nic.at
the austrian registry

ISPA Academy
DNSSEC Workshop

Salzburg, 19.5.2010
Otmar Lendl <lendl@nic.at>

nic.at
the austrian registry

Programm

- Warum DNSSEC
  - DNS Basics
  - Angriffsszenarien
  - Der Kaminsky-Attack
- Wie funktioniert DNSSEC
- Internationaler Stand der Dinge
- Technische Probleme
- Was ändert DNSSEC im Markt?
- Software

Vorweg ….

Das ist ein Workshop und soll nicht ein reiner Frontalvortrag werden, daher

Fragen sind willkommen!

Danke an Michael Braunöder, Olaf Kolkman, Phil Regnauld, … für die Erlaubnis, aus ihren Slides zu zitieren.

Kurz über mich

- Mag. Otmar Lendl
- Hier studiert
- ´97 – 2002: ISPs
  - ping
  - Eunet
  - kpnqwest
  - Eunet v2
  - Tiscali
- 2002 – 2007: R&D bei nic.at
- 2007 – : Team Lead CERT.at

DNS: Was ist das?

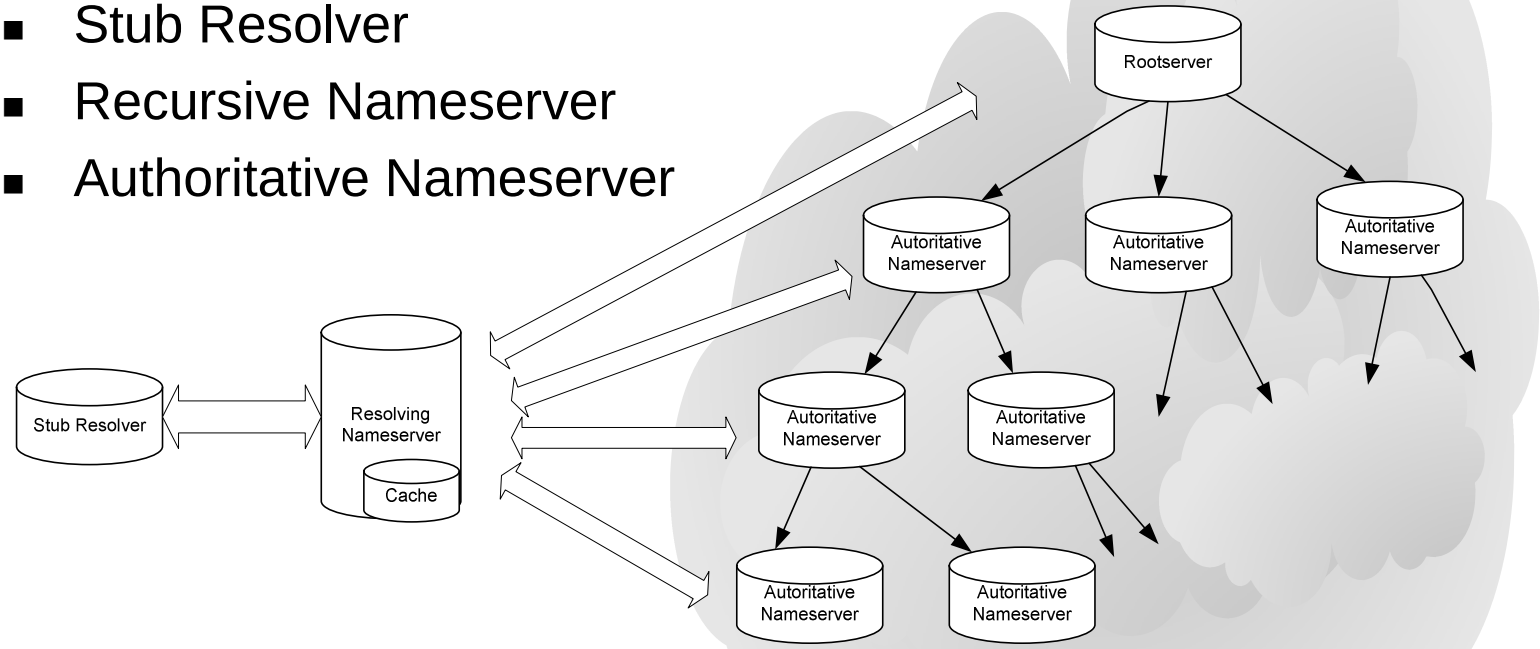
- Global, distributed Database
- Input: Domain name
- Output: Resource Record **Sets**
  - A, AAAA — IP addresses
  - MX — Mail routing
  - CNAME — Aliasing
  - NS — Delegation
  - PTR, NAPTR, SRV,
  - RRSIG, DS, NSEC, NSEC3
- Transport: mainly UDP
- Lots of caching

DNS: Warum ist es wichtig?

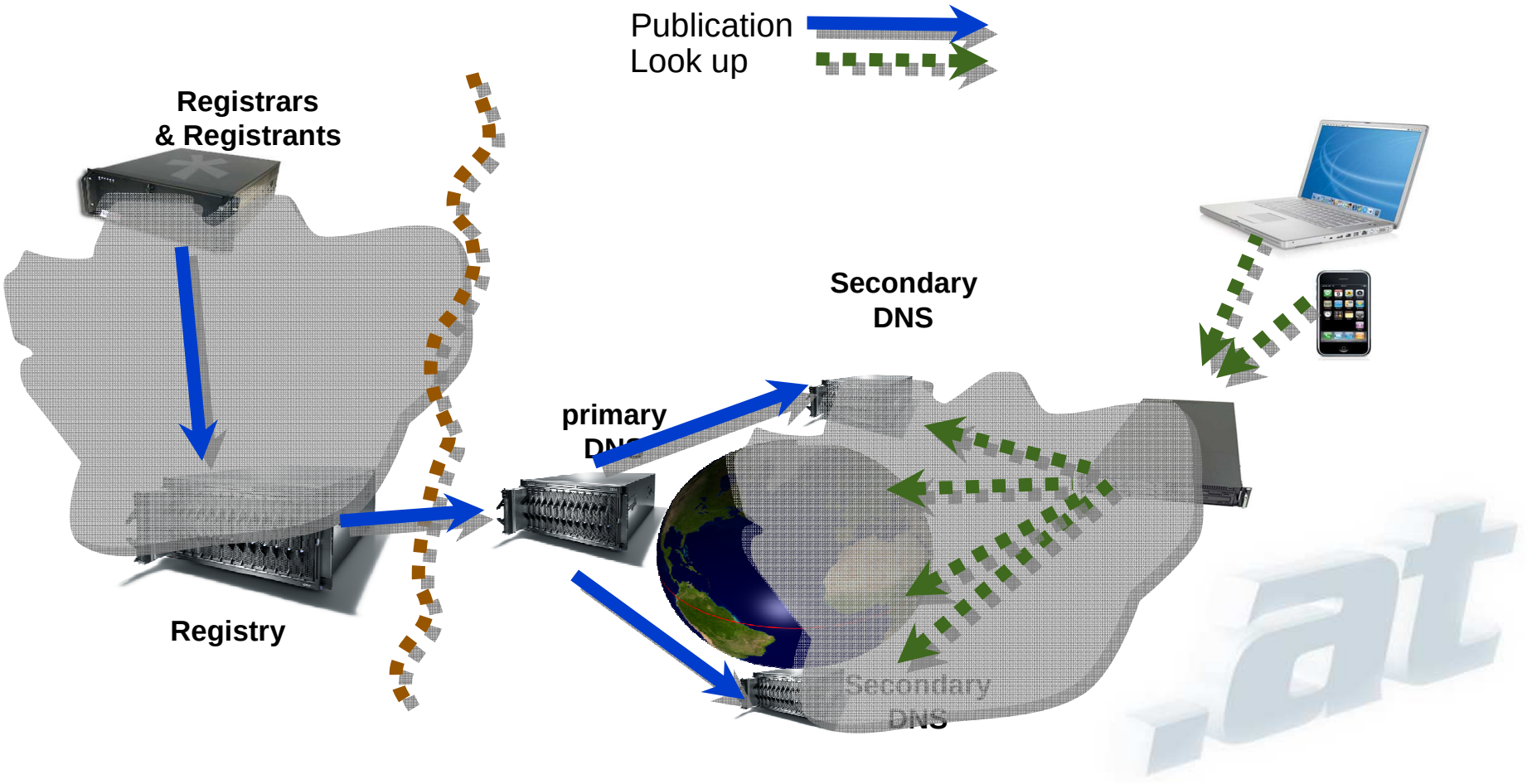
- DoS
- Man-in-the-middle almost *everything*
  - Phishing
  - Email hijacking
- Password reset emails
- Software Updates
- SSL and PKI for the rescue?
  - How do users react to X.509 errors?
  - CA email-loop
  - CA whois lookup
- Für den Enduser ist „DNS Kaputt“ nicht von „Internet ist kaputt“ unterscheidbar

