The .de DNSSEC testbed

- notes from about half the way -

Peter Koch <koch@denic.de>

Praha, 06 May 2010

.de DNSSEC testbed: headlines

More than 250,000 domains secured by DNSSEC!

.de DNSSEC testbed: roadmap

- Stage 0 -- DNS **2009-12-01**
  - Unsigned DE zone published on dedicated infrastructure
- Stage 1 -- DNSSEC **2010-01-05**
  - Signed DE zone published on dedicated infrastructure
- Stage 2 -- DNSSEC + DS/DNSKEY **2010-03-02**
  - Signed DE zone contains DS-RRs
    - DNSKEY is subject of registration
- Testbed scheduled to last until *2010-12-31*

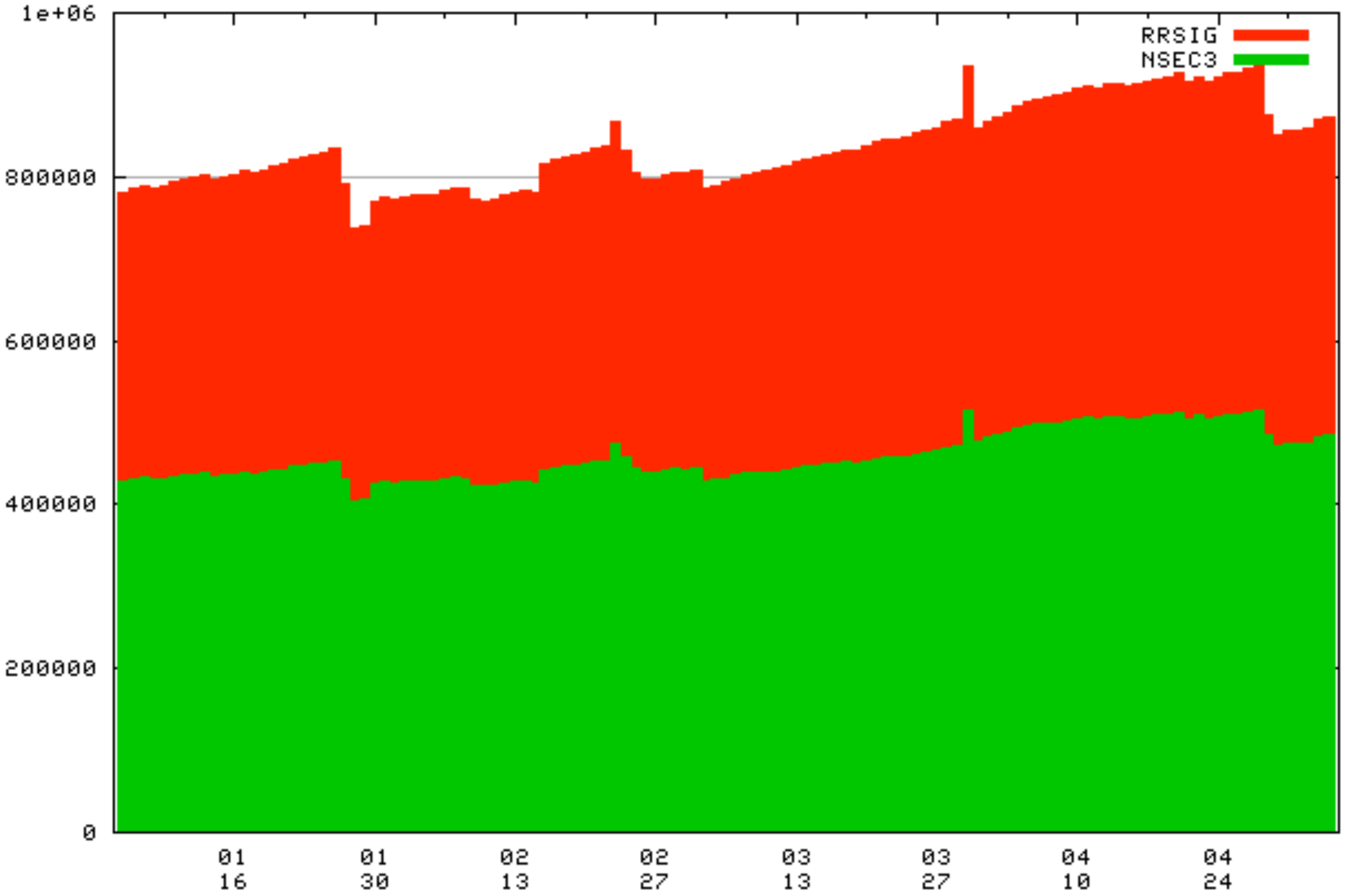
.de DNSSEC testbed: data points

- Dedicated authoritative servers
  - 2 European locations („nice" RTTs): AMS, FRA
  - 1 „remote" location (HK, bandwidth*delay)
- Signed version of a live DE zone
- NSEC3, RSA/SHA256
  - BIND 9.7 (9.6), Unbound 1.4.4, Vantio
- Zone data changes (a.k.a „updates")
  - Twice per day (every 2 hrs in real world DE)
  - Frequency of changes to be increased beyond status quo

.de DNSSEC testbed: signing details

- ZSK (1024bit RSA/SHA256)
  - SW based on David Blacka‘s java DNSSEC signer
    - Added PKCS#11 support
  - HW: SCA6000
    - HSM, FIPS 140-2 Level3, PKCS#11
    - 2 locations, 2 systems per location, 2-3 cards per system
- KSK (2048bit RSA/SHA256)
  - Signatures generated in advance, SCA6000 again
  - Apex `DNSKEY` RRSet only signed by KSK
- NSEC3 opt-out, salt, 32 iterations
- *DNSSEC Practices Statement* to be published in June

Counting NSEC3/RRSIG RRs



Getting DNSSEC key material into the testbed

- … via registrars (as usual)
- Subject to some technical / protocol checks
- Submission of `DNSKEY`-RRs into the production registry database
  - RRI/MRIv2 (DENIC‘s flavour of a realtime provisioning protocol)
  - RRI web interface
- Immediately visible through …
  - … the registry interfaces
    - where it may well be ignored
  - … information services (`whois`, web whois)
  - … the DNS: `DS`-RRs will only appear in the testbed!

