babiel

# Hands-on DNSSEC

**Armin Pech** ‹a.pech@babiel.com›

**Babiel GmbH**

`dig 19.03.2016. @chemnitzer.linux-tag.de`

# Agenda

- Überblick & Funktion
- Hands-on #1
- DNSSEC nutzen
- DNSSEC verwalten
- Hands-on #2
- Q&A, Diskussion

# Überblick: Warum DNSSEC ?

- **Sichere DNS-Auflösung**
  - Authentizität: MITM, Spoofing erkennen
- **Abwärtskompatible Erweiterung**
  - Transparente Integration
  - DNS-Konzept erhalten
- **Key Authentication (DANE, SSH, …)**
  - Publikation von Key Fingerprints
- **Warum jetzt?**

# Überblick: DNSSEC Historie

- 1999: Publikation RFCs
- 2010: Aktivierung auf Root-Servern
- 2011: DeNIC implementiert DNSSEC
- 2015: - 84% TLDs mit DNSSEC
  - 42.000 .de Domains signiert

# Überblick: Was es (nicht) ist

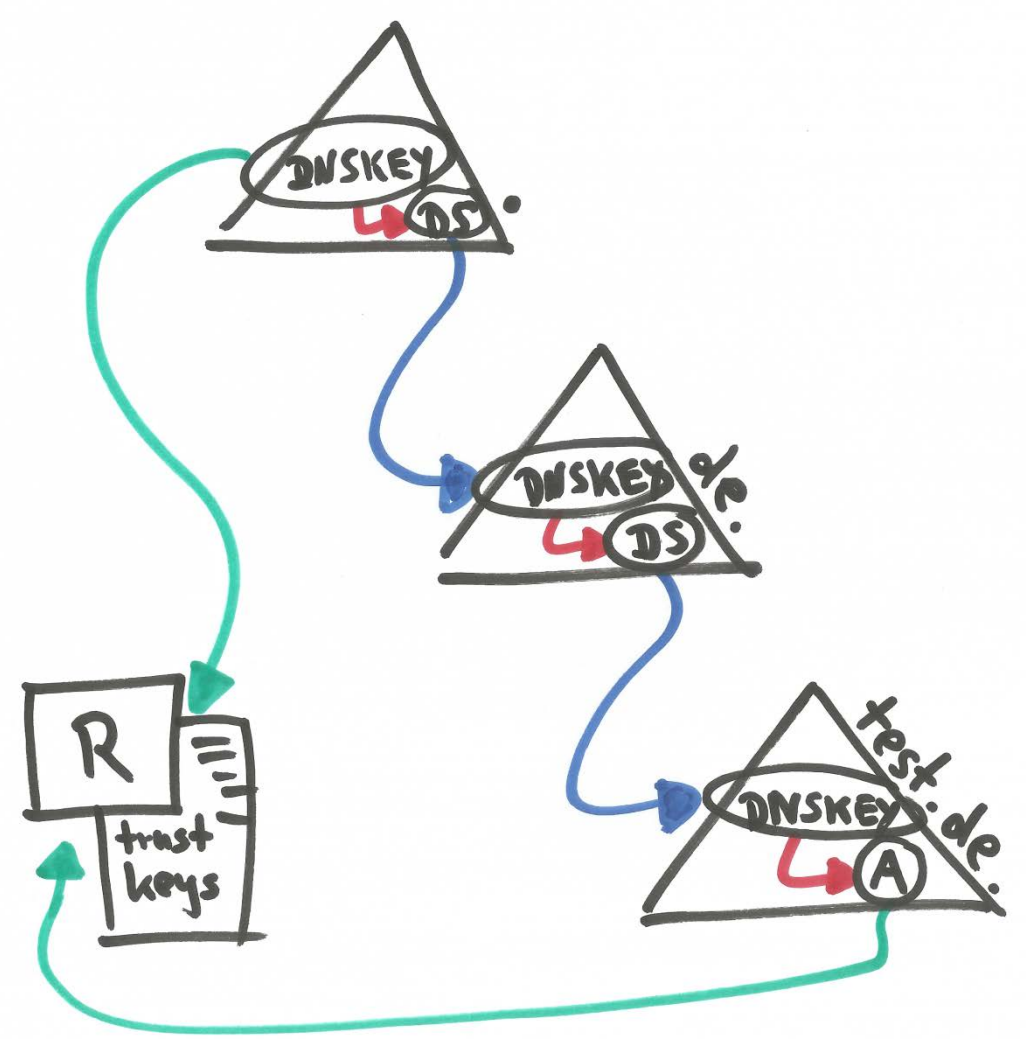
## DNS Security Extensions

- **Echtheit von Daten gewährleisten**
  - Asymmetrische Schlüssel / Signaturen
- **Keine verschlüsselte Übertragung!**
- **Neue Records: DNSKEY, RRSIG, DS, NSEC**
- **Zone immer vollständig signiert**
- **DNSSEC kein Zwang**

# Funktion: DNSKEY, RRSIG

- **DNSKEY: Öffentlicher Schlüssel**
  - Validierung von Signaturen
  - Key-Tag zur Identifikation
  - Typen: KSK & ZSK
- **RRSIG: Resource Record Signature**
  - Private Key signiert RRSet
  - Mitgeliefert zum angefragten Record

