The DNS Security Extensions (DNSSEC)

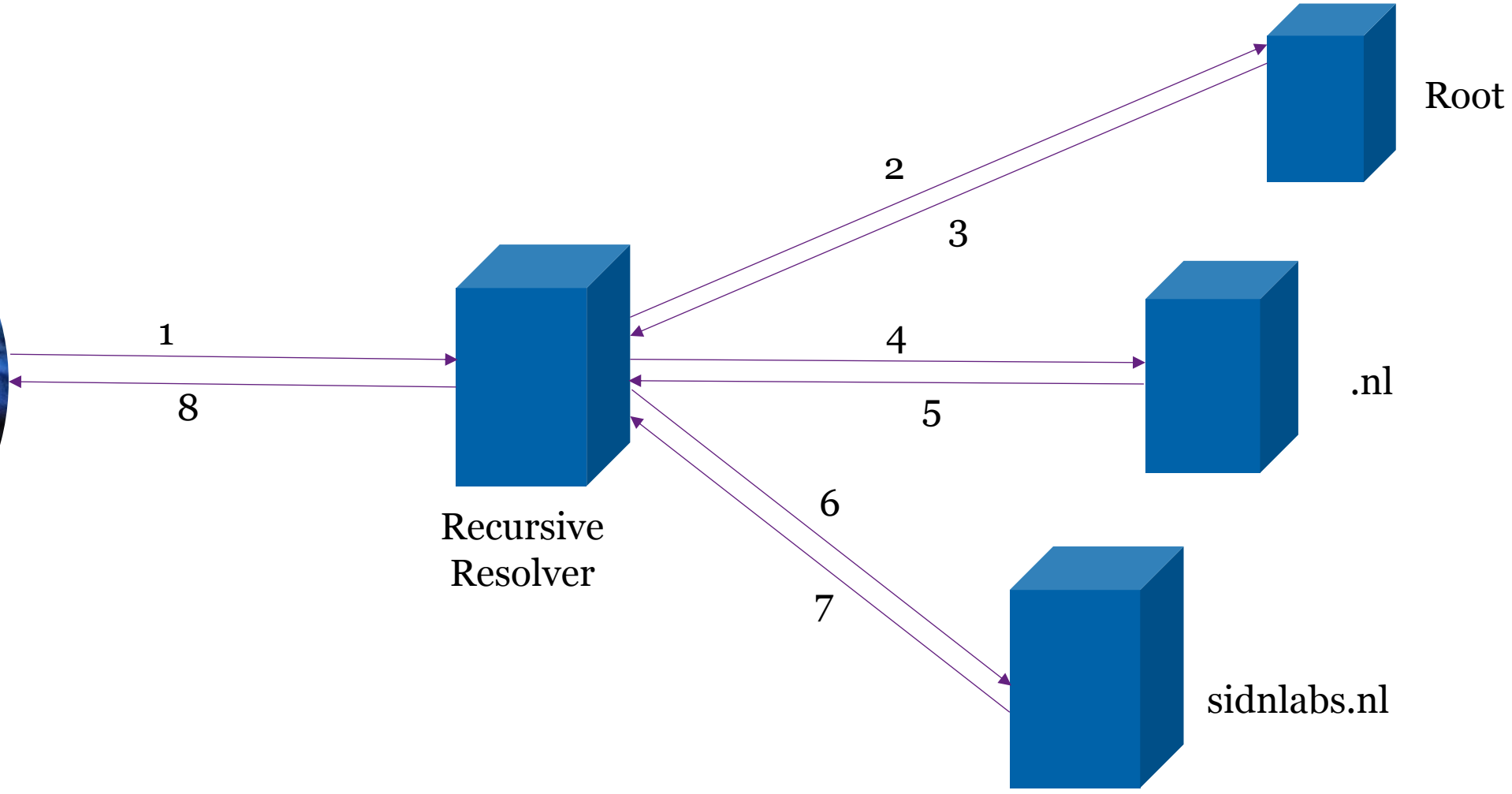
Moritz Müller | Applied Cryptography

30 May 2023

DNS refresher

- Domain Name System
- First specified in 1987
- DNS lookup at the start of almost every connection attempt on the Internet
- Authoritative name servers
- Recursive resolvers
- Stub resolvers

The DNS lookup

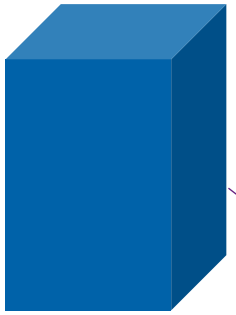


DNS Cache Poisoning

- Approach: convince a resolver that a domain name has a different IP address, MX record, TXT record …
- 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



Recursive Resolver

What is the IP address of www.sidnlabs.nl.?	
Source Port	553
Query ID	54375

sidnlabs.nl

www.sidnlabs.nl A 35.190.27.69

Cache Poisoning

The IP address of www.bth.se. is [EVIL IP ADDRESS]	
Source Port	553
Query ID	54375

