Measuring Occurrence of DNSSEC Validation

Matthäus Wander, Torben Weis

<dnssec@vs.uni-due.de>

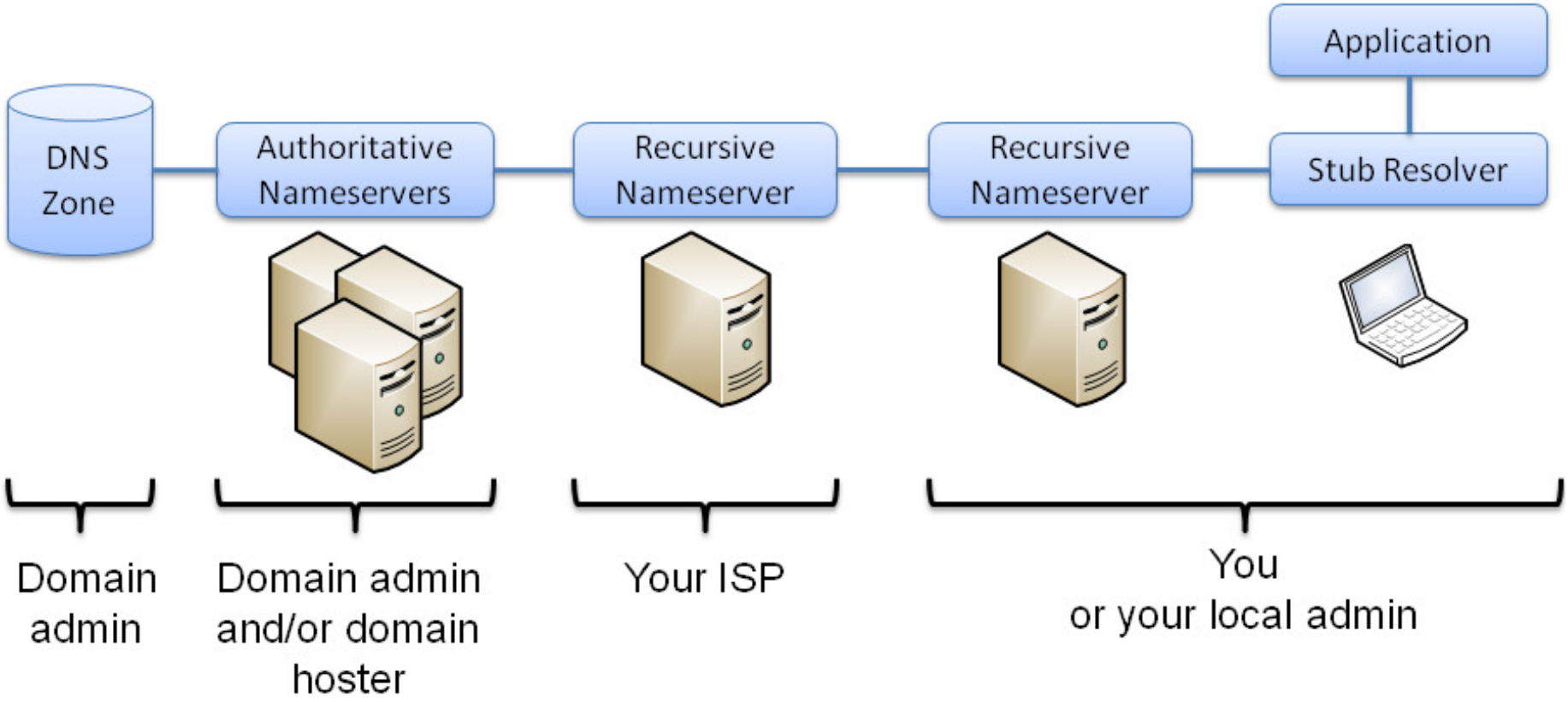
Passive and Active Measurements Conference

