Sichere Namensauflösung mit DNSSec

Chemnitzer Linux Tage 2010

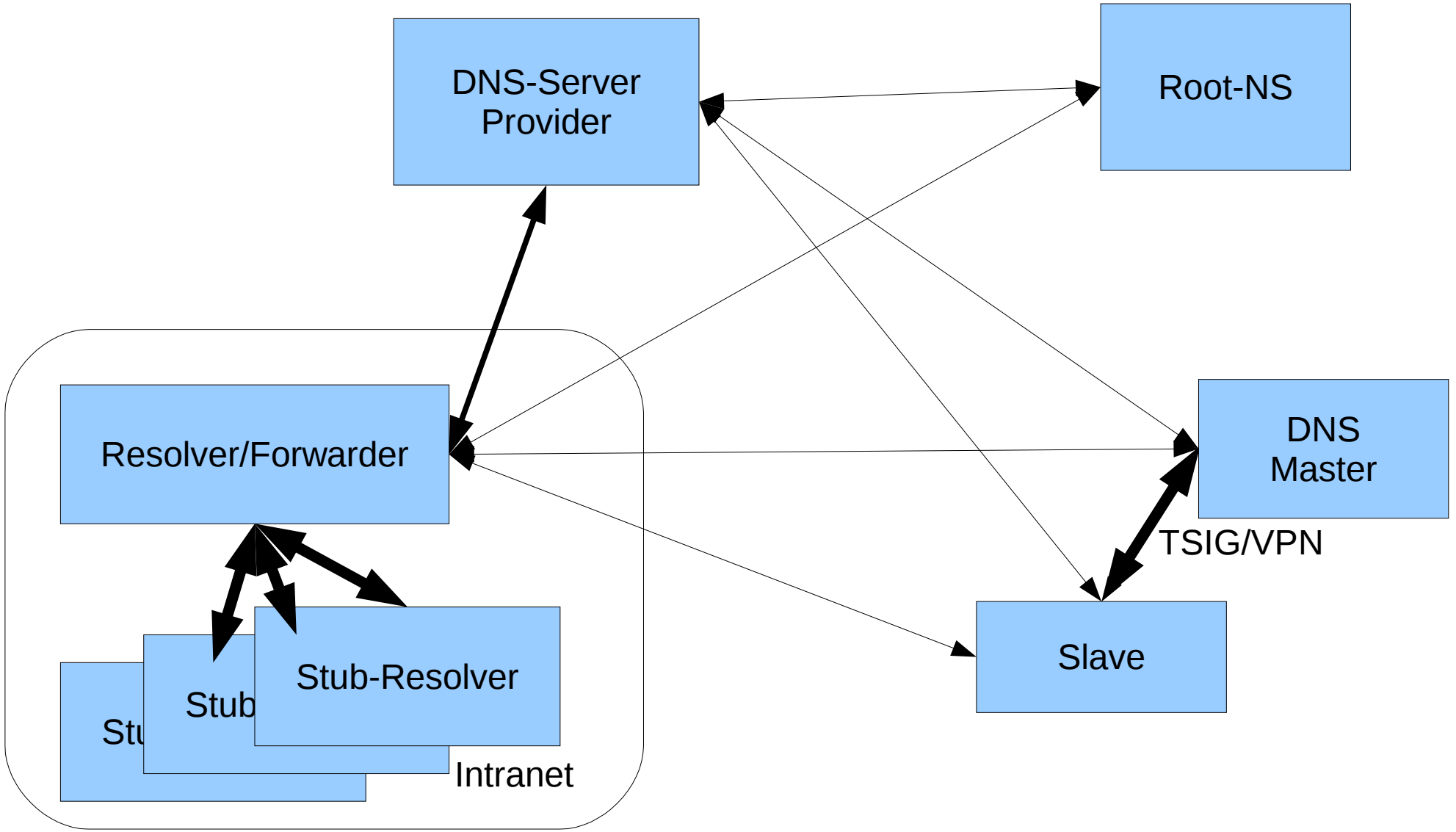
Heiko Schlittermann
Marcus Obst

http://www.schlittermann.de/doc/clt2010/

Inhalt

- Stand der Technik
- Motivation zum DNSSEC-Einsatz
- Sicherung mit TSIG
- Sicherung mit DNSSEC
  - Wiederholung: Public Key Verfahren
  - DNSSEC-Validierung mit dig
  - DNSSEC-Validierung im Resolver
- Risiken und Nebenwirkungen
- Aufgaben für den Zonenverwalter