Mitspieler

- Stub Resolver
- Recursive Nameserver
- Authoritative Nameserver



Resolution is nur die halbe Miete



Gefahrenanalyse

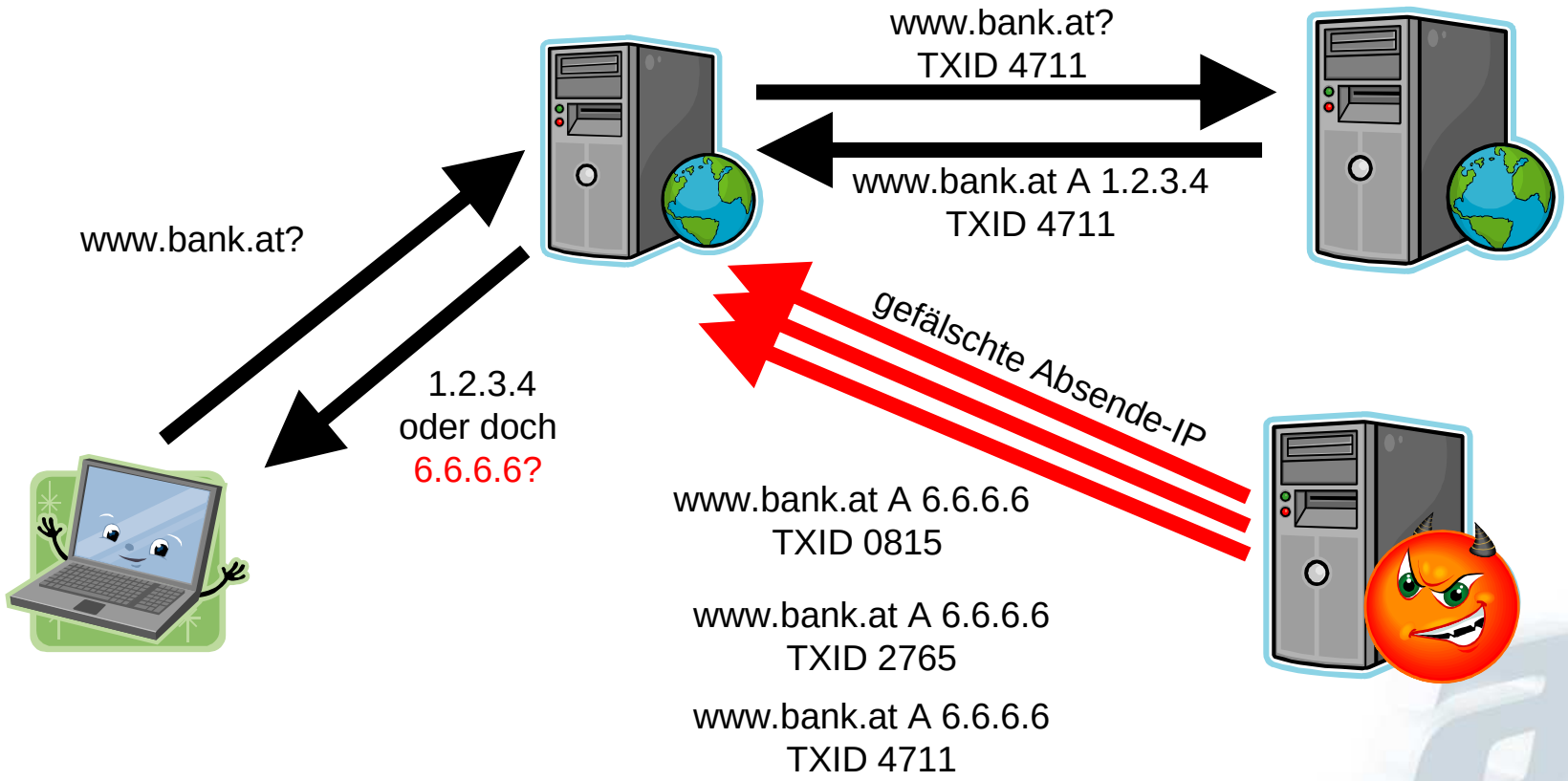
- Cache poisoning
  - Off-path attacks
  - On-path attacks
- Name chaining
- Falsche Antwort durch den Recursor
  - Sitefinder
  - NXdomain monetizing

- Siehe auch RFC 3833

Cache Poisoning (off-path)

- Das ist nichts neues.
  - Kashpureff
  - Triviale Query-ID
  - Parallele Anfragen
- Berechnungen zur Erfolgswahrscheinlichkeit in RFC 5452

DNS Cache Poisoning



Anatomy of a DNS Answer

```
$ dig cert.at MX
[…]
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8861
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;cert.at.                       IN      MX

;; ANSWER SECTION:
cert.at.                7200    IN      MX      100 nuwen.cert.at.

;; AUTHORITY SECTION:
cert.at.                6450    IN      NS      ns1.cert.at.
cert.at.                6450    IN      NS      ns5.univie.ac.at.

;; ADDITIONAL SECTION:
nuwen.cert.at.          7200    IN      A       83.136.33.135
```

Bailiwick checks

- Legitimate Servers can play games, too.

```
;; ADDITIONAL SECTION:
nuwen.cert.at.          7200    IN      A       83.136.33.135
```

- What stops a server from adding?

```
;; ADDITIONAL SECTION:
nuwen.cert.at.          7200    IN      A       83.136.33.135
xxx.                   50000    IN      NS      ns1.cert.at.
xxx.                   50000    IN      NS      ns2.cert.at.
```

- “in-bailiwick checks”: only accept what you were asking for. See RFC 2181 for details.

Security?

This is the safety net

```
$ dig cert.at MX
[…]
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8861
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;cert.at.                       IN      MX

;; ANSWER SECTION:
cert.at.                [illegible]

;; AUTHORITY SECTION:
cert.at.                [illegible]
cert.at.                [illegible]

;; ADDITIONAL SECTION:
nuwen.cert.at.          [illegible]
```

16 bits of entropy might have been enough in 1987, but not in 2008.

Pre-Kaminsky

- An attack needs to match
  - Question section
  - The ID field
  - IP address of the nameserver queried
  - IP address / port from which the query was sent
- How often can an attack take place?
  - Each query from a recursor starts a race.
  - Forcing a query helps the attacker
  - The cache limits attacks to once per Time-To-Live for the same query

Attacking www.example.org

```
;; QUESTION SECTION:
;345678.example.org.            IN      A

;; ANSWER SECTION:
345678.example.org.  3600      IN      A       192.0.2.1

;; AUTHORITY SECTION:
example.org.         100000    IN      NS      ns1.evil.net.
example.org.         100000    IN      NS      ns2.evil.net.
```

Source: IETF namedroppers list. (P. Koch, T. Finch)

Oder ...

```
;; QUESTION SECTION:
;345678.www.example.org.                A

;; AUTHORITY SECTION:
www.example.org.     NS ns1.evil.net.
www.example.org.     NS ns2.evil.net.
```

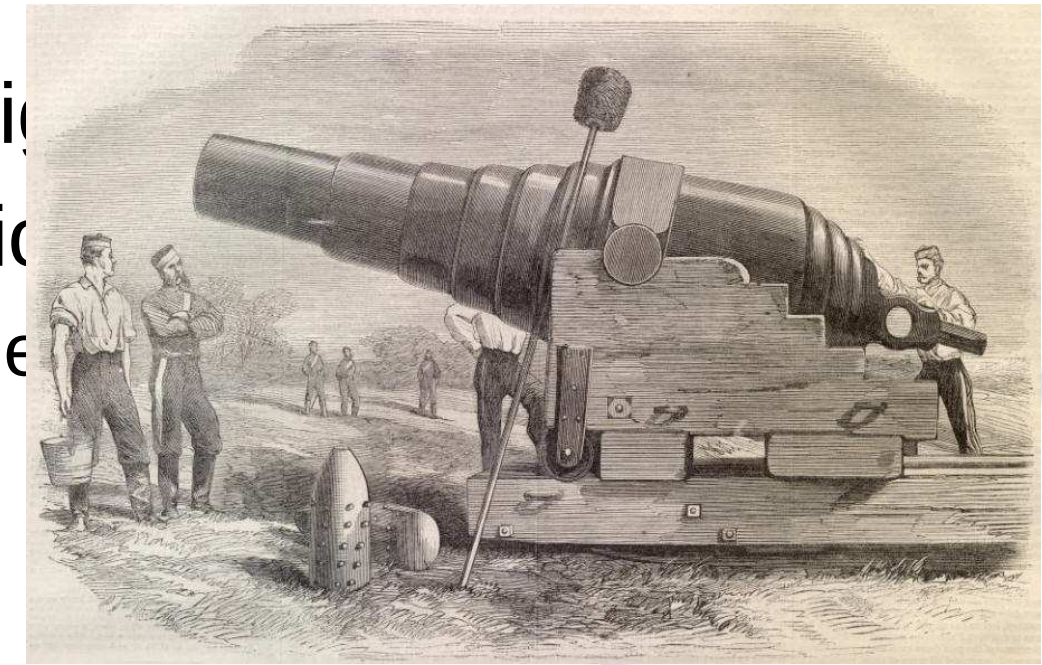
… oder …

```
;; QUESTION SECTION:
;345678.example.org.            IN    A

;; ANSWER SECTION:
345678.example.org.     CNAME www.example.org.
www.example.org.        A     192.0.2.80  ; evil
```

What can be done?

- Maximize Entropy
- New Resolver behaviour
- Agile Defenses
- Link Security (tsi
- Protocol Extensi
  - Simple Entropy e
  - DNScurve
  - DNSSEC



DNSSEC

- DNS Securitiy Extension
- Paul Vixie: „DNSSEC is an Internet Standard meaning that it came from IETF, took years longer than it should have, has some features that almost nobody now remembers the reason for, and lacks some features that almost everybody wishes it had. So, it‘s a lot like IPv6 or IPSEC. And yet, it works.“

DNSSEC

- Details zum Nachlesen:
  - RFC4033, “DNS Security Introduction and Requirements” (2005)
  - RFC4034, “Resource Records for the DNS Security Extensions”
  - RFC4035, “Protocol Modifications for the DNS Security Extensions”
  - RFC5011, “Automated Updates of DNS Security (DNSSEC) Trust Anchors“
  - RFC5155, “DNS Security (DNSSEC) Hashed Authenticated Denial of Existence” (2008)
- 1. Versuch war schon RFC 2535 (1999)

Welche Security?