Hong Kong, March 19, 2013

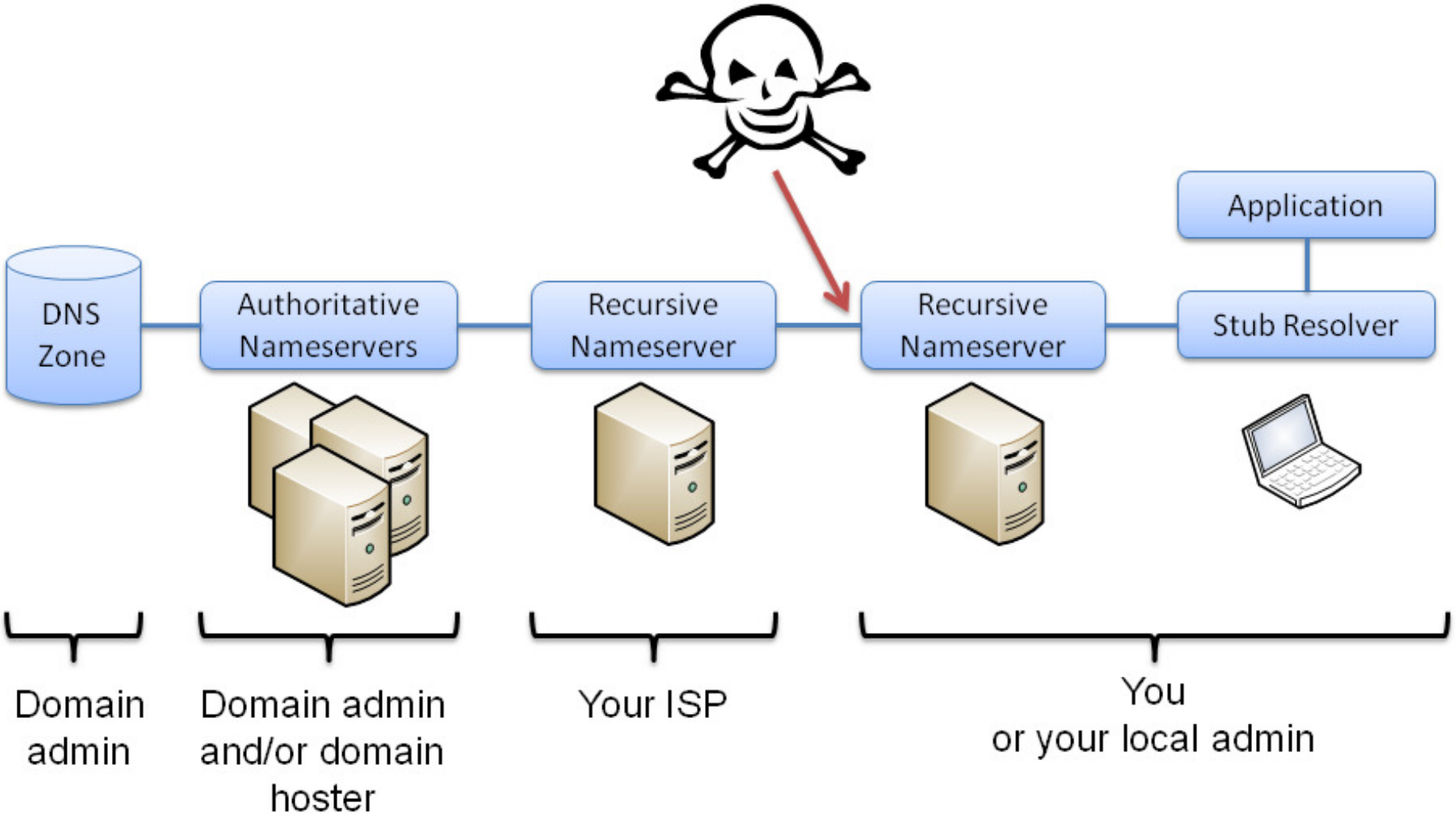
Overview

- Introduction to DNSSEC
- Measurement methodology
- Result analysis

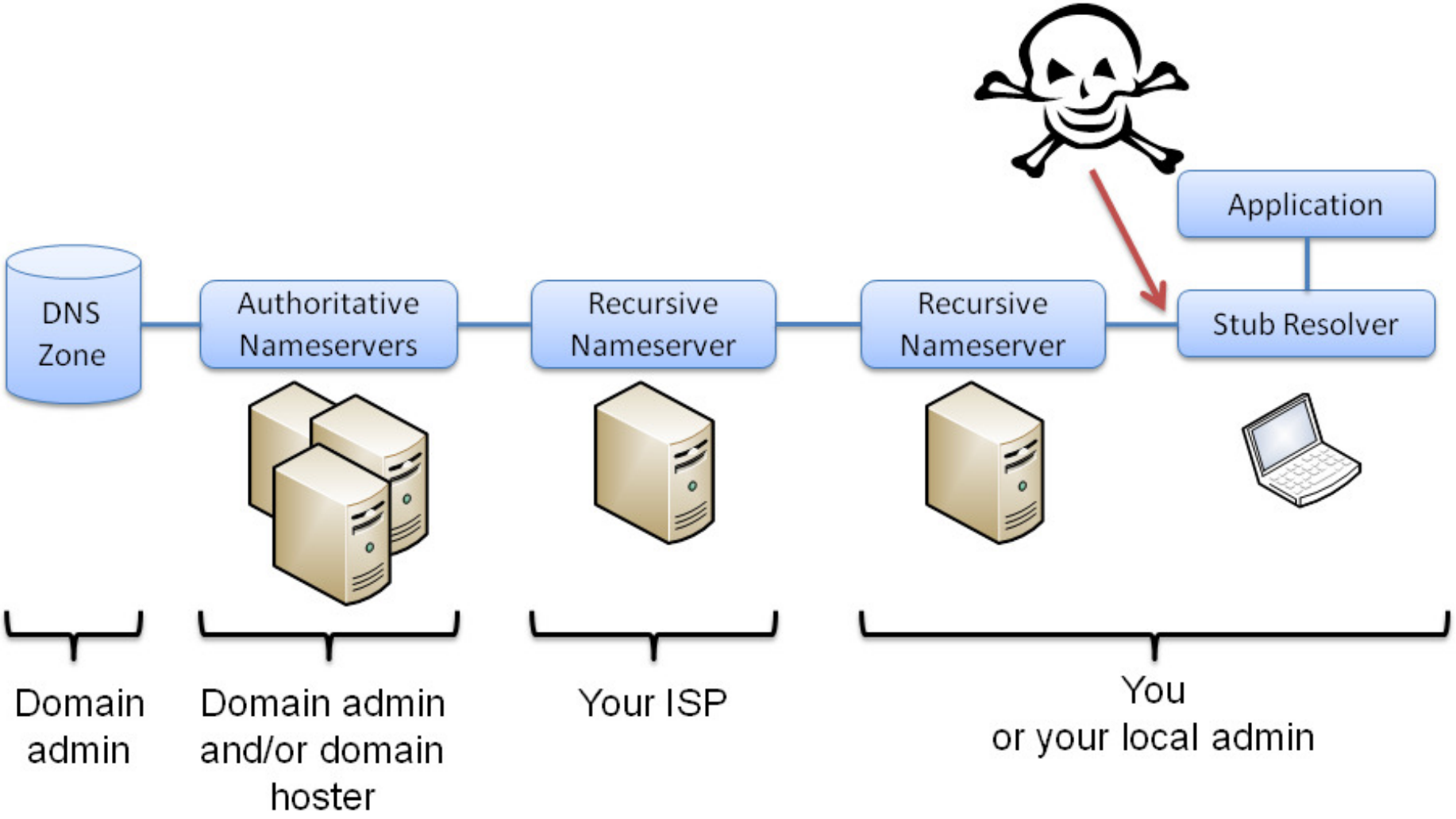
Domain Name System



Remote DNS Spoofing



Local DNS Spoofing



DNSSEC

- Domain Name System Security Extensions
- Uses cryptography to achieve data integrity and authenticity
  - Note: not confidentiality, not availability
- Sign resource records with private key 🔑
- Publish signatures as RRSIG record

```
example.net.    IN  A     1.2.3.4
example.net.    IN  RRSIG A 5 3 600 20120519... m1TWzfNDMg8NpgTo4i...
```