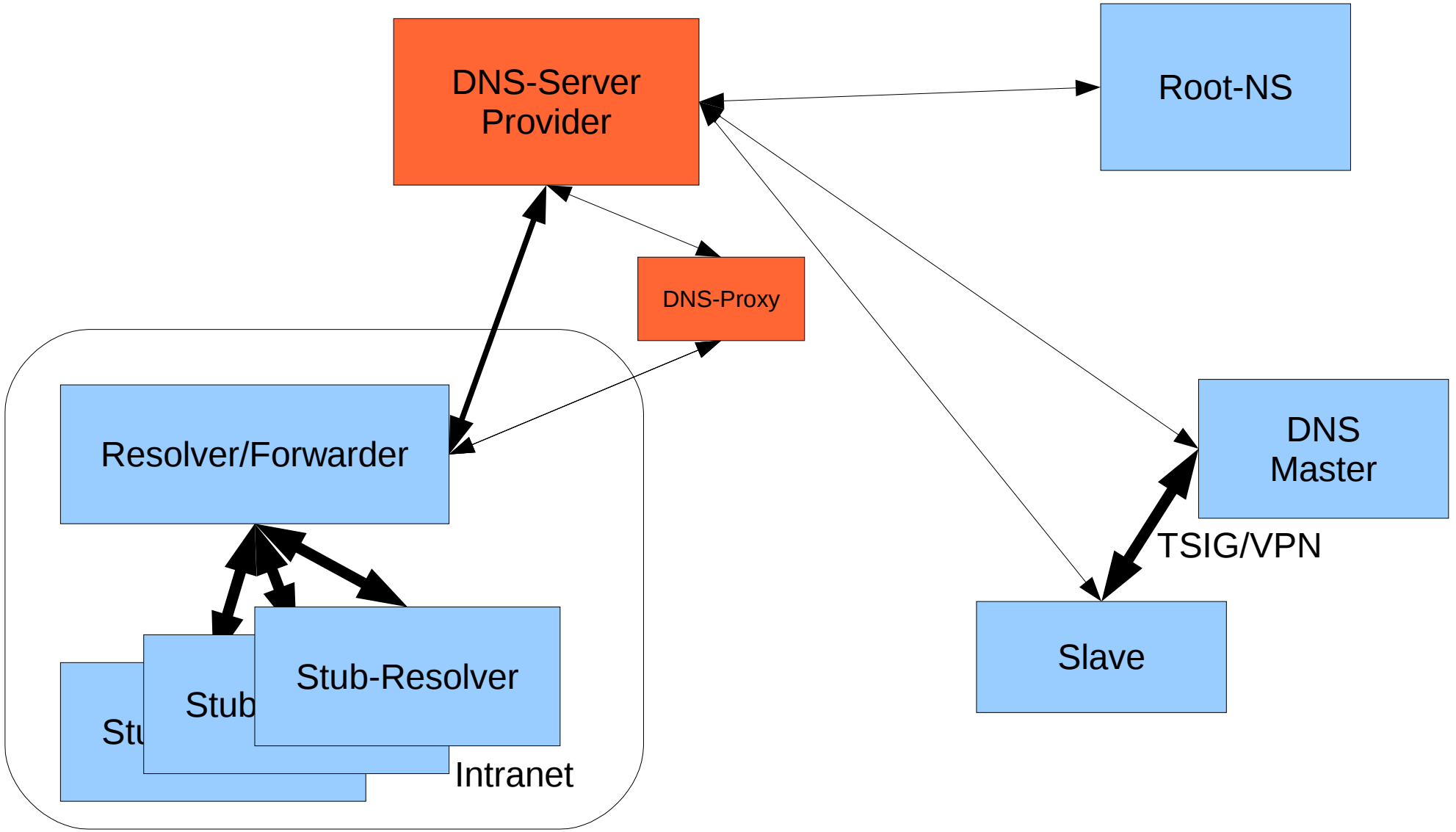
Stand der Technik



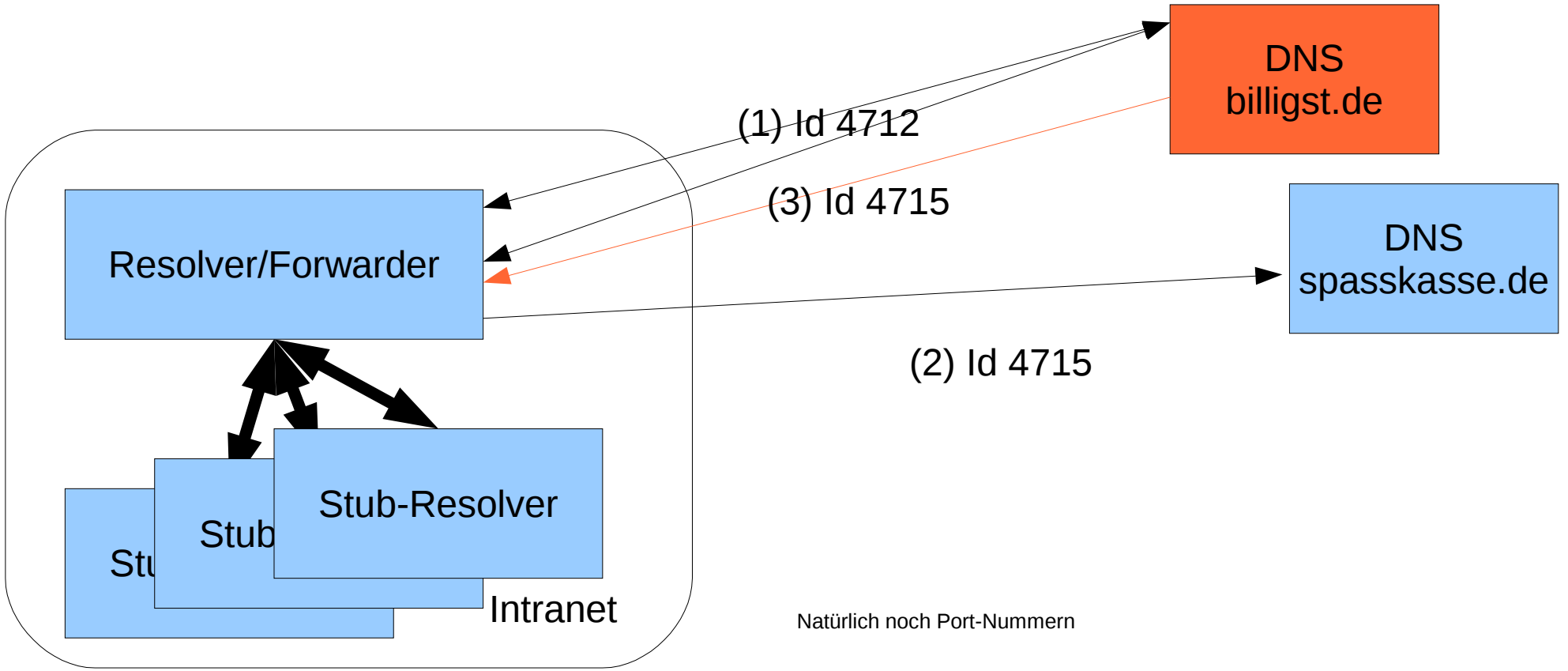
Motivation

- Eingriffe und Angriffe
- Zentrale Rolle von DNS für
  - hostbasierte Authentisierungsverfahren
  - Spamabwehr (SPF, DKIM)
  - SSH-Hostkeys
  - Ressource-Adressierung (SRV, MX, A)

