DNSSEC for DE

- developing the testbed into production service -

ICANN DNSSEC Workshop, 2011-06-22 ; Jörg Schweiger

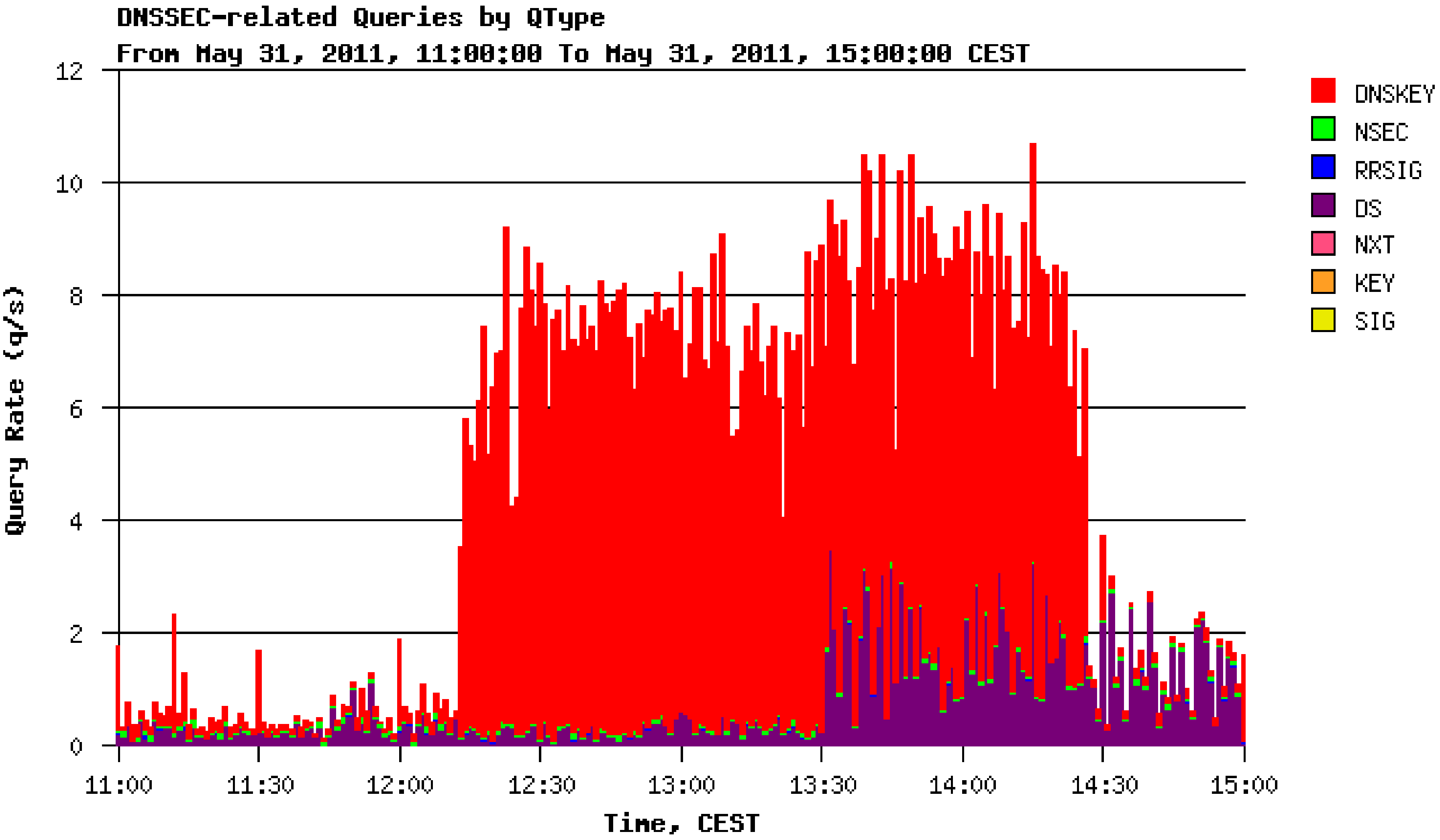
DNSSEC for DE -- Timeline

- DNSSEC Testbed
  - 2010-01-04 Signed DE
  - 2010-03-02 Accepted DNSKEY RRs for delegated SLDs

