Testbed: DNSSEC für DE

- Abschlußbericht -

Peter Koch <koch@denic.de>
Marcos Sanz <sanz@denic.de>

Frankfurt/Main, 8. Februar 2011

Testbed-Chronologie

2010

Moderne Kommunikation schreibt sich mit .de

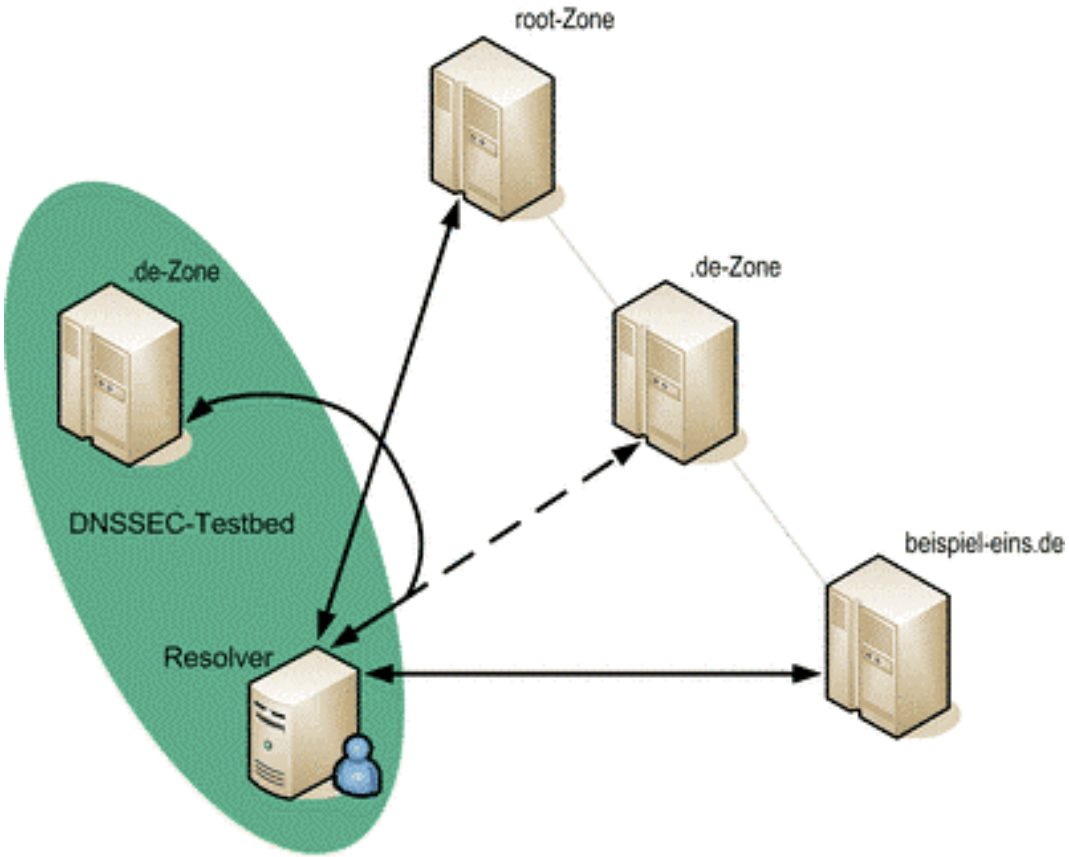
DENIC .de

Dezember 09	Januar	Februar	März	April	Mai	Juni	Juli	August	September	Oktober	November	Dezember	Januar 11
1 Di 49	1 Neujahr	1 Domain pulse	1	1 Do	1 Tag der Arbeit	1 Di	1 Do	1 So	1 Mi	1 Fr	1 Allerheiligen	1 Mi	1 Sa
2 Mi	2 Sa	2 Domain pulse	2 Di	2 Karfreitag	2 So	2 Mi	2 Fr	2 Mo 31	2	2 Sa	2 Di 44	2 Do	2 So
3 Do	3 So	3 Mi 5	3 Mi	3 Sa	3 Mo 18	3 Fronleichnam	3 Sa	3 Di	3 Fr	Tag d. Dt. Einheit	3 Mi	3 Fr	3 Mo 1
4 Fr	4	4 Do	4 Do	4 Ostersonntag	4 Di	4 Fr	4 So	4 Mi	4 Sa	4 Mo 40	4 Do	4 Sa	4 Di
5 Sa	5 Di	5 Fr	5 Fr	5 Ostermontag	5 Mi	5 Sa	5 Mo 27	5 Do	5 So	5 Di	5 Fr	5 2. Advent	5 Mi
6 2. Advent	6 Hl. Drei Könige	6 Sa	6 Sa	6 Di 14	6 Do	6 So	6 Di	6 Fr	6 Mo 36	6 Mi	6 Sa	6 Mo 49	6 Hl. Drei Könige
7 Mo 50	7 Do	7 So	7 So	7 Mi	7 Fr	7 Mo 23	7 Mi	7 Sa	7 Di	7 Do	7 So	7 Di	7 Fr
8 Di	8 Fr	8 Mo 6	8 Mo 10	8 Do	8 Sa	8 Di	8 Do	8 So	8 Mi	8 Fr	8 Mo 45	8 Mi	8 Sa
9 DNSSEC-Testbed	9 Sa	9 Di	9 Di	9 Fr	9 So	9 Mi	9 Fr	9 Mo 32	9 Do	9 Sa	9 Di	9 Do	9 So
10 Do	10 So	10 Mi	10 Mi	10 Sa	10 Mo 19	10 Do	10 Sa	10 Di	10 Fr	10 So	10 Mi	10 Fr	10 Mo 2
11 Fr	11 Mo 2	11 Do	11 Do	11 So	11 Di	11 Fr	11 So	11 Mi	11 Sa	11 Mo 41	11 Do	11 Sa	11 Di
12 Sa	12 Di	12 Fr	12 Fr	12 Mo 15	12 Mi	12 Sa	12 Mo 28	12 Do	12 So	12 Di	12 Fr	12 3. Advent	12 Mi
13 3. Advent	13 Mi	13 Sa	13 Sa	13 Di	13 Christi Himmelfahrt	13 So	13 Di	13 Fr	13 Mo 37	13 Mi	13 Sa	13 Mo 50	13 Do
14 Mo 51	14 Do	14 So	14 So	14 Mi	14 Fr	14 Mo 24	14 Mi	14 Sa	14 Di	14 Do	14 So	14 Di	14 Fr