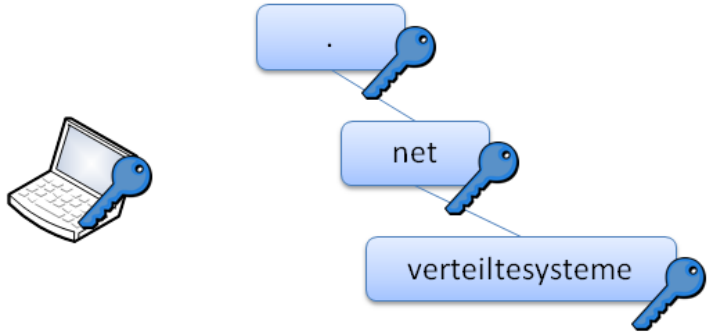
- Publish public key as DNSKEY record 🔑

```
example.net.    IN  DNSKEY   256 3 8 BQEAAAABv5hDo9fIU91cSFaDmnNPg...
```

- Tie DNSKEY with parent zone to create chain of trust

Secure Delegations

- DS record for secure delegation
  - Indicates whether child zone is signed
  - Contains hash of DNSKEY
  - DS record is signed, too
- Resolver must know a trust anchor (root key) beforehand

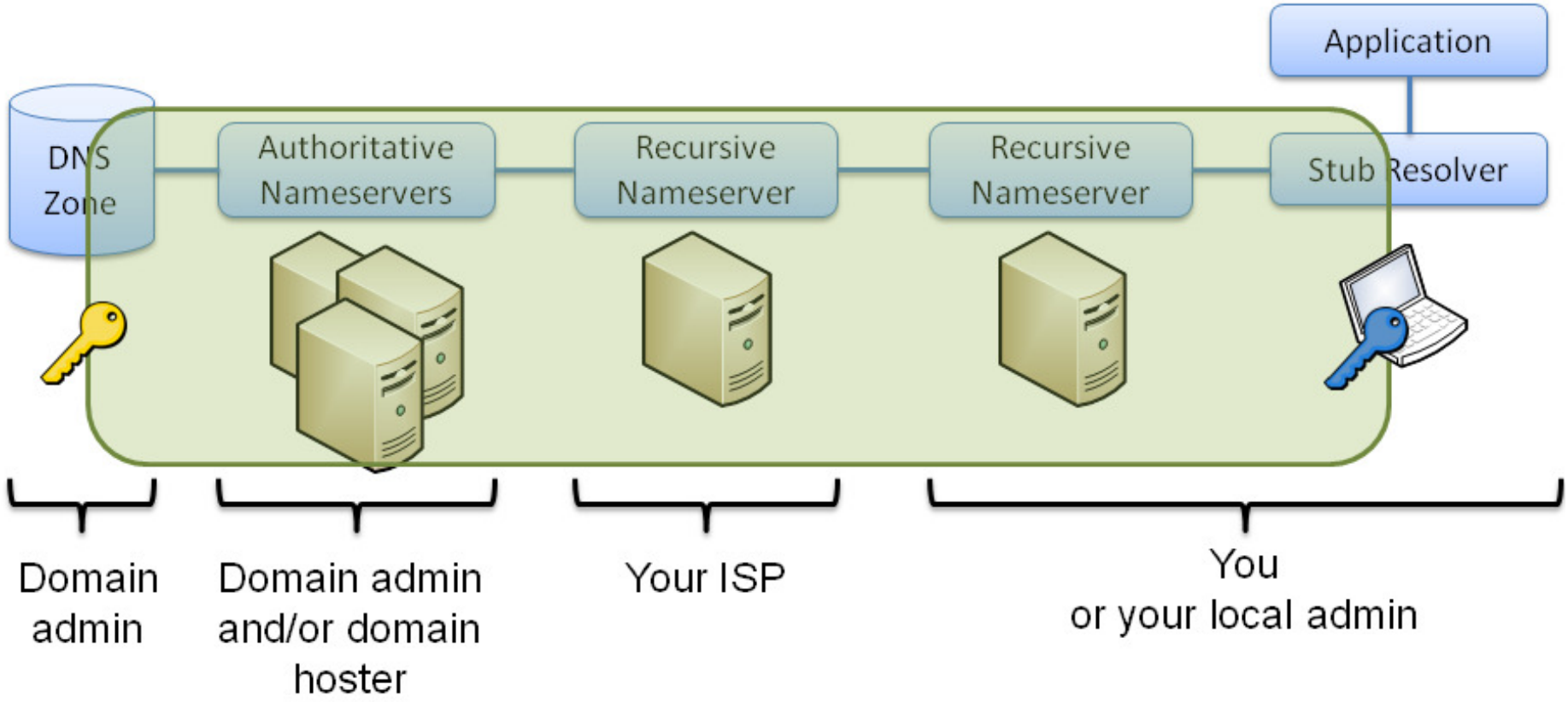



```
verteiltesysteme.net.      IN  NS     ns1.verteiltesysteme.net.
verteiltesysteme.net.      IN  NS     ns2.verteiltesysteme.net.
verteiltesysteme.net.      IN  DS     61908 5 1 3497D121F4C91369E95DC73D8...
verteiltesysteme.net.      IN  DS     61908 5 2 2F87866A60C3603F447658AC3...
verteiltesysteme.net.      IN  RRSIG  DS 8 2 86400 20130103051550 2012122...

ns1.verteiltesysteme.net.  IN  A      134.91.78.139
ns2.verteiltesysteme.net.  IN  A      134.91.78.141
```

