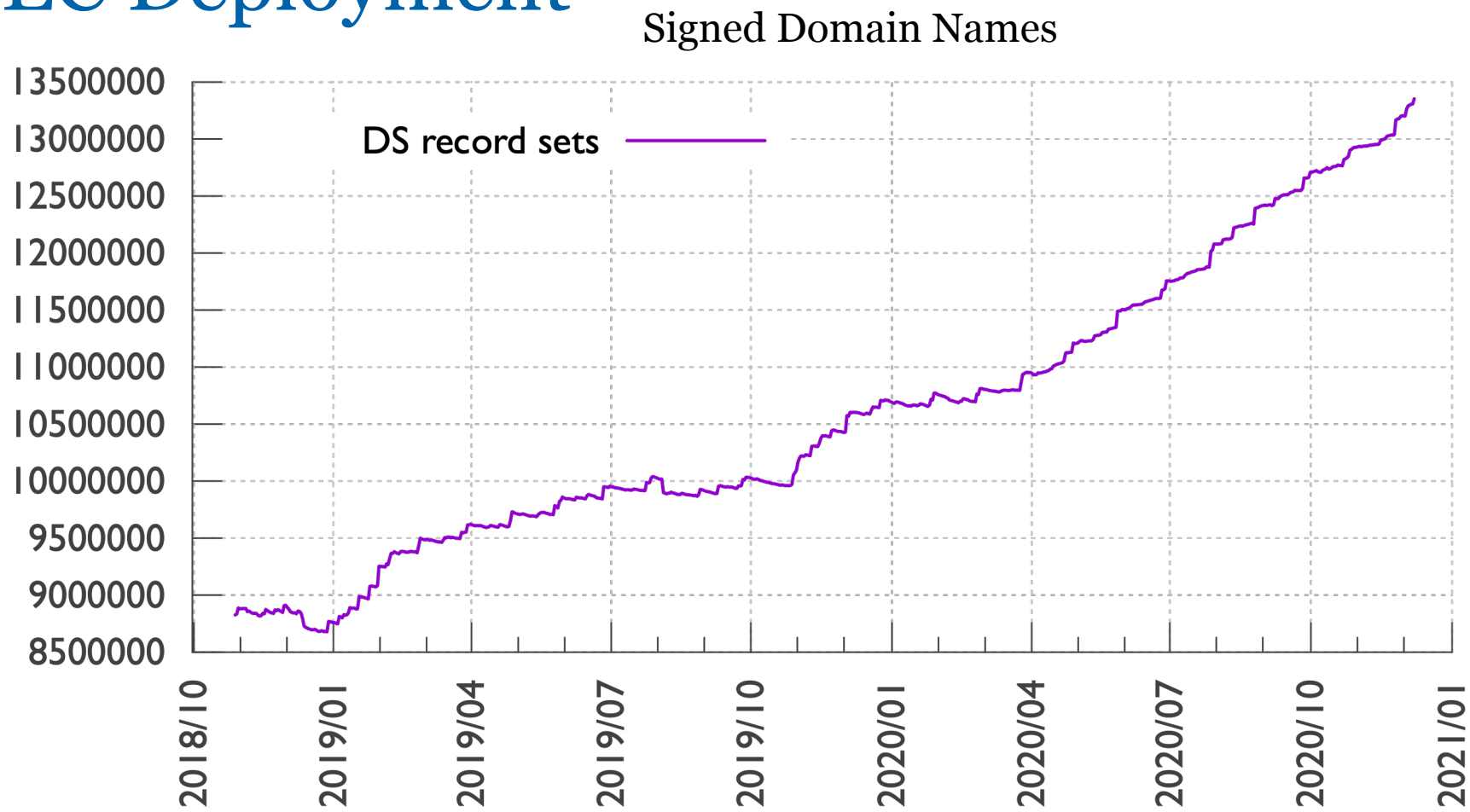
DNSSEC set up

- Operators often use two keys:
  - Zone Signing Key (ZSK) to sign the resource records (A, AAAA, MX)
  - Key Signing Key (KSK) to sign the ZSK
  - DS record is the hash of the KSK
- Makes key operations easier
  - Exchanging keys, without interaction with the parent
  - Different security model: e.g. lower security for ZSK
- KSK and ZSK can be combined in a Combined Signing Key (CSK)

Visualizing and Debugging DNSSEC

- Helpful tool: **dnsviz**
- Correct and working example sidnlabs.nl: https://dnsviz.net/d/sidnlabs.nl/X8l8rA/dnssec/
- Weird but working example bth.se: https://dnsviz.net/d/bth.se/X89Wog/dnssec/
- Broken example (expired signatures): https://dnsviz.net/d/servfail.nl/X5wKQA/dnssec/