15 Di	15 Fr	15 Mo 7	15 Mo 11	15 Do	15 Sa	15	15 Do	15 Mariä Himmelfahrt	15 Mi	15 Fr	15 Mo 46	15 Mi	15 Sa
16 Mi	16 Sa	16 Di	16 Di	16 Fr	16 So	16 DNSSEC-Testbed	16 Fr	16 Mo 33	16 Do	16 Sa	16 Di	16 Do	16 So
17 Do	17 So	17 Mi	17 Mi	17 Sa	17 Mo 20	17 Do	17 Sa	17 Di	17 Fr	17 So	17 Buß- und Bettag	17 Fr	17 Mo 3
18 Fr	18 Mo 3	18 Do	18 Techn. Meeting	18 So	18 Di	18 Fr	18 So	18 Mi	18 Sa	18 Mo 42	18 Do	18 Sa	18 Di
19 Sa	19 Di	19 Fr	19 Fr	19 Mo 16	19 Mi	19 Sa	19 Mo 29	19 Do	19 So	19 Di	19 Fr	19 4. Advent	19 Mi
20 4. Advent	20	20 Sa	20 Sa	20 Di	20 Do	20 So	20 Di	20 Fr	20 Mo 38	20 Mi	20 Sa	20 Mo 51	20 Do
21 Mo 52	21 Do	21 So	21 So	21 Mi	21 Fr	21 Mo 25	21 Mi	21 Sa	21 Di	21 Do	21 So	21 Di	21 Fr
22 Di	22 Fr	22 Mo 8	22 Mo 12	22 Generalversammlung	22 Sa	22 Di	22 Do	22 So	22 Techn. Meeting	22 Fr	22 Mo 47	22 Mi	22 Sa
23 Mi	23 Sa	23 Di	23 Di	23 Fr	23 Pfingstsonntag	23 Mi	23 Fr	23 Mo 34	23 Do	23 Sa	23	23 Do	23 So
24 Heiligabend	24 So	24 Mi	24 Mi	24 Sa	24 Pfingstmontag	24 Do	24 Sa	24 Di	24 Fr	24 So	24 DNSSEC-Testbed	24 Heiligabend	24 Mo 4
25 1. Weihnachtstag	25	25 Do	25 Do	25 So	25 Di 21	25 Fr	25 So	25 Mi	25 Sa	25 Mo 43	25 Do	25 1. Weihnachtstag	25 Di
26 2. Weihnachtstag	26 Di	26 Fr	26 Fr	26 Mo 17	26 Mi	26 Sa	26 Mo 30	26 Do	26 So	26 Di	26 Fr	26 2. Weihnachtstag	26 Mi
27 So	27 Mi	27 Sa	27 Sa	27 Di	27 Do	27 So	27 Di	27 Fr	27 Mo 39	27 Mi	27 Sa	27 Mo 52	27 Do
28 Mo 53	28 Do	28 So	28 So	28 Mi	28 Fr	28 Mo 26	28 Mi	28 Sa	28 Di	28 Do	28 1. Advent	28 Di	28 Fr
29 Di	29 Fr		29 Mo 13	29 Do	29 Sa	29 Di	29 Do	29 So	29 Mi	29 Fr	29 Mo 48	29 Mi	29 Sa
30 Mi	30 Sa		30 Di	30 Fr	30 So	30 Mi	30 Fr	30 Mo 35	30 Do	30 Sa	30 Di	30 Do	30 So
31 Silvester	31 So		31 Mi		31 Mo 22		31 Sa	31 Di		31 Reformationstag		31 Silvester	31 Mo 5