Query ID	54374

Query ID	54373

Recursive Resolver

What is the IP address of www.sidnlabs.nl.?	
Source Port	553
Query ID	54375

sidnlabs.nl

DNS Cache Poisoning

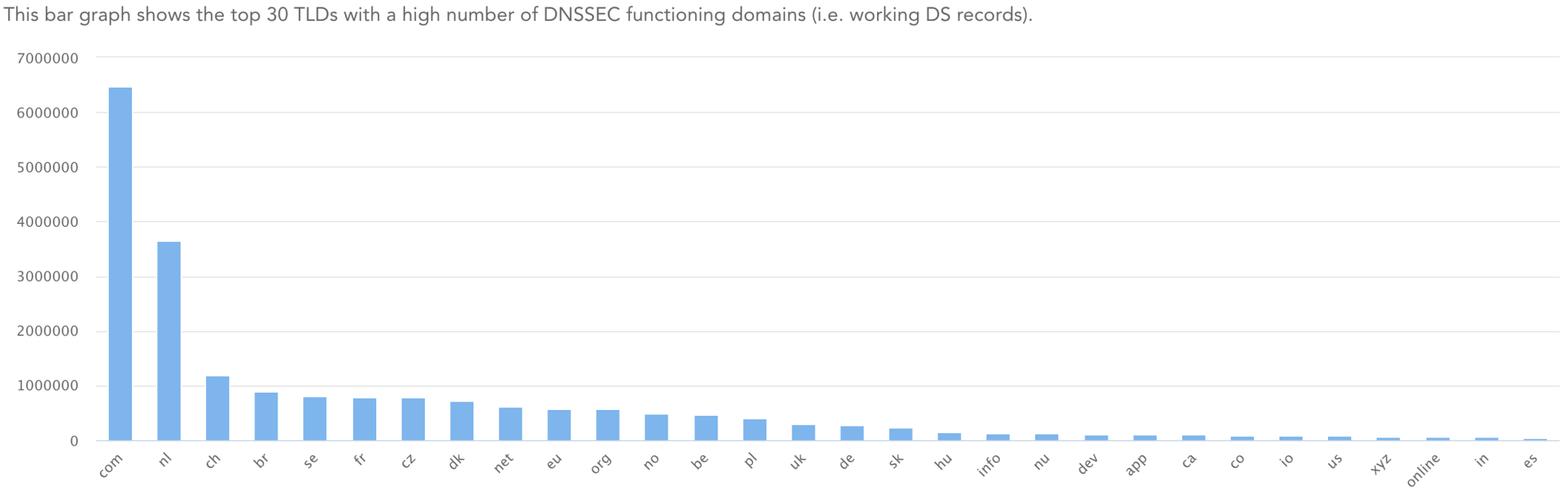
- Proposed solutions:
  - Randomize source port (adds another 2^16 possibilities)
  - Randomize query name capitalization (wWW.sIdn.Nl)
- Only one real solution:
  - DNSSEC

DNSSEC

- DNS Security Extensions
- Add 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 Deployment

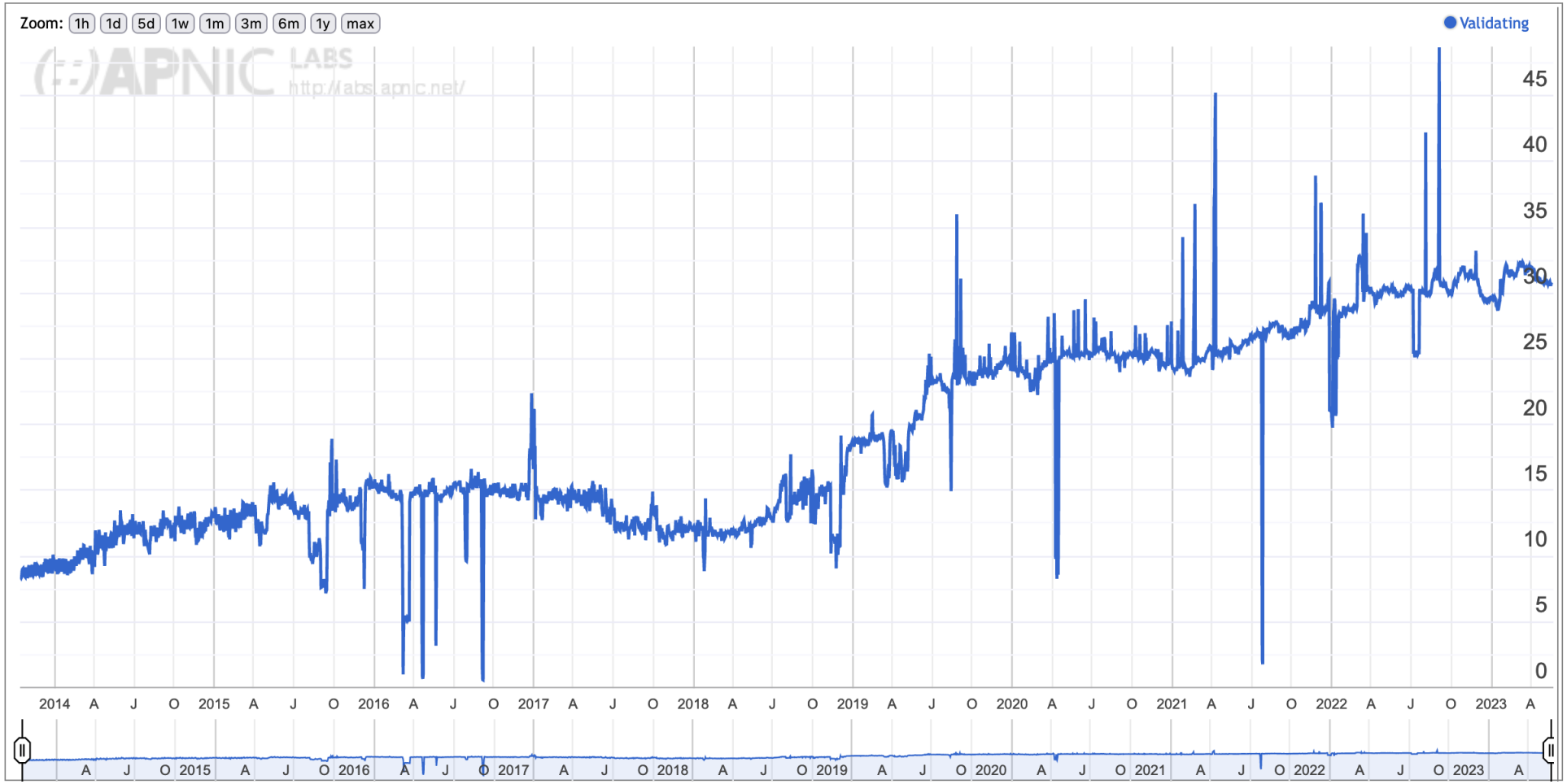
Signed zones of second-level domain names



Source: https://stats.dnssec-tools.org/#/https://stats.dnssec-tools.org/?top=tlds&tld_tab=0