- Confidentiality
  - Kann wer mitlesen?
- Integrity
  - Stimmt das, was ich bekommen habe?
- Availability
  - Bekomme ich überhaupt eine Antwort?

DNSSEC betrifft ausschließlich „Integrity“!

Grundidee

- Kompatible Erweiterung des DNS
- Public Key Kryptografie Signaturen innerhalb der DNS Antworten
- Schutz der Daten, nicht Schutz des Transports
- Delegationshierarchie des DNS wird auch zur Trust-Hierarchie

New Resource Records

- Three Public key crypto related RRs
  - RRSIG — Signature over RRset made using private key
  - DNSKEY — Public key, needed for verifying a RRSIG
  - DS — Delegation Signer; ‘Pointer’ for building chains of authentication
- Two RR for internal consistency
  - NSEC — Indicates which name is the next one in the zone and which typecodes are available for the current name.
  - NSEC3 — NSEC++

RRSIG – Signature

- 16 bits - type covered
- 8 bits - algorithm
- 8 bits - nr. labels covered
- 32 bits - original TTL
- 32 bit - signature expiration
- 32 bit - signature inception
- 16 bit - key tag
- signer's name

RRSIGs gelten nicht ewig!

Absolute Zeit

```
nlnetlabs.nl.  3600 IN  RRSIG   A 5  2 3600  (
            20050611144523 20050511144523  3112 nlnetlabs.nl.
            VJ+8ijXvbrTLeoAiEk/qMrdudRnYZM1VlqhN
            vhYuAcYKe2X/jqYfMfjfSUrmhPo+0/GOZjW
            66DJubZPmNSYXw== )
```

Beispiel

test.at. IN SOA ns1.mib.test.at. mib.nic.at. (824800004 3600 600 604800 10)
)

RRSIG SOA 7 2 1800 20081210085140 (
20081110085140 47927 test.at.
PYBNzMAU/A2eUaHenhDn7vNkKx2EKhozXh+D
fU6+SFbuyttWff1N1O8zWkcvKkE3+Z8nzKSp
lGfF7chfBzM7mlLgv8YfgOpt14CCOKLd7ukc
jKlLBvE4ctrw7DBBh49gLxFtZE16B4u2OH4g
LUco9MKv/lkFRzbomuAk+reUrM0=)

NS ns1.mib.test.at.
NS ns2.mib.test.at.

RRSIG NS 7 2 1800 20081210085140 (
20081110085140 47927 test.at.
ArI5PU4wo2zBog8NQLXmzPvkm7IJNt0hSyrN
RZdOZplQdB0TNCf/y8slQtjJxA3LbC8inwq2
feHYTmgX4ND1wAZtLpI5mvenZ1oeim9Saz38
BGOiESYbXVK4FQV8JrJnE0BbnglD9QPjw69b
+K0zj3ug2U7jDD6F8kN3Ozz3hD4=)

DNSKEY – Public Key

- 16 bits: FLAGS
- 8 bits: protocol
- 8 bits: algorithm
- N*32 bits: public key

```
nlnetlabs.nl. 3600 IN DNSKEY  256 3 5 (
          AQOvhvXXU61Pr8sCwELcqqq1g4JJ
          CALG4C9EtraBKVd+vGIF/unwigfLOA
          O3nHp/cgGrG6gJYe8OWKYNgq3kDChN)
```

Delegation Signer (DS)

- Delegation Signer (DS) RR indicates that:
  - delegated zone is digitally signed
  - indicated key is used for the delegated zone

- Parent is authorative for the DS of the child's zone
  - Not for the NS record delegating the child's zone!
  - DS **should not** be in the child's zone

DS – Key of Subdomain

- 16 bits: key tag
- 8 bits: algorithm
- 8 bits: digest type
- 20 bytes: SHA-1 Digest

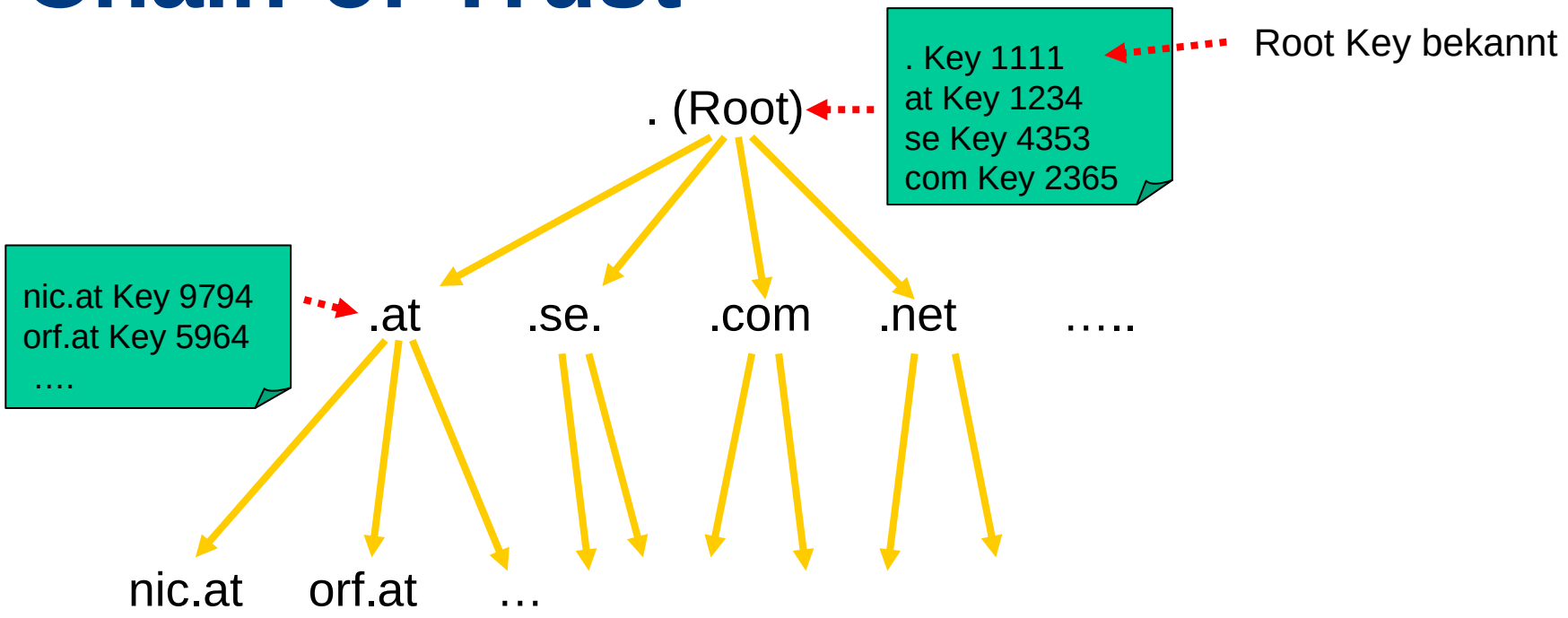
```
$ORIGIN nlnetlabs.nl.
lab.nlnetlabs.nl.   3600 IN   NS  ns.lab.nlnetlabs.nl
lab.nlnetlabs.nl.   3600 IN   DS  3112   5  1 (
                                    239af98b923c023371b52
                                    1g23b92da12f42162b1a9
                                  )
```

Public-Keys und Vertrauen

- Die Public-Keys zur Überprüfung werden in der Zone selbst publiziert
  - z.B.: test.at DNSKEY 256 3 7 (
    AwEAAag5EG6+V01LqB03SnIKtskcswtIf2BU
    xyUlbl/sIhEVKqO/qIbhVqBjmTx6c8x+i41j
    xRC9Nir3IWuhzrl50SKD88TO+PQc4aV8eaT3
    sDKeUxFhvOj0DkMEVFMd61TBFD7AMxnJ+dlR
    txhkb4MIBZ57ifr+l73zTUnD5fBAgfUP
) ; key id = 47927
- Problem: Vertrauen in den Schlüssel
  - Der Schlüssel zur Überprüfung der Information kommt aus der gleichen Quelle wie die Information selbst

  -> Vererbtes Vertrauen von oben nach unten (Chain-of-Trust)

Chain-of-Trust



Der Public-Key der Rootzone muss lokal bekannt sein

Beispiel für Chain-of-Trust

In der Zone test.at:

```
domain1.test.at.        NS    ns1.mib.test.at.
                        NS    ns2.mib.test.at.
                        NS    ns3.mib.test.at.
                        DS    23433 7 1 (
                              0F3A407A2B8921FC4B201F5525AAF15D672C
                              8123 )
                        RRSIG DS 7 3 1800 20081210085140 (
                              20081110085140 47927 test.at.
                              AE0fnjrwn+LKon3XNg9chCqWAzzVMMhpLn8q
                              4P0CRHHfDtYOcSHE4VGXTmZinSZkCJqPapaF
                              HUfx2R4z+sMs/8ToU+UHBBGfT610wffHf3M9
                              IKauAZIX68tvEGA86U9QxO3HLe1NpuH+ayj4
                              9k/m+SODyEsCsum9MOzeUL/fj78= )
```

Der RRSIG-Record wurde mit dem Private-Key von test.at erstellt.

