The .de DNSSEC testbed

- halftime, no break -

Peter Koch <koch@denic.de>

Bruxelles, 23 Juin 2010 / Brussel, 23 Juni 2010

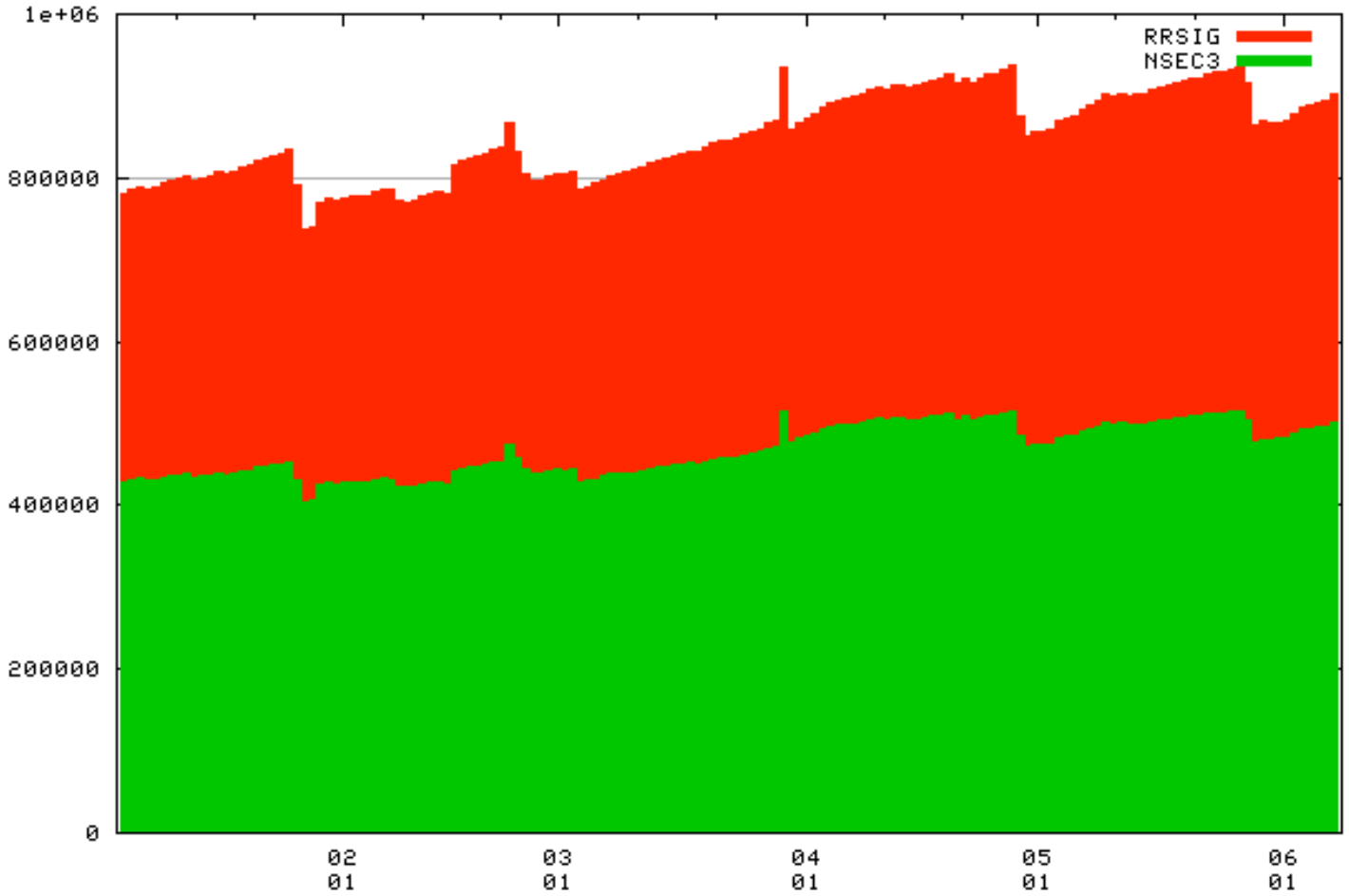
.de DNSSEC testbed: roadmap

- 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 server clusters: AMS, FRA
- Signed version of a live `DE` zone
- NSEC3 + OptOut, RSA/SHA256
- Zone data changes (a.k.a. „updates“): twice per day

Counting NSEC3/RRSIG RRs



Getting DNSSEC key material into the testbed

- … via registrars (as usual)
  - without further sign-up
- Subject to some technical / protocol checks
- Submission of `DNSKEY`-RRs **into 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)
  - … (not) the DNS: `DS`-RRs will only appear in the testbed!

