# Testbed: DNSSEC für DE

## - Kurz vor dem Halbzeitpfiff -

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

Frankfurt/Main, 16. Juni 2010

# DNSSEC-Testbed: Roadmap

- Testbed Phase 0 -- DNS 1.12.2009
  - Betrieb des Setups mit unsignierter DE-Zone
- Testbed Phase 1 -- DNSSEC 5.1.2010
  - Betrieb mit signierter DE-Zone
- Testbed Phase 2 -- DNSSEC + Schlüssel 2.3.2010
  - Betrieb mit signierter DE-Zone und DS-Records
    - Übergabe/Provisionierung von Schlüsselmaterial (DNSKEY)
- Entscheidung über Produktion nach dem Testbed

# Rahmenbedingungen

- Separate Infrastruktur
  - 2 Standorte Europa („gute“ RTTs)
  - 1 Standort „remote“ (HK, bandwidth*delay)
- NSEC3 (BIND 9.7 (9.6), Unbound 1.4.4, Vantio)
- Zonenaktualisierungen
  - Derzeit **zweimal täglich**
  - Kontinuierliche Frequenzerhöhung (über status quo hinaus)
- Original-Delegationsdaten

# Provisionierung von Schlüsselmaterial

- … erfolgt durch Registrare (DENIC-Mitglieder)
- Hinterlegung von DNSKEY-RRs in der Produktionsdatenbank
  - MRI und RRI werden unterstützt
  - Dto. RRI-Webclient
- Unmittelbare Sichtbarkeit für alle
  - … an den Registrierungsschnittstellen
    - kann gezielt „überlesen“ werden
  - … in den Auskunftsdiensten („whois“, Domainabfrage)
  - … DS-RRs im DNS: nur im Testbed!

# DNSKEY-Registrierung: Prüfungen

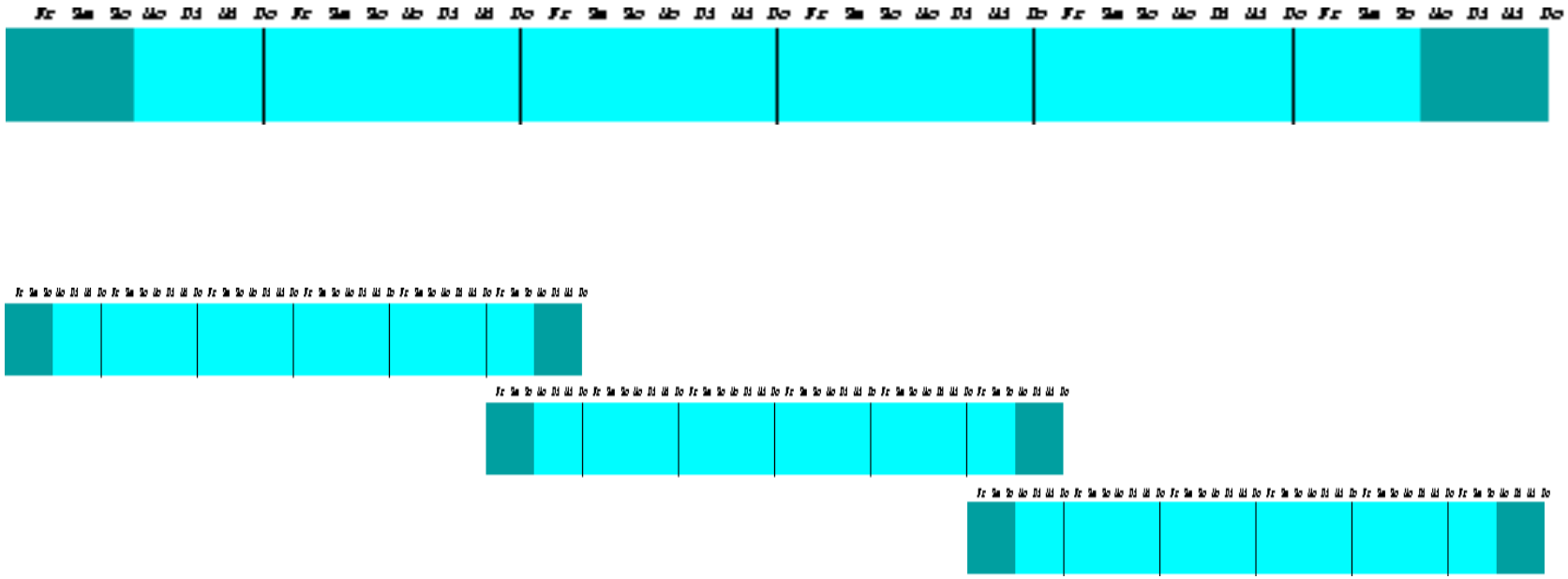
- SEP-Bit erwünscht, aber nicht erzwungen
- REVOKE-Bit nicht gesetzt
- Bei IANA registrierte, nicht-private Algorithmen
  - Derzeit RSA, DSA, demnächst evtl GOST
- Schlüsselparameter innerhalb der Spezifikationen
  - Z.B.: RSA-Modulus 512 - 4096 bit
- SOA-RR muß mit mindestens einem *Trust Anchor* validieren
  - Dadurch auch Vorabregistrierung nicht sichtbarer TAs möglich