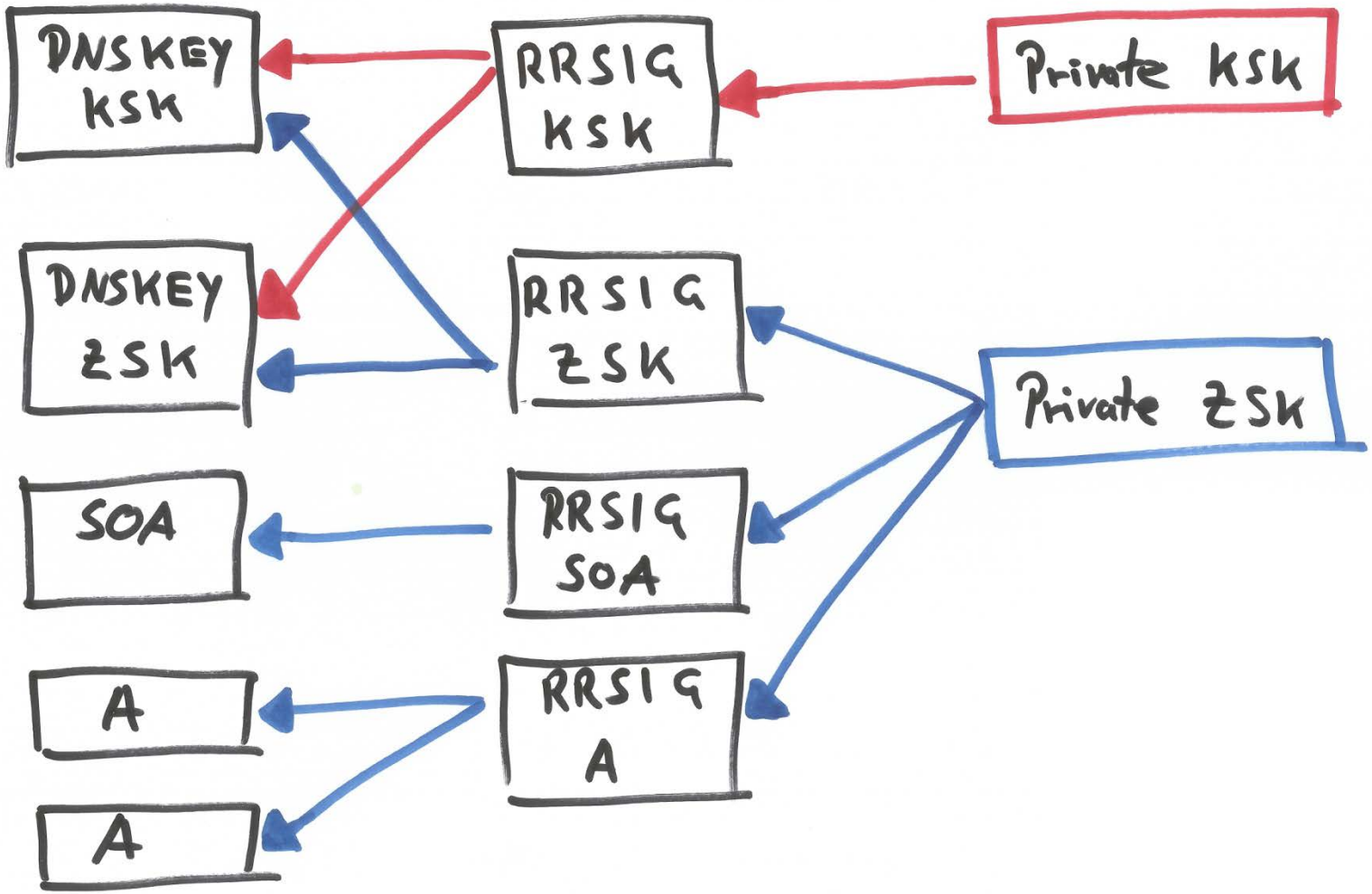
# Funktion: Chain of Trust



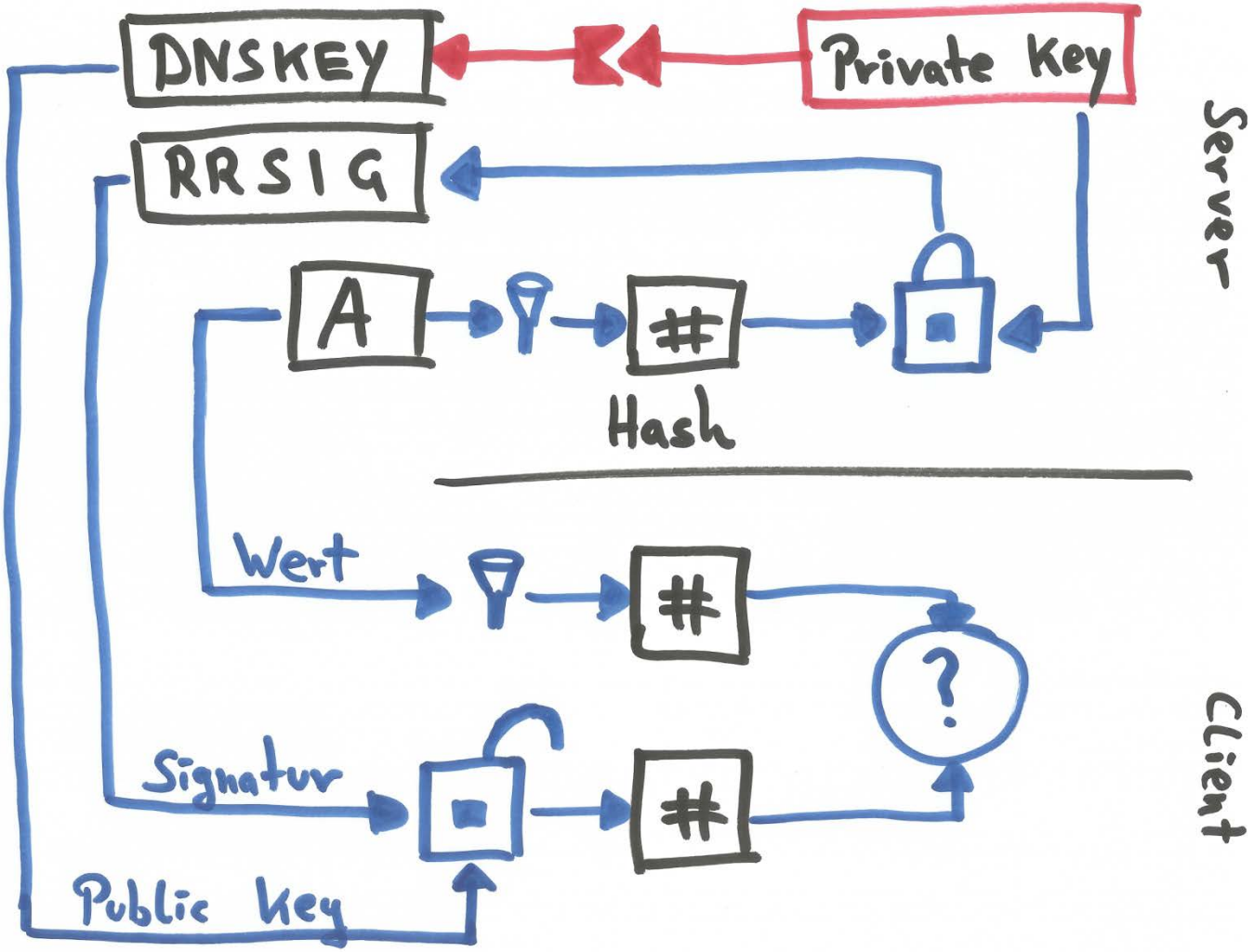
# Funktion: Key authentifizieren

- **Resolver prüft DNSKEY**
- **Automatische Authentifizierung**
  - Keys der Rootserver (Trust Anchor)
  - DS aus Parent
  - DNSKEY aus Zone
- **Trusted vs. Managed Keys**
- **Caching von RRSET + DNSKEY zusammen**

# Funktion: DNSKEY Typen



# Funktion: DNSKEY, RRSIG



# Funktion: DNSKEY, RRSIG

```
$ dig -t DNSKEY de. @a.nic.de. \
      +dnssec +noall +answer +multi

de.   7200   IN   DNSKEY   256 3 8 (
      AwEAAYjFWYHsE5sTvfaYnmWZ910K9+Q/ViOwF [...]
) ; ZSK; alg = RSASHA256; key id = 39669

de.   7200   IN   DNSKEY   257 3 8 (
      AwEAAYbcKo2IA8l6arSIiSC+l9vgNXrxjBJK+ [...]
) ; KSK; alg = RSASHA256; key id = 24220

de.   7200   IN   RRSIG    DNSKEY 8 1 7200
20151119120000 20151029120000 24220 de.
LZiw5R6wC6U8HSfPTgUtxyT69bRbC9uuQCs [...]
```