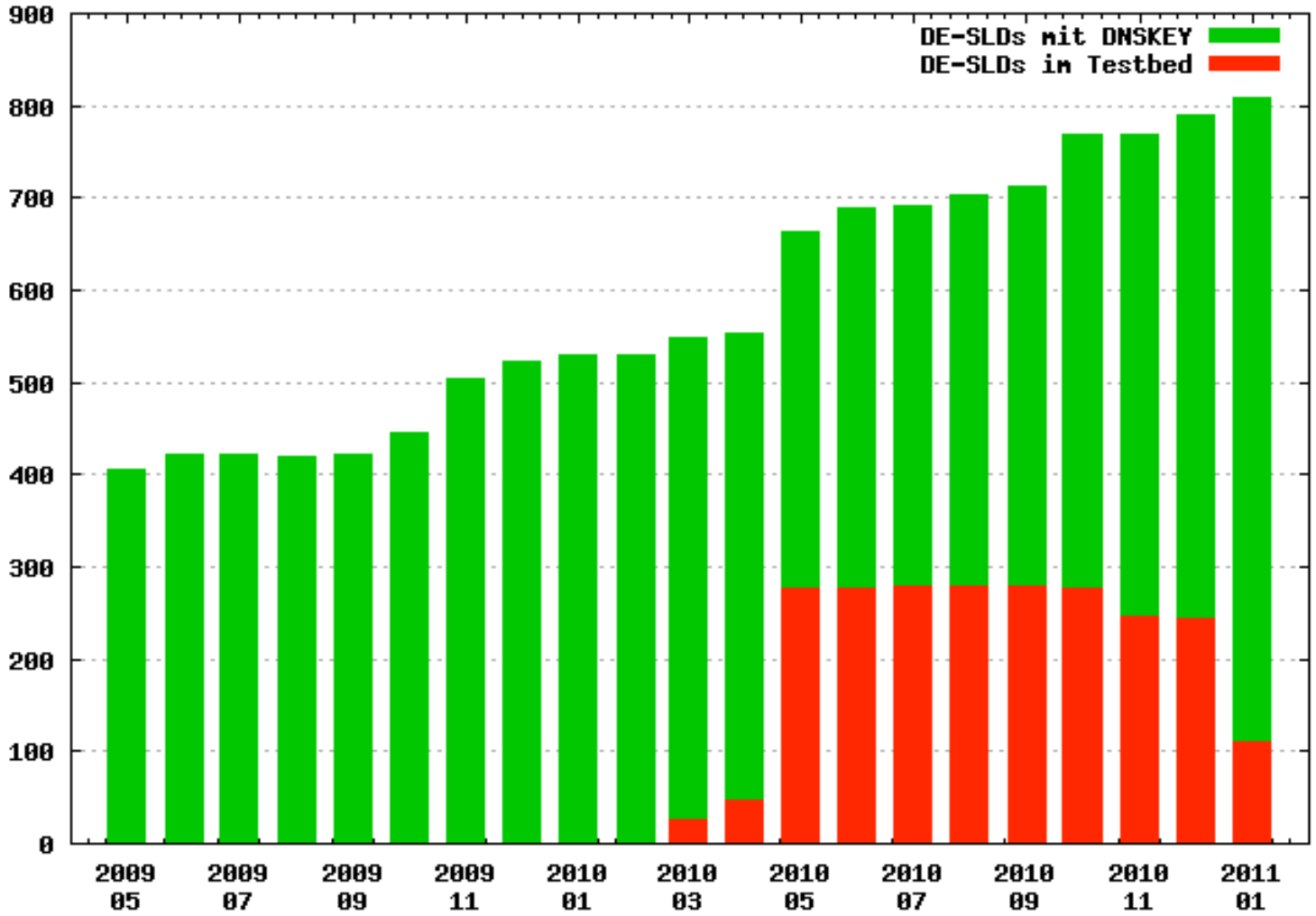
Testbed-Rahmen

- DNSSEC-Signierstationen in FRA und AMS
  - ZSK in HSM Sun SCA6000
- Separate Nameserver-Cluster in FRA und AMS
  - Gleiche Architektur wie DE-Produktion
- Resolver-Teilnahme (ab 5.1.2010)
  - BIND, Unbound, Vantio, …
- Registrierung von Schlüsselmaterial (ab 2.3.2010)
  - … durch die Produktionsschnittstelle für Registrare

Testbed - Schematische Darstellung



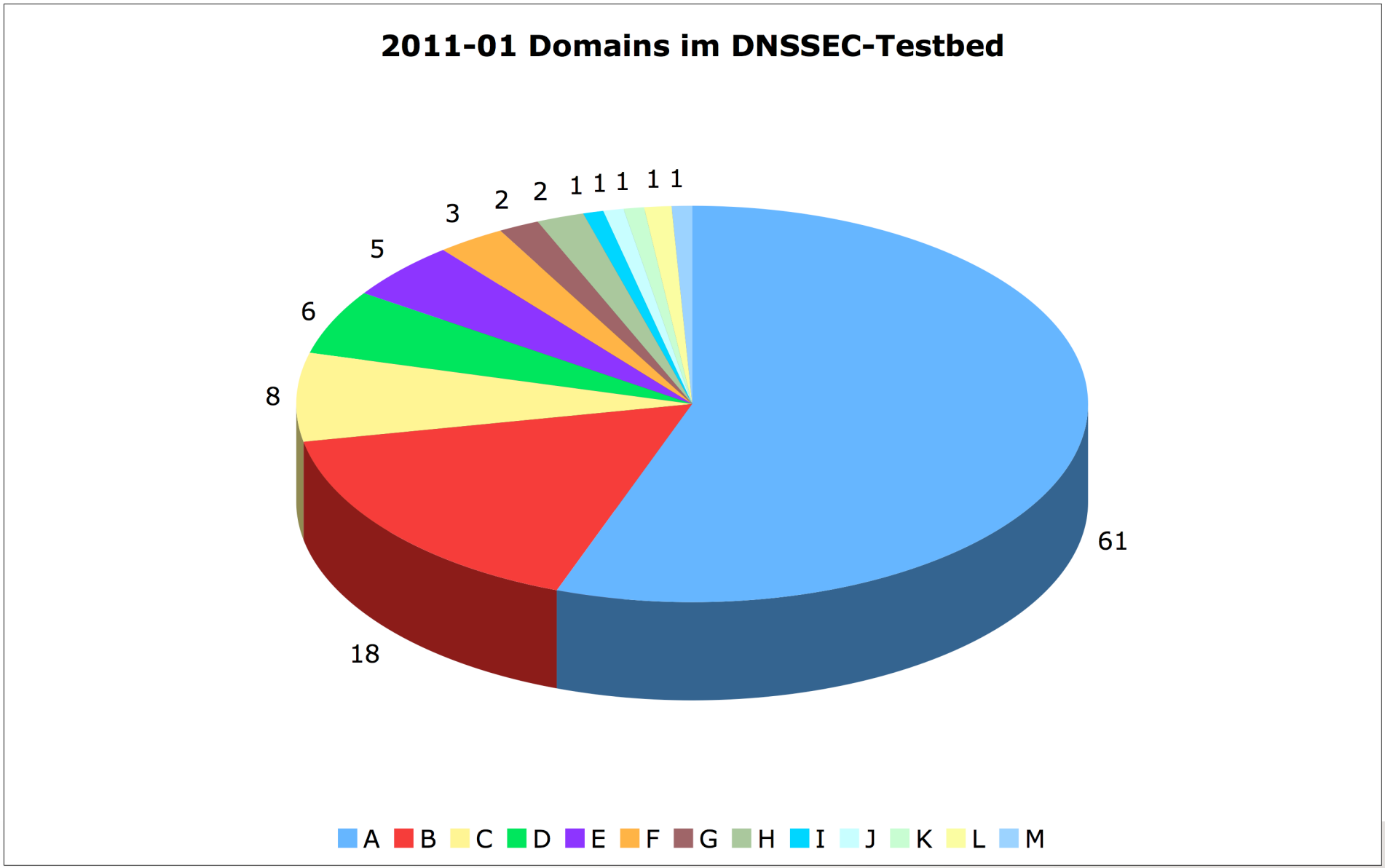
Entwicklung DNSKEY unter DE (01/2011)