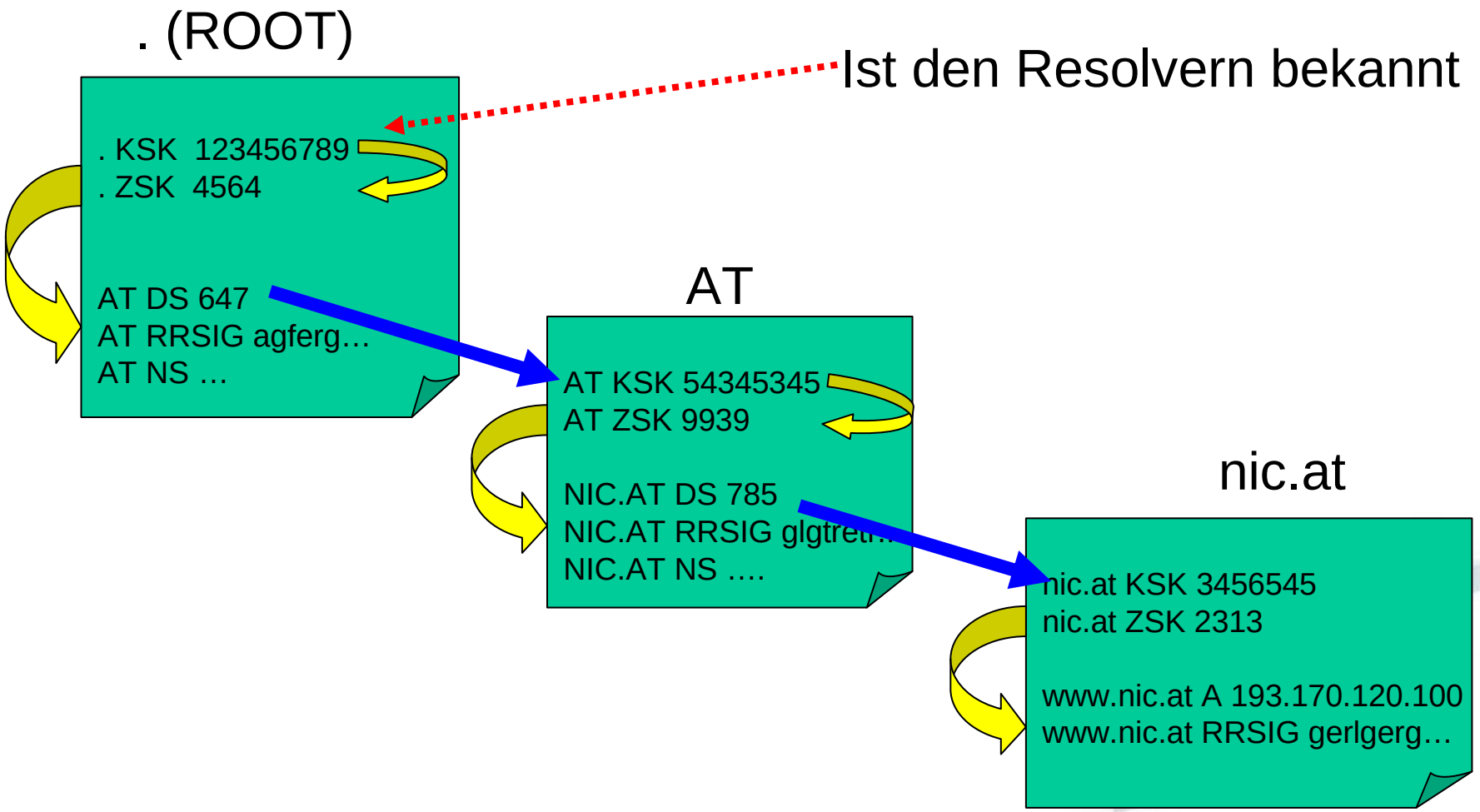
Problem Schlüssellänge

- Lange Schlüssel
  - Sicherer -> weniger Schlüsselwechsel notwendig (weniger Interaktion mit übergeordneter Stelle (Registry, IANA) notwendig -> weniger Fehlermöglichkeiten
  - Signieren dauert länger
  - Das signierte Zonefile wird größer
- Kurze Schlüssel
  - Weniger sicher -> häufigere Schlüsselwechsel notwendig (mehr Interaktion mit übergeordneter Stelle notwendig -> mehr Fehlermöglichkeiten
  - Signieren geht schneller
  - Das signierte Zonefile wird kleiner

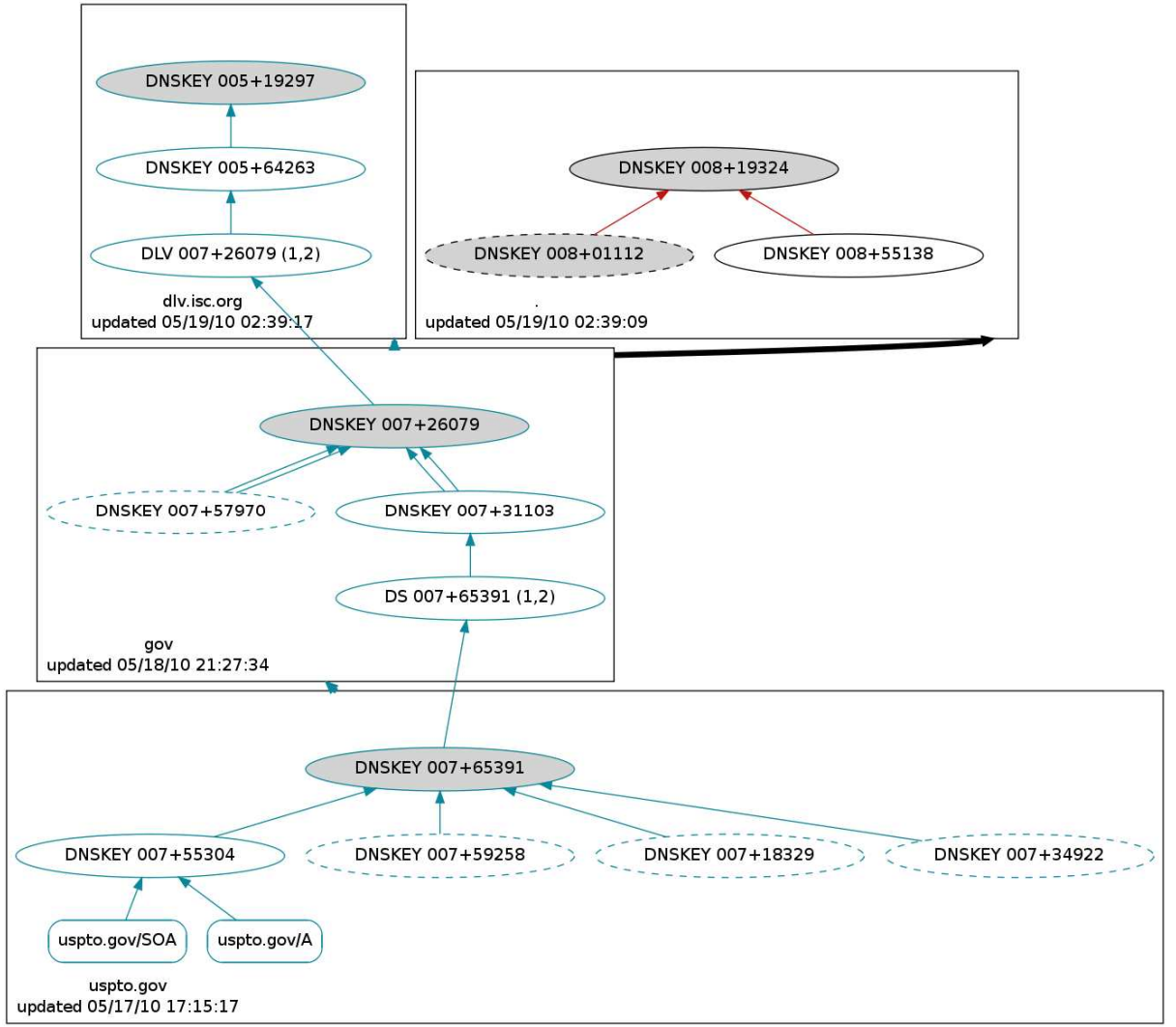
Nyckelsigneringsnyckel

- Lösung: beide Schlüsseltypen verwenden:
  - 1 langer Schlüssel, welcher in der übergeordneten Stelle bekannt ist (für die Chain-of-Trust) -> Key Signing Key (KSK)
  - 1 kurzer Schlüssel, welcher vom langen Schlüssel signiert wurde und für die „tägliche“ Arbeit verwendet wird. Kann lokal ohne Interaktion gewechselt werden. -> Zone Signing Key (ZSK)

KSK/ZSK – Chain-of-Trust Übersicht



http://dnsviz.net/



Problem: Beweis von Nicht-Existenz

- Wie kann man beweisen dass etwas nicht existiert (und das möglichst für den Client überprüfbar)?
  - generelles, signiertes NXDOMAIN nicht möglich (Replay-Attacke)
  - offline generieren aller möglichen Anfragen und signieren der möglichen Antworten nicht praktikabel
  - On-the-fly Signierung der Antworten bietet DoS-Potential und Sicherheitsrisiko (Private Schlüssel auf allen Nameservern)
- Lösung: Man zeigt was man hat.