A sample testbed participant

```
; <<>> 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
```

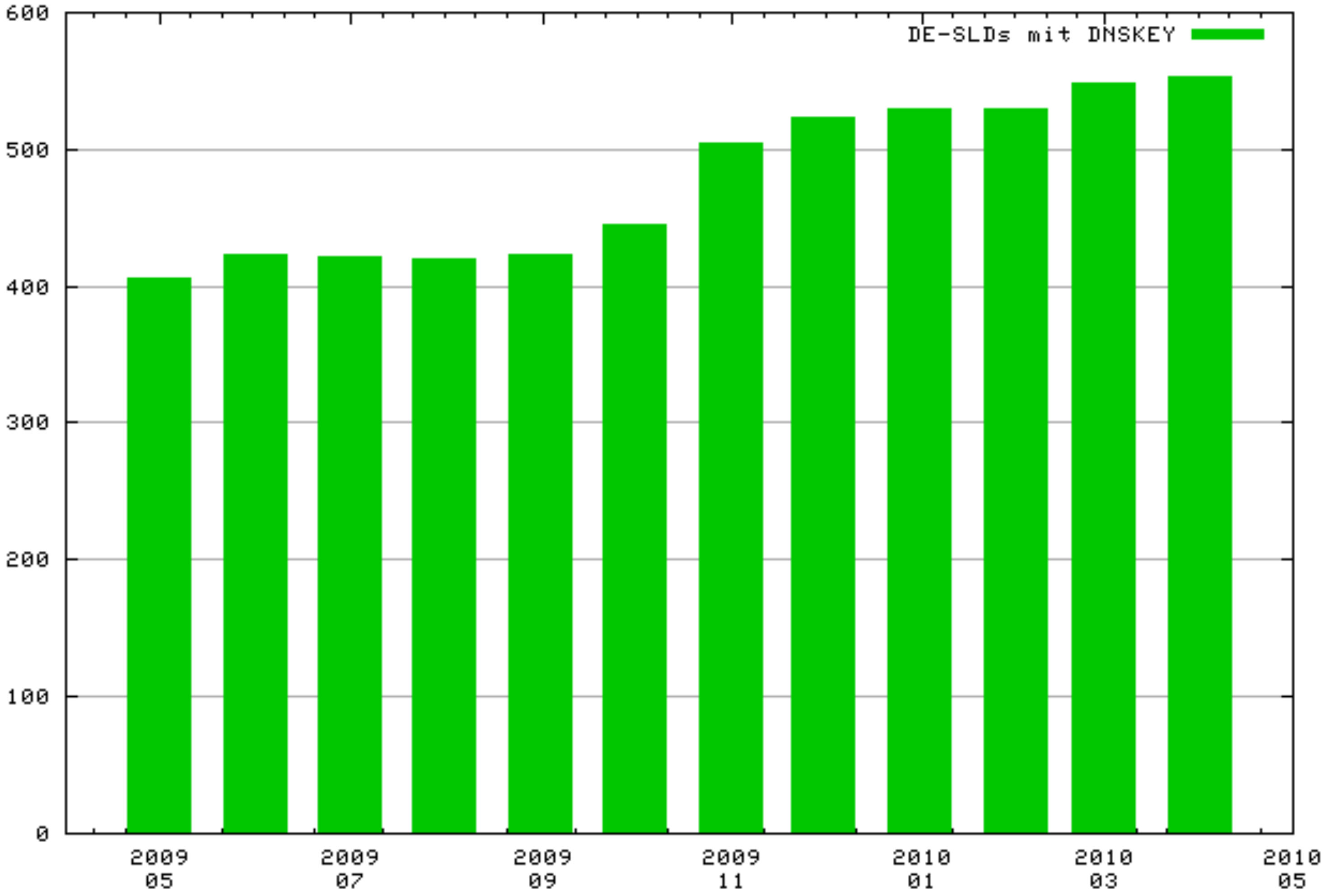
Prerequisites for DNSKEY registration

- SEP recommended, not required
- REVOKE-Bit must not be set
- DNSKEY algorithms with IANA assigned code points (non-private)
  - Currently RSA, DSA; GOST may follow next
- Other key parameters MUST obey specification
  - E.g., RSA modulus 512 - 4096 bit
- SOA-RR validates against at least one submitted *Trust Anchor*
  - Purpose: pre-registration of not-yet-visible TAs

.de DNSSEC testbed: observations

- 25 zones signed and participating
- approx. 600 queriers, but < 10qps
- no news is good news!

DE-Zones with apex DNSKEY



.de DNSSEC testbed: next steps

- Expand logging and reporting
- Increase distribution frequency
  - Continuous signing in DB
  - More, but smaller increments
- Publish test program
  - NSEC3 rollover
  - Operator change under DNSSEC
  - …

?

Please participate!

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