Das DNSSEC-Testbed

- 21 Tage und ein bißchen weiser -

Peter Koch, Marcos Sanz

Frankfurt, 26. Januar 2010

Agenda

- **DNSSEC-Testbed - Überblick und Infrastruktur**
- **Krypto- und andere Parameter**
- **Erste Zahlen**
- **Nächste Schritte**
- **Zusammenfassung und Diskussion**

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

DNSSEC-Testbed: Zielsetzung und Gesamtsicht

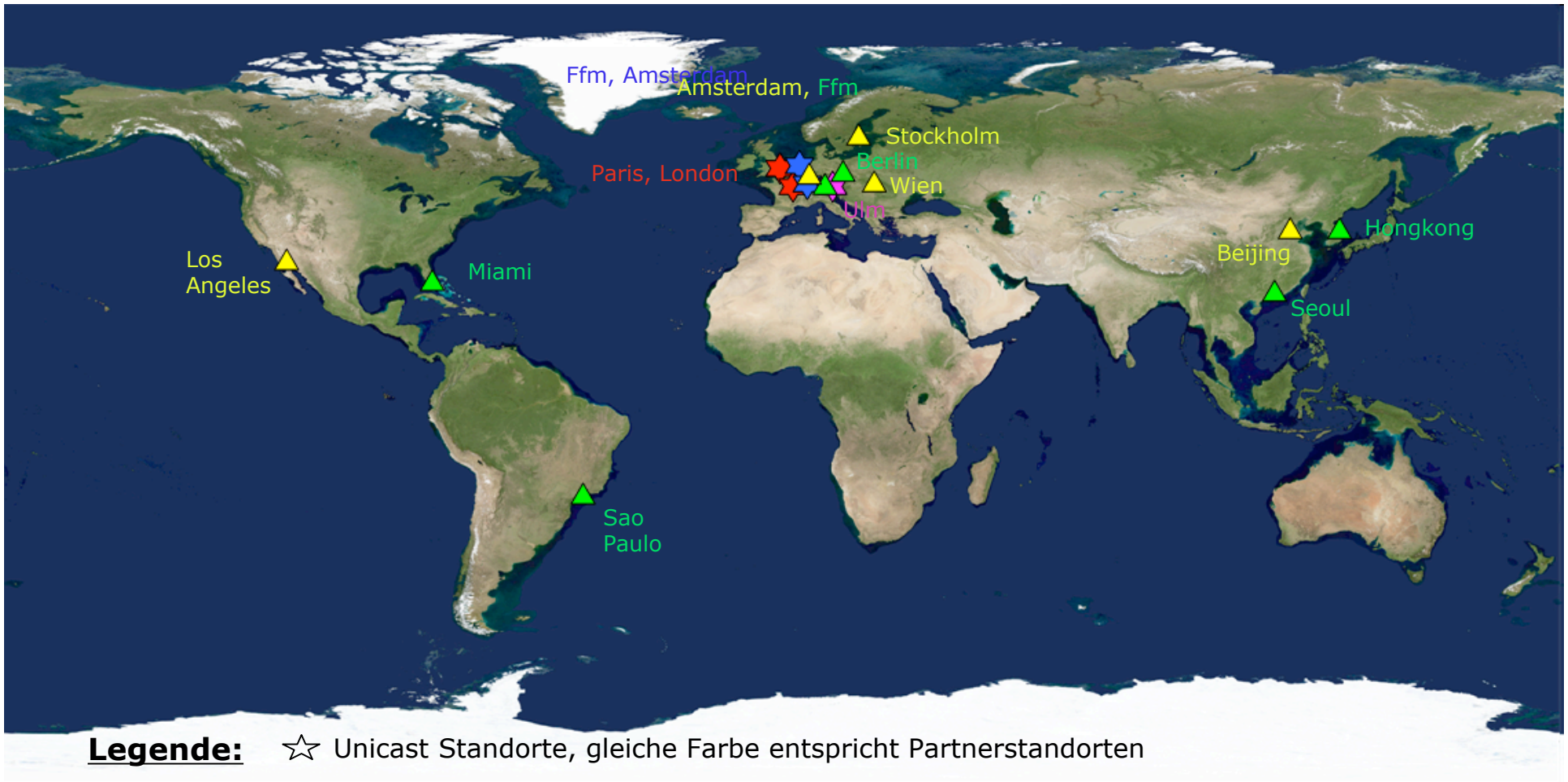
- Erprobung von DNSSEC unter realistischen Einsatzbedingungen
- Ermittlung der technischen und operativen Reife
  - Protokoll an sich ist stabil
  - Operative Details sind aber z.T. offen
- Test der Akzeptanz im Markt
- Prüfung technischer Hürden
  - Siehe Vortrag zu Heimroutern und DNSSEC
  - Kritische Verkehrsmuster

DNSSEC-Testbed: Teilnahme

Wer kann am Testbed teilnehmen?