# Funktion: Key Signing Key

- **Signiert nur DNSKEYs**
  - Alle ZSKs und KSKs
- **Flag ID 257**
  - Secure Entry Point (SEP)
- **Starker Key: 2048 Bit RSA/SHA-256**
- **Nutzungsdauer ~1-3 Monate**
- **Delegation Signer in Parent**
  - Wartungsintensiv

# Funktion: Zone Signing Key

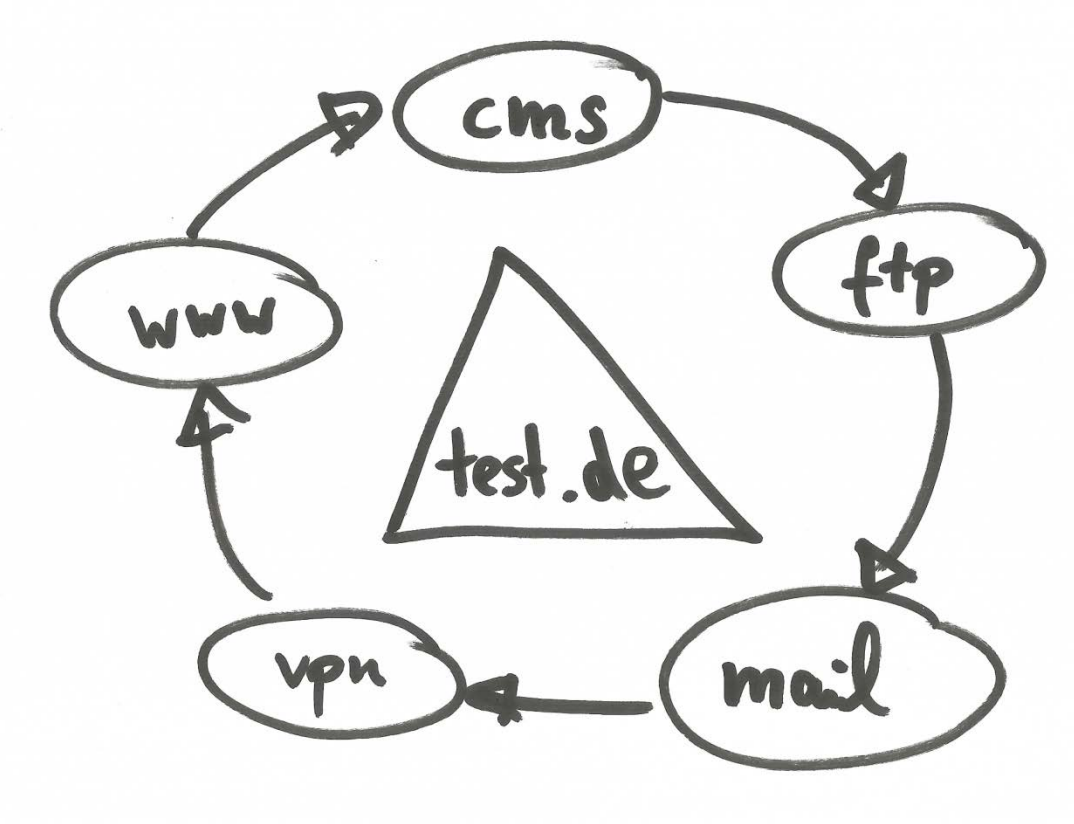
- **Signiert alle Records**
- **Flag ID 256**
- **Schwacher Key: 1024 Bits RSA/SHA-256**
- **Schnelle Signatur-Validierung**
- **Kurze Nutzung ~21-40 Tage**
  - Angriffe unattraktiv
- **Automatischer Austausch und Deployment**

# Funktion: Delegation Signer

- Hash vom DNSKEY (KSK)
- Authentifiziert DNSKEY einer Subdomain
- Eintragung in Parent => Vertrauensstellung
- `de. 86400 IN DS 24220 8 2 FFE926ACA […]`
- `name ttl IN DS key#tag algo #type hash`

# Funktion: Next Secure

- Gibt es einen Namen nicht?



# Funktion: Next Secure

- **NSEC**
  - Sichert NXDOMAIN
  - Verkettet alle Namen / Zone Walking :-(
  - NSEC3: Nachfolger mit Hashing
- **NSEC3PARAM**
  - Hashing Parameter für NSEC3
  - `de. 0 IN NSEC3PARAM 1 0 15 BA5EBA11`