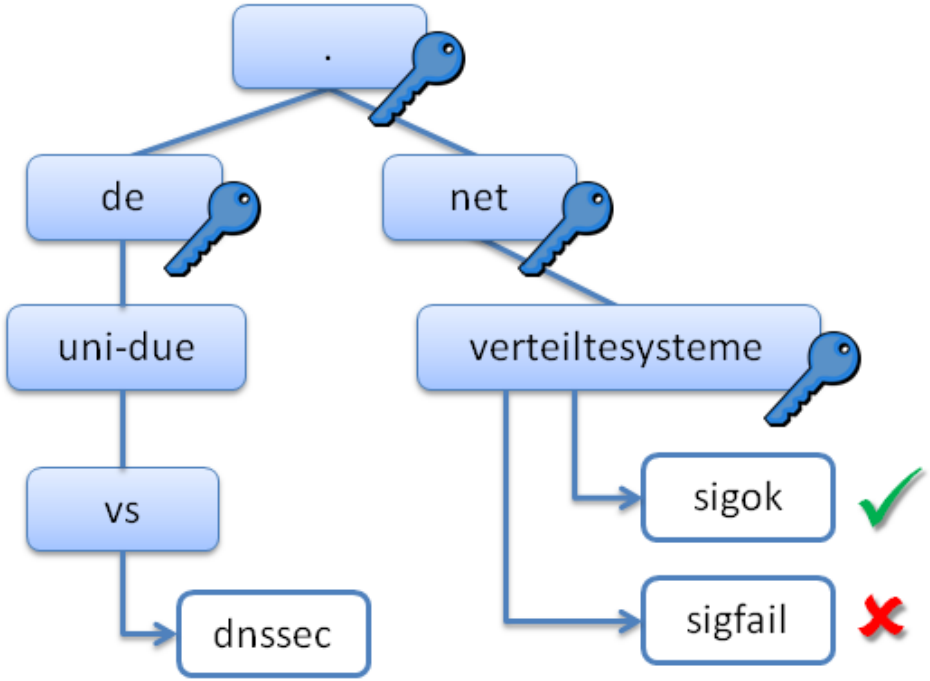
```
verteiltesysteme.net.      IN  DNSKEY 257 3 5 BQEAAAABy5oBPRz/mSEcFYXlcL...
```

Protection by DNSSEC



⇨ How many clients are protected by DNSSEC?

Measurement Methodology

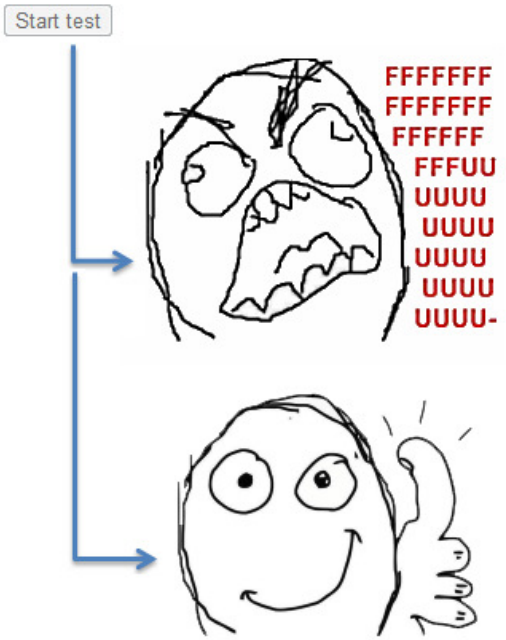


- Signed zone `verteiltesysteme.net`
  - Domain name `sigok` ✓ with valid signature
  - Domain name `sigfail` ✗ with broken signature
- Two web-based resolver tests (interactive, hidden)