NSEC – Proof of non-existance

- FQDN: Next Name in Zone
- N*32 bit map: RRTypes present

```
www.nlnetlabs.nl. 3600 IN   NSEC z.nlnetlabs.nl. A RRSIG NSEC
```

NSEC Records

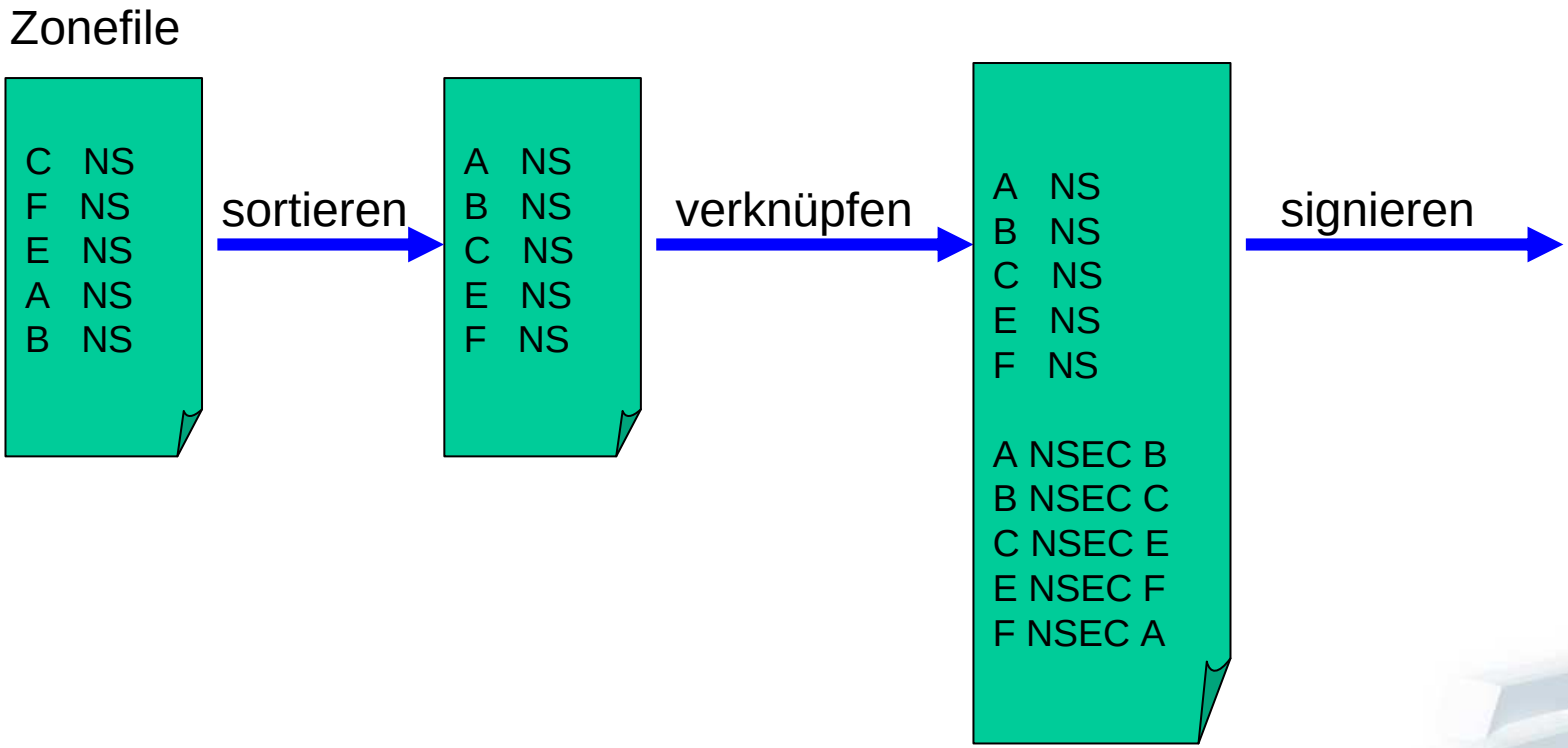
- NSEC RR provides proof of non-existence
- If the servers response is Name Error (NXDOMAIN):
  - One or more NSEC RRs indicate that the name or a wildcard expansion does not exist
- If the servers response is NOERROR:
  - And empty answer section
  - The NSEC proves that the QTYPE did not exist
- More than one NSEC may be required in response
  - Wildcards
- NSEC records are generated by tools
  - Tools also order the zone

NSEC Walk

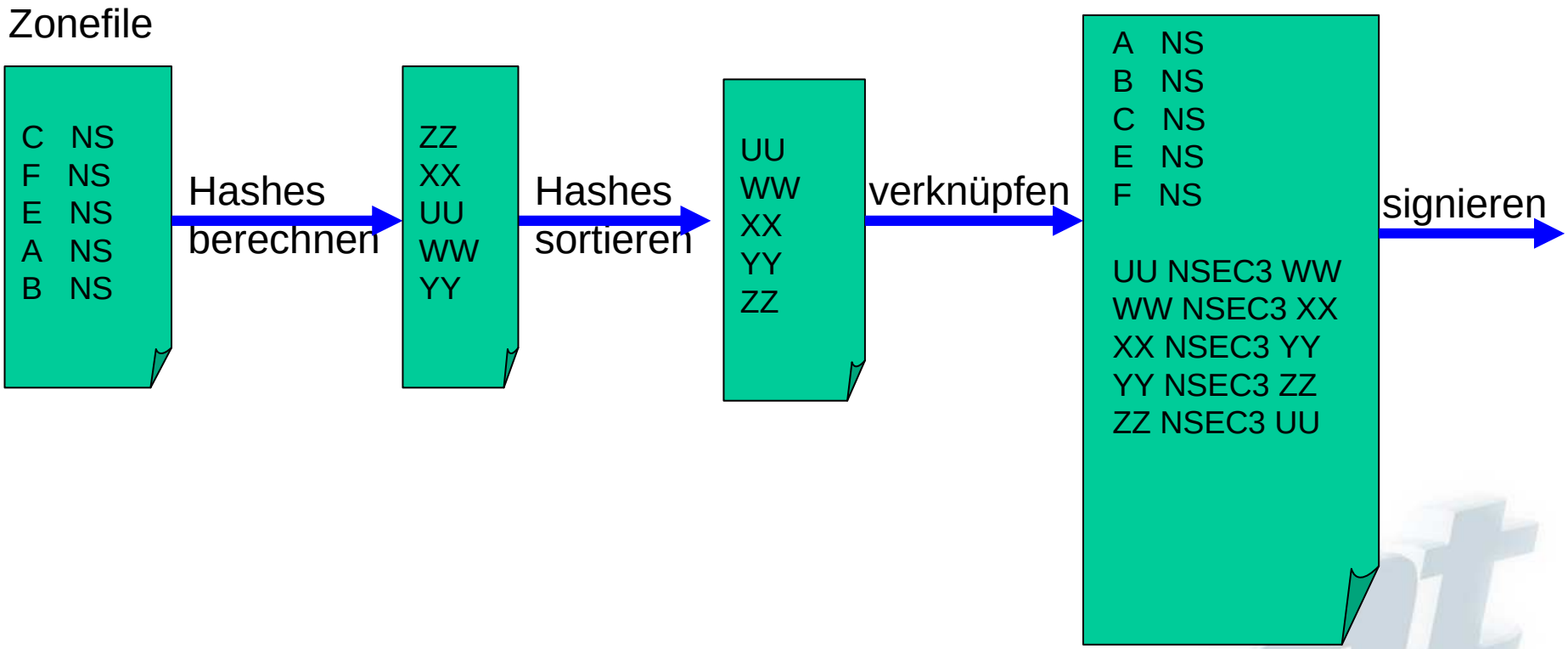
- NSEC records allow for zone enumeration
- Providing privacy was not a requirement at the time
- Zone enumeration is a deployment barrier

- Solution is developed: NSEC3
  - RFC 5155
  - Complicated piece of protocol work
  - Hard to troubleshoot
  - Only to be used over Delegation Centric Zones
  - Opt-out Feature

NSEC


Zonefile
C NS
F NS
E NS
A NS
B NS
sortieren
A NS
B NS
C NS
E NS
F NS
verknüpfen
A NS
B NS
C NS
E NS
F NS
A NSEC B
B NSEC C
C NSEC E
E NSEC F
F NSEC A
signieren

NSEC3


Zonefile
C NS
F NS
E NS
A NS
B NS
Hashes berechnen
ZZ
XX
UU
WW
YY
Hashes sortieren
UU
WW
XX
YY
ZZ
verknüpfen
A NS
B NS
C NS
E NS
F NS
UU NSEC3 WW
WW NSEC3 XX
XX NSEC3 YY
YY NSEC3 ZZ
ZZ NSEC3 UU
signieren

Glue

- NS records in der Parent Zone sind nicht signiert.
- Glue records auch nicht.
- Downgrade-attack?

```
;; AUTHORITY SECTION:
ijji.se.                86400   IN      NS      ns1.fastpark.net.
ijji.se.                86400   IN      NS      ns2.fastpark.net.
ijji.se.                7200    IN      NSEC    ijk.se. NS RRSIG NSEC
ijji.se.                7200    IN      RRSIG   NSEC 5 2 7200
20100526124808 20100518231127 14421 se.
aWgByzy2VC80r+8oktjODrcDzn1I4qGhEhBewyY98SY5HgvzBB31QZ7n
ia4fz2npTvXZ+3QM8NVHTBr20o3nUsTA++JjDvK/5BkyW6f93Zp22XQY
fUl+Jly7H3O9uGW3oQzDkRbEsFywKaAq9ayU1vgnGcFjs1Mtt2IqwWX8 O8o=
```

DNSSEC Queries

- DO
  - DNSSEC OK (EDNS0 OPT header) to indicate client support for DNSSEC options
  - EDNS0 is required for DNSSEC
- CD
  - “Don’t check signatures for me, just give me the raw DNSSEC records”

DNSSEC Answers

- SECURE Validated with key
  - AD – bit set in Packet
- INSECURE Validated but no key
- BOGUS Validation failed
- UNKNOWN ServFail etc

Deployment Server-side

- Key management
  - Generate keys
  - Add DNSKEY records
- Sign zone
  - Signing & serving need not be performed on same machine
  - Signing system can be offline
- Make sure authoritative nameservers handle DNSSEC
- Communicate your keys to parent zone

Deployment Client-side

- Stub-Resolver speaks DNSSEC
  - Inefficient
  - Slow rollout
  - Upsides in User-Interface
- Recursor does DNSSEC Validation
  - Need a way to secure last hop
  - Huge multiplier possibilities
- Secure Entry Points?