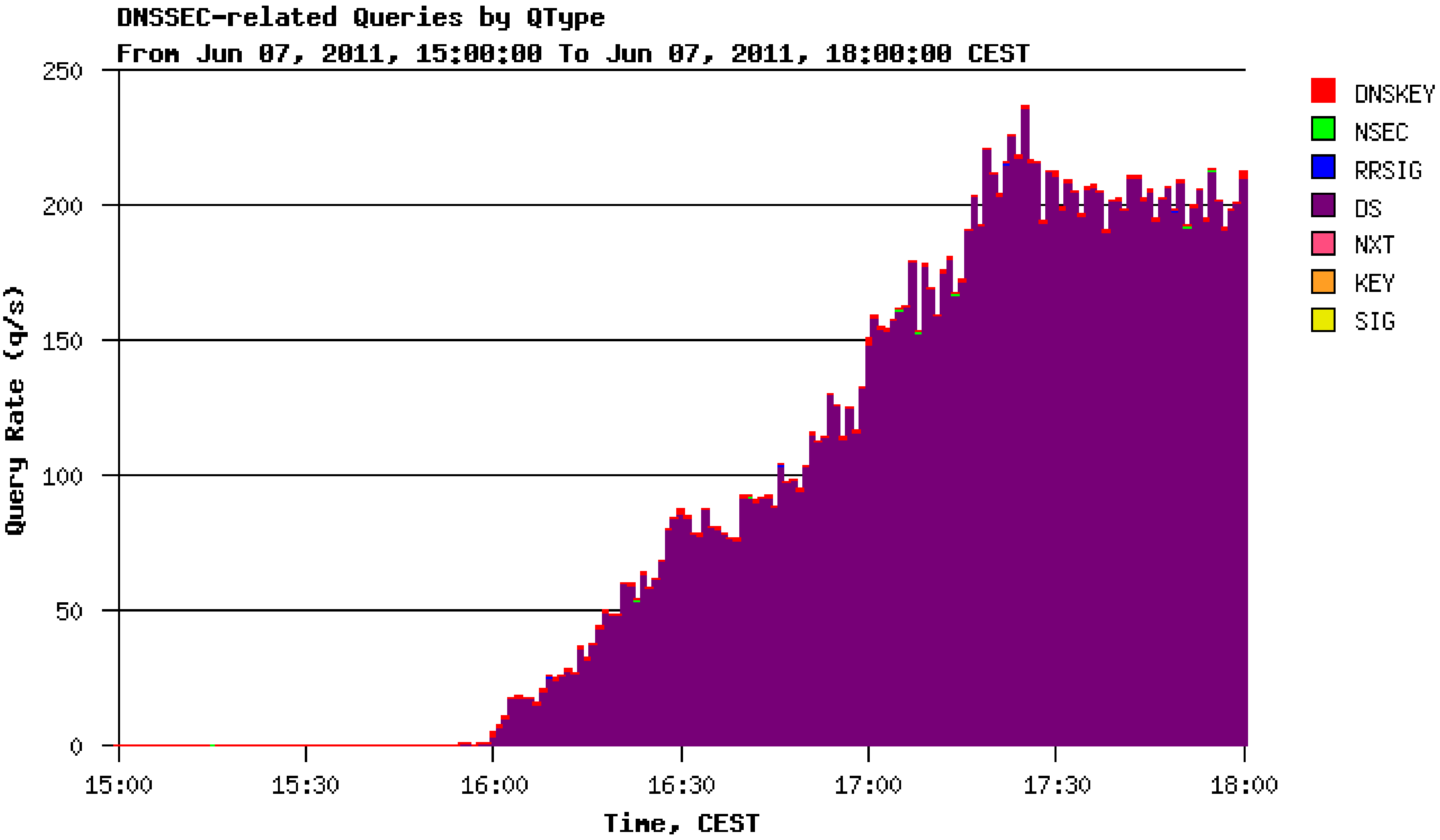
- Go Live
  - 2010-05-19 DUdeZ rollout to our 16 locations begins
  - 2011-05-31 DNSKEY RRSet (KSK and ZSK) unblinded
  - 2011-06-07 DS RR for DE appears in the root zone