- Registrar
- Domaininhaber
- DNS-Operator (autoritativ)
- Resolver-Operator
- (Endnutzer)

DENIC eG - NSL-Standorte 2010 (**IPv4**)



Legende: ☆ Unicast Standorte, gleiche Farbe entspricht Partnerstandorten

△ Anycast Standorte, gleiche Farbe indiziert gleiche Wolke a.nic (grün) bzw. z.nic (gelb)

16 Standorte, 10 Exchanges

DNSSEC-Testbed: Infrastruktur

- eigenständige Infrastruktur zur Beantwortung von DNS-Querys
  - Amsterdam
    - `auth-ams.dnssec.denic.de`
    - 87.233.175.25
  - Frankfurt
    - `auth-fra.dnssec.denic.de`
    - 81.91.161.228
    - `2A02:568:0:1::53`
  - Hongkong
    - derzeit nur intern

DNSSEC - Schlüssel zu DE

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10671
;; flags: qr aa; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
de.                     86400   IN      DNSKEY  256 3 8 (
                                                AwEAAZKVktO3zdcHBsjdEGtn0NjXF2z6Owc5RSUXxaqY/wMW8gFUM1GG
                                                4hZOmZmRucT/mG4C6nxqOzg7zlCYrqGcsi0iWor2qXtfptWPqS2EKXwE
                                                XgW3rt1T9JcECLjJ8a9wYCSqYV595HdmWmtf0JQbmirOAOY9XiWAiyjU
                                                YDU0oTKn ) ;{id = 3754 (zsk), size = 1024b}
de.                     86400   IN      DNSKEY  257 3 8 (
                                                AwEAAZ1FqQED8QBrk3Jk4q96lggh4uiwlbdbZ0posfIgcaJJqfTNBfEh
                                                n6PEPqqRP73libD55vujfYzKMN0fVd34wrdOpSTpMbw+oqQpJyecfGVY
                                                H1fnqws23n5QE03/7SN98O8Cm+HBpB66JurTHWD3f4es8IUoumb/SXY4
                                                4qb+oqWfmM3wS8aQVA5d2gHpKrRIPlDHA/MB3FHGL64VpfV8KJ76kp1R
                                                BthR7Y0qalTskOouVeCOEa7gUiIljt1kTf64HFGsRi11klpCHBjtTiTg
                                                7MFN25nASuhbyTmWlRxPyg79BK7EDQ+tAe09NYkS1P7tOe8ola9IpQHT
                                                WO6ttTmSnyE= ) ;{id = 63505 (ksk), size = 2048b}
de.                     86400   IN      RRSIG   DNSKEY 8 1 86400 20100211120000 20100121120000 63505 de. (
                                                ZQ0egBXXcfysWhOc6EmlptekmlSIWf4kb+eCzaiY9s4IXmeB2zGAFon7
                                                9mYgVVikKdzdBHVSkDwPnSvnYBgqgpuFbDyHrvjDgdhD6E7glXYQ3RGO
                                                n6RcbqxqKTZMYbSpZxhLV11rt7UXPkyJG566U6CKf5rVvlw7edPfuQyf
                                                yfL2+PwaMSvB3Hx18KUkyuZ+9yMARRzSsN9dqsRSp+K25ZFVs2rZGUxn
                                                fHQbnoc8Tvf61dOdrGEmNSZK/9oKEdoUjfeHDL5hVX0jsVlIn/KtbWCE
                                                JU7VprewB4CbI7rq5CRjgLdOnoR/6R0mqiMAvLLwQOZlRyhi5Ril7HkK
                                                h0ZYSg== )
;; SERVER: 81.91.161.228#53(81.91.161.228)
;; MSG SIZE  rcvd: 745
```

DNSSEC - Schlüssel zu DE (lesbare Variante)

- Key Signing Key (KSK) / Trust Anchor
  - 2048 bit RSA/SHA256 (RFC5702)
  - Rollover: *Double Signature,* noch kein Termin
  - Signaturgültigkeit: 3 Wochen
- Zone Signing Key (ZSK)
  - 1024 bit RSA/SHA256
  - Rollover: *Pre-Publish*, alle fünf Wochen, 3.5 Tage Vor- und Nachlauf
  - Signaturgültigkeit: 1 Woche
  - Keine Signatur über DNSKEY-RRSet

DNSSEC - NSEC3