Interactive Test

⇨ http://dnssec.vs.uni-due.de

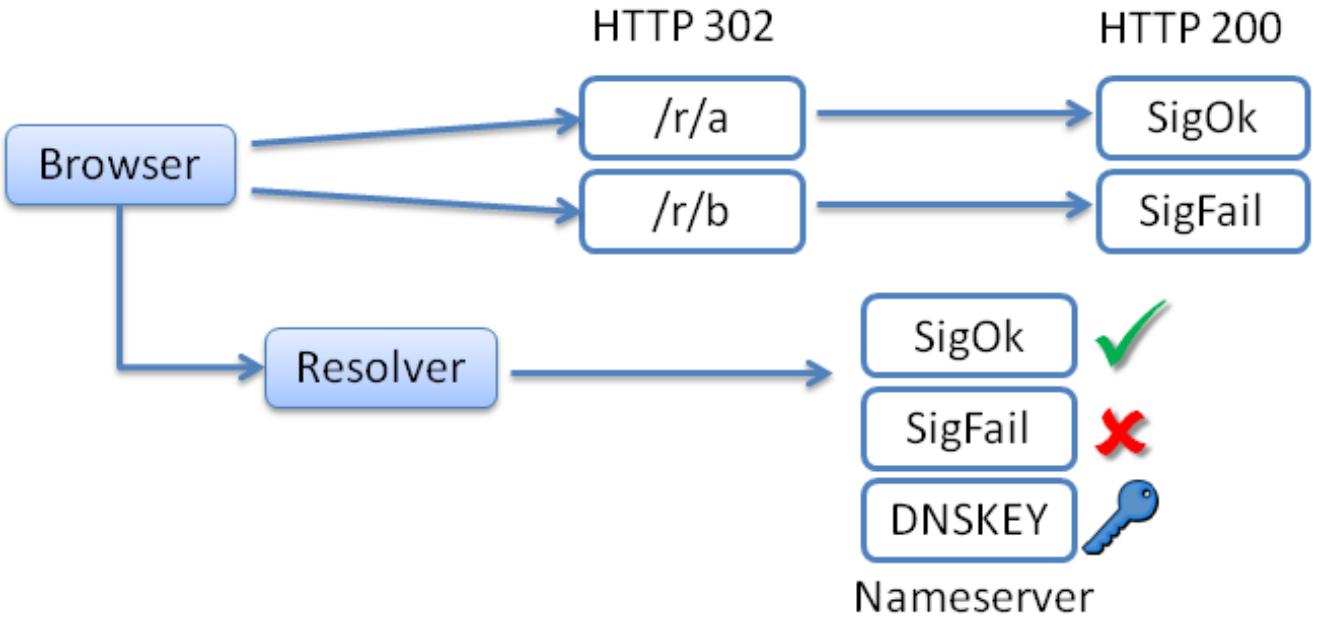
- Client-side JavaScript and images
- Load image from `sigfail` ✘ domain name
  - Success: no DNSSEC validation
  - Failure: go ahead
- Load image from `sigok` ✓ domain name
  - Success: DNSSEC validation enabled
  - Failure: inconclusive result
- Result is shown to the user and POSTed to our webserver



Hidden Test

- Load transparent 1x1 pixel images from `sigok` ✓ and `sigfail` ✘
  - Static HTML snippet (no JavaScript)

```
<img src="http://dnssec.vs.uni-due.de/r/a" alt="" height="1" width="1">
<img src="http://dnssec.vs.uni-due.de/r/b" alt="" height="1" width="1">
```



- HTTP and DNS requests logged and evaluated offline

Client Identification

- Correlate client with resolver IP address in different server logfiles

```
77.181.135.120 "GET /ok.png?aa53 HTTP/1.1" 200 413
62.53.190.69#22782: query: aa53.sigok.verteiltesysteme.net IN A -ED
```

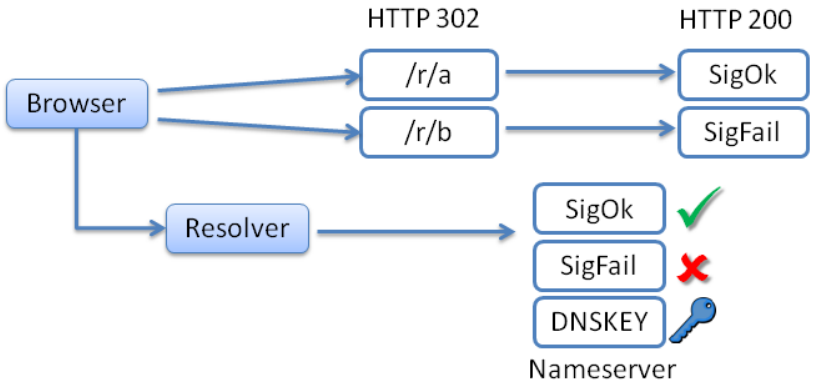
- HTTP redirect to `http://ID.sigok.verteiltesysteme.net/ok.png?ID`
  - Where `ID` := hex(SHA256(client_ip))[0:4]
  - Stateless mapping of client IP address to 16 bit ID
  - Unlikely to collide at the same time with different clients
- Pre-generated zone with 2^{19} resource record (88 MB)
  - Delivers broken signatures without nameserver adaptation
  - Vanilla zone layout

Accuracy

- `sigfail`✘ might fail to load for unrelated reasons → **false positive**
- Require loading `sigok`✓ to exclude some fault sources, e.g.:
  - failing to receive EDNS0 messages with packet size >512 bytes
  - not loading images or not following cross-domain HTTP redirects
- Some fault sources remain, e.g.:
  - network fault
  - user closes browser tab prematurely
- Another possible fault: `sigfail`✘ loads, `sigok`✓ fails
  - Harmless invalid result (false negatives are not possible)
  - Same fault pattern like a false positive (occurs with non-validators only) → estimate ratio of false positives

Result Analysis

- 4.6M DNS/HTTP requests since May 2012
  - Grouped by ID into 562k Bernoulli trials
  - Δtime between requests <30s
- Required requests:
  - Both HTTP redirects
  - DNS request for `sigok` ✓ and `sigfail` ✗
  - HTTP 1x1 image request from `sigok` ✓
- DNSSEC validation enabled:
  - no `sigfail` ✗ HTTP query **OR**
  - all DNS queries without `DNSSEC OK` flag



Invalid Trials

- Removed 203k incomplete trials
  - Same client visiting several pages + browser caching
  - Redirects queried from different IP addresses
  - Robots and other noise