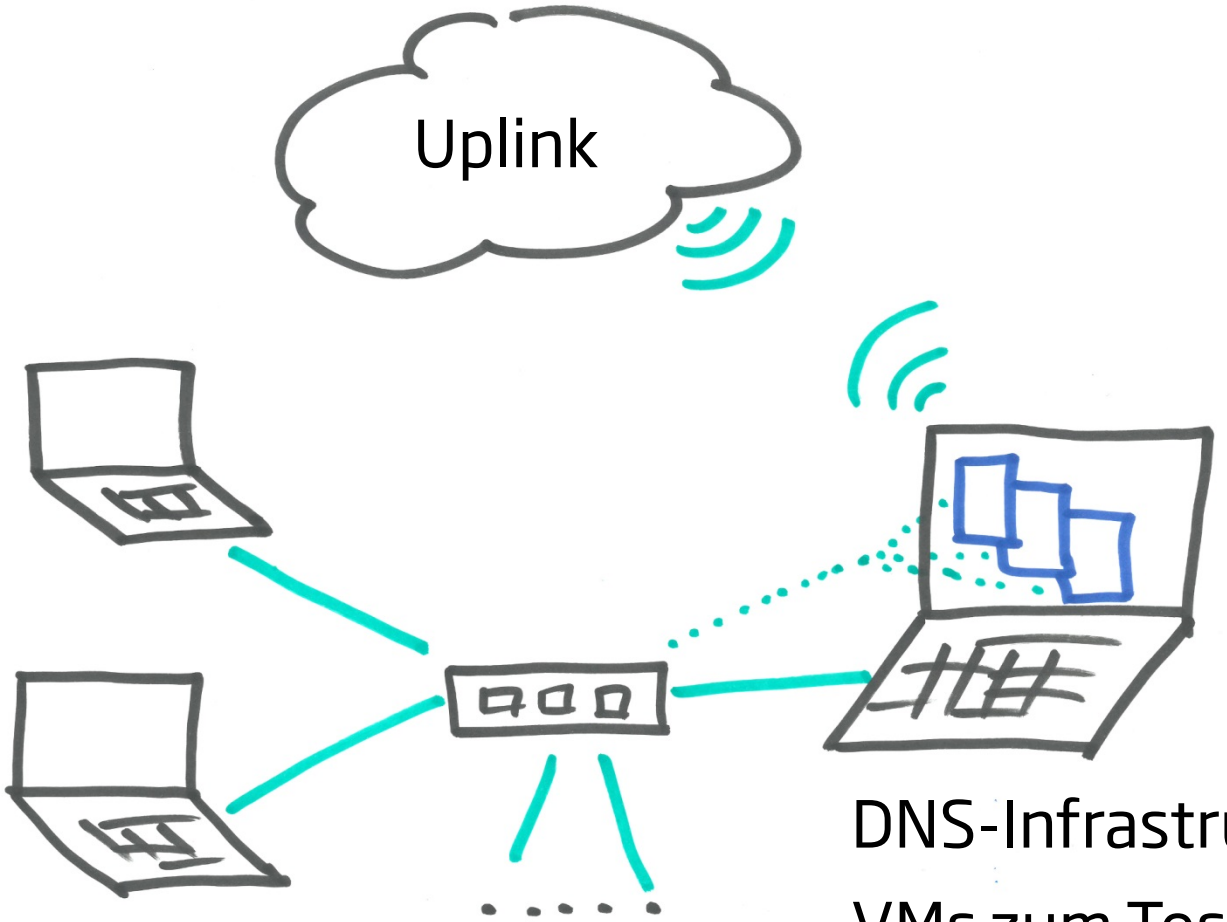
# Funktion: Neue DNS Header

- **CD – Checking Disabled**
  - Request: Client wünscht keine Validierung
  - Unsicherer Response möglich
- **DO – DNSSEC OK**
  - Resolver versteht DNSSEC-Records
- **AD – Authenticated Data**
  - Response: Alle Records authentisch

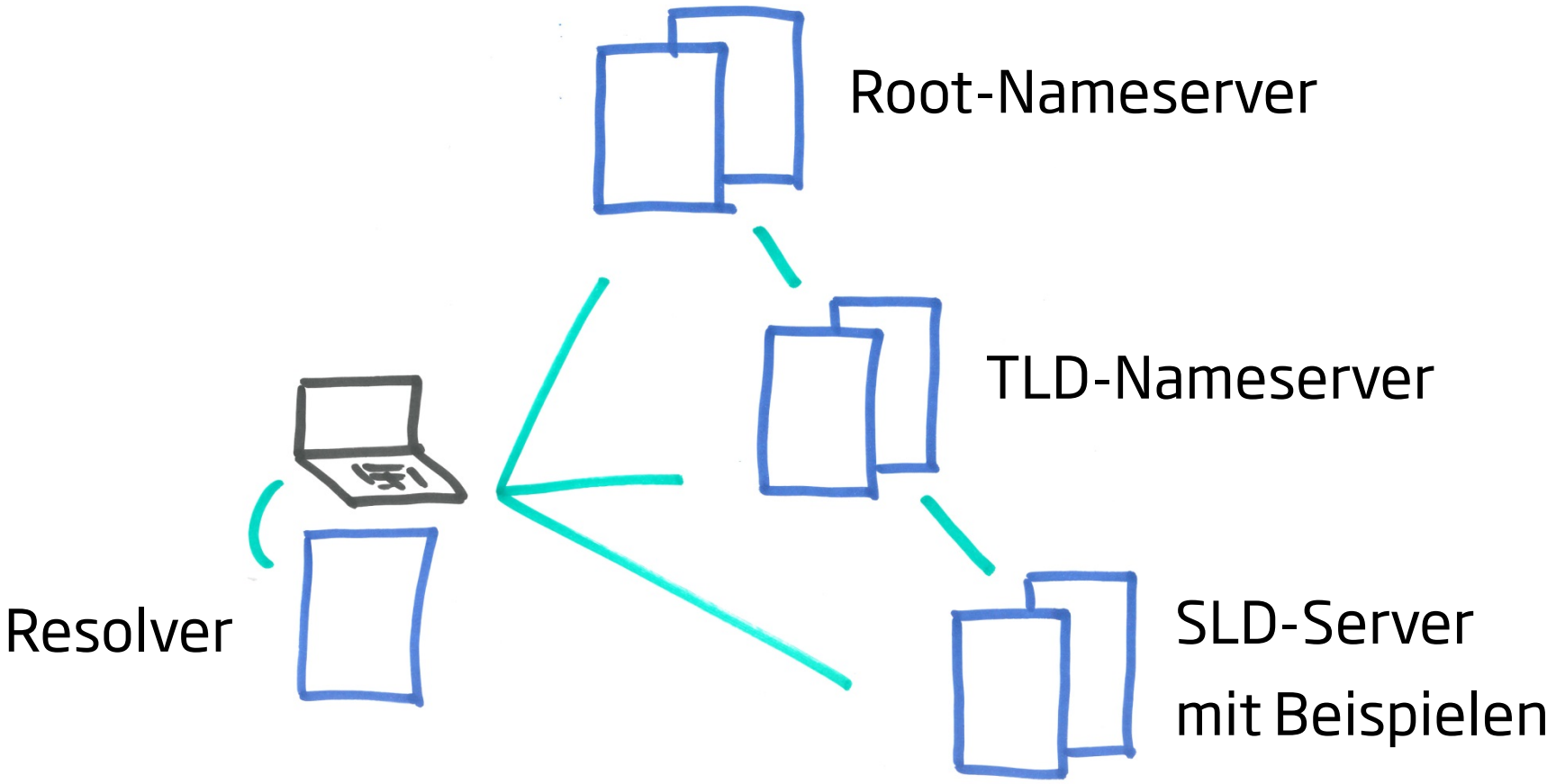
# Voraussetzungen

1. TLD/Registry
2. Registrar
3. Schlüssel-Management, Key-Server
4. Nameserver
   - In-Line Signing Feature (BIND)
5. EDNS
6. TCP-Fallback
7. Auslastung: CPU, RAM, Traffic

# Workshop Umgebung



# Workshop Infrastruktur



# Hands-on DNSSEC #1

- Informationen und Setup des Workshop
- Umgebung erkunden
- DNSSEC Informationen abfragen
- Eigene Domain anlegen
- DNSSEC für Domain einrichten

# Setup: BIND konfigurieren

- server { }
  - edns yes;  # default
  - edns-udp-size 4096;  # default
- options { }
  - dnssec-enable yes;
  - key-directory "/etc/bind/keys";
  - dnssec-update-mode maintain;  # default
  - dnssec-loadkeys-interval 60;  # default/hours
  - sig-validity-interval 21 7;  # default/days

# Setup: BIND konfigurieren

- `zone "babiel.eu" IN { }`
  - `type master;`
  - `file "/etc/bind/pri/babiel/babiel.eu.zone";`
  - `auto-dnssec maintain;`
  - `inline-signing yes;`
- **Neu laden**
  - *`$ rndc reload`*
- **Zone ohne DNSSEC**
  - Verhalten unverändert – kein AD-Flag