# DNSSEC - Schlüssellaufzeiten

- Dokumentation der KSK- und ZSK-Daten
- KSK:
  - 2048 bit RSA/SHA256
  - 3 Wochen Gültigkeit der RRSIGnatur
  - Unterschrift über das DNSKEY-RRSet jeweils donnerstags
- ZSK:
  - 1024 bit RSA/SHA256
  - 1 Woche Gültigkeit der RRSIGnatur
    - Neusignierung jeder Zonenversion
  - Unterschrift über alle RRSets
    - Außer DNSKEY-RRSet

# DNSSEC - ZSK-Rollover

- ZSK-Rollover alle fünf Wochen, eine Woche Überlappung
- *Pre-Publish* nach RFC 4641



# Eine Beispieldomain

```
; <<>> DiG 9.6.1-P1 <<>> +norec +dnssec @81.91.161.228 example.dnsop.de.
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28134
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.dnsop.de.          IN     A

;; AUTHORITY SECTION:
dnsop.de.           86400   IN     NS     fra.dnsop.de.
dnsop.de.           86400   IN     NS     ns.ogud.com.
dnsop.de.           86400   IN     DS     2467 8 2 6593B7C779085BAF810501D16A381BC50B20E0D697EDD1464848CFDD
0172EF54
dnsop.de.           86400   IN     RRSIG  DS 8 2 86400 20100513040000 20100506040000 44820 de.
lrB5bzUTrOY8GwzXeNluXU74AUWcJs7fWea5j+ySQoFhyKDGhED8nbvn
TgN2ekP5ajKICkQ6ru4iw1clXpHm+rggDKoPKsithM/MpFN9Co64TcQT
sLbA/rxGad8k/XLtZGdIeAtjlZj94JRtnvOFzmjdYSQdAlpnmdK0Se4U MJc=

;; ADDITIONAL SECTION:
fra.dnsop.de.       86400   IN     A      81.91.161.78

;; Query time: 75 msec
;; SERVER: 81.91.161.228#53(81.91.161.228)
;; MSG SIZE  rcvd: 314
```