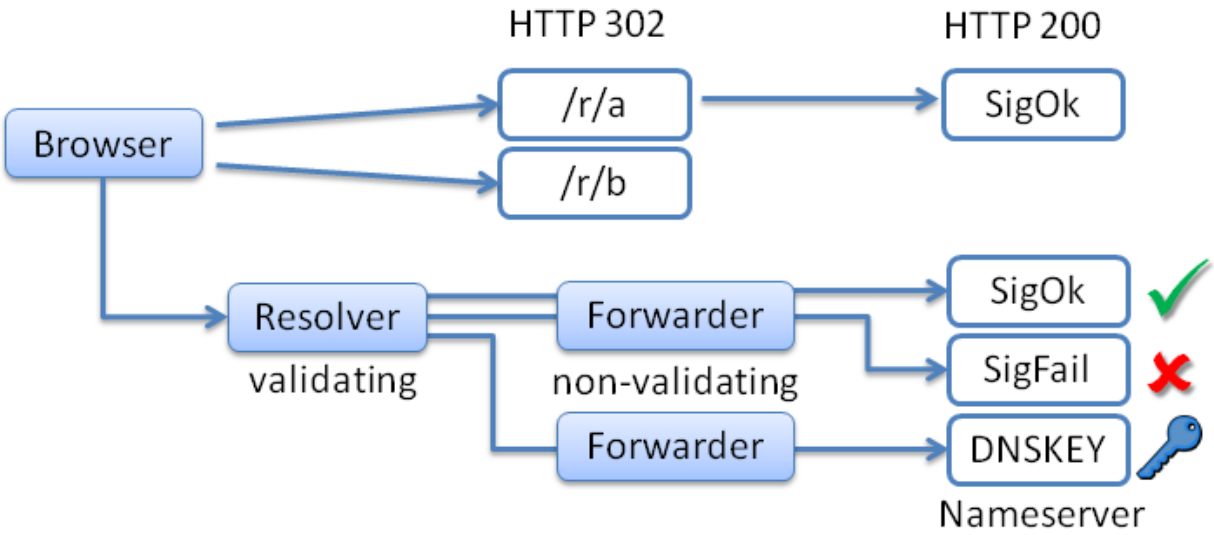
Missing Query	Count
HTTP Redirects	
RedirOk+RedirFail	79255
RedirOk	6171
RedirFail	6818
DNS Queries	
SigOk+SigFail	99836
SigOk	5542
SigFail	2713
HTTP Image	
SigOk+SigFail	2009
SigOk	470

Estimate ratio of false positives:

- HTTP `sigok` ✓ query missing
- HTTP `sigfail` ✗ query exists
- Non-validating resolver
- 470 trials (0.13%)

DNSKEY Missing

- Seemingly positive result but DNSKEY🔑 query is missing
- Indicates **false positive**
  - Occurred in 521 trials (0.14%), comparable to estimate
- Limitation: we correlate DNSKEY🔑 via IP address, not ID
  - Might be a true positive in forwarding scenario



Data Cleaning

- Filter positive result when DNSKEY🔑 is missing (0.14%)
- Filter duplicate results per IP address within 12h (49.5%)
  - Count each client once per browsing session
  - For dynamic IP addresses, count different clients on same address
  - Xie (2007): time interval between two users on same dynamic IP is $>$12h in 80% of all cases
- Filter ID hash collisions ($<$0.01%)
  - Different client IP addresses with same ID