Ein^H^H^HAngriff 1



Angriff 2



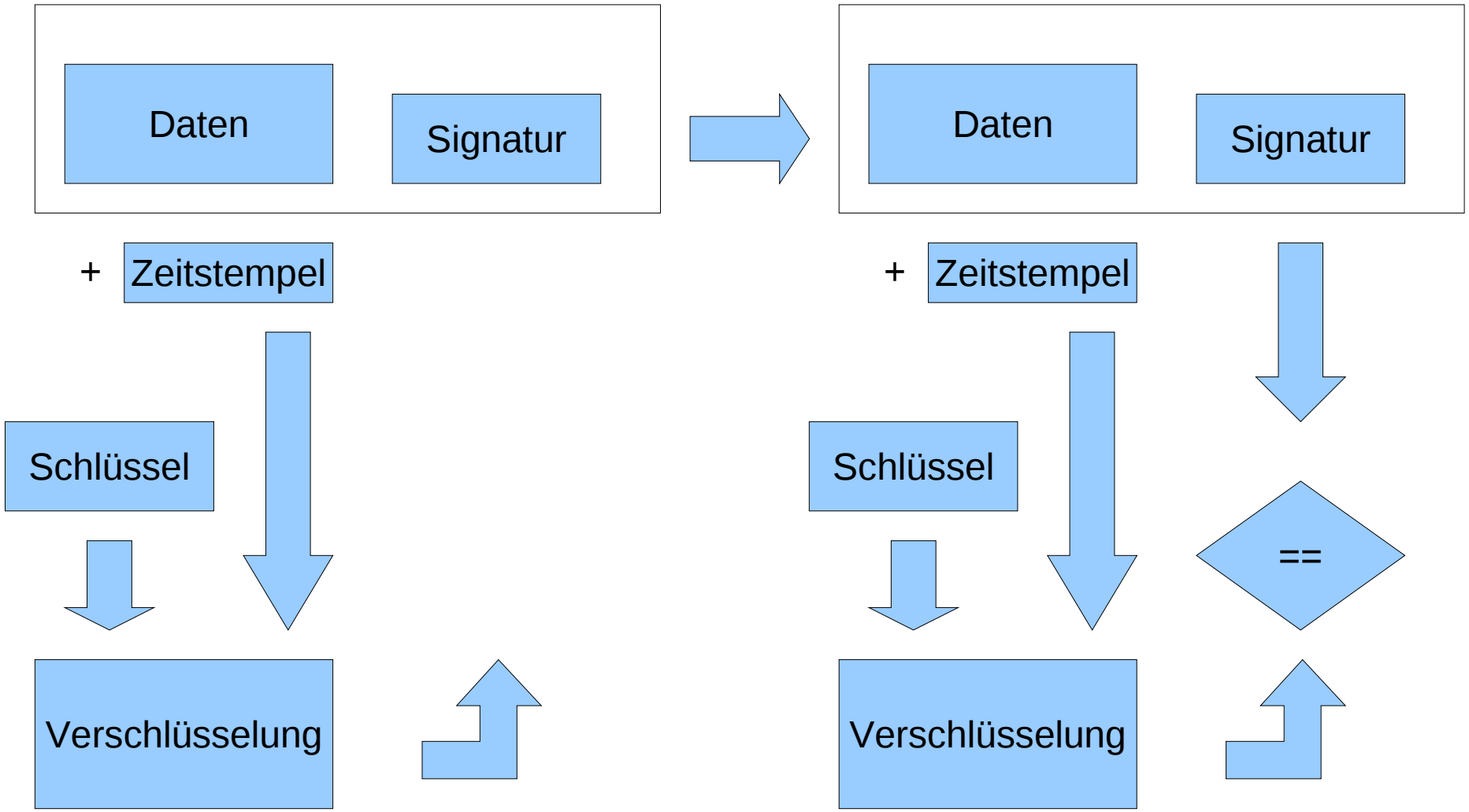
Natürlich noch Port-Nummern

Stand der Technik: TSIG – Transaction Signature

```
heiko@jumper:/tmp$ dig -k K*private @hh.schlittermann.de axfr schlittermann.de
; <<>> DiG 9.5.1-P3 <<>> -k Kpu.schlittermann.de.+157+03472.private @hh.schlittermann.de axfr schlittermann.de
; (1 server found)
;; global options:  printcmd
schlittermann.de.  86400   IN  SOA pu.schlittermann.de. hostmaster.schlittermann.de. 2010022300 86400 7200 604800 86400
schlittermann.de.  86400   IN  A   212.80.235.130
schlittermann.de.  86400   IN  MX  80 ssl.schlittermann.de.
...
xxx.schlittermann.de. 86400   IN  NS  hh.schlittermann.de.
xxx.schlittermann.de. 86400   IN  NS  pu.schlittermann.de.
xxx.schlittermann.de. 86400   IN  A   192.168.231.97
schlittermann.de.  86400   IN  SOA pu.schlittermann.de. hostmaster.schlittermann.de. 2010022300 86400 7200 604800 86400