Trust Anchors

- Irgendwem muss der Client vertrauen
  - Hardcoded (domain, DNSKEY) Paare in der resolver-config
  - Analog zu dem „root.hints“ File
- Optimal:
  - Root ist signiert, alle TLDs, ….
- Realität:
  - Es gibt signierte Inseln:

Status 2009

Source: http://www.xelerance.com/dnssec/

Zwischenlösungen

- Selber Trust Anchors zusammensuchen
- DNSSEC Lookaside Validation (DLV)
  - <fqdn>.dlv.isc.org
- Trust Anchor Registries:
  - IANA Interim Trust Anchor Repository
    - https://itar.iana.org/
  - RIPE NCC?
    - http://www.ripe.net/ripe/tf/dnssec-key/
- Private, signed roots

Trust Anchor Troubles

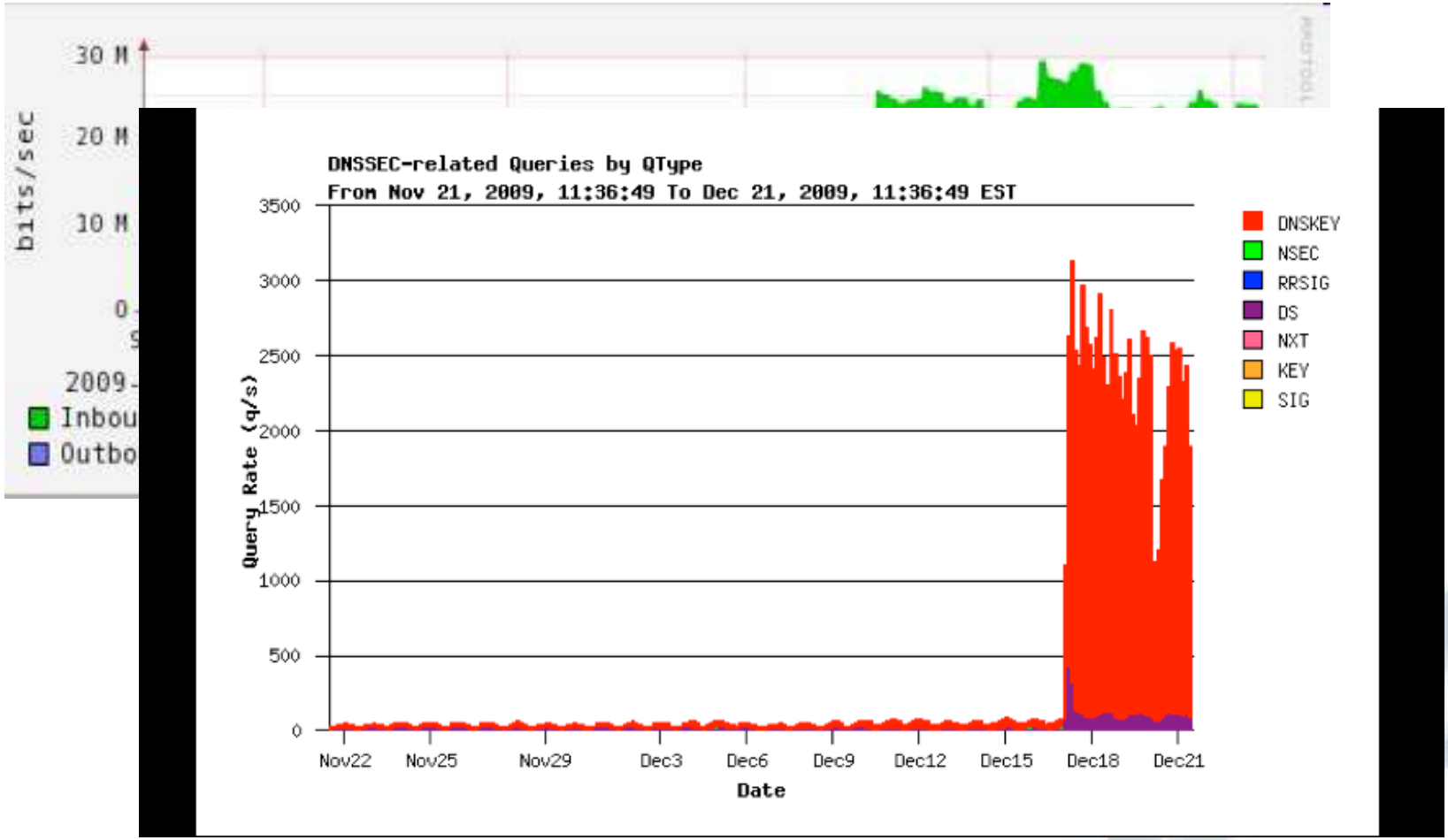
- Publizieren / Eintragen ist einfach
- Aktuell halten ist schwierig
  - Key rollover sind aber nötig
  - Aktuelles Beispiel:
    - RIPE SEPs in Fedora
      - http://www.mail-archive.com/bind-users@lists.isc.org/msg04918.html
  - Revocation ist schwierig
    - DNSSEC einfach abschalten geht nicht.
- Statisches Eintragen ohne automatisches Update ist keine gute Idee.

Roll Over and Die

- http://www.potaroo.net/ispcol/2010-02/rollover.html
  - **George Michaelson, Patrik Wallström, Roy Arends, Geoff Huston**
- Falsche Trust-Anchors im Recursor
  - Obsolete
  - Fehler in der Zone
- Aggressives Verhalten des Recursors
- Massive Last am Authoritiven NS
- Ist im neuesten Bind gefixt