⇨ 181k remaining results from 136k distinct IP addresses

DNSSEC Validation Ratio

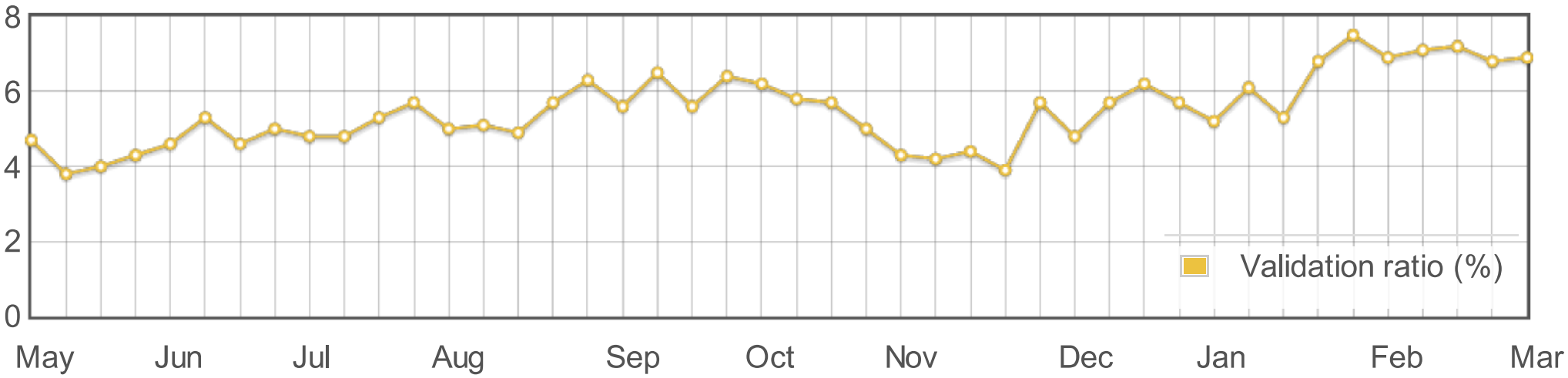


Chart 1: Validation ratio per calendar week, overall 5.3%

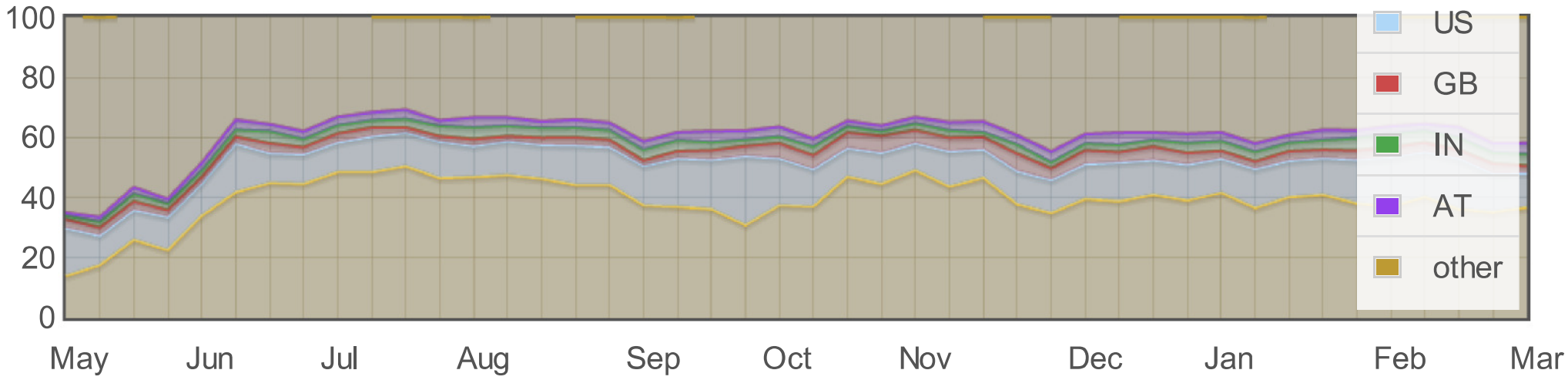
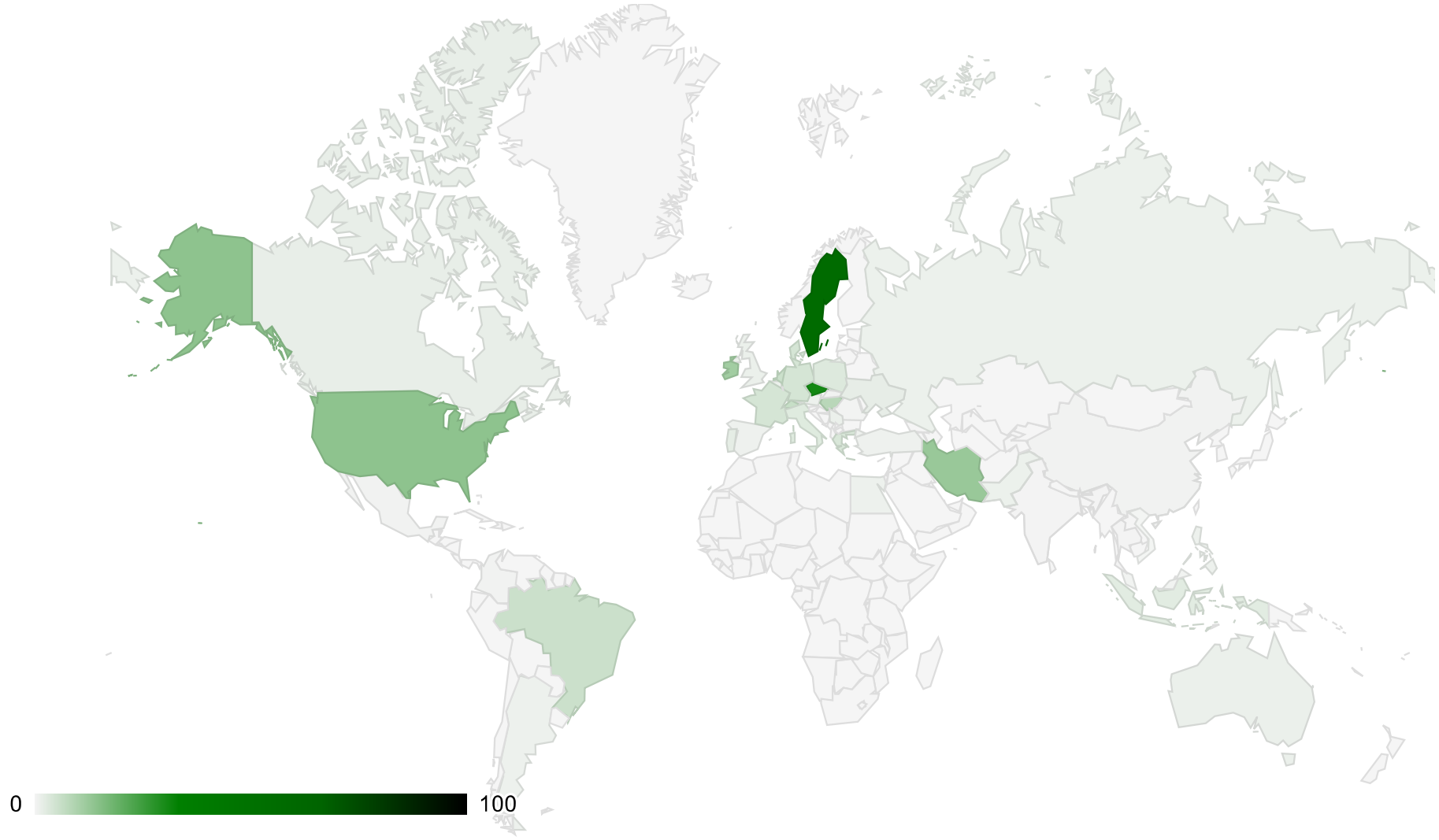


Chart 2: Top 5 participating countries

DNSSEC per Country (Map)



45 Countries with > 500 results

DNSSEC per Country (Table)