```
;; QUESTION SECTION:
;de.                            IN      TXT

;; AUTHORITY SECTION:
de.                     7200    IN      SOA     f.nic.de. its.denic.de. 2010012561 7200 7200 3600000 7200
de.                     7200    IN      RRSIG   SOA 8 1 86400 20100201130000 20100125130000 3754 de. (
                                                hUG9HSSI/mbV33dxUmG6q1//aLbNcgslc7ad6nc4cavRoXFR8lpaRnpw
                                                J5kK2bTw2WBZWuLQ0UoMn8HDNSYG41j6N1Kk5kBuVwdwO7ejrOzaYyt+
                                                W486MFvGWwC5nk/uJrf9HnPWRMMAnzCpjdawu0dtglSciMCRqlSNbUB3
                                                w9I= )

3K7UC41UOSLRR6B2FL0H3BG1S2QODATF.de. 7200 IN NSEC3 1 1 31 DE15C001 3K7VC4P10IIJQR0RMBQ2F407077B6JDH (
                                                 NS SOA NAPTR RRSIG DNSKEY NSEC3PARAM )

3K7UC41UOSLRR6B2FL0H3BG1S2QODATF.de. 7200 IN RRSIG NSEC3 8 2 7200 20100201130000 20100125130000 3754 de. (
                                                JmyoN/A/oZ5wh6NLsoc19rm9MFxYxkshzqV3/XKVA5mMSAnyatOMZ/av
                                                NkbF3om5ZDyKYJVwG9T2f0CmLWyZFY9zbrxmRt+uRmRkIGwgNSoRKiWD
                                                KDwa5iHise5vHzkkqz5h3UfBiWoe716/WF239wE83m3jt1JQxDhLFuj0
                                                7xE= )
```

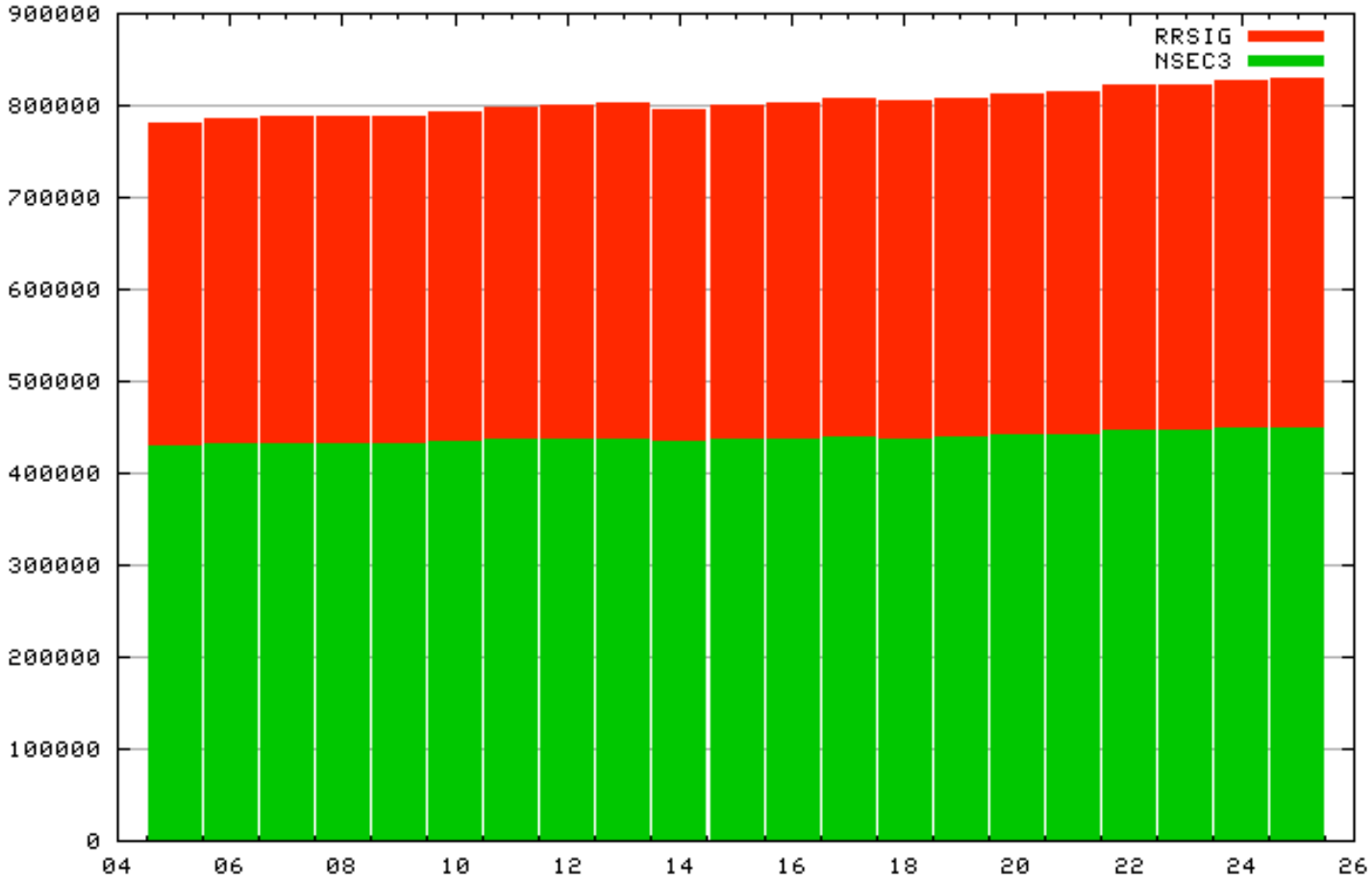