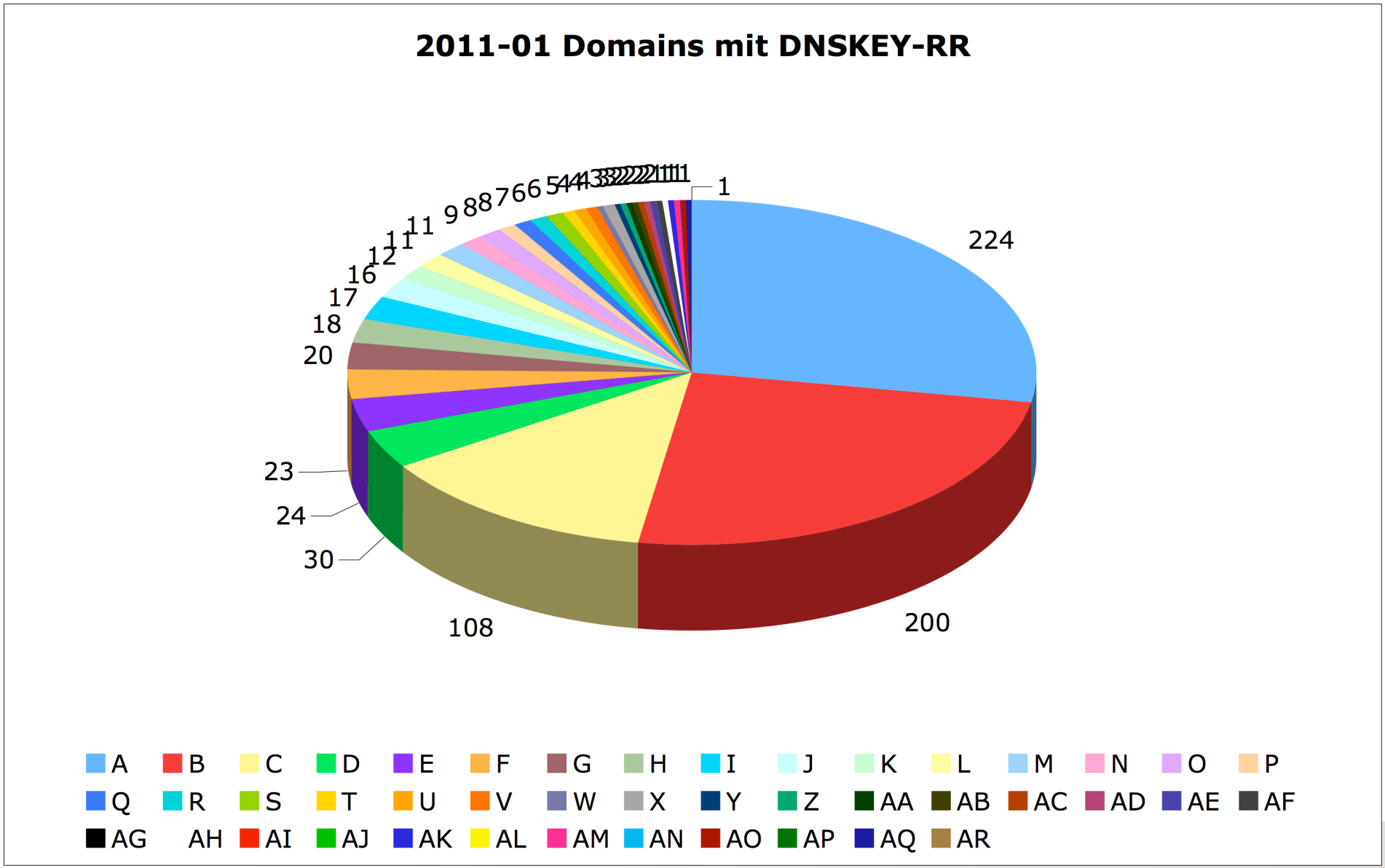
Testbed-Status

- Testbed endete offiziell zum 31.12.2010
  - Infrastruktur wird weiter betrieben
- noch 110 Domains im Testbed
  - 13 RegAccs
- ca. 120 q/s im Tagesmittel
  - davon 20-30% via IPv6
- 230 Abonnenten auf der Testbedliste
- Zonenaktualisierung zwölf Mal täglich