# Eine Beispieldomain (whois-Ausgabe)

Domain: dnsop.de

Domain-Ace: dnsop.de

Nserver: fra.dnsop.de 81.91.161.78

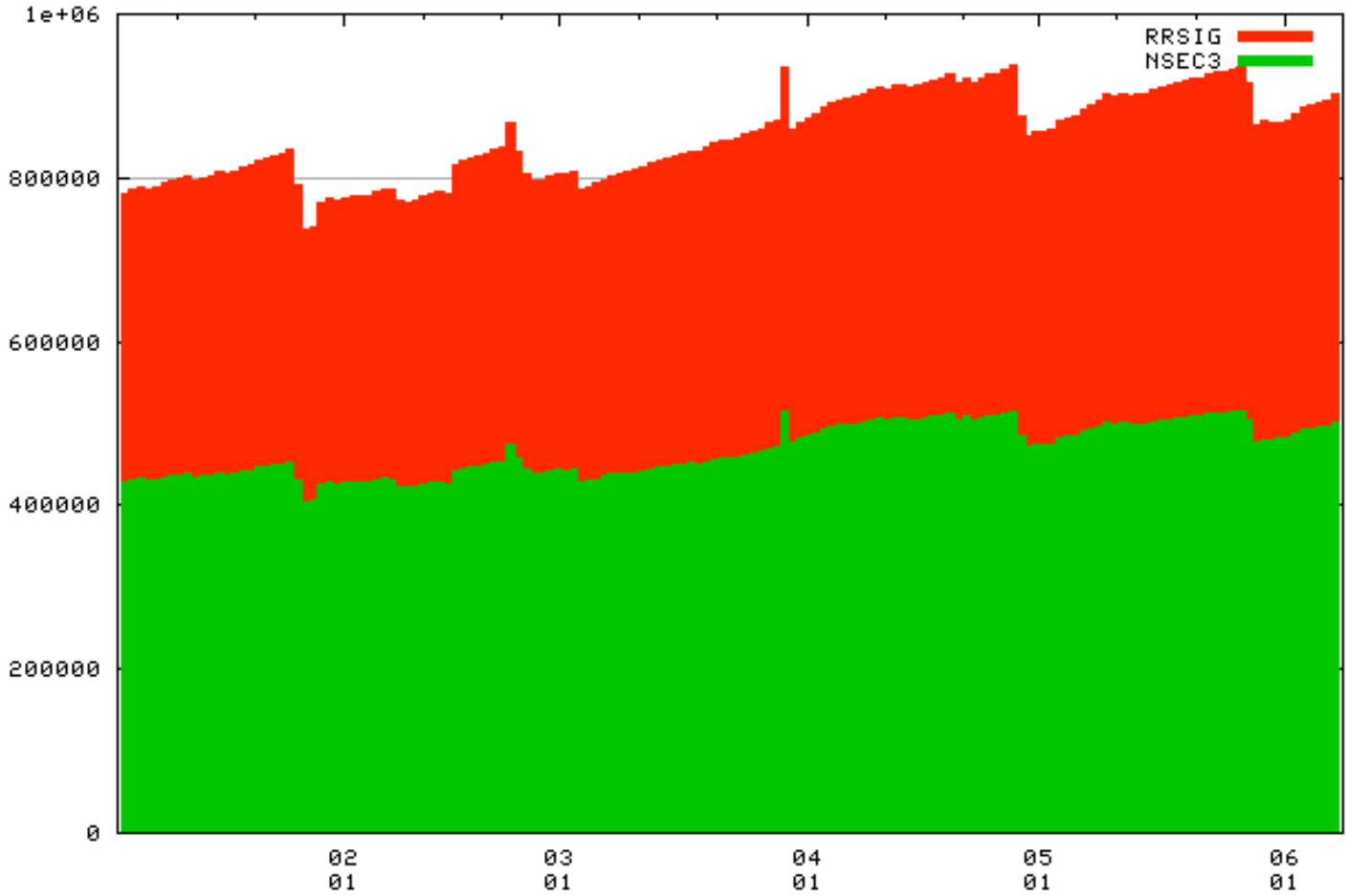
Nserver: ns.ogud.com

**Dnskey: 257 3 8**
**AwEAAaV35xrg5IQBIAF9ppsxPcCveCITErRDV5UelO7PeLTgywnJyRP**
**wrAq7tCsSRBY0rCLN7WguX/X+9rfRBz3I24RbYgoGRjpc3JJlpO3C4t**
**LdekdLJE62zgvoM2FPp4ujte7CWDPXpe8xN51XXFTUl4586Iej1iyaIrJ**
**9XeLn4tSc2GJOd6tsZjk7+VZwbQzsTRk2vO5MJhbQYFno2IXuadCfHo**
**8P53UEKiyPSKTsVCQ1Khxvgy/lL1FEzi2wFKZ52fhaiVyKs4DTfDhb/3**
**Sxv5dVlF7HVKDxrNUHKV/rg16lE1AxZ21EP5zgvOAyh+n7N0BwO70**
**TGEVgVhhKC9giU+U=**