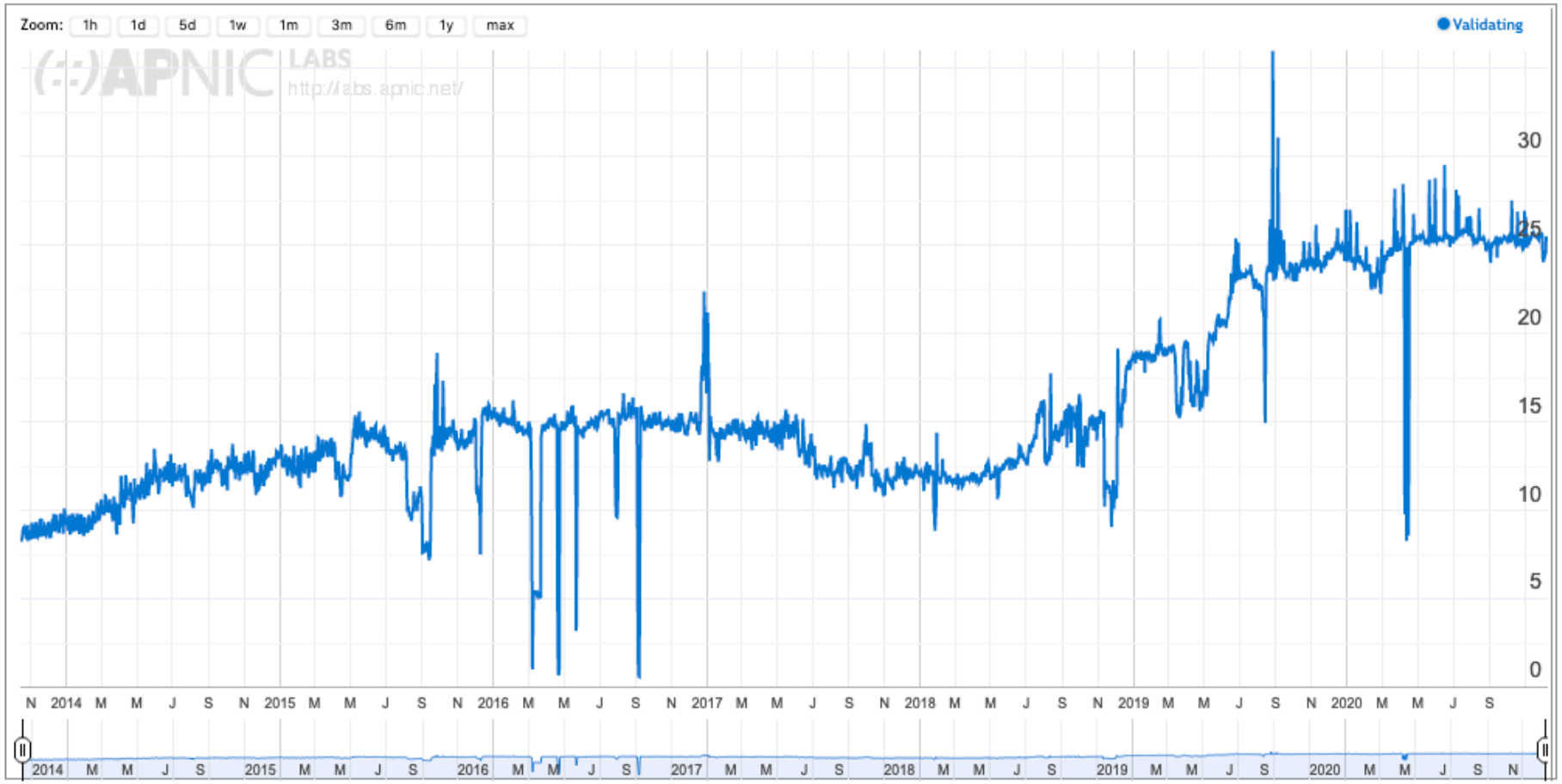
DNSSEC Deployment



- Signing (https://stats.dnssec-tools.org/)
- ~370M domain names registered
- > 50% of all .nl and .se domain names are signed

DNSSEC Deployment

Clients using validating resolvers (%)



- Validation (https://stats.labs.apnic.net/dnssec/XA)
- ~ 90% in .se (!), ~50% in .nl (☹)

DNSSEC Downsides

- Makes DNS more complicated
- Misconfigurations can lead to rendering your own domain offline
  - E.g. when replacing a KSK
  - Or when forget to update signatures
- Not much client-side validation (but Apple is considering it)
- Larger payload makes DNSSEC interesting for DDoS reflection attacks
  - `dig A www.bth.se +multiline` = 55 bytes
  - `dig A www.bth.se +multiline +dnssec` = 349 bytes
  - `dig DNSKEY bth.se +multiline +dnssec` = 2021 bytes

SIDN LABS

Getting started with DNS(SEC)

- DNS Software:
  - Bind9 (Name Server & Resolver)
  - Unbound (Resolver)
  - NSD (Name Server)
- Tools:
  - Dig (command line tool)
  - Dnsviz (dnzviz.net)
- Further reading:
  - https://powerdns.org/hello-dns/ (introduction to DNS)
  - IETF Request for Comments (RFCs)

SIDN LABS

Other DNS challenges

Confidentiality

- DNS queries can leak sensitive information
- Local networks (e.g. coffeeshops or hotel W-LAN) intercept and manipulate DNS queries
- ISPs sell DNS query data

→ Encrypt DNS traffic

- DNS over TLS (DoT)
- DNS over HTTPS (DoH)

Photo by Simone Secci on Unsplash

Q&A

www.sidnlabs.nl | stats.sidnlabs.nl

Moritz Müller
Research Engineer
moritz.muller@sidn.nl