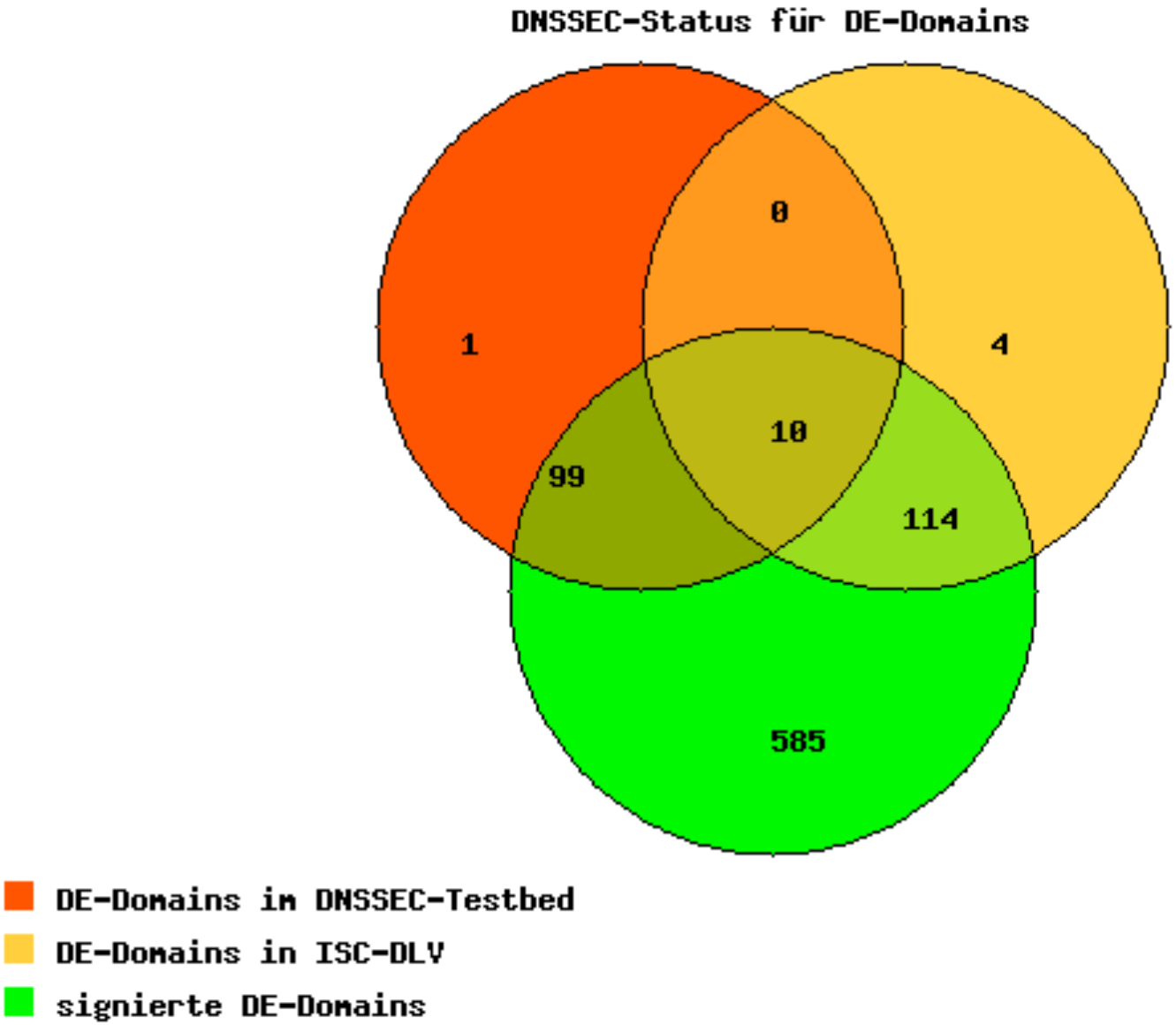
RegAccs mit DNSSEC-Kunden im Testbed



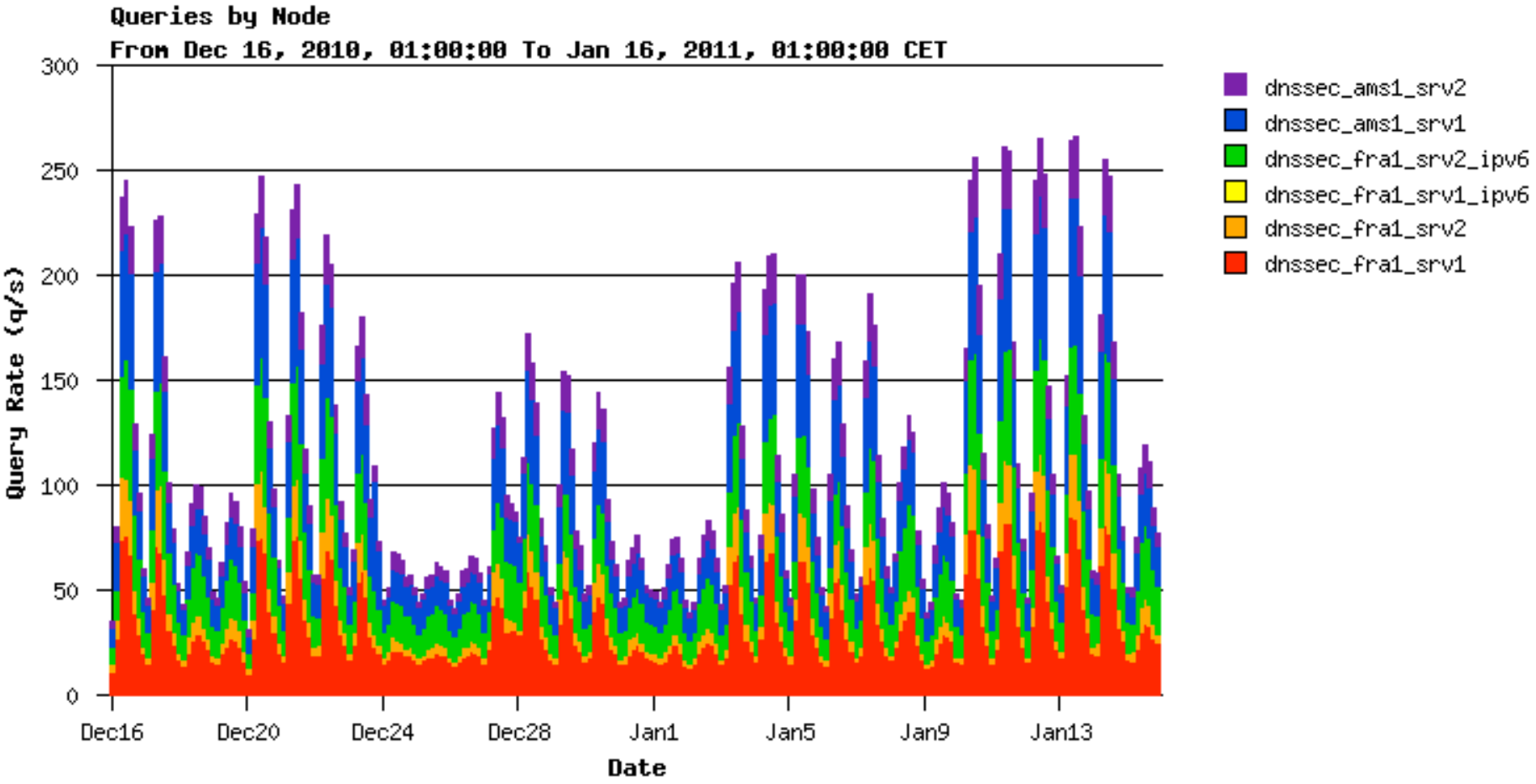
RegAccs mit DNSSEC-Interessenten aktuell