# Setup: Keys einbinden

- Key Signing Key generieren
  - `$ dnssec-keygen -n ZONE -f KSK \`
    `-a RSASHA256 -b 2048 \`
    `-K /etc/bind/keys babiel.eu`
- Zone Signing Key generieren
  - `$ dnssec-keygen -n ZONE -3 \`
    `-a RSASHA256 -b 1024 \`
    `-K /etc/bind/keys babiel.eu`
- Key eintragen, Zone signieren
  - `$ rndc sign babiel.eu`

# Setup: Key Metadaten

**Filenames:** `Kzone+alg+tag.{key|private}`

Kbabiel.eu.+008+18249.key [ *Kbabiel.eu.+008+18249.private* ]

```
; This is a zone-signing key, keyid 18249, for babiel.eu.
; Created:  20151031212215 (Sat Oct 31 22:22:15 2015)
; Publish:  20151031212215 (Sat Oct 31 22:22:15 2015)
; Activate: 20151031212215 (Sat Oct 31 22:22:15 2015)
; Inactive: 20151104190648 (Wed Nov  4 20:06:48 2015)
; Delete:   20151104210648 (Wed Nov  4 22:06:48 2015)
babiel.eu. 86400 IN DNSKEY 256 3 8 AwEAAdPS0s0lFFl+Ba […]
```

# Setup: NSEC3 einrichten

- **Records mit Next Secure + Hashing sichern**
  - *$ rndc **signing -nsec3param** 1 0 20 $(openssl rand 4 -hex) babiel.eu*
    - 1: SHA1
    - 0: Opt-Out deaktivieren
    - 20: Hashing Iterationen
    - $(): Generierung HEX-Salt
    - Domain
  - info: zone babiel.eu/IN (signed): zone_addnsec3chain (1,CREATE|OPTOUT,20,44DB2B21351CC10E)

# Setup: Records aktualisieren

- Originales Zone-File weiter verwenden
- BIND pflegt Unsigned und Signed Files
- Einfach Records wie vorher ändern
- RRSIG, NSEC3 automatisch aktualisiert
- Key Management über `dnssec-settime`

# Setup: Going Live per DS

- **Delegation Signer von KSK an Parent**
  - DNSKEY oder DS via Registrar
  - `$ grep DNSKEY Kbabiel.eu.+008+29305.key | \`
    `cut -d ' ' -f 8- | tr -d ' '`
  - `$ dnssec-dsfromkey Kbabiel.eu.+008+29305.key`
  - whois/Nameserver von Registry aktualisiert
    - babiel.eu – Keys:
      - flags: KSK
      - protocol: 3
      - algorithm: RSA_SHA256
      - pubKey: AwEAAaxds7l09cz4m0iL1zoPwV6iGxea8Er [...]

# Setup: Keys & DS prüfen

- *$ dig +dnssec +sigchase -t A www.babiel.eu*
- *$ drill -S www.babiel.eu*
- http://dnsviz.net/d/www.babiel.eu/dnssec/
- http://dnssec-debugger.verisignlabs.com/www.babiel.eu

# Funktion: Debugging per CMD

- DNSKEYs der Rootserver als Trust Anchor

```
$ dig +noall +answer -t DNSKEY . >trusted-key.key
```

- DNSSEC Validierung anfragen

```
$ dig +dnssec –t NS .      # ggf. Answer Flag AD
```

- Delegation & Signaturen prüfen

```
$ dig +dnssec +sigchase +topdown –t A babiel.eu
$ drill –S babiel.eu
```

- EDNS und TCP Support testen

```
$ dig +edns=0 +noall +comments -t SOA babiel.eu
$ dig +tcp -t SOA babiel.eu
```

# Nutzen: SSH Keys

- Host Key authentifizieren
- OpenSSH: Client prüft
  - `VerifyHostKeyDNS yes`
- Fingerprint erstellen
  - *`$ ssh-keygen -r ssh.babiel.eu.`*
  - `ssh.babiel.eu. IN SSHFP algo fptype fprint`

# Nutzen: DANE & TLSA

## DNS-Based Authentication of Named Entities

- **Richtlinien für Zertifikate & CAs**
  - Ports, Protokoll, CA, CN korrekt?
- **TLSA-Record mit Key Fingerprint**
  - *$ openssl x509 -in www.babiel.eu.crt *
    *-outform DER | sha256sum*
  - `_443._tcp.www.babiel.eu. IN TLSA 3 1 1 df4d7c947fed35a5b3a56df0f5ad6 […]`