DNSSEC - NSEC3 (auch hier: lesbare Variante)

- NSEC3 mit Opt-Out
  - Wirkt *Zone Walking* entgegen
    - Mit Salt (wird gelegentlich gewechselt)
    - Mehrere Hash-Iterationen
  - Begrenzt das Zonenwachstum
    - NSEC3 nur bei autoritativen Daten

Eigenschaften der DE-Zone

- Mehr als 13 Millionen Domains
  - Überwiegend Delegationen
  - Wenige 100.000 Domains autoritativ in der Zone
    - Davon etliche mit *Empty Non Terminals*
    - NSEC3 an autoritativen Daten und ENTs
    - ==> ca.800.000 Signaturen

DNSSEC - RRSIG- und NSEC3-RRs



Ablauf Signierung

- 1:1-Kopie der DE-Zone
  - Derzeit einmal täglich
- Signierung mit ZSK
  - HW-Unterstützung mit SCA6000
    - HSM, FIPS 140-2 Level3, PKCS#11
    - Beschleunigung!
  - Doppelt redundante Auslegung (2*FRA, *2*AMS*)
  - Java-basiertes Signierwerkzeug mit eigenen Erweiterungen
- KSK-Signaturen vorproduziert
  - Ebenfalls SCA6000-basiert

DNSSEC - erste Zahlen

- Zonendatei
  - 1.0 GB -> 1.3 GB (*wire format*: 0.8 GB -> 1.0 GB)
  - Kompression nur noch ca. 50% (wegen `NSEC3/RRSIG`)
  - Ein Inkrement: ca. 0.3 GB
- Memory-Footprint
  - 8GB (BIND 9.7)
- Querys
  - Noch keine sinnvollen Aussagen möglich, < 10 q/s pro Standort
  - Ca. 500 Anfrager

DNSSEC - nächste Schritte

- Provisionierung von Schlüsselmaterial (ab 2.3.2010)
  - … erfolgt durch Registrare (DENIC-Mitglieder)
  - Hinterlegung von `DNSKEY`-RRs in der Produktionsdatenbank