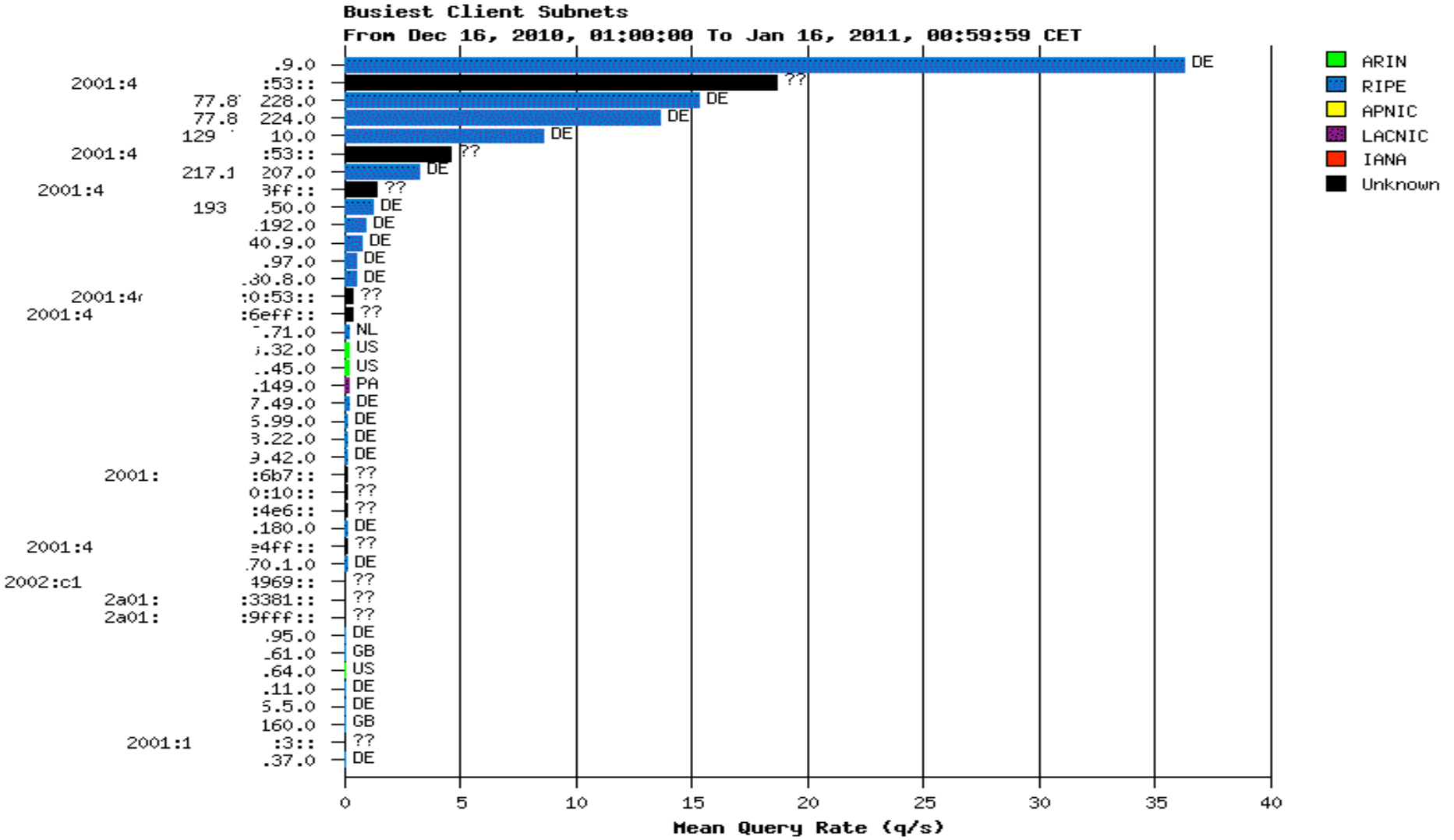
Signiert vs. Testbed vs. ISC-DLV (2011-01-31)



Testbed-Querys Dezember 2010/Januar 2011



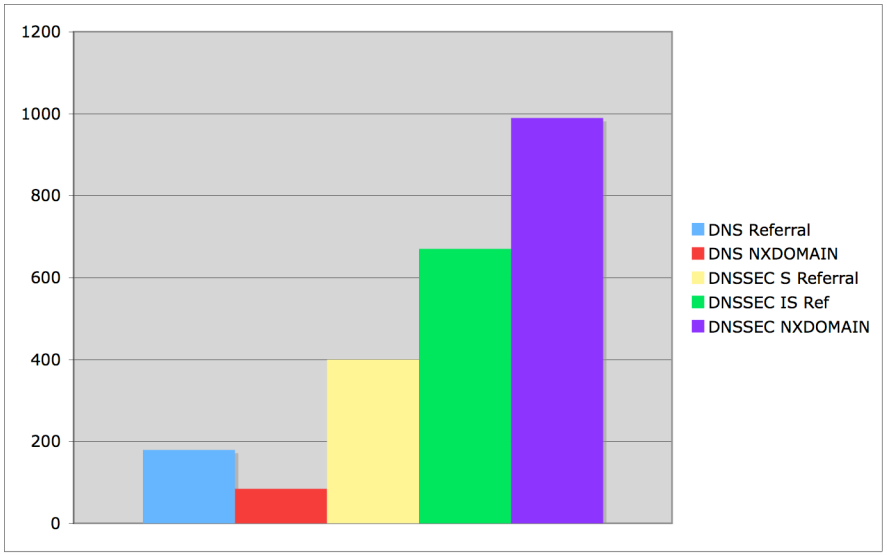
Quellen Testbed Dezember 2010/Januar 2011