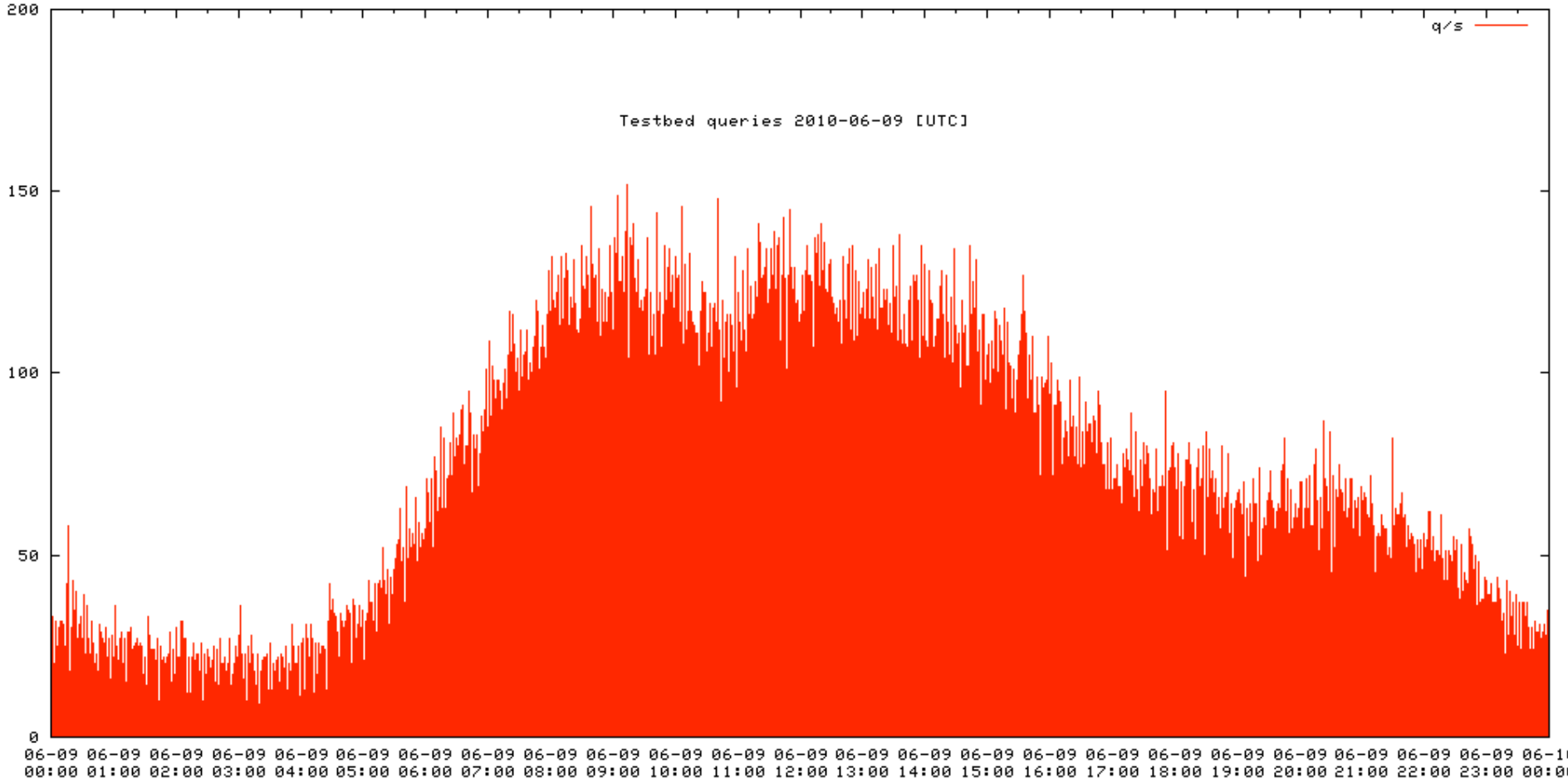
Status: connect

Changed: 2010-03-03T08:16:36+01:00