nic.at
the austrian registry

Roll Over and Die: RIPE NS

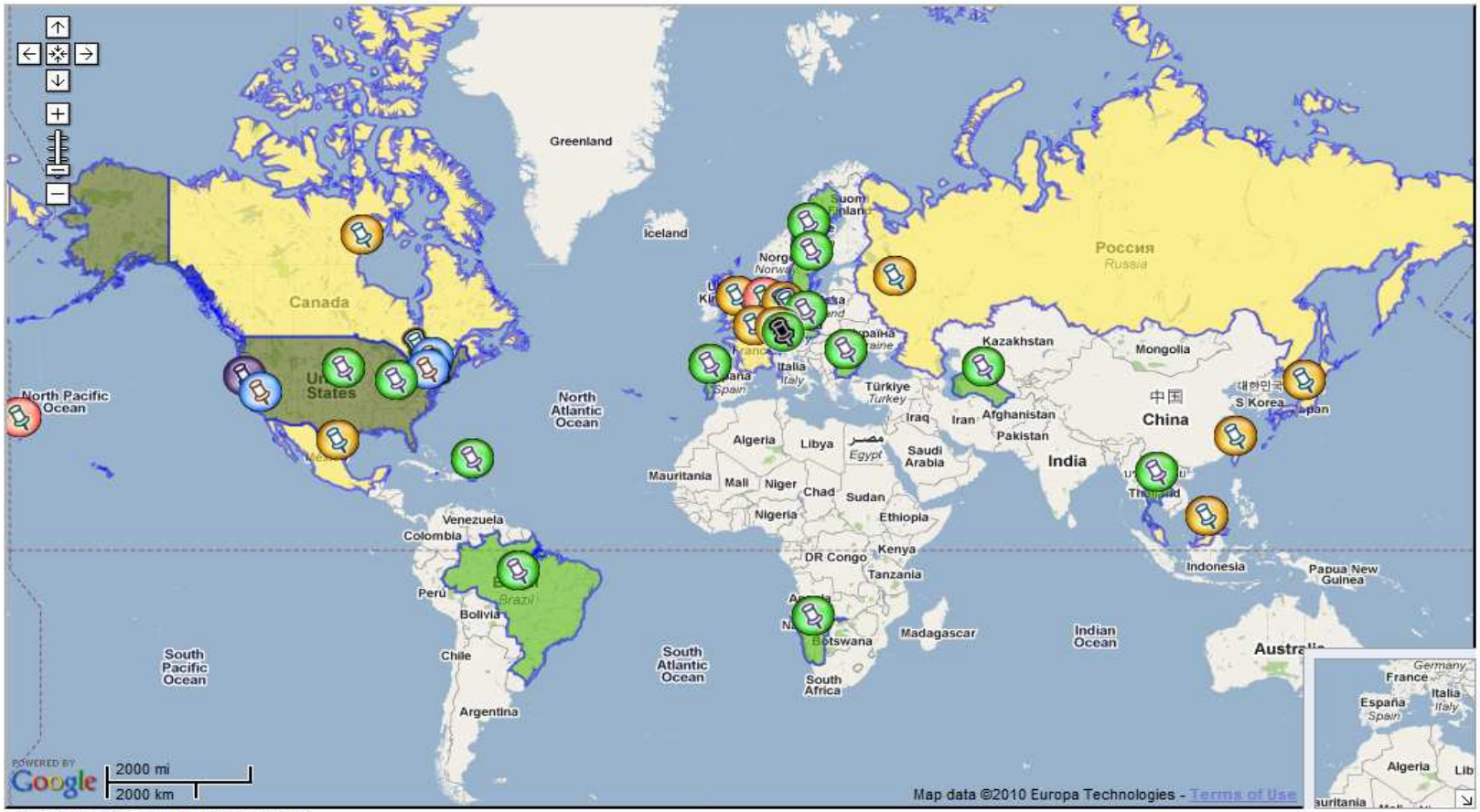


Deployment Update

- Quellen
  - https://www.dnssec-deployment.org/
  - http://ccnso.icann.org/surveys/dnssec-survey-report-2009.pdf
- .org: 2009/07
- .na: 2009/07
- .tm: 2009/09
- Alles unter .gov sollte mit Ende 2009 signiert sein. (20% haben es geschafft)
- .pt: 2010/01
- .ch/.li: 2010/02
- .edu: 2010/04
- .us/.biz: Q2 2010
- .nl: 2010/08
- .jp: 2010/12

nic.at
the austrian registry

Status 2010/02

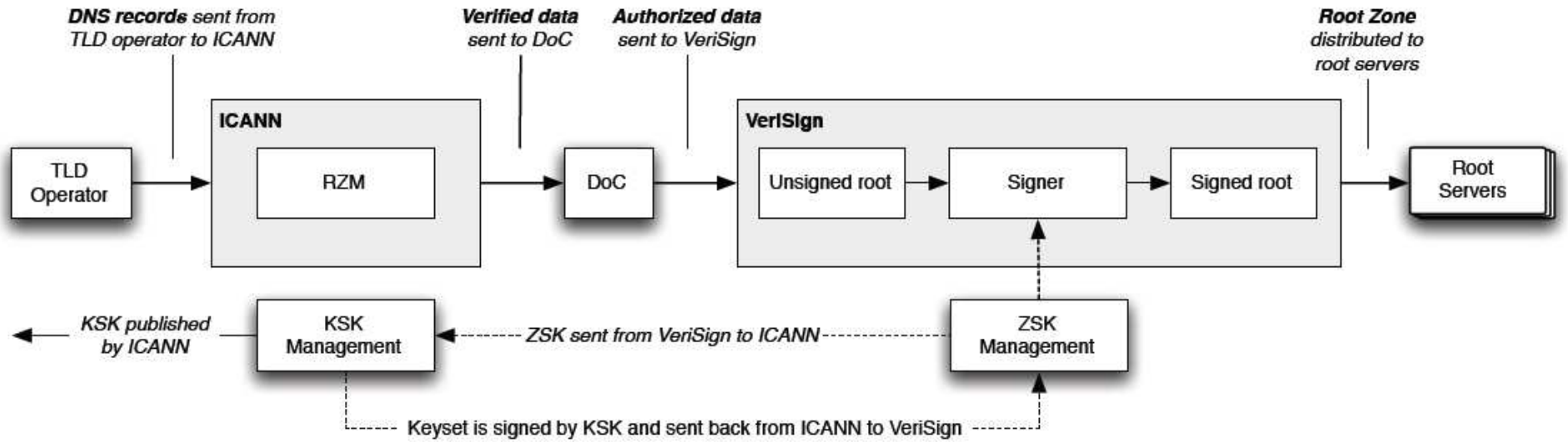


This map was created by Paul Wouters

2010: Das Jahr in dem „.‘ signiert wurde

- Langer (politischer) Streit um „wer hat die Keys der Root“
- 3. Juni 2009: Einigung
  - http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
  - ICANN hat KSK
  - DoC macht weiterhin Freigabe von Changes
  - Versign hält den ZSK und signiert
- http://www.root-dnssec.org/
  - http://www.root-dnssec.org/wp-content/uploads/2009/12/rootsign-ietf76-infosession.pdf

Setup Overview




nic.at
the austrian registry

.at

Policy Side

- Das Protokoll ist komplex, aber beherrschbar
- Die Software wird laufend besser

- Aber: Welche Grundannahmen des DNS-Business kollidieren mit DNSSEC?

Sicherheit vs. Verfügbarkeit

- Plain DNS ist robust
  - Sehr fehlertolerant.
  - Oft komplett auf Autopilot.
- DNSSEC ist spröde
  - Ein falsches Bit und die Zone ist offline.
  - Kompetentes Operating nötig.

Caching

- Bekanntes Problem:
  - Vor Änderungen TTL runtersetzen
- Mit DNSSEC deutlich böser:
  - Bei allen Änderungen (key rollover, …) muss man bedenken, welche alte DS und DNSKEY Records noch in den Caches sind.
  - DNSSEC abschalten geht nicht einfach so.

Registrarmodell

- Registry
- Registrar
- Registrant

- Wo ist da der Nameserverbetreiber?

Woher kommt der DS Record?

- Wer erzeugt den DNSKEY?
- Wer kann mit der Registry sprechen?

- Technisch einfach:
  - Erweiterung von EPP (RFC4310)
- Aber sonst?
  - Rechtliches (Haftung!)
  - Process?
  - Soll die Registry gemeldete DS testen?

Registrarwechsel?

- Unterstützt der neue DNSSEC?
- Rolle für die Registry?
  - DNSSEC Support vorschreiben?
  - Transfer verhindern?
  - Anderweitig reingreifen?

NS-Operator Wechsel

- NICHT Registrar-Wechsel!
- Ziel: Zone durchgehend signiert
  - Das ist NICHT trivial.
  - Geht ohne Kooperation des alten nicht

Beispiel

- Step 1:
  - Losing and Gaining include both of sets of ZSK keys in their DNSKEY RRset.
  - Losing DNSKEY RRSET:
    - Losing KSK
    - Losing ZSK
    - Gaining ZSK
  - Gaining DNSKEY RRSET:
    - Losing ZSK
    - Gaining KSK
    - Gaining ZSK
- Step 2:
  - Parent adds Gaining KSK to DS, listing both KSKs
- Step 3: (actual transfer) (wait at least 1 DS TTL)
  - Parent updates NS from losing NS-set to gaining NS-set.

Packet Sizes

- RFC 1034 sagt UDP bis 512 Byte
- Das reicht für DNSSEC nicht
  - EDNS0: Client sagt, er kann mehr
    - UDP bis MTU
    - Fragmentiertes UDP
    - RFC2671, 1999. Kein universelles Deployment
  - Fallback to TCP

- Tests:
  - https://www.dns-oarc.net/oarc/services/replysizetest
  - http://k.root-servers.org/replysizetest
    - Ganz neu: http://labs.ripe.net/content/measuring-dns-transfer-sizes-first-results
  - http://netalyzr.icsi.berkeley.edu/

- Legacy Firewall Rules
  - DNS per TCP überhaupt erlaubt?
  - Fragmentierte UDP Paket?
  - Obsolete „intelligente“ Regeln

Kriterien

- EDNS0_Size
  - positive integer, the buffer size advertised by EDNS0
- DO_DNSSEC
  - boolean, the DO flag indicating DNSSEC support by the resolver
- Min_Response_Size
  - integer, the minimum (after dropping unnecessary RR) size of the DNS response sent by the authoritative server
- Clean_path_for_fragments
  - boolean, indicates that UDP fragments can travel from the authoritative name server to the resolver
- Clean_Path_For_EDNS0
  - boolean, indicates that EDNS0 responses (which may be larger than 512 bytes) can travel from the authoritative name server to the resolver
- Can_TCP
  - boolean, indicates that the resolver can ask through TCP (which implies a clean TCP patch and an authoritative name server which accept TCP)