Ergebnisse und Beobachtungen

Wachstum -- gestiegener Ressourcenbedarf

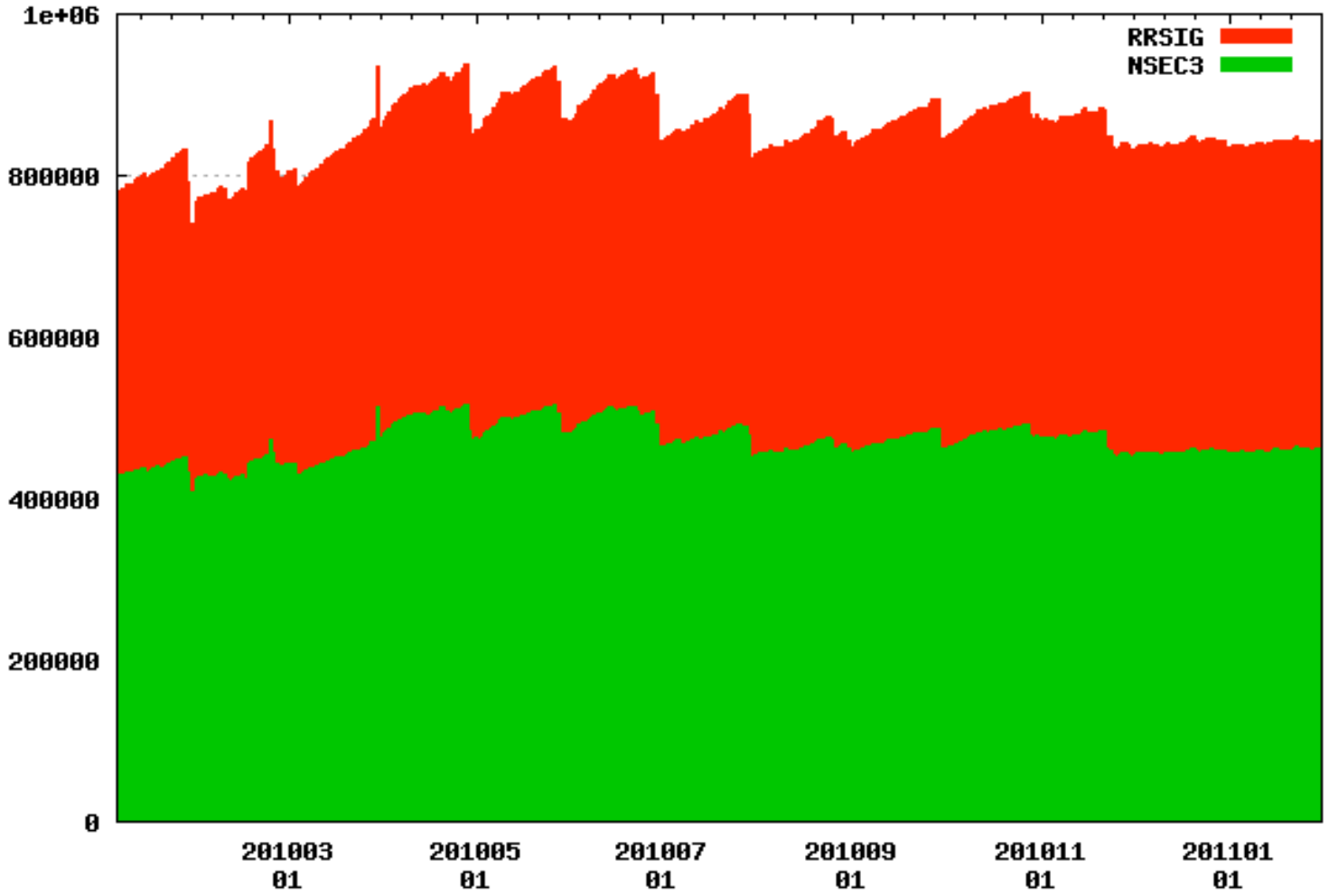
- Zone bzw. Zonendatei
  - Wachstum etwa 30%
- Bandbreite
  - Übertragung der Zone
  - DNS-Querys/-Responses
    - NSEC3 dominiert die Antwortgrößen
- Hauptspeicher der Nameserver
- Signatursysteme
  - Performanz



Antwort auf das *zone walking problem*: NSEC3

- Mitarbeit an der Spezifikation (IETF, vor 2008)
- Test (Workshops)
- Einsatz im Testbed
  - inklusive *opt-out*
- Prüfung der Stärke
  - Vortrag von Florian Obser (3. Meeting, Juni 2010)

Anzahl NSEC3/RRSIG-RRs (2011-01-31)



Ergebnisse

- Anpassung des Registrierungssystems und der damit verbundenen Auskunftssysteme
  - `DNSKEY`-RR als Registrierungsobjekt
  - DENIC-12p, DENIC-23p, sowie weitere Dokumentationen für Mitglieder
- Signierung
  - Auswahl und Implementierung eines HSM-basierten Signierungssystems mit rollenbasiertem Zugriff (Schlüsselverwaltung)
  - DNSSEC Practices Statement

Weitere Ergebnisse

- Verfahren zum Operatorwechsel unter DNSSEC
- DNSSEC-spezifische Predelegationcheck-Policy
  - konzipiert
  - als Open Source implementiert
  - als Webdienst …

Nameserver Predelegation Check Webinterface

Mit dem NAST Webinterface können Sie einen Nameserver Predelegation Check durchführen. Die Nameserver Ihrer Zone (Domain) werden dabei verschiedenen Tests unterzogen, um sicherzustellen, dass sie korrekt konfiguriert sind und die Domain sicher und einfach delegiert werden kann. Damit wird ein hoher Grad an Qualität für die Domain erzielt.

Bitte tragen Sie im Formular Ihre Domain ein. Die Angabe der Nameserver ist optional. Sind die Nameserver nicht angegeben, so werden diese automatisch aus dem DNS ermittelt. Dies ist natürlich nur bei bereits registrierten Domains möglich.