pu.schlittermann.de.  0   ANY TSIG    hmac-md5.sig-alg.reg.int. 1267398057 300 16 AovtKkSoUUj4gDyOAFCY3Q== 19555 NOERROR 0
;; Query time: 338 msec
;; SERVER: 213.128.132.49#53(213.128.132.49)
;; WHEN: Sun Feb 28 23:58:36 2010
;; XFR size: 259 records (messages 1, bytes 6135)
```

- Dynamisch generierte Signatur (verschlüsselte Prüfsumme über Daten und Zeitstempel)
- Shared Secret
- Skaliert nicht

TSIG – Transaction Signature



TSIG – Transaction Signature: Facts

- **Gemeinsamer** privater Schlüssel
- Signaturerzeugung „on the fly“ beim Absender
- Authentisierung der Query und der Antwort
- Integrität/Authentizität der Daten

TSIG – Transaction Signature: Tasks

- Schlüssel erzeugen

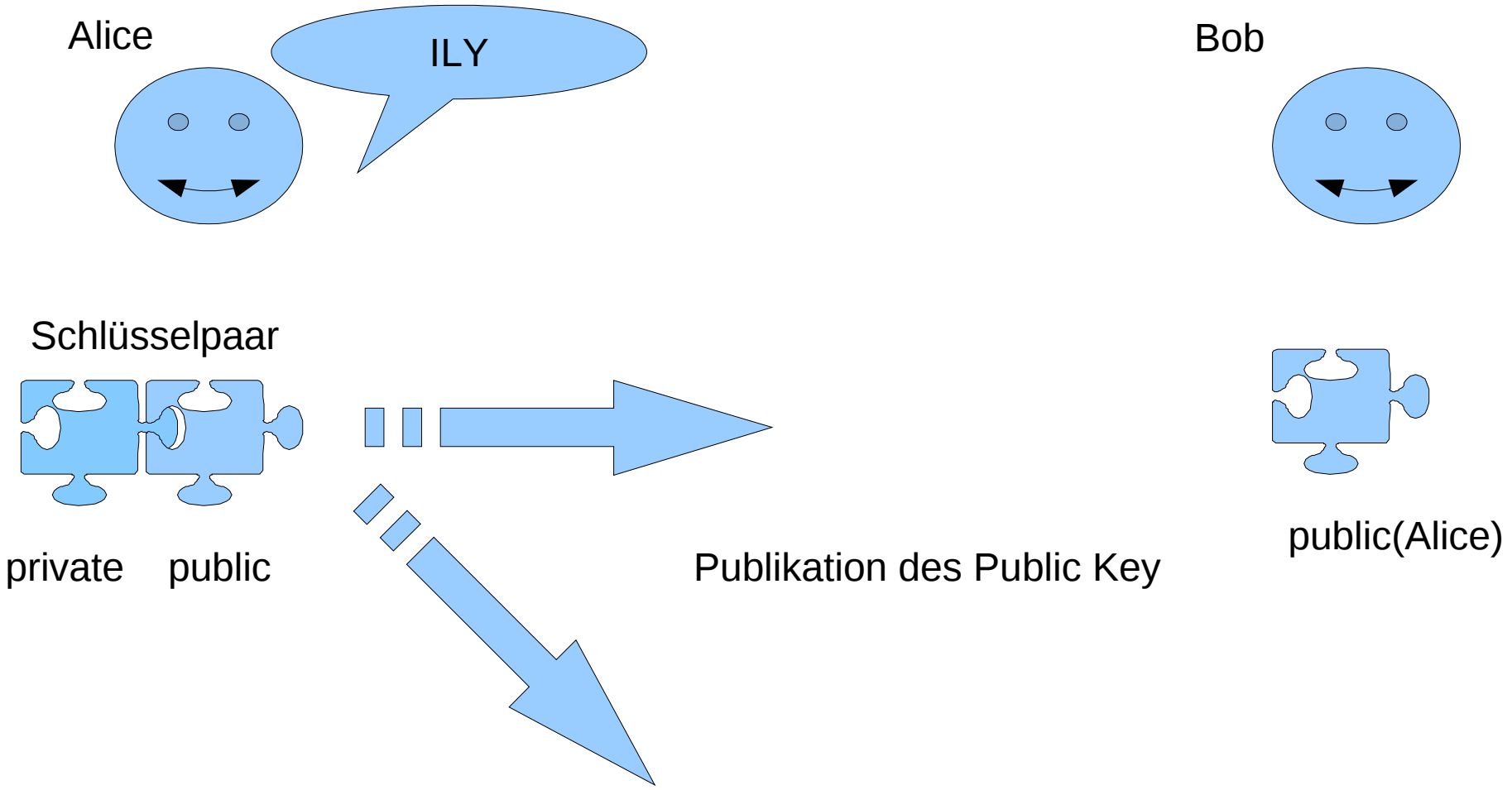
```
dnssec-keygen -a hmac-md5 \
  -b 512 -n HOST Schlüssel-Name
```