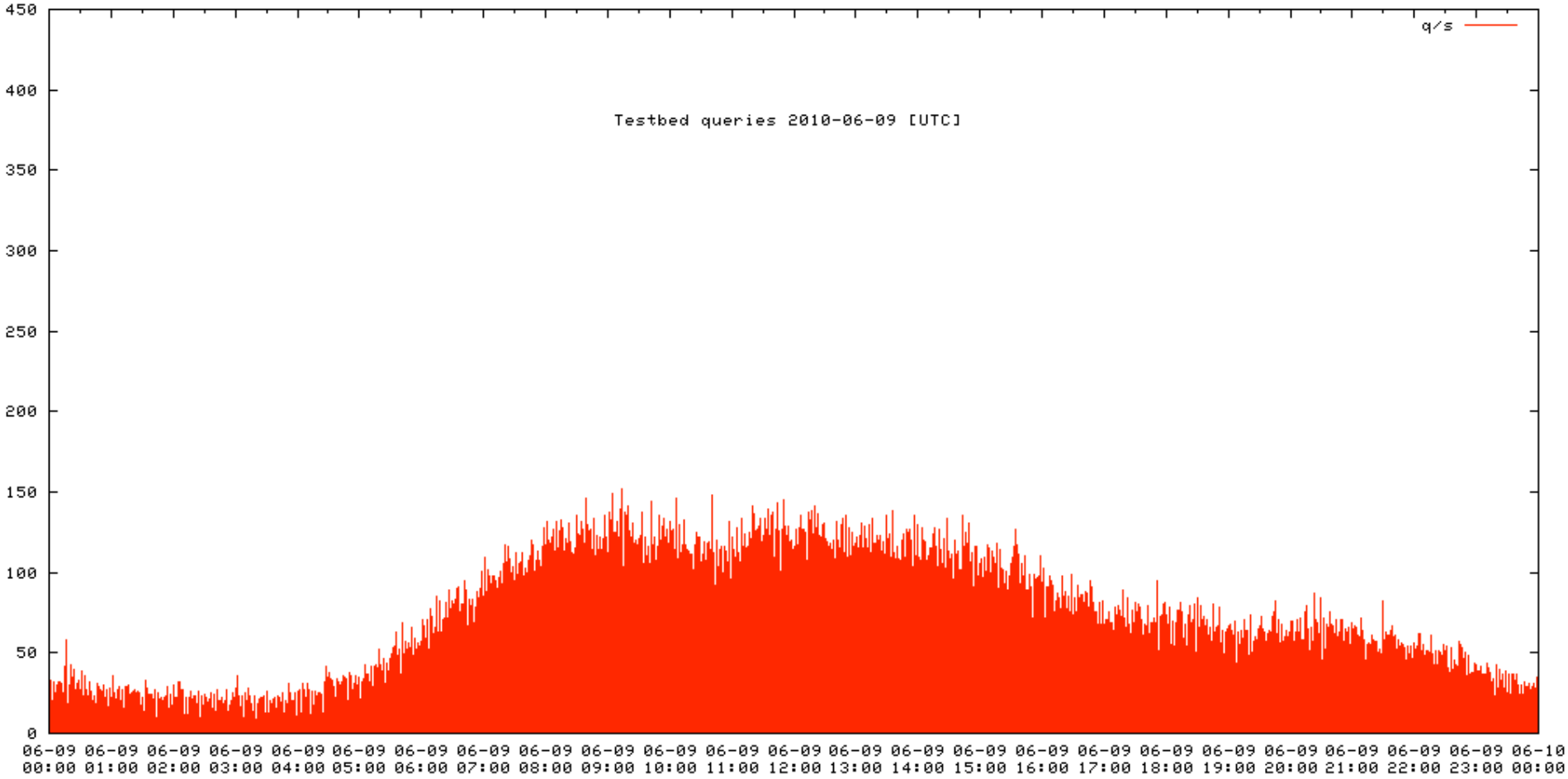
# Anzahl NSEC3/RRSIG-RRs



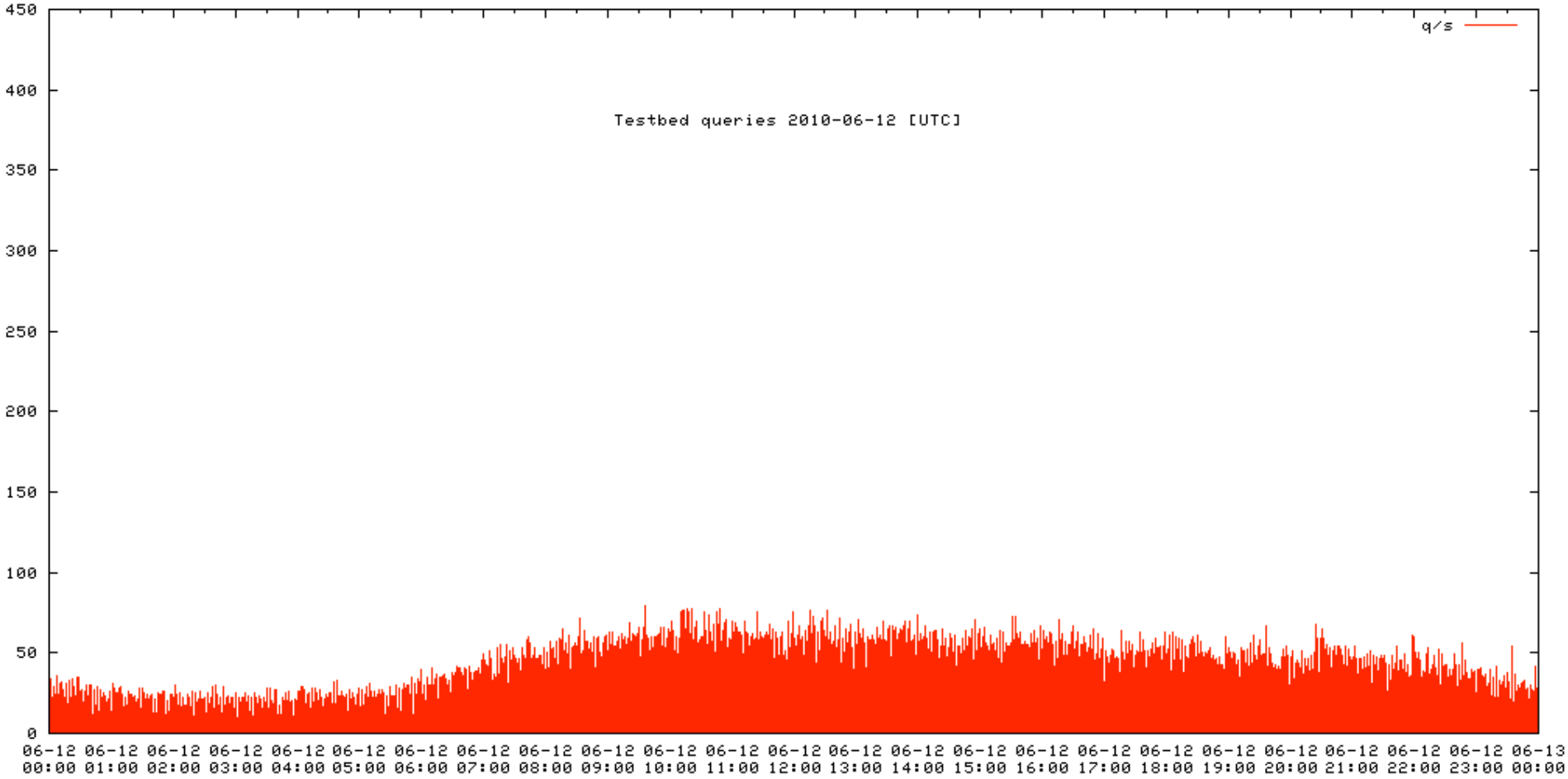