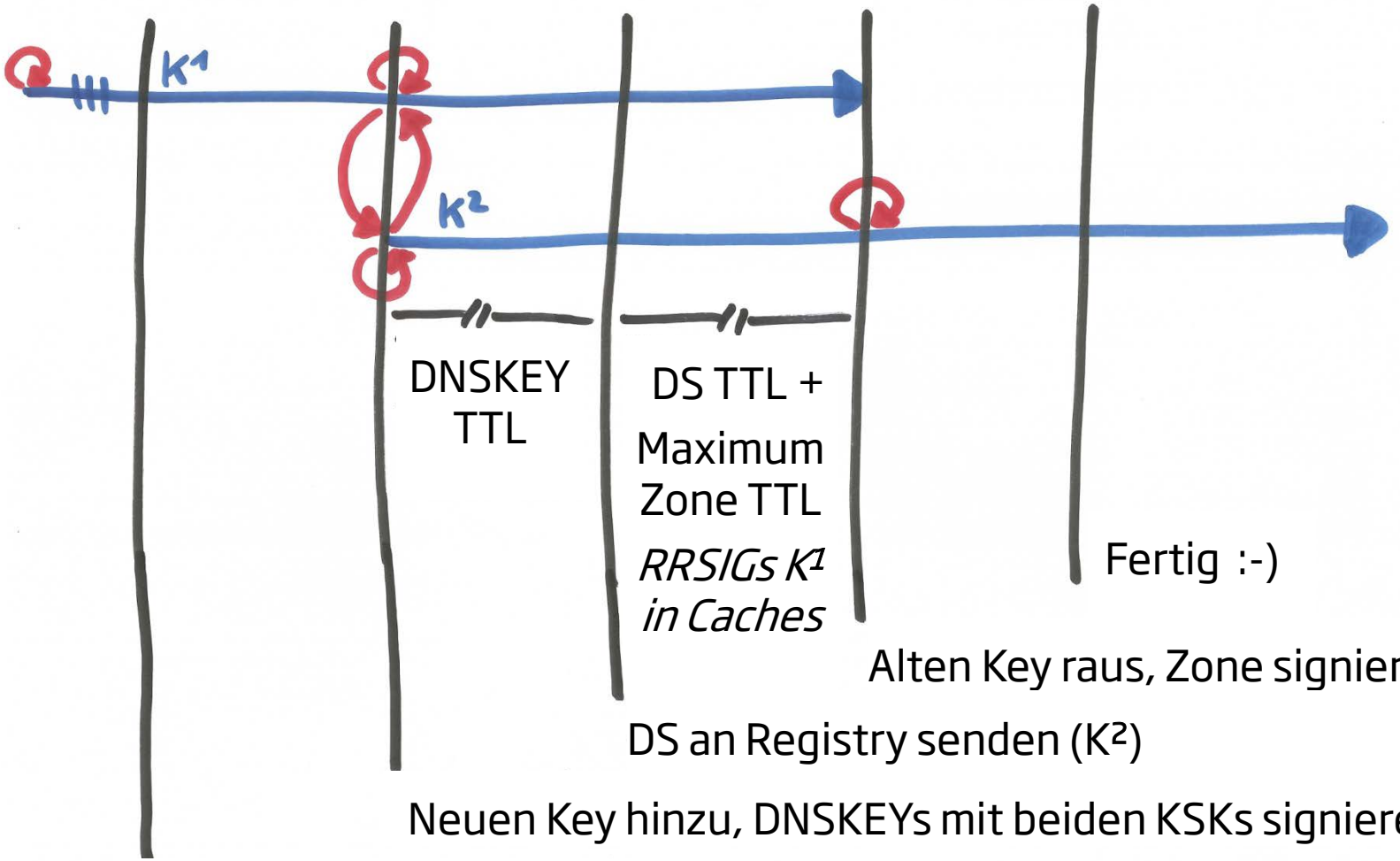
# Nutzen: Mailing

- **GPG Key als TXT-Record**
- **Mailing Settings authentifizieren**
  - SPF
  - DKIM, DMARC
- **Postfix: SSL-Zertifikate prüfen**
  - `smtpd_use_tls = yes`
  - `smtp_tls_security_level = dane`
  - `smtp_dns_support_level = dnssec`

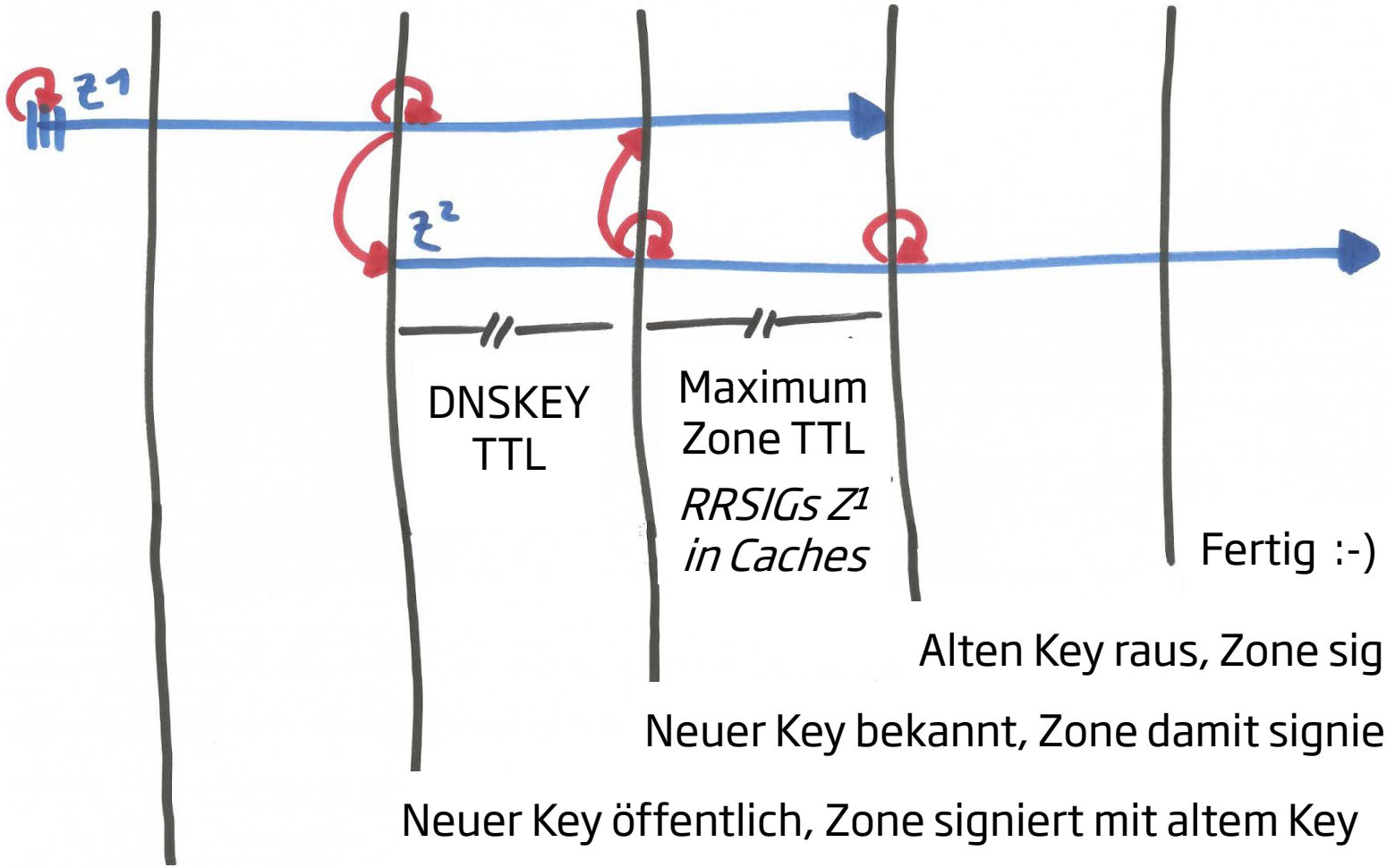
# Funktion: Key Rollover

- **Key-Tausch üben**
- **KSK: Double Signature**
  - 1x whois Update bei Registry
  - Dauer: DS + DNSKEY TTL – 2 Keys aktiv
- **ZSK: Pre-Publication**
  - Geringer Speicherbedarf, schnelles Signing
  - Dauer: 2x DNSKEY TTL – 1 Key aktiv