DNSSEC Deployment

Users relying on a validating resolver



Source: https://stats.labs.apnic.net/dnssec/XA?hc=XA&hx=0&hv=1&hp=1&hr=1&w=1&p=0

A DNSSEC signed resource record

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 3600 (20230603061206 20230520060714 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzlog==)

sidnlabs.nl

```
dig @ns1.sidnlabs.nl +dnssec +multiline www.sidnlabs.nl A
```

A DNSSEC signed resource record

Resource Record Type covered

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 3600 (20230603061206 20230520060714 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzlog==)

sidnlabs.nl

A DNSSEC signed resource record

Cryptographic algorithm and hash algorithm

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A **13** 3 3600 (20230603061206 20230520060714 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzlog==)

sidnlabs.nl

Algorithm 13: ECDSA Curve P-256 with SHA-256
Full list here

A DNSSEC signed resource record

Number of labels of the covered domain name

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 **3** 3600 (20230603061206 20230520060714 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzlog==)

sidnlabs.nl

A DNSSEC signed resource record

Time to live of covered record

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 **3600** (20230603061206 20230520060714 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzl0g==)

sidnlabs.nl

A DNSSEC signed resource record

Inception and validity of signature

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 3600 (**20230603061206 20230520060714** 11261 sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzl0g==)

sidnlabs.nl

A DNSSEC signed resource record

Key identifier

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 3600 (20230603061206 20230520060714 **11261** sidnlabs.nl. 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzl0g==)

sidnlabs.nl

A DNSSEC signed resource record

Key “owner”

Zone excerpt	
A	35.190.27.69
RRSIG	RRSIG A 13 3 3600 (20230603061206 20230520060714 11261 **sidnlabs.nl.** 8iiG3/D+MCFVgwZi70ZHmwLVhS16jwErejQxZQDpaz9m XIyApGUd1RDrEM6xGl7+IGYN4cnn9zlAwoQzYSzlog==)

sidnlabs.nl

No signature without a key

Zone excerpt	
DNSKEY	DNSKEY 257 3 13 (Pv+xZDOZj/d3mGLPppY5Z/fATmA7 FMjTIxiqHUeHAzzJh4LqCZX35BT4 UdnqtupebkHToavzaXyB5zjV0s703w ==) ; KSK; alg = ECDSAP256SHA256 ; key id = 11261
RRSIG	…

sidnlabs.nl

No signature without a key

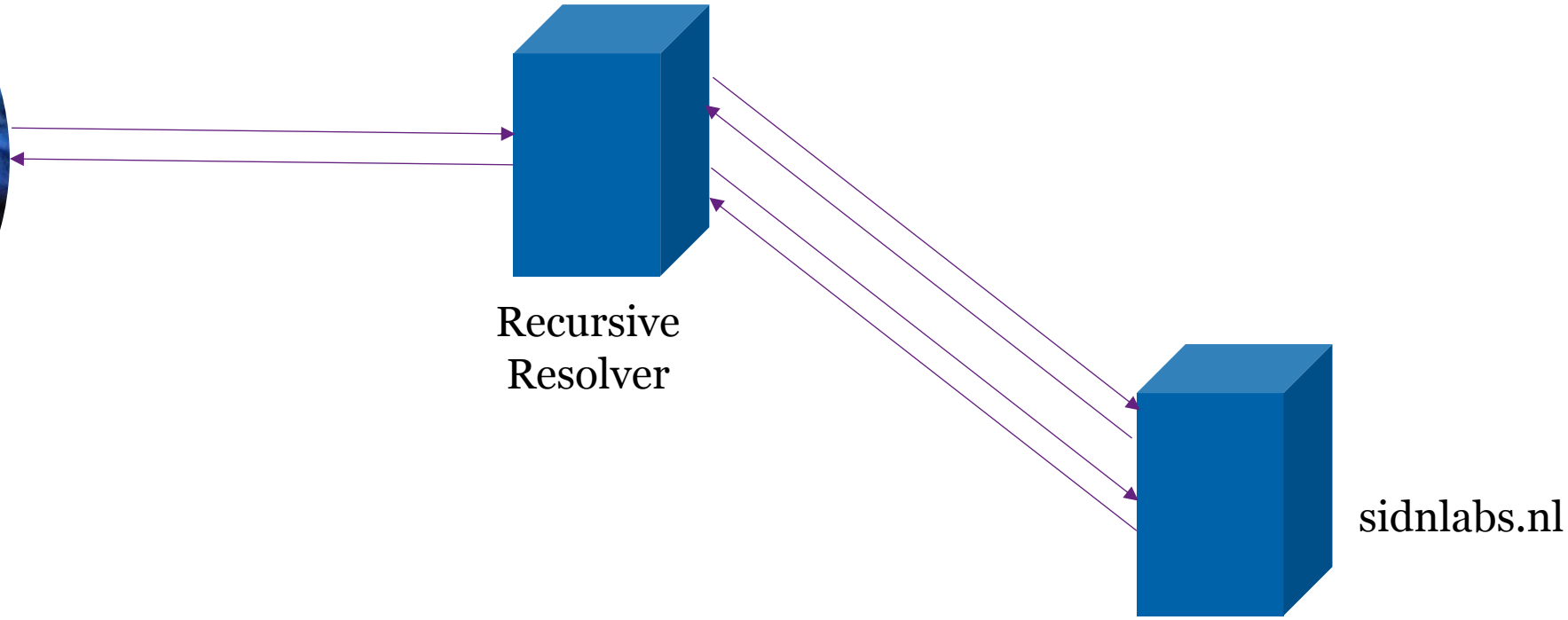
Key Signing Key

Zone excerpt	
DNSKEY	DNSKEY **257** 3 13 (Pv+xZDOZj/d3mGLPppY5Z/fATmA7 FMjTIxiqHUeHAzzJh4LqCZX35BT4 UdnqtupebkHToavzaXyB5zjV0s703w ==)
RRSIG	…