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
- DNSKEY RRSet validates against at least one submitted *Trust Anchor*
  - Purpose: *proof of possession*
- SOA-RR validates against at least one submitted *Trust Anchor*
  - Purpose of „at least“: pre-registration of not-yet-visible TAs

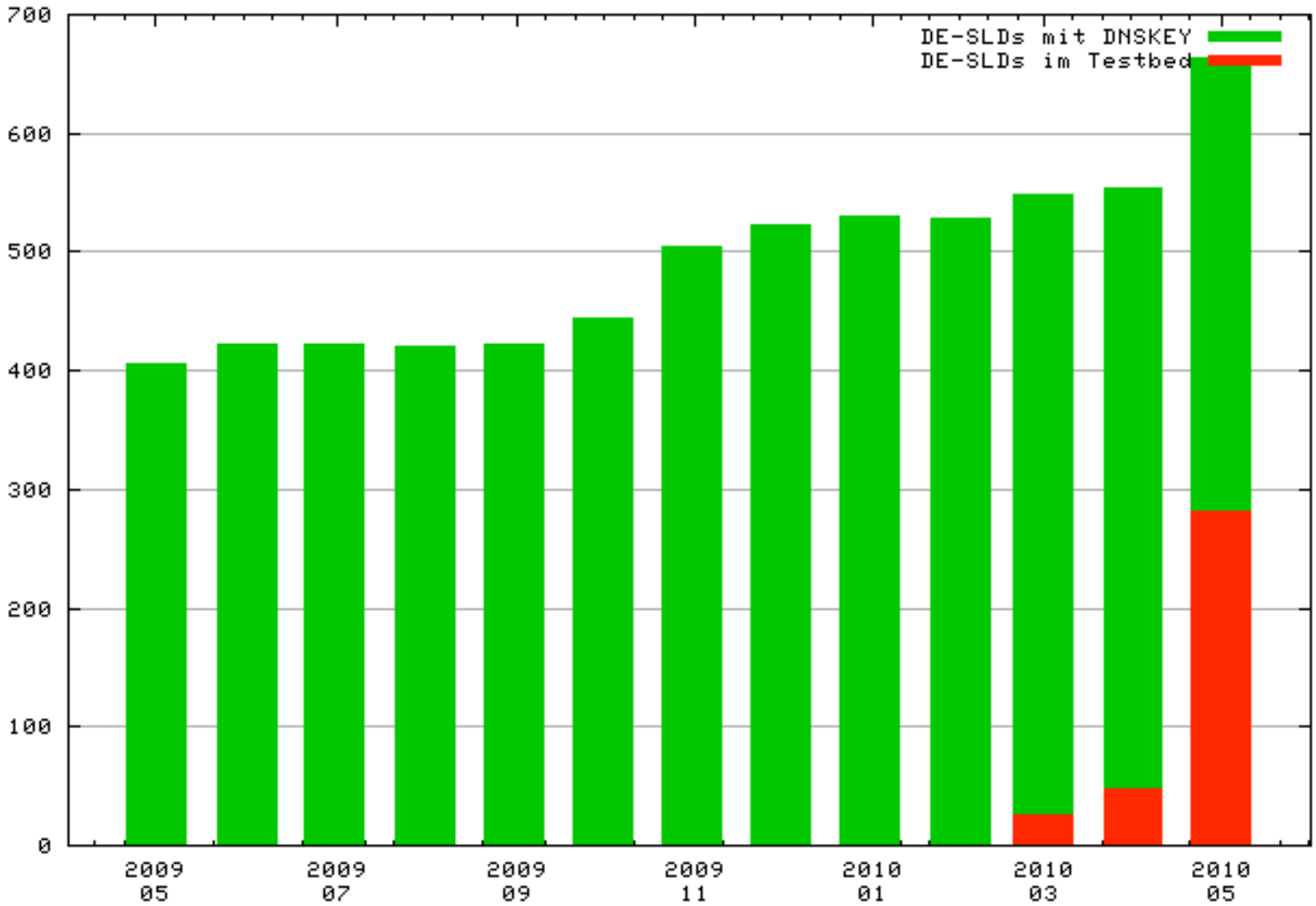
.de DNSSEC testbed observations: headlines

More than 250,000 domains secured by DNSSEC!

.de DNSSEC testbed observations: fineprint

- approx. 300 zones signed and participating
- approx. 100 queriers/day
  - some very active
  - 1st resolver/2nd resolver setups
- avg 150 q/s
- minor SW bugs/config issues in validators found
  - all reported back and solved

DE-Zones with apex DNSKEY



.de DNSSEC testbed: next steps

- Increase change distribution frequency
  - Continuous signing in DB
  - More, but smaller increments
- Publish test program
  - NSEC3 rollover
  - Operator change under DNSSEC
  - …
- 4th public DNSSEC testbed meeting 2010-11-24

?

Please participate!

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