Domain :

dnsop.de

Nameserver ermitteln und Prüfung ausführen

Nameserver automatisch ermitteln

Nameserver 1:	fra.dnsop.de	IPs :	81.91.161.78
Nameserver 2:	ns.ogud.com	IPs :	
Nameserver 3:		IPs :	

Mehr Nameserver

Dnskey 1

SEP, Flags Bit 15: (•) gesetzt ( ) nicht gesetzt

Algorithmus : RSA/SHA256

Public Key :

AwEAAaV35xrg5IQBIAF9ppsxPcCveCITErRD

Mehr Dnskeys

Eingaben zurücksetzen

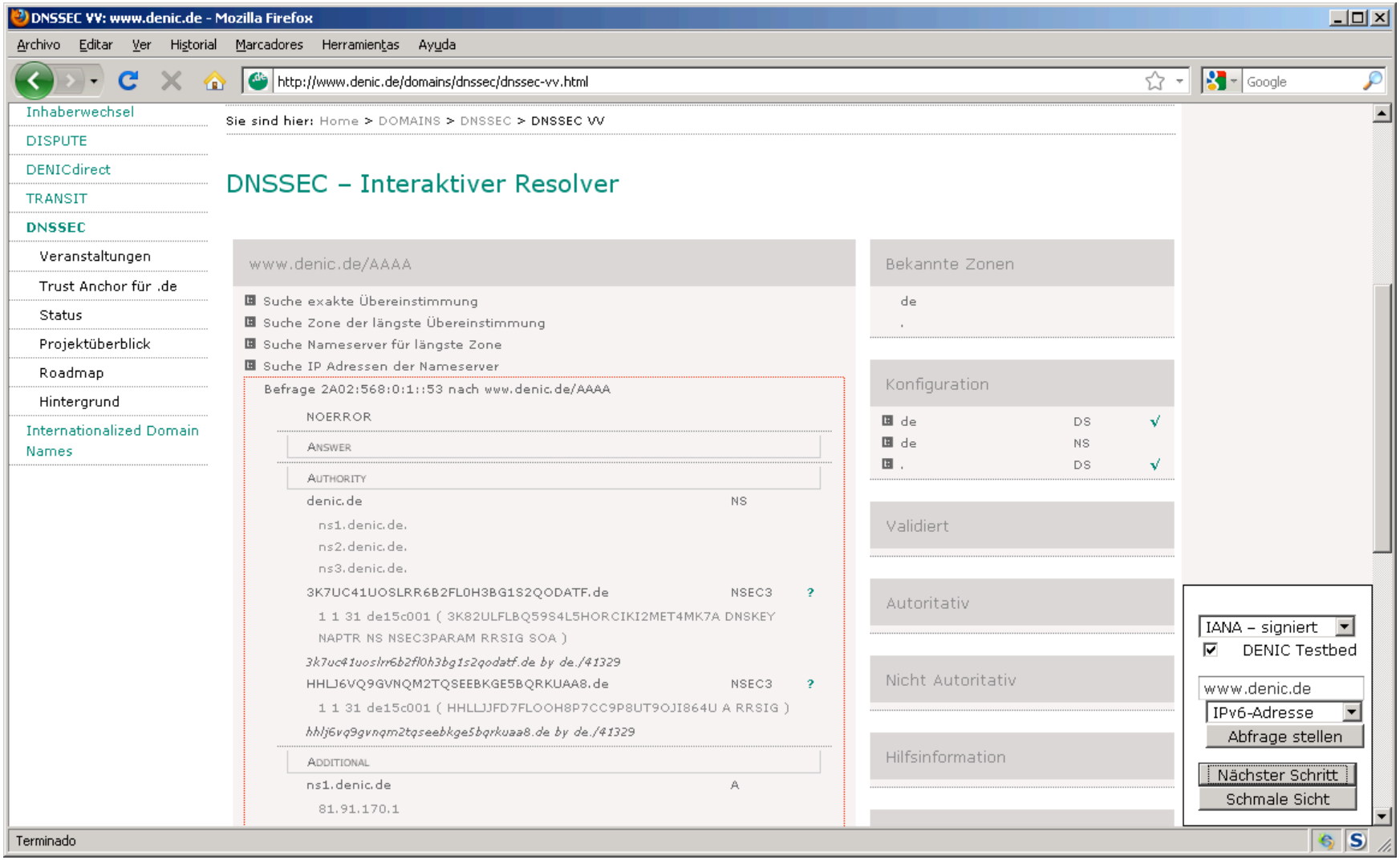
Prüfung ausführen

BIND-Konfiguration: neu, mit Patch

```
zone de {
    type static-stub;
    server-addresses {87.233.175.25; 81.91.161.228;};
    // server-names {};
};
```

- Neuer Zonentyp `static-stub`
- Fragen nicht mehr „rekursiv“
- Feature verfügbar als Patch gegen BIND 9.7.2-P3
- **Integration in BIND ab Version 9.8.0**
- **Auch für „split DNS“-Konfigurationen interessant**

Visualisierung der Validierung



Kommunikation

- Fünf Meetings
  - 250 Teilnehmer, 26 Vortragende
  - 2 Hintergrundvorträge für Neueinsteiger
  - Produktübersicht (November 2010)
- Beiträge extern
  - VoIP Germany, 2009
  - RIPE-60, 2010
  - DomainPulse, 2011
- Diverse Medienanfragen
- Projektwebseite

Weitere Ergebnisse: „Eigenbedarf“

- Betrieb eines validierenden Resolvers
- Test aller unserer Systemkomponenten auf Stabilität und Massenbetrieb
- Neue, DNSSEC-relevante interne Abläufe eingeführt und geübt

Fazit

- Technik beherrschbar
  - Tücken im Detail
- Prozesse sind der kritische Part
  - aber zu meistern
- Teilnahme recht zurückhaltend
  - aber engagiert

?

Vielen Dank!

<http://www.denic.de/dnssec>