# Querys an einem Mittwoch



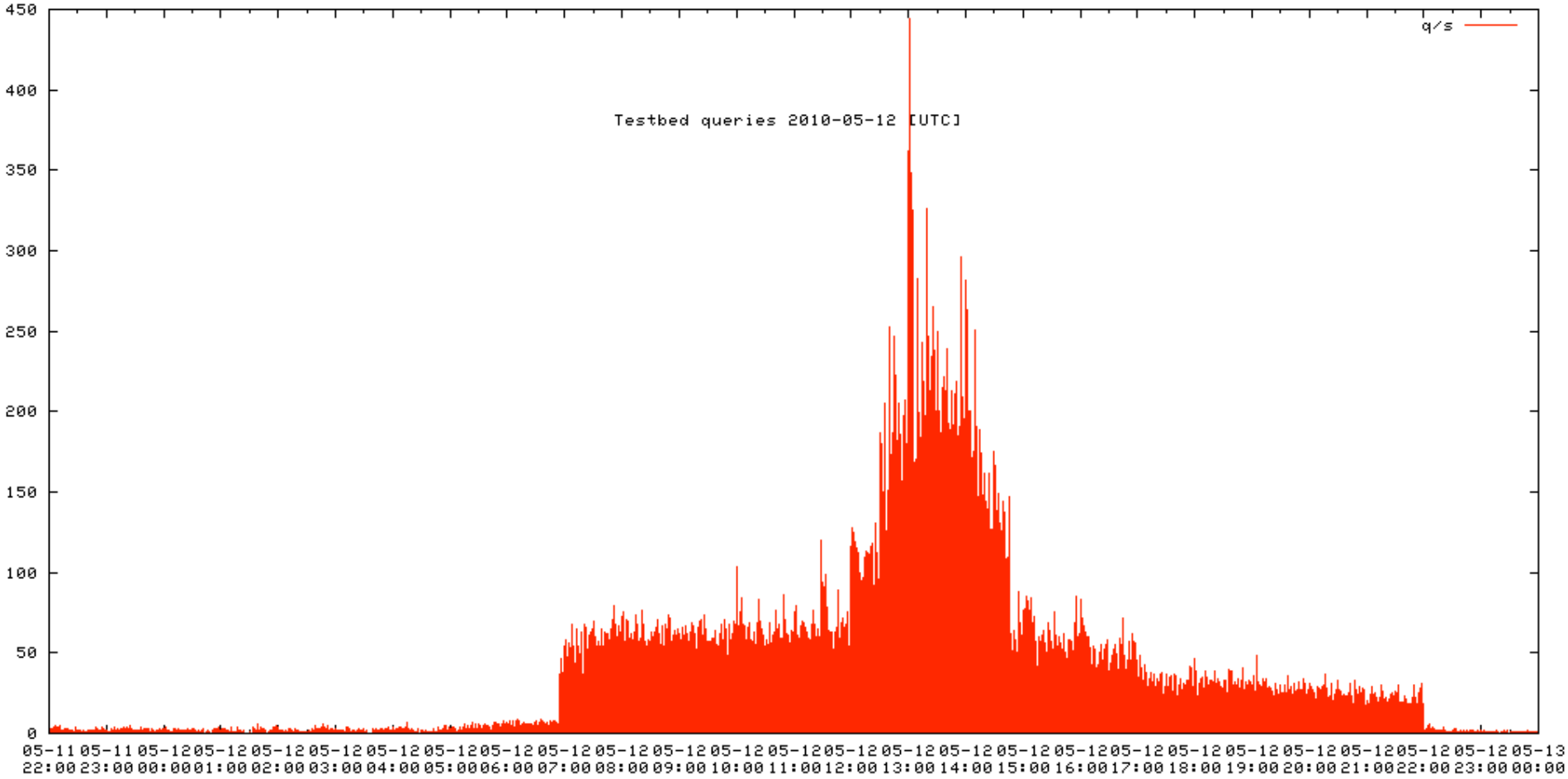
# Querys an einem Mittwoch (skaliert)