# Funktion: KSK Rollover



# Funktion: ZSK Rollover



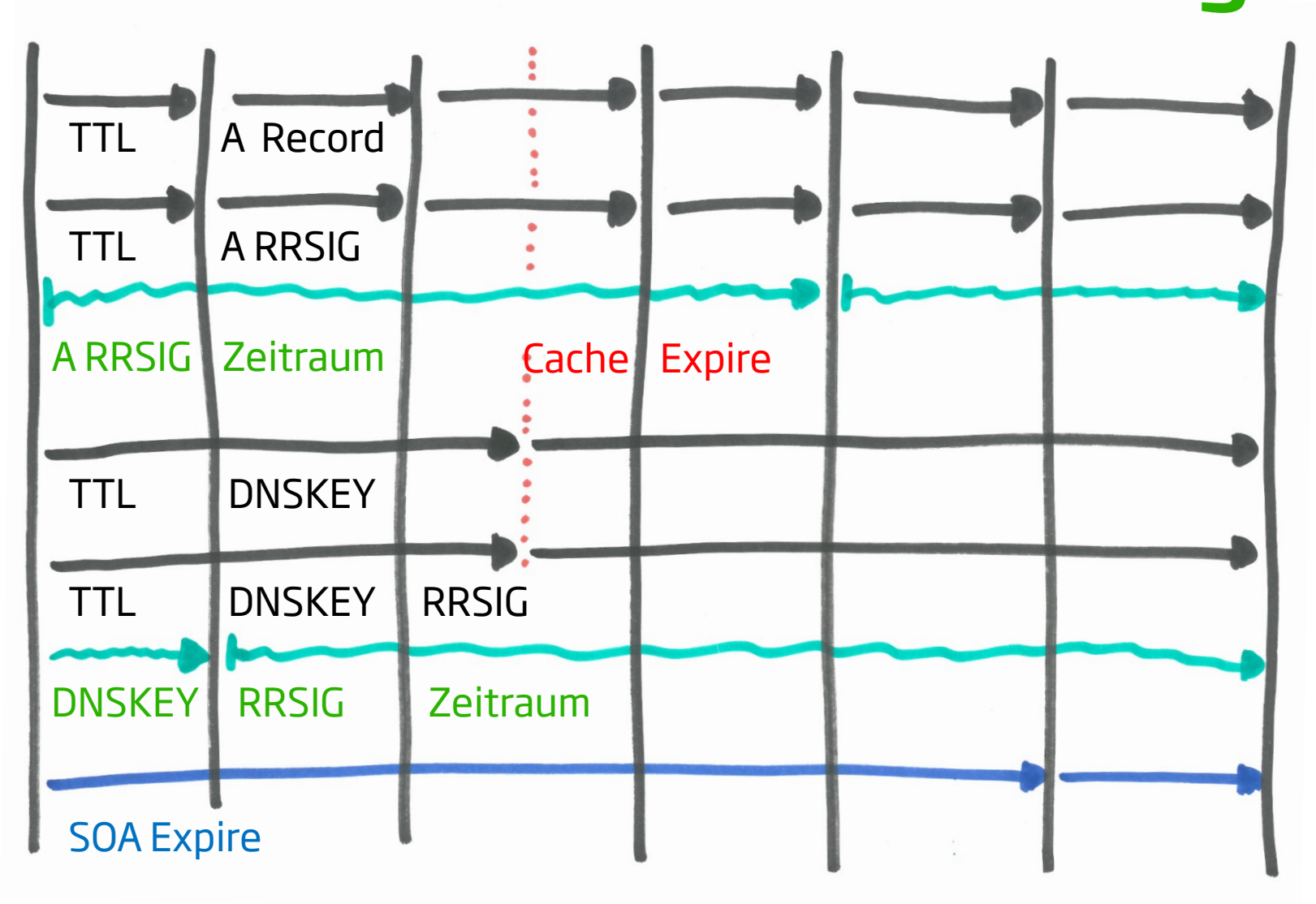
# Setup: Key Rollover

- Neuer Key mit Publication + Activation Date
  - `$ dnssec-keygen [...] -P now -A +1d babiel.eu`
- Alter Key: Update Inactivity + Deletion Date
  - `$ dnssec-settime -I +1d -D +2d Kbabiel.eu*.key`
- BIND lädt Keys automatisch
- Bei KSK: DS in TLD aktualisieren!
- Optimal: Alle Dates beim keygen setzen
- Automatisierung (rollerd, Scripts)

# Funktion: DNSSEC Tuning

- **Single-Type Signing Scheme (CSK)**
  - Optimal wenn DS-Update automatisiert
  - DNSSEC Payload kleiner
  - `zone "babiel.eu" IN { update-check-ksk no; }`
  - Rollover per Double Signature
- **Elliptic Curve Algorithmus** (ECGOST / ECDSA)
  - RRSIG + DNSEKY kürzer
  - Signieren schnell (Validierung langsam)

# Funktion: DNSSEC & Timing



# Setup: TTL Einstellungen

- **Alle TTLs > 30 Sekunden**
  - Validierung: RRSIG muss zu RRSet passen
  - Auslastung: Responses größer und häufiger
  - Richtwert: 1 Stunden < TTL < 1 Woche
- **DNSKEY TTLs auspendeln**
  - Zu groß: Rollover und Emergency Deletion schwierig
  - Zu klein: Auslastung und DNSKEY RR größer;
    Cache Purge RRSet/SIG in Resolver nach TTL
- **RRSIG Intervall > SOA Expire**
  - Sonst Validierungsfehler bei Transfer-Problemen

# Setup: Key Algorithmen

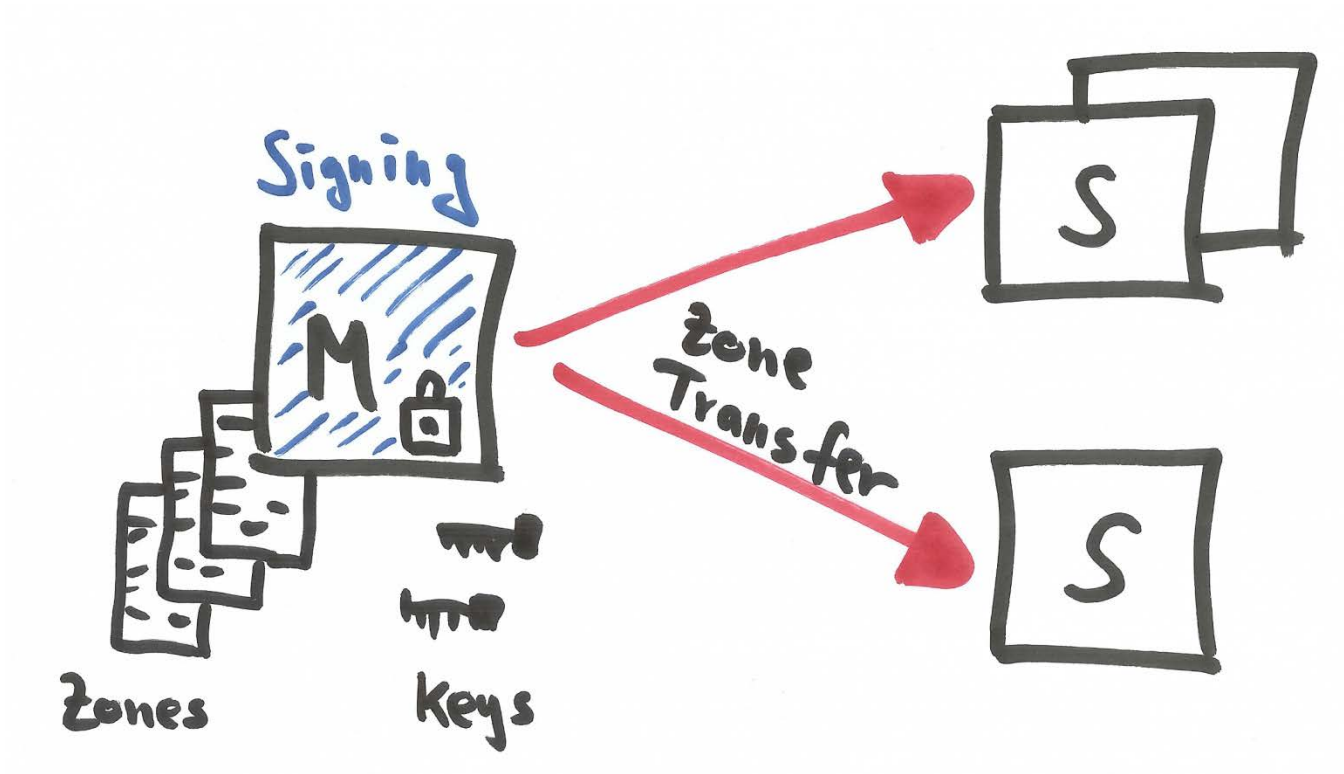
- **Key Size variabel**
  - ~~3 DSA/SHA1~~
  - ~~5 RSA/SHA1~~
  - ~~6 DSA-NSEC3/SHA1~~
  - ~~7 RSA-NSEC3/SHA1~~
  - **8 RSA/SHA-256**
  - 10 RSA/SHA-512
- **Key Size statisch**
  - 12 ECCGOST
  - **13 ECDSA Curve P-256/SHA-256**
  - **14 ECDSA Curve P-384/SHA-384**