- http://www.bortzmeyer.org/files/dns-size-pseudocode.txt

DURZ

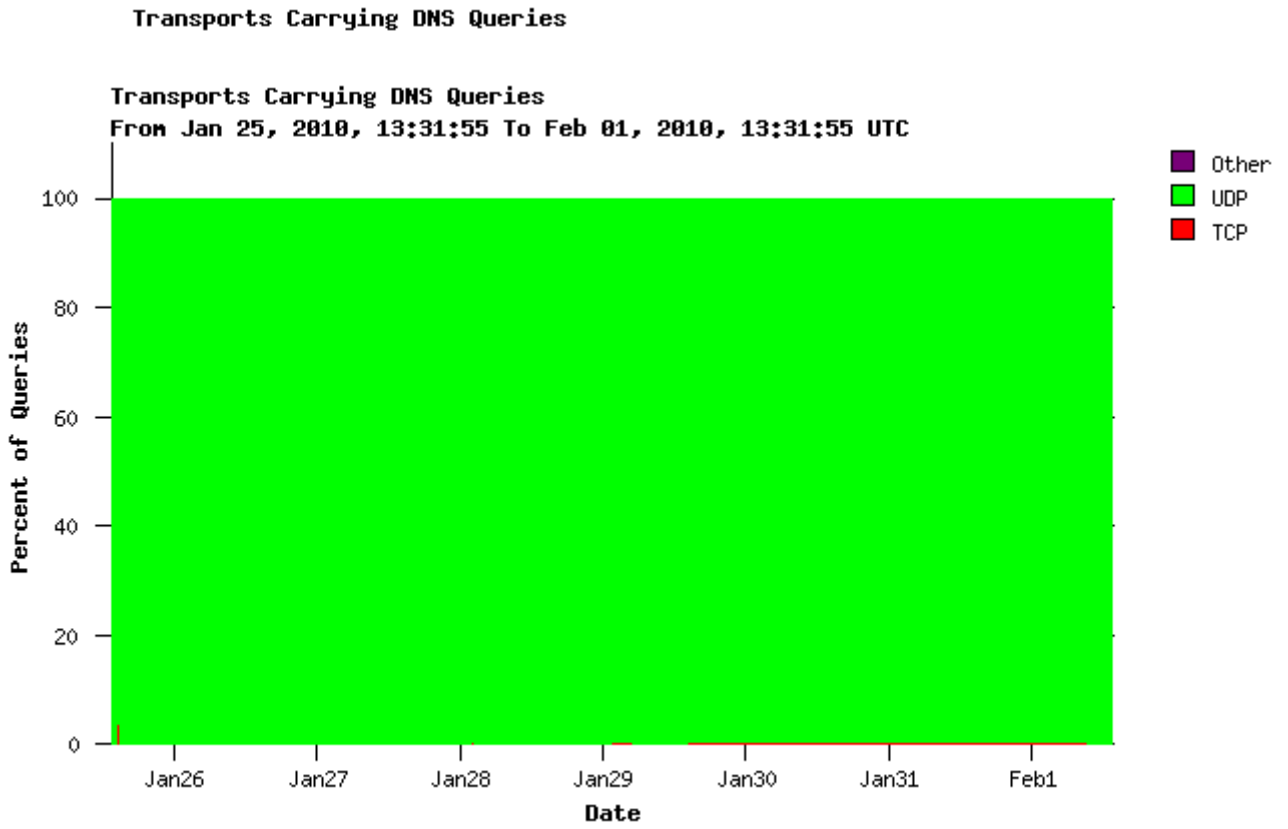
- Die Root ist nicht ganz unkritisch.
  - *hüstel*
- Schrittweises Deployment
  - Genug Zeit zum Beobachten, wie alles funktioniert.
    - Packet size issues
    - TCP fallback
  - Abbruch muss möglich sein
- deliberately unvalidatable root zone: DURZ

l.root-servers.net ist signiert

```
$ dig DNSKEY . @l.root-servers.net +dnssec

.                       86400   IN      DNSKEY  256 3 8 AwEAAa1Lh+++++++++++++++
+THIS/IS/AN/INVALID/KEY/AND/SHOU LD/NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/OR
G/FOR/MOR E/INFORMATION++++++++++++++++++++++++++++++++++++++++ +++++++8
.                       86400   IN      DNSKEY  257 3 8 AwEAAawBe+++++++++++++++
+THIS/IS/AN/INVALID/KEY/AND/SHOU LD/NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICANN/DOT/OR
G/FOR/MOR E/INFORMATION++++++++++++++++++++++++++++++++++++++++ ++++++++++++
++++++++++++++++++++++++++++++++++++++ ++++++++++++++++++++++++++++++++++++
++++++++++++++++++ ++++++++++++++++++++++++++++++++++++++++++++++++++++ ++
++++++++8=
.                       86400   IN      RRSIG   DNSKEY 8 0 86400 20100214235959
20100131000000 19324 . v2DVoP16w3dqsOooCxAb393ExF6p1t3d3qJsYPkeV96/t3HIuVLnxpbV
02Wx+BR7dwLiURASmebvEhZrR4gNqO15M5gerrzDdY0IXA0q0xVAUj/J NvkdiniXjoQYGUwjJsdfqxv
D7NQPtSz4YTuOvMlVffV1F2Bc6Woid7AK JGkb24MeQlAMy/gQqcLPs6c3a9RvZEwofMul66bUswGS+Y
sL8x9A6Cbt 1bdyhRUNYSl7AifA4++Pu+0MLpbrxH7DLI8O9ZfCA3LsEQUOFjYA+2jJ mzgFqZAU0Hvx
eQyStnLF3/bf7qifRegrn6+cTKjKtUZ52/kUFiaqgT2t 9TemTg==
```

Erste Erfahrungen



nic.at
the austrian registry

DNSSEC für den NS-Betreiber

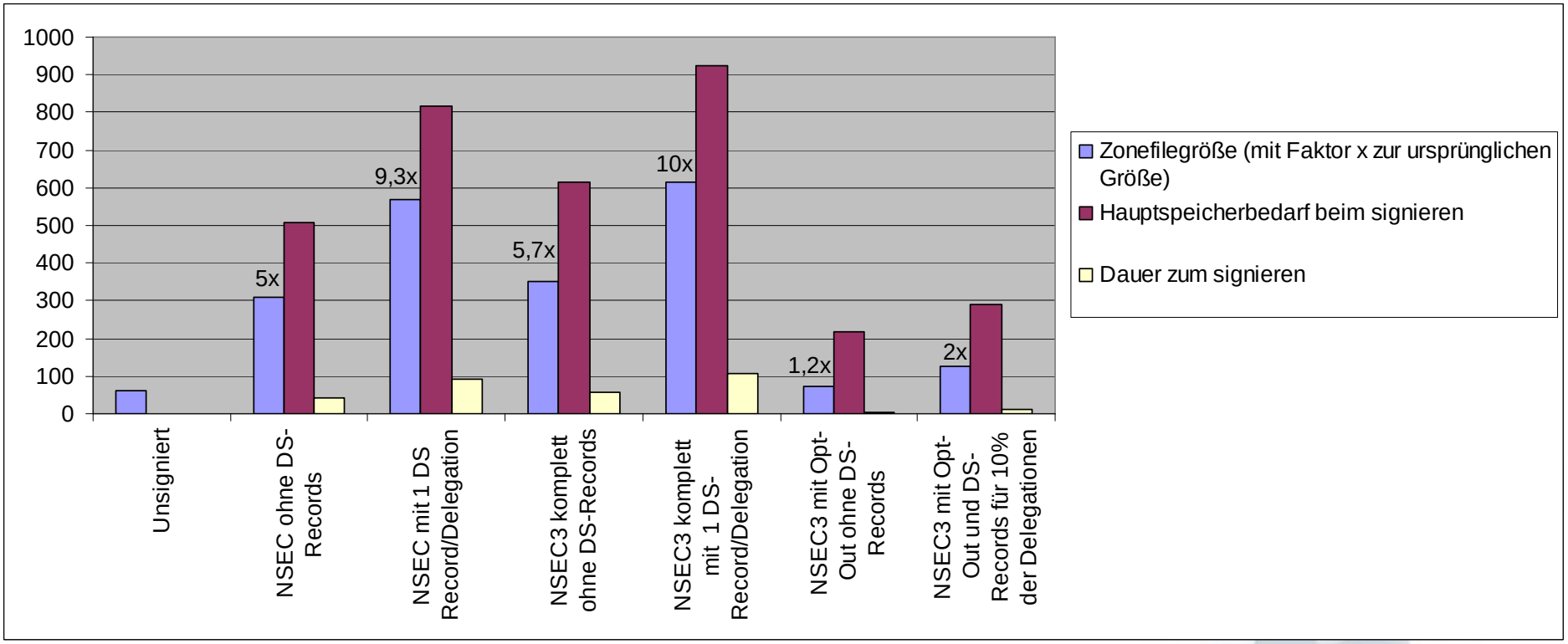
- Software support?
- Wie groß wird das Zonefile?
- Wo signiere ich?
- Key-Management
- Security der private keys?
  - Anforderungen wie an eine CA?
  - HSM
  - Pure Software-Lösungen

Emergency Procedures

- Key Compromise
  - Emergency Rollover
- Probleme im Zonefile?
  - Siehe .se
  - Zonefiles in Reserve
- Notfallsplanung nötig, da komplexe abhängigkeiten.

Vergleich Zonefilegröße

- Ausgangsfile: .AT-Zone mit ca. 60MB



ISP Recursors

- Last am Server
- Helpdesk Schulung
- Was tun, wenn wichtige Zone Probleme mit DNSSEC hat?

Software

- Open Source
  - NSD
  - Bind 9.6: raw support
  - Bind 9.7: „DNSSEC for Humans“
  - Unbound
  - OpenDNSSEC
- Closed Source
  - PowerDNS
  - Secure64
  - …
- Bugs sind noch einige zu erwarten

Warnung!

- Schlüsselverwaltung ist Neuland für den typischen ISP / Registrar / Webhoster.
- Manuelle Prozesse funktionieren nicht!
- Gute Tools nötig
- Auch für debugging
- Schulungen!

Kommerziell?

- Erfahrungen aus Schweden
  - Mehr Geld dafür verlangen funktioniert nicht.
- Tschechien
  - Einfach für alle Kunden aufdrehen.
- USA / .gov
  - Vorgeschrieben.
- Neue TLDs
  - ICANN verlangt DNSSEC support.

Business-case?

- DNSSEC ist kein Selbstläufer
- Kosten/Nutzen
  - Typische Privatdomain
  - e-Commerce
- Was kann ich an DNSSEC in Zukunft anhängen?
  - Ersatz für X.509?
  - ….

DNSSEC in .at

- http://www.nic.at/uebernic/aktuelles/nicat_und_dnssec/

- nic.at verfolgt die Entwicklung
- Interne Vorbereitungen
- Kein Zeitplan zur Einführung

- Die Minen soll wer anderer wegräumen.

nic.at
the austrian registry

Fragen?