    - MRI und RRI werden unterstützt
  - Unmittelbare Sichtbarkeit für alle
    - … an den Registrierungsschnittstellen
      - kann gezielt „überlesen“ werden
    - … in den Auskunftsdiensten („whois“)
    - … `DS`-RRs im DNS: nur im Testbed!
  - Start in Produktion und Mitgliedertestumgebung

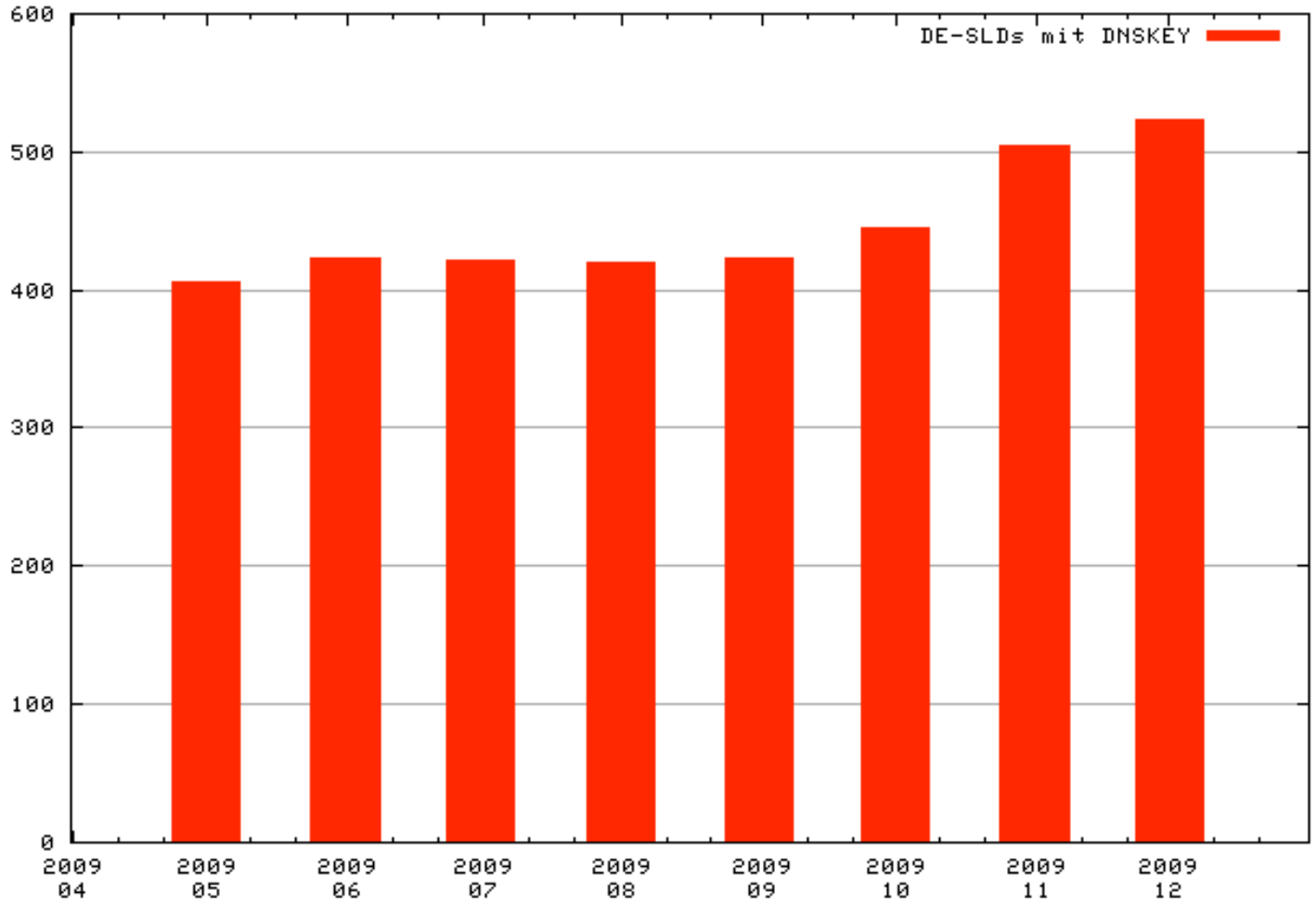
DNSSEC - nächste Schritte: DNSKEY-Registrierung

- Tests der übermittelten DNSKEY-Daten **[Stand der Diskussion]**
  - SEP-Bit erwünscht, aber nicht erzwungen
  - 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
  - Sind *Trust Anchor* mit gesetztem REVOKE-Bit sinnvoll?

DNSSEC - nächste Schritte

- Aufstellung eines detaillierten Testplans
  - Daten-Surveys, Signaturabläufe etc.
  - KSK-Rollover
  - Provider+Operatorwechsel
  - NSEC3-Rollover
- Umstellung auf datenbankbasierte Zonensignierung
  - Kleinere Schritte, IXFR, analog neuer Infrastruktur
  - Voraussichtlich zur Jahresmitte

Second Level Domains mit DNSKEY-RRs



Zusammenfassung

- Testbed-Phase 1 planmäßig aktiv
  - Signierte DE-Zone
  - noch sehr wenige aussagekräftigen Daten
- DNSKEY-Provisionierung ab 2.3.
  - In der Produktionsdatenbank
- Weiterentwicklung des Testplans
  - Provider/Operatorwechsel
- Nächstes DNSSEC-Testbed-Meeting: 16. Juni 2010

?

Vielen Dank!

Peter Koch, Marcos Sanz
DENIC eG

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