# Hands-on DNSSEC #2

- DNSSEC nutzen
- Key Management
- DNSSEC Validierung im Nameserver einrichten
- Weitere DNSSEC Informationen prüfen
- Fehler provozieren und beheben
- Erweiterung des Setups

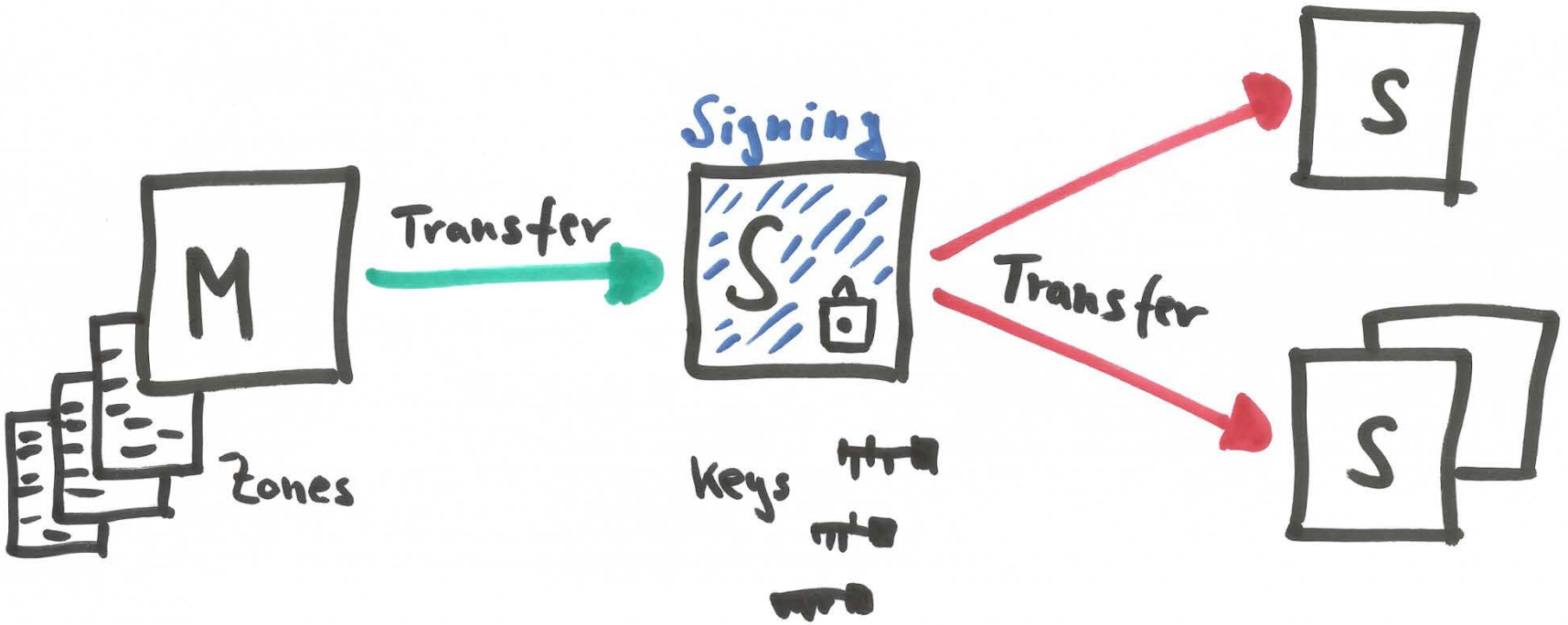
# Setup: DNS Infrastruktur

- Signing Master



# Setup: DNS Infrastruktur

- Bump On Wire Signing



# Hinweise

- TSIG für Zone Transfers
- Monitoring DNSSEC Zonen und Keys
- Insecure: unsignierte externe CNAME-Ziele
- Bogus: DNSKEY / DS fehlt, RRSIG abgelaufen
- Debug: Signed zu Plain Zone-File
  - ```
    $ named-compilezone -f raw -F text \
        -o pri/babiel/babiel.eu.zone babiel.eu \
        pri/babiel/babiel.eu.zone.signed
    ```
    ```

# Links und Referenzen

- https://tools.ietf.org/html/rfc4033
- https://tools.ietf.org/html/rfc6781
- https://www.denic.de/denic-im-dialog/news/4083.html
- http://www.iana.org/assignments/dns-parameters
- https://www.isc.org/blogs/dnssec-readiness/
- http://users.isc.org/~jreed/dnssec-guide/dnssec-guide.html
- https://www.dnssec-tools.org/
- https://wiki.icinga.org/display/howtos/DNS+Monitoring
- https://www.dns-oarc.net/

# Links und Referenzen

- http://www.internetsociety.org/deploy360/resources/dane/
- https://www.dnssec-validator.cz/
- https://www.nlnetlabs.nl/projects/dnssec-trigger/
- https://www.opendnssec.org/

# Vielen Dank für euer Interesse!

- talk.babiel.com/clt2016/dnssec
- github.com/pecharmin/dnssec-workshop

- babiel.com/jobs
- twitter.com/Babiel
- facebook.com/babiel.gmbh