No.	Country	Trials	Validation	σ
1.	Sweden	1465	57.6%	±1.3
2.	Czech Republic	1554	30.7%	±1.2
3.	United States	22021	14.0%	±0.2
4.	Iran	644	12.4%	±1.3
5.	Ireland	557	11.1%	±1.3
6.	Hungary	670	8.2%	±1.1
7.	Switzerland	4254	6.1%	±0.4
8.	Brazil	1862	5.7%	±0.5
9.	Netherlands	3015	5.7%	±0.4
10.	Denmark	711	4.4%	±0.8
11.	Germany	65779	4.3%	±0.1
12.	France	4026	4.2%	±0.3
13.	Greece	2783	3.7%	±0.4
14.	Poland	3293	3.2%	±0.3
15.	Italy	2240	2.9%	±0.4
16.	Indonesia	1671	2.6%	±0.4
17.	Portugal	781	2.0%	±0.5
18.	Ukraine	2115	1.9%	±0.3
19.	Canada	2304	1.6%	±0.3
20.	Australia	1420	1.3%	±0.3
21.	United Kingdom	5871	1.3%	±0.1
22.	Serbia	1568	1.3%	±0.3
23.	Belgium	1246	1.2%	±0.3

No.	Country	Trials	Validation	σ
24.	Russian Federation	3630	1.2%	±0.2
25.	Pakistan	759	1.1%	±0.4
26.	Philippines	1053	1.0%	±0.3
27.	Egypt	1011	1.0%	±0.3
28.	Argentina	708	1.0%	±0.4
29.	Austria	4630	1.0%	±0.1
30.	European Union	932	0.9%	±0.3
31.	Turkey	1580	0.8%	±0.2
32.	Spain	4285	0.8%	±0.1
33.	China	942	0.6%	±0.3
34.	Slovakia	1022	0.6%	±0.2
35.	Colombia	699	0.6%	±0.3
36.	Mexico	1267	0.6%	±0.2
37.	Malaysia	939	0.4%	±0.2
38.	Romania	1885	0.3%	±0.1
39.	India	4883	0.2%	±0.1
40.	Thailand	544	0.2%	±0.2
41.	Viet Nam	3177	0.1%	±0.0
42.	Israel	990	0.0%	±0.0
43.	Bulgaria	654	0.0%	±0.0
44.	Saudi Arabia	650	0.0%	±0.0
45.	Singapore	506	0.0%	±0.0

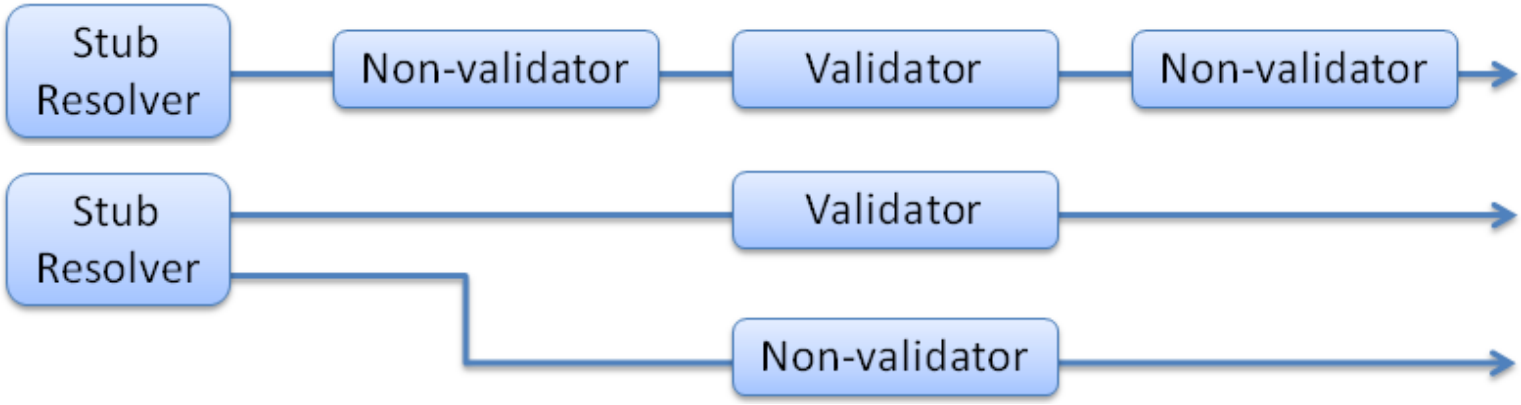
Top Validating Networks

No.	AS	Organization	Count	$\frac{V}{V_{total}}$	$\frac{V}{V+N}$	client=resolver
1.	7922	Comcast	2786	29.2%	71.3%	0.9%
2.	29562	KabelBW	1417	14.9%	87.4%	0.4%
3.	8767	M-Net	519	5.4%	42.8%	4.6%
4.	3301	TeliaSonera	297	3.1%	76.9%	1.7%
5.	5610	O2 Czech	279	2.9%	72.3%	1.4%
6.	29484	rub.de	198	2.1%	46.0%	0.0%
7.	2119	Telenor	188	2.0%	53.9%	1.1%
8.	680	DFN	152	1.6%	4.3%	3.9%
9.	6661	pt.lu	145	1.5%	83.8%	0.0%
10.	1257	Tele2	127	1.3%	53.4%	0.8%
7083 other AS			3433	36.0%	2.0%	17.8%

- No AS is fully protected by DNSSEC
- Most validating clients rely on their AS operator for DNS resolution

Related Work

- Web clients protected by DNSSEC validation



- Analysis of partial network traces of top-level domain servers
  - Gudmundsson for .org in 2010/2011 (0.8% validating resolvers)
  - Fujiwara for .jp in Feb 2012 (10.000 validating resolvers)
- Web-based tests
  - Wessels (VeriSign): analysis of resolver query pattern
  - SIDN: checks whether DNSKEY query occurred

Conclusion

- Download anonymized result set: http://dnssec.vs.uni-due.de
- Willing to contribute?
  - Point your friends to our website
  - Add HTML snippet to your website
- Some clients use mixed validating and non-validating resolvers
  - Get SERVFAIL from validator, fall back to non-validator
  - Our test yields negative result in case of mixed validation
  - **Except** when application aborts waiting for name resolution

⇨ Effect of mixed validation needs to be investigated further