- Schlüssel verteilen (rsync, scp, ...)
- Schlüssel testen
  `dig -k KSchlüssel-Name*private ...`
- Konfiguration Nameserver/Clients anpassen

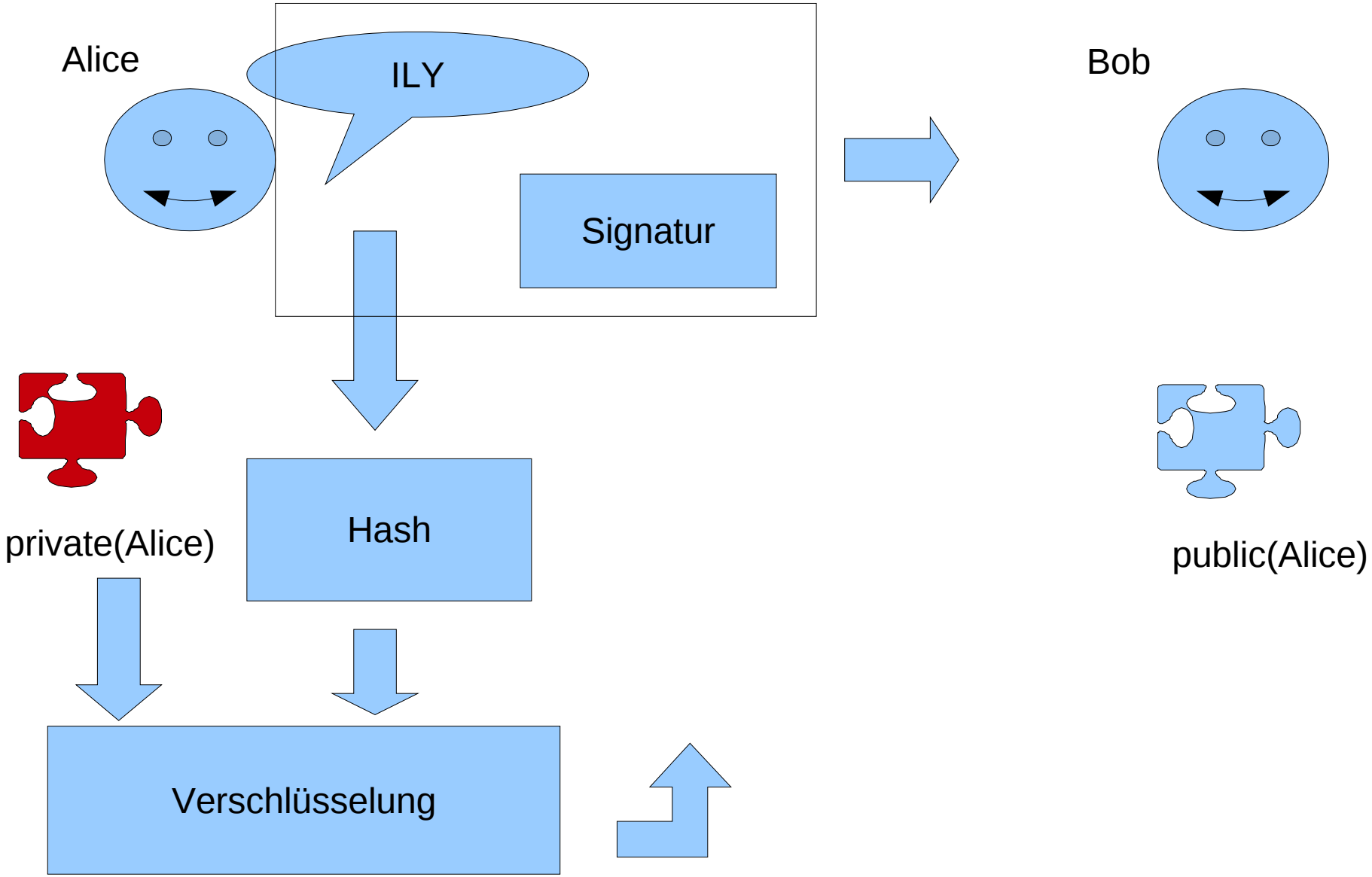
DNSSec: Public Key Kryptographie

Kurze Wiederholung

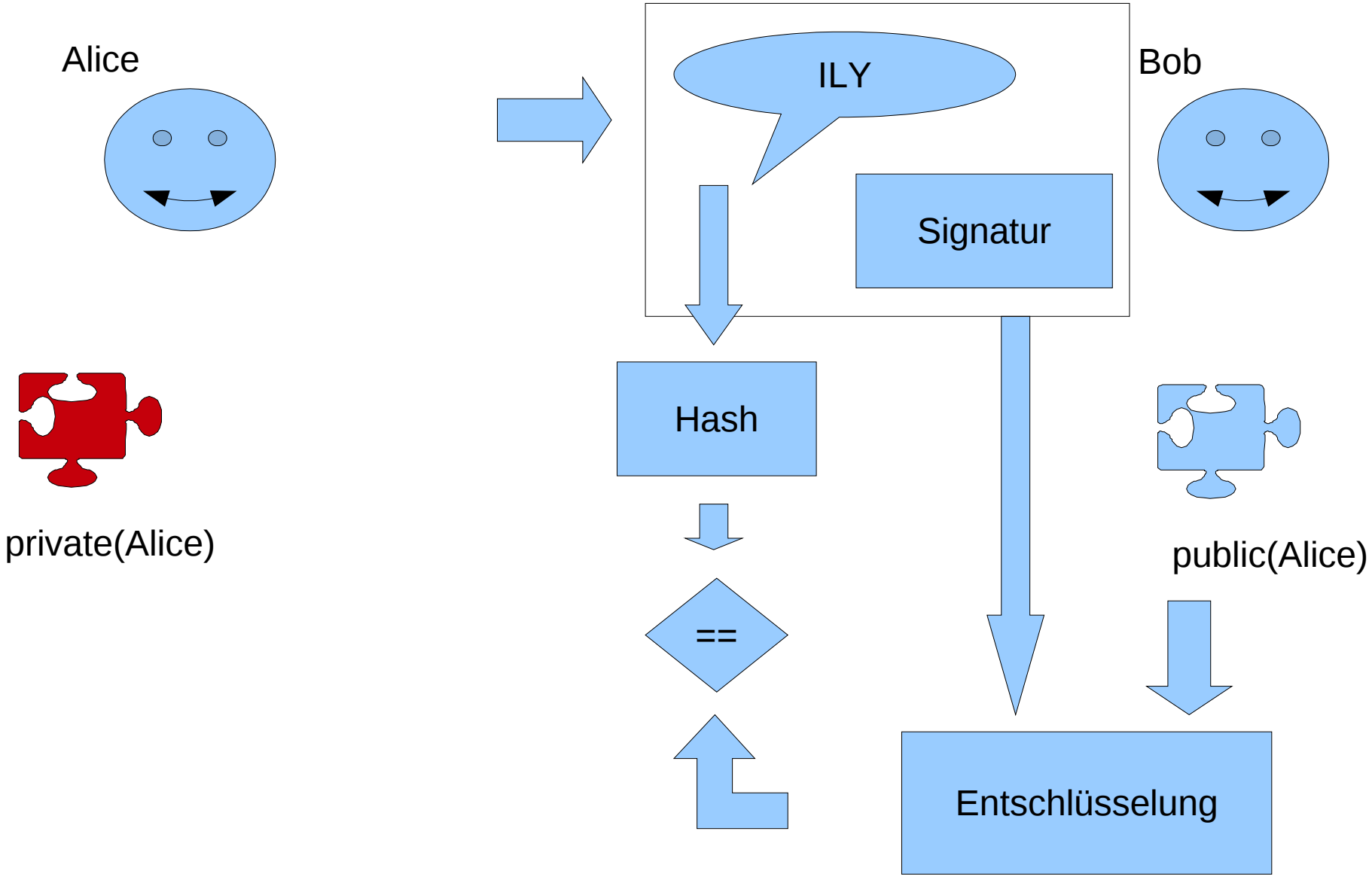
Public Key Kryptographie (1)



Public Key Kryptographie (2)



Public Key Kryptographie (3)



Public Key Kryptographie: Facts

- Signierung von Daten (Authentizität/Integrität)
- Einfachheit beim Key-Management: nur öffentliches Wissen (Public Key) wird verteilt
- Skaliert gut: nur ein Key-Paar beim Sender