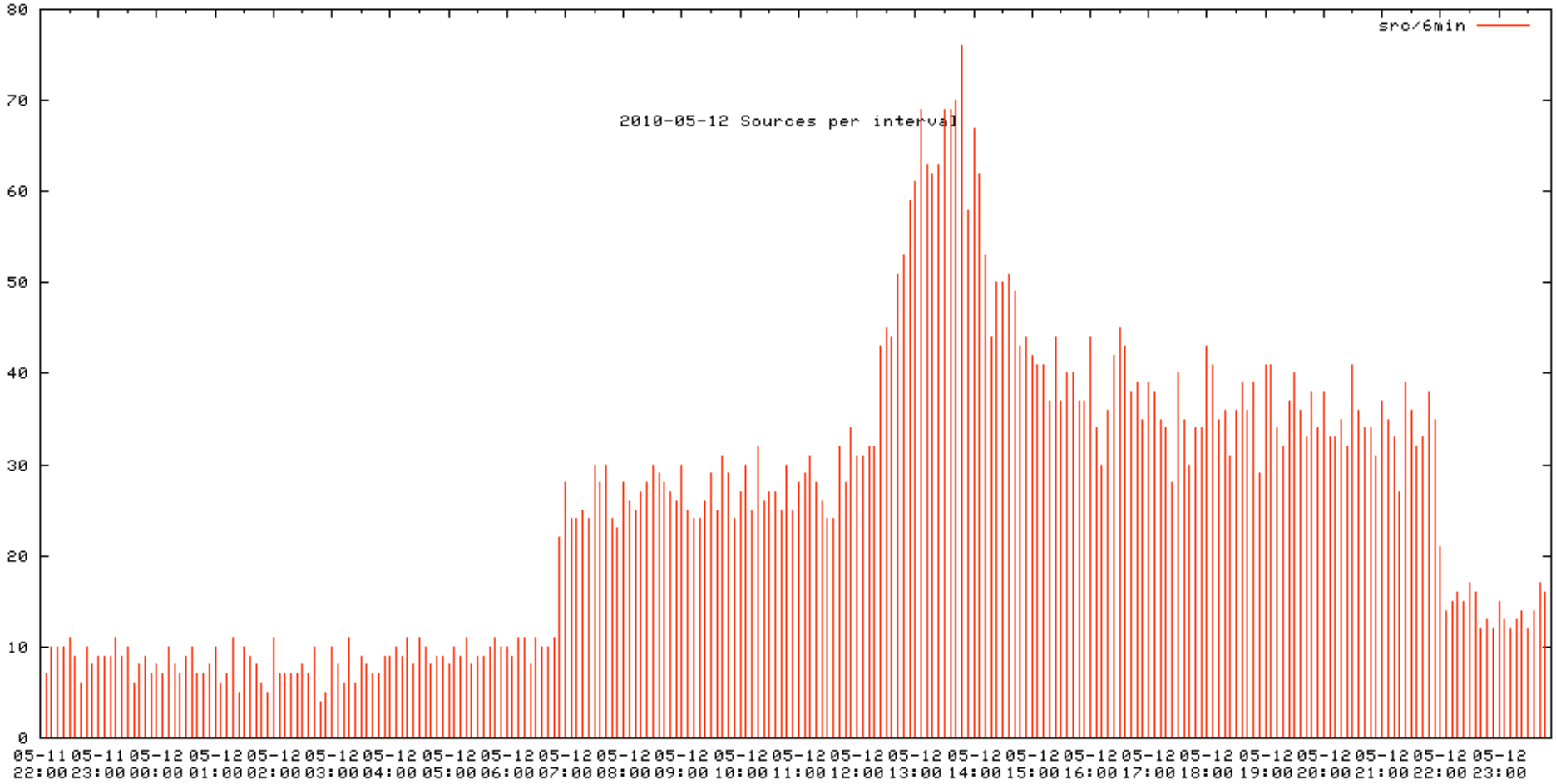
# Querys an einem Wochenende



# Querys einen Monat zuvor



# Anzahl „Teilnehmer“ am 12. Mai



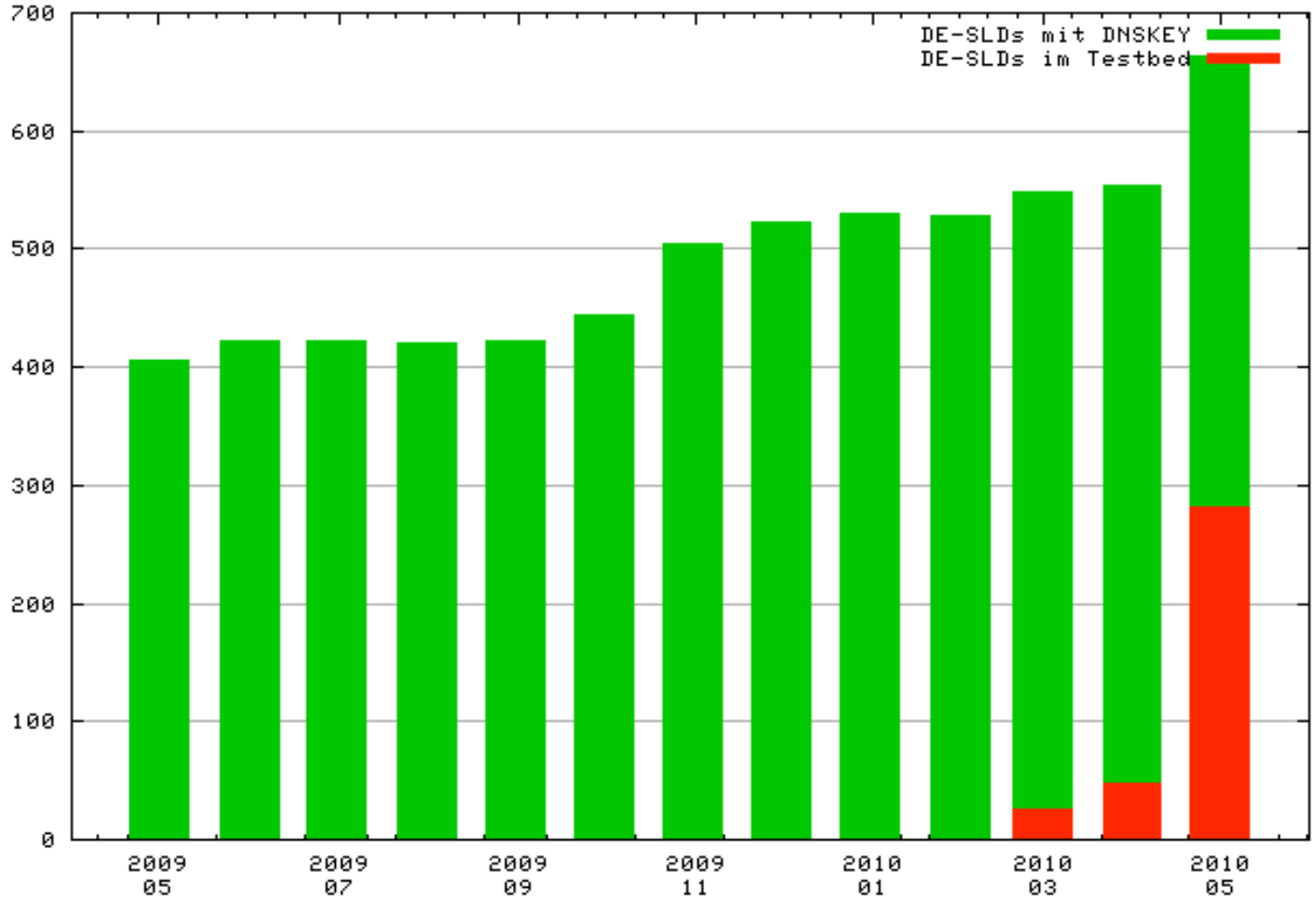
# DNSSEC-Testbed - Zahlen und Beobachtungen

- 200 q/s in FRA, 130 q/s in AMS pro Standort in der Spitze
- Ca. 500-600 Anfrager seit Beginn (100 täglich)
- ca. 280 DS-RRs im Testbed
  - RSA/SHA-1 „beliebteste“ Algorithmenkombination
- `bund.de` signiert
- Bug in Unbound entdeckt
  - Zu intelligente Fehlererkennung vor 1.4.4
  - Schnell behoben, Dank an NLnetLabs