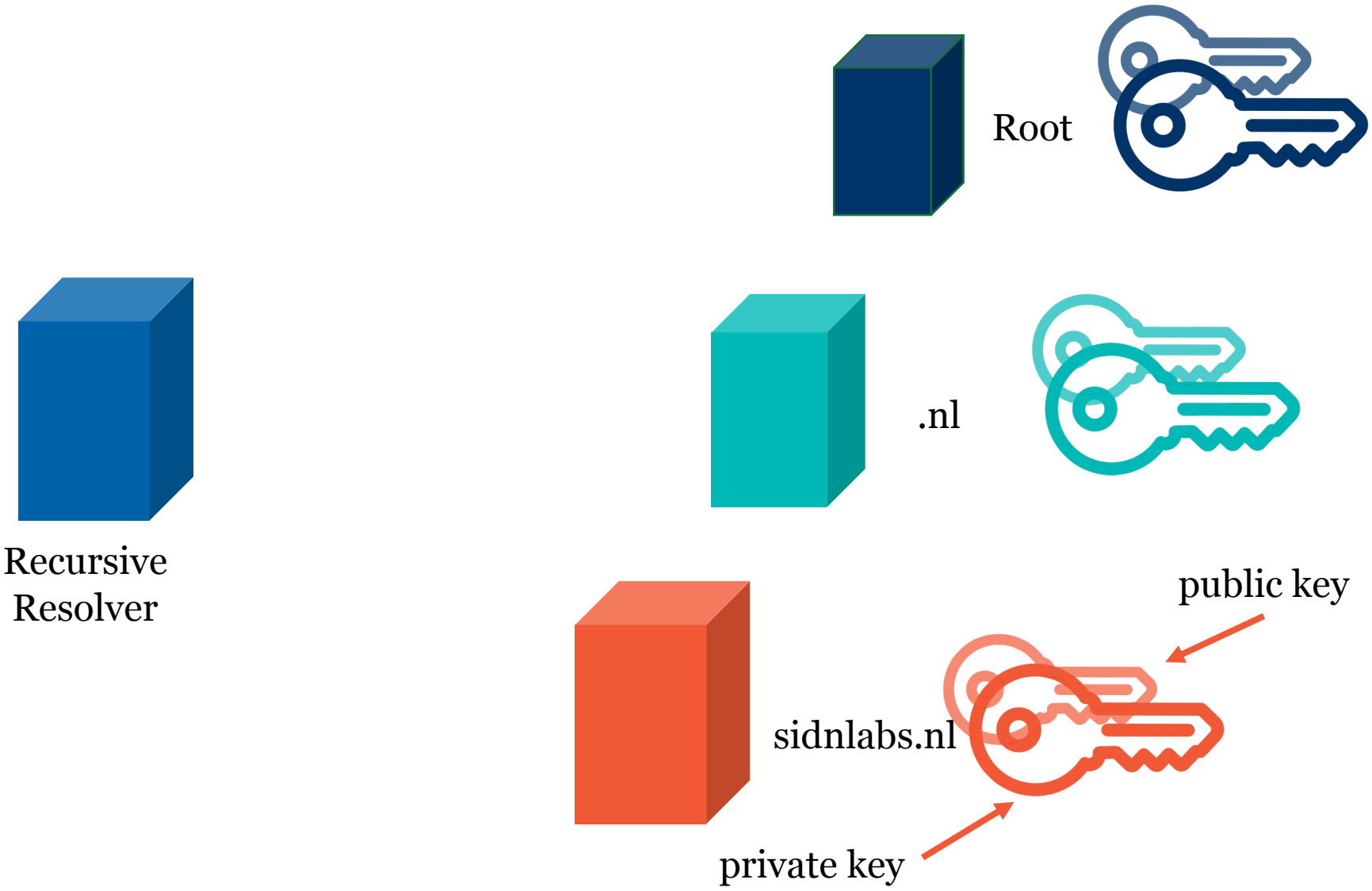
sidnlabs.nl

SIDN LABS

The DNSSEC lookup

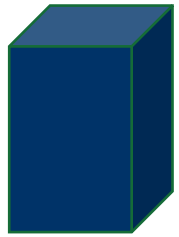


Trust in DNSSEC



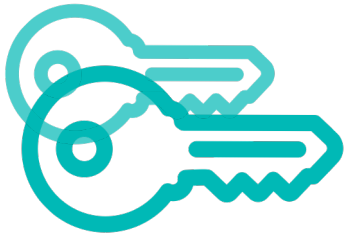
Trust in DNSSEC

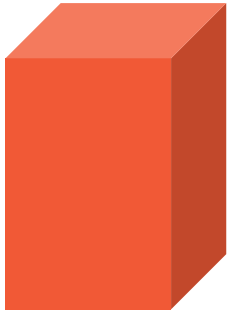
Recursive Resolver



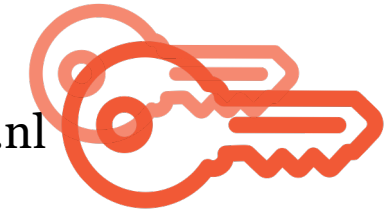
Root

.nl

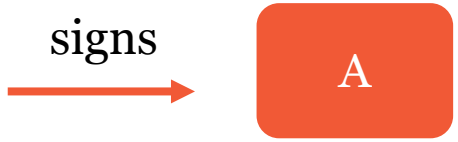




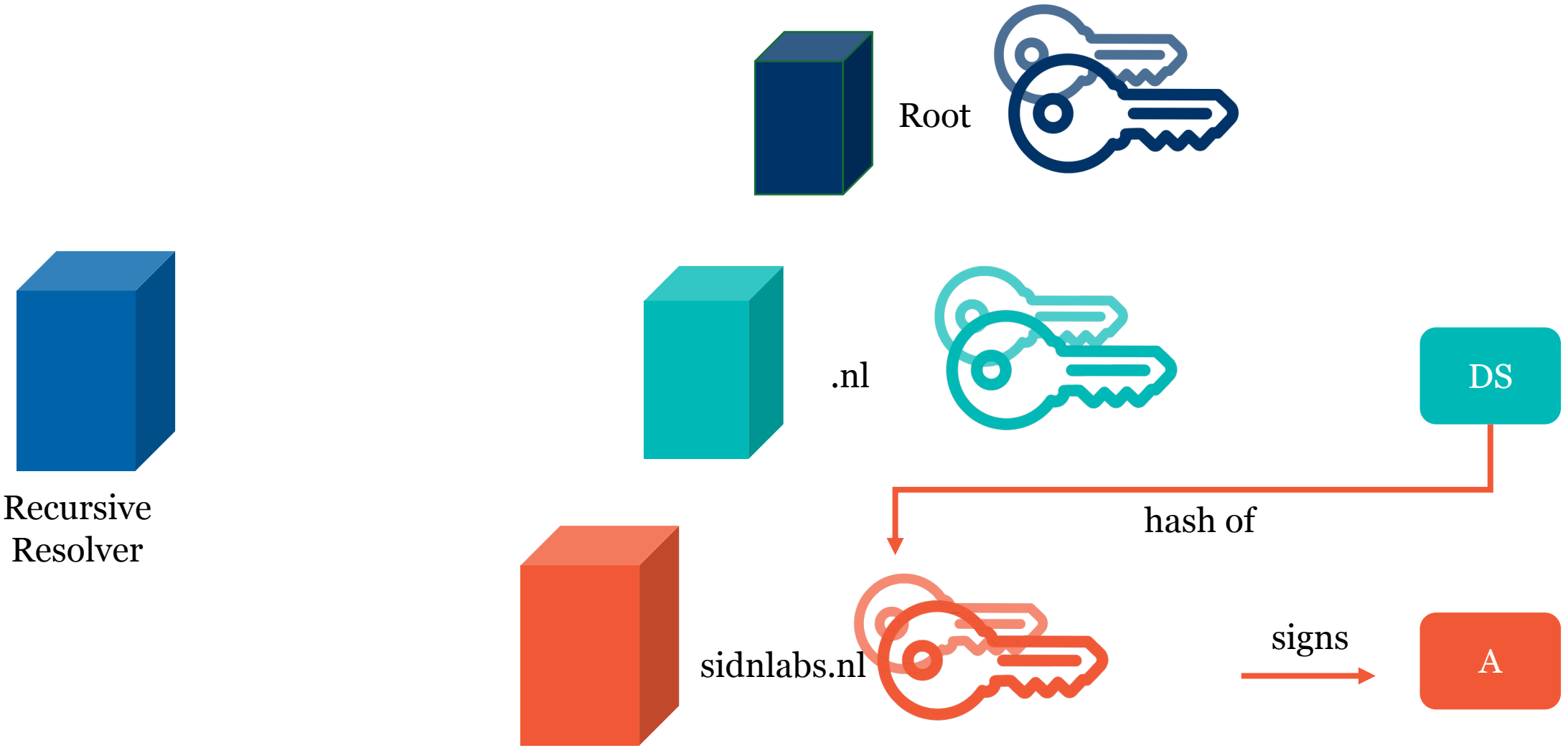
sidnlabs.nl



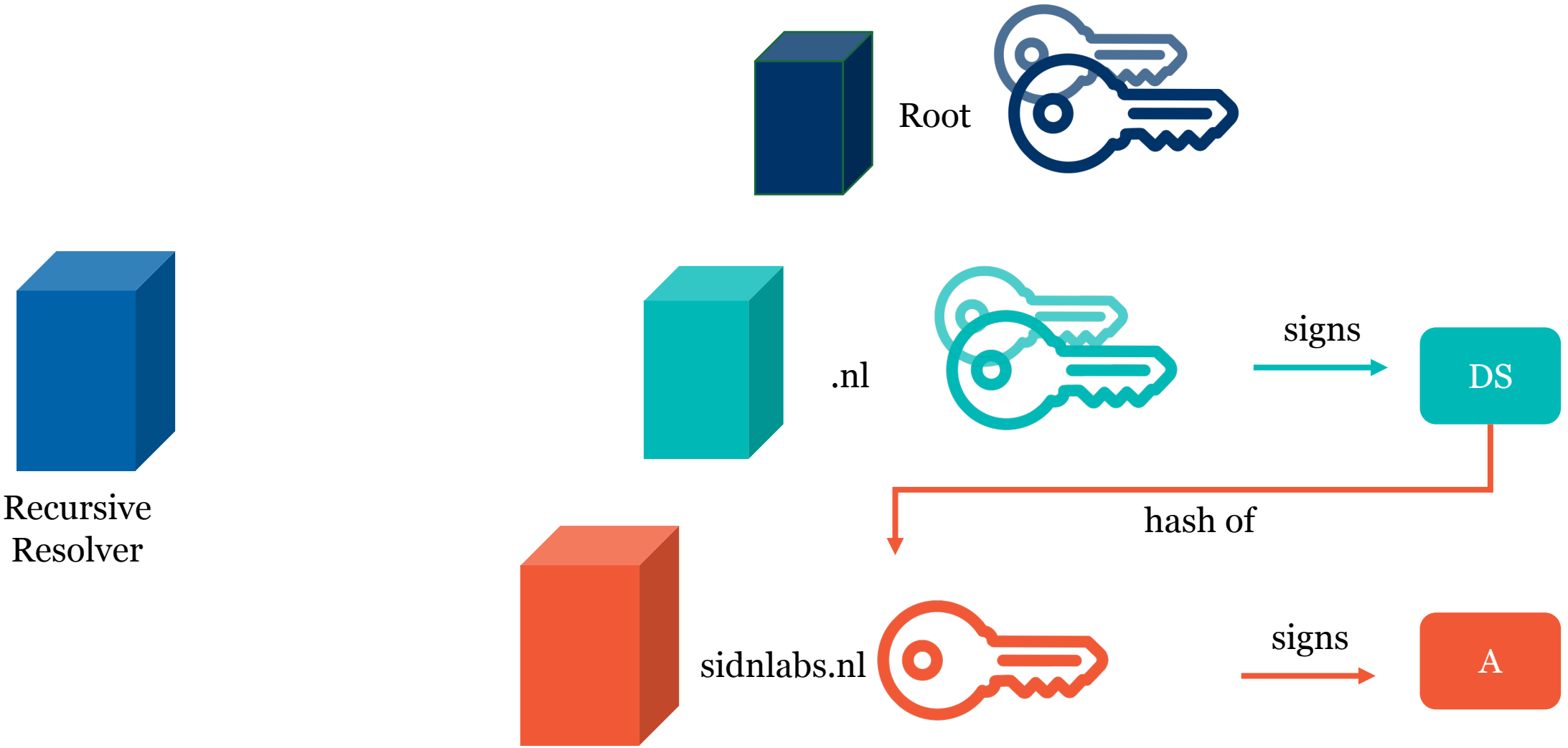
signs



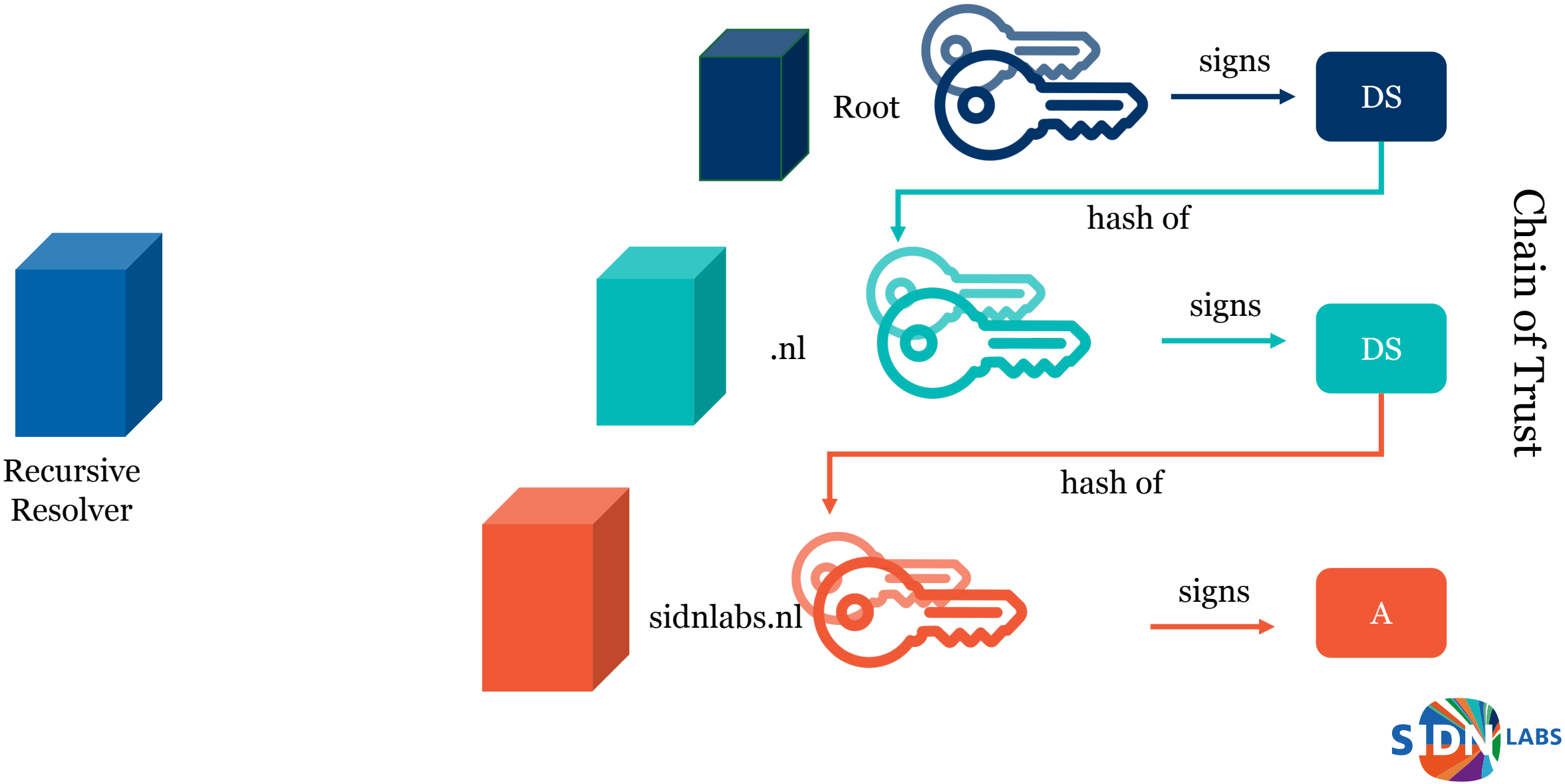
Trust in DNSSEC



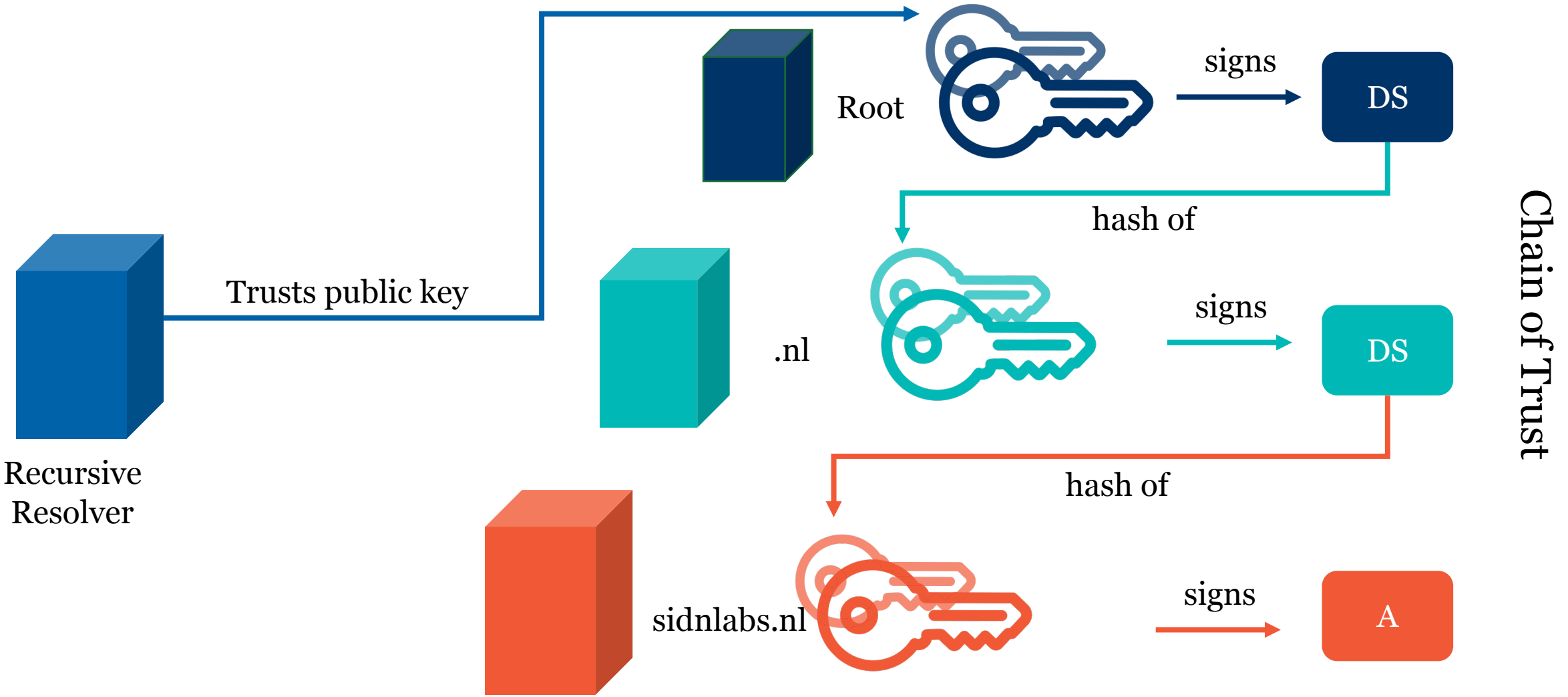
Trust in DNSSEC



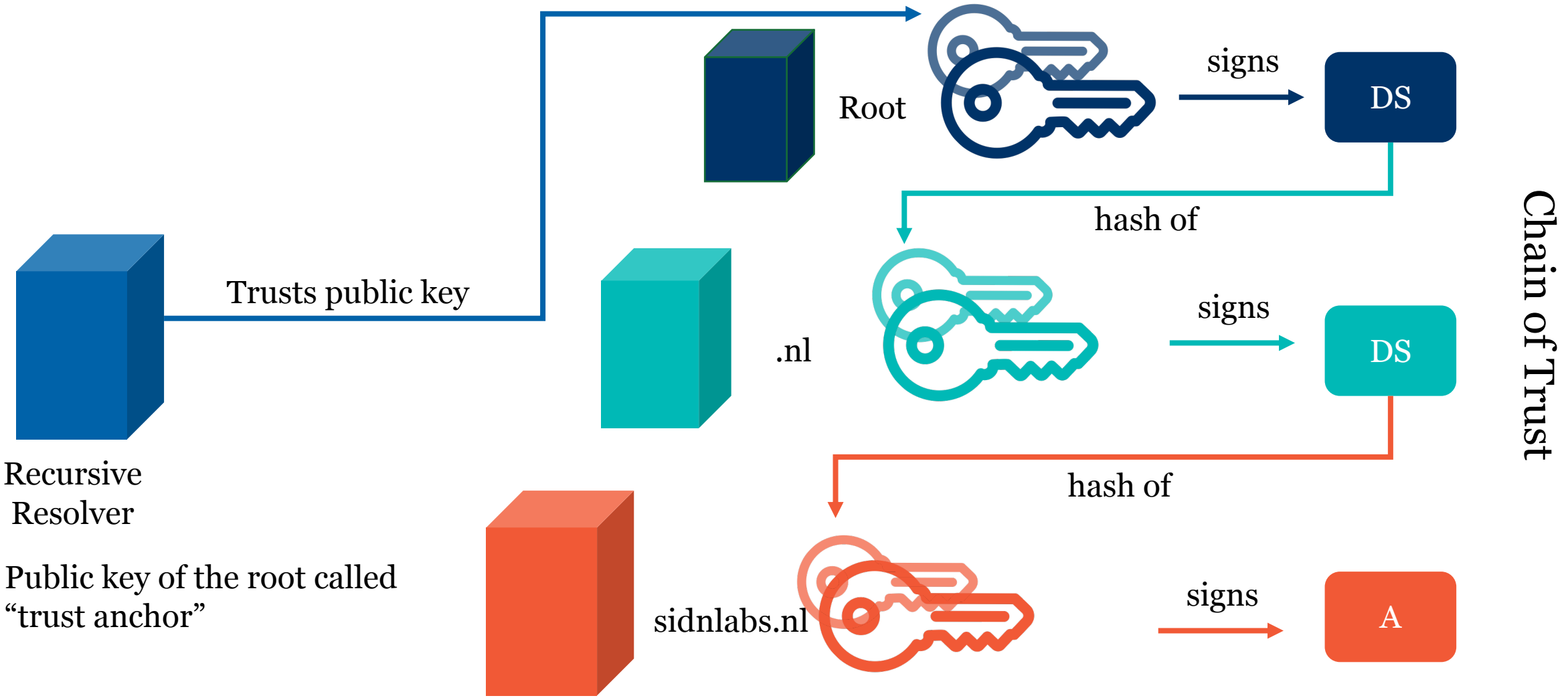
Trust in DNSSEC



Trust in DNSSEC



Trust in DNSSEC

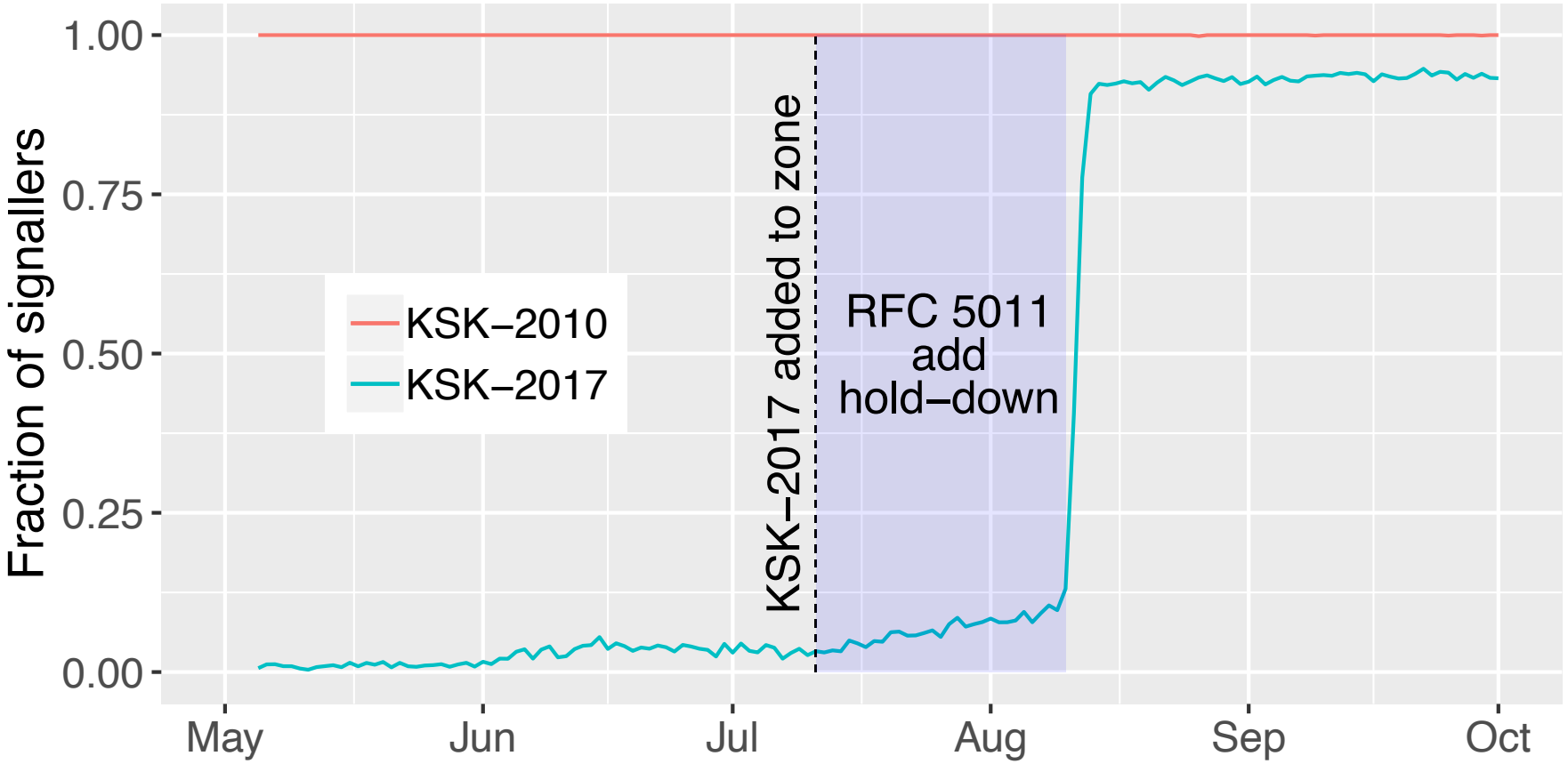


- Public key of the root called "trust anchor"