➡ No unusual / unexpected traffic patterns (or volumes) seen

Unblinding the DE DNSKEY RRSet



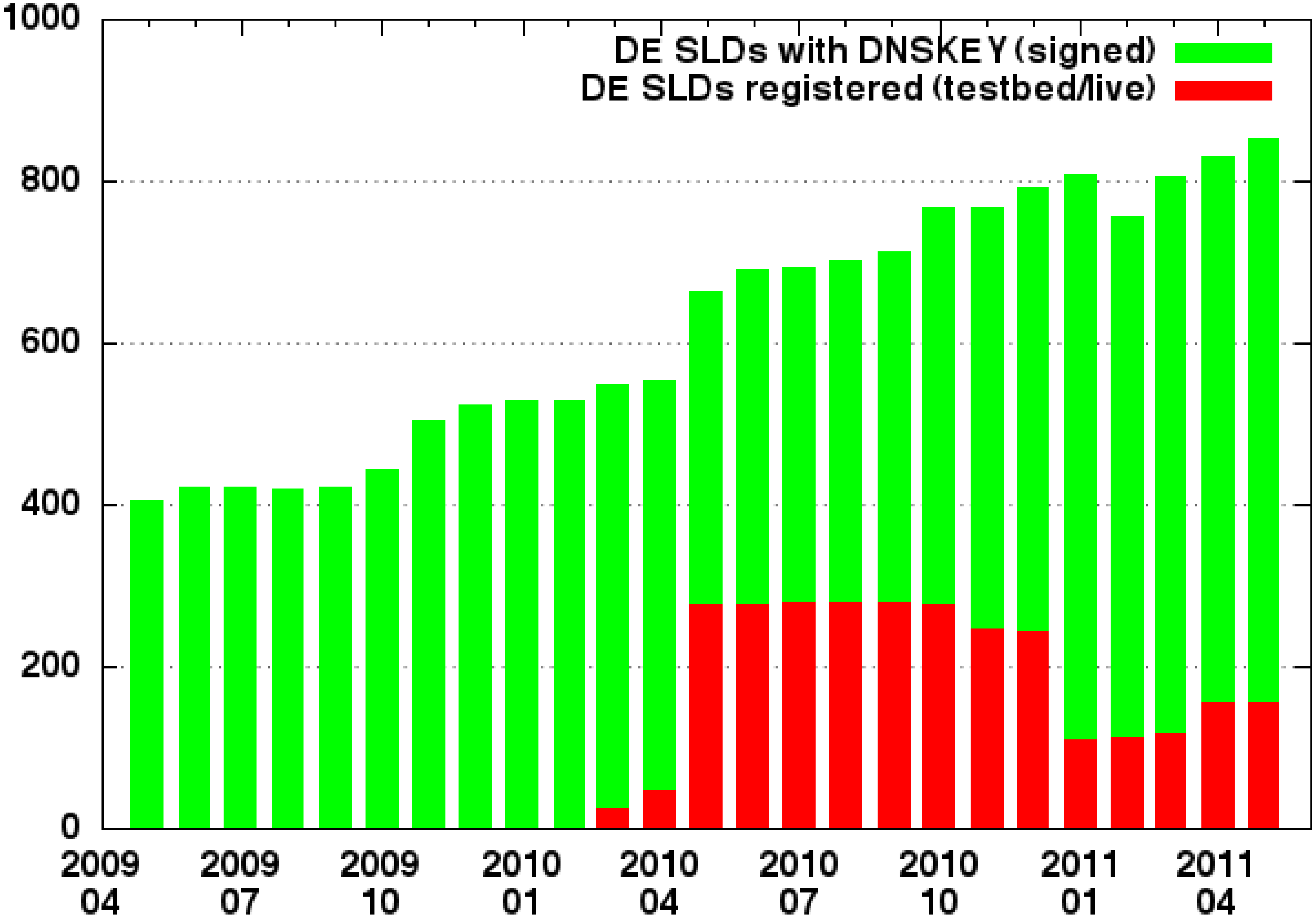
DNS query pattern change when DE DS RR appears in the root



DNSSEC for DE -- Today

> 200,000 domains signed!

Signed Second Level Domains (SLDs) in DE



DNSSEC for DE -- Technical Parameters & Details (1)

- Registration based on DNSKEY RR
  - What the client has ... (key instead of a hash prefered)
  - Syntax and validation check at registration time
    - No assessment of key length or strength, though
    - Integrated into *name server tester* (NAST) standard checks
  - Up to five DNSKEY RRs (to support standby and rollover)

DNSSEC for DE -- Technical Parameters & Details (2)

- Key and Signing algorithms
  - RSA/SHA256
  - 1024bit ZSK, 2048bit KSK
- NSEC3
  - To mitigate zone walking
  - To benefit from opt-out
  - Reduced hash iterations from 32 to 16 (re-assessed performance impact)
- Various Post Signature Checks
  - Comparison (unsigned zone vs signed zone after removing signatures)
  - NSEC3 chain
  - Signature Validation, …

DNSSEC for DE -- Keys and Signing

- KSK
  - Locked workstation with SCA6000 HSM (FIPS140-2/level3)
  - KSK crypto officers (n-of-m)
  - ZSK crypto officers (n-of-m)
  - Vault maintainers (on and off site backup)
  - Master of ceremonies
  - Internal audit

  - No special KSK publication channel provided
  - No scheduled KSK rollover as yet
- ZSK
  - Two data centers with two signing systems each (FRA/AMS)

DNSSEC for DE -- Change Operator

- Operator Change Support (name server changes)
  - Developed smooth handover based on RFC4641bis
  - Registry serves as dropbox for new ZSK
  - Cooperation with other TLD registries
  - IETF Internet-Draft available

Q&A

?

Thanx !

Further information: www.denic.de/en/domains/dnssec.html
schweiger@denic.de