- „**Restproblem**“: Vertrauenswürdigkeit des public Key

DNSSec: Ein erstes Beispiel

- Abfrage einer bereits eingerichteten Zone

```
heiko@jumper:~$ dig +dnssec a.xxx.schlittermann.de

; <<>> DiG 9.5.1-P3 <<>> +dnssec a.xxx.schlittermann.de @212.80.235.130
(...)
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;a.xxx.schlittermann.de.      IN  A

;; ANSWER SECTION:
a.xxx.schlittermann.de.   86400   IN  A   194.39.236.1
a.xxx.schlittermann.de.   86400   IN  RRSIG   A 5 4 86400 20100401212456 20100302212456 50433 xxx.schlittermann.de.
trIKy8DjuhGchQ8uaMazR08zpMLnFmHBZ3rnrlO0gP/Qru6/8XGUaY...

;; AUTHORITY SECTION:
xxx.schlittermann.de. 86400   IN  NS  pu.schlittermann.de.
xxx.schlittermann.de. 86400   IN  NS  hh.schlittermann.de.
xxx.schlittermann.de. 86400   IN  RRSIG   NS 5 3 86400 20100401212456 20100302212456 50433 xxx.schlittermann.de.
JvOd/DKqFtRRHLlISaYeywP2FxpgvDLWFHbC094RZwBEznibrOfVh...

;; ADDITIONAL SECTION:
hh.schlittermann.de.  86400   IN  A   213.128.132.49
pu.schlittermann.de.  86400   IN  A   212.80.235.130

;; Query time: 37 msec
;; WHEN: Tue Mar  2 23:22:47 2010
```

Neue Resource-Records

- **RRSIG**: Signatur