Trust Anchor Management

- Shipped with software release
- Automatic update (RFC 5011)
  - New key added to the DNSKEY set and signed with the leaving key
  - Resolver queries for the DNSKEY set of the root once per day
  - If it sees the key 30 days in a row it adds the new key to the trust anchor

Automatic Trust Anchor Management



[1]

Authenticated denial of existence

- Use case: Queried domain name does not exist or the queried record does not exist
- Introducing NSEC (RFC 3755): Proving that the “holes” in a zone do not exist
- Approach: Sort records, add NSEC records, sign NSEC record

Authenticated denial of existence

- Approach: Sort records, add NSEC records, sign NSEC reocrds
- Assuming a zone containing:
  - *example.com SOA*
  - *a.example.com A*
  - *c.example.com A, TXT*
- To prove that b.example.com does not exist add NSEC record:
  - *a.example.com NSEC c.example.com*

Authenticated denial of existence

- What about a query for a non-existing record?
- Assuming a zone containing:
  - *example.com SOA*
  - *a.example.com A*
  - *c.example.com A, TXT*
- Construct NSEC record that covers all existing record types.
  - *a.example.com. NSEC c.example.org. A NSEC RRSIG*

Authenticated denial of existence

- What about a query for a wildcard?
- In DNS, wildcards can be used to define all names for a certain type:
- Assuming a zone containing:
  - *example.com SOA*
  - **.example.com TXT "a wildcard record"*
  - *a.example.com A*
  - *c.example.com A, TXT*