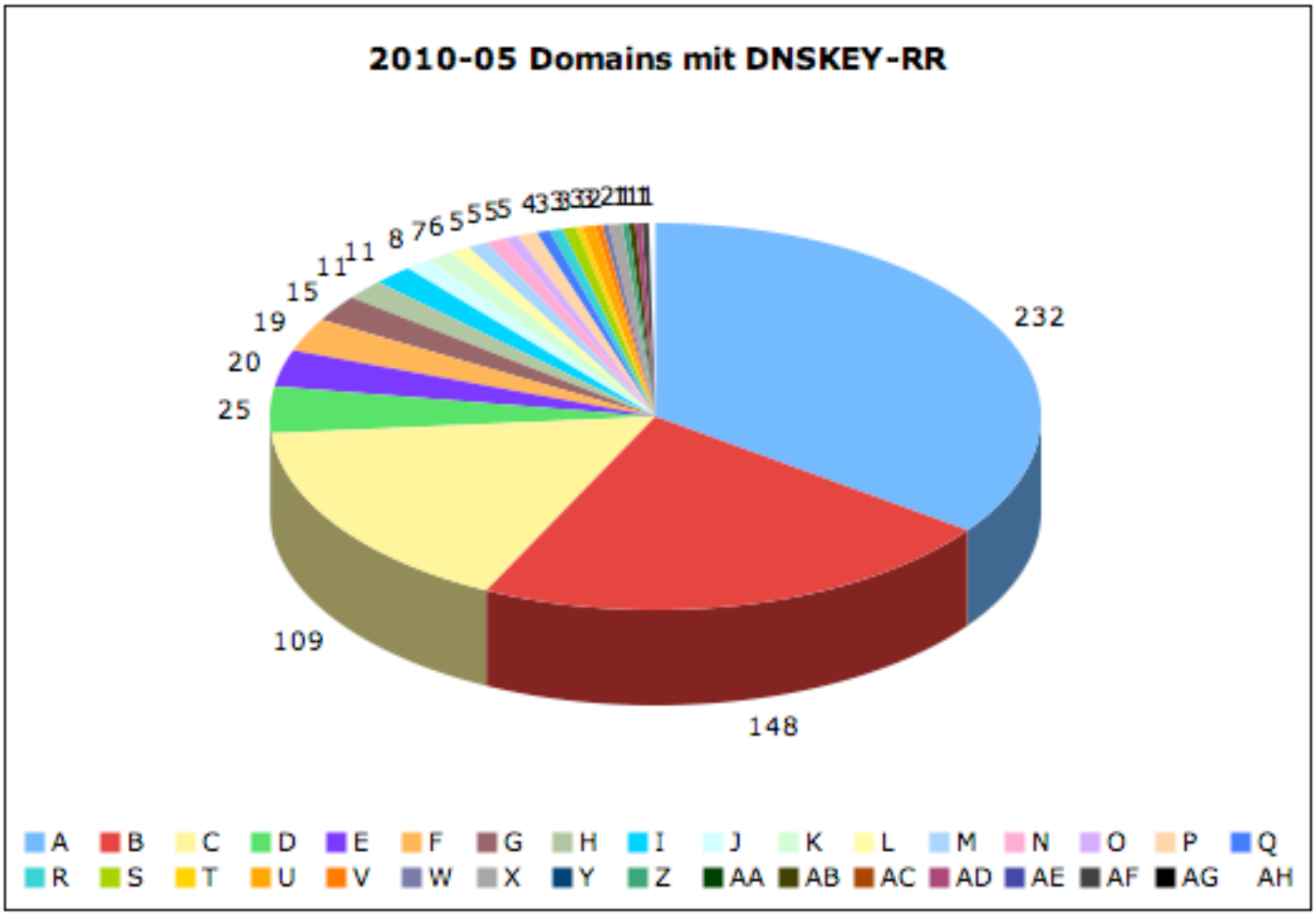
# DNSSEC-Testbed - Ausfall am 9.5.2010

- 3 von 4 autoritativen Servern „abgestürzt“
- SW-Problem in BIND9.7 rc
  - IXFR-Code, NSEC3 und laufende Querys
  - Behoben durch Upgrade auf 9.7-P1
- Redundanz bei der Lastverteilung unzureichend
  - Besser, aber wir arbeiten weiter daran
- Monitoring unzureichend
  - Fixed

# Entwicklung DNSKEY unter DE (Ende 05/2010)



# „Betroffene“ Registrare im Mai …



# BIND-Konfiguration

- Umlenkung
- aber „rekursiv“
- und unübersichtlich
  - bogus
- Lösung: neues BIND-Feature
- Unbound und Vantio stehen Pate

```
zone "de" {
        type forward;
        // Die Reihenfolge der beiden Adressen kann beliebig gewaehlt
        // werden
        forwarders {
                81.91.161.228;  // auth-fra.dnssec.denic.de
                87.233.175.25;  // auth-ams.dnssec.denic.de
                // IPv6 nur bei geeigneter Konnektivität aktivieren
                // 2A02:568:0:1::53;    // auth-fra.dnssec.denic.de
        };
        forward first;
};

// WICHTIG: Diese Liste muss regelmaessig gepflegt werden und
//          darf nur im Zusammenhang mit der Testbed-Infrastruktur
//          eingesetzt werden!
//          Die Markierung als "bogus" verhindert, dass die offiziellen
//          Nameserver gefragt werden.
server 194.0.0.53       { bogus yes; }; // a.nic.de
server 81.91.164.5      { bogus yes; }; // f.nic.de
server 77.67.63.105     { bogus yes; }; // l.de.net
server 195.243.137.26   { bogus yes; }; // s.de.net
server 194.246.96.1     { bogus yes; }; // z.nic.de

server 2001:678:2::53   { bogus yes; }; // a.nic.de
server 2001:608:6:6::10 { bogus yes; }; // f.nic.de
server 2001:668:1f:11::105      { bogus yes; }; // l.de.net
```

# Signierwerkzeug

- VeriSign jDNSSEC Tools
  - `http ://www.verisignlabs.com/dnssec-tools/`
  - DENIC-Erweiterungen für PKCS#11
    - Fließen in das Open-Source-Projekt ein
- dnsjava
  - `http ://www.dnsjava.org/`

# Nächste Schritte

- Inkrementelle Signierung und Verteilung
  - DB-basiert, Konzept- und Designphase
  - Interaktion mit anderen Projekten
- Testplan (nur Ideensammlung)
  - NSEC3-Rollover
  - ggf. KSK-Rollover
  - „Operator"-Wechsel
  - Last-Tests (auch Schlüsselwechsel)
- Erfahrungsbericht für etwaigen Produktionsgang

?

# Vielen Dank!

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