- Construct NSEC record that covers the wildcard and return it with the response.
- **.example.com NSEC TXT RRSIG NSEC*

Authenticated denial of existence

- Problems with NSEC:
  - Reveals the content of the zone
  - Requires large zones to create a lot of NSEC records
- NSEC3 solves this to some extent, explanation skipped for today

Operations

- Signing
- Signature lifetime
- Rollovers
  - Frequency
  - Signaling mechanisms

Problems with DNSSEC

- Increase in response size:
  - Misused in DDoS amplification attacks
  - Fall-back to TCP instead of UDP
- Dynamic responses require online signing
- Makes DNS more complicated
- Not protecting the connection between recursive resolver and stub resolver

Reference and other reading material

- [1] Moritz Müller, Matthew Thomas, Duane Wessels, Wes Hardaker, Taejoong Chung, Willem Toorop, and Roland van Rijswijk-Deij. 2019. Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover. In Proceedings of the Internet Measurement Conference (IMC '19). Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3355369.3355570
- More about NSEC and NSEC3:Whitepaper
- More details on DNS, DNSSEC, DoH, DoT, DNS Abuse … :van der Toorn, O., Müller, M., Dickinson, S., Hesselman, C., Sperotto, A., & van Rijswijk-Deij, R. (2022). Addressing the Challenges of Modern DNS: A Comprehensive Tutorial. *Computer Science Review*, *45*, 100469.

Follow us

SIDN.nl


@SIDN

SIDN

Thank you for your attention!

We're also looking for students! Please contact:
moritz.muller@sidn.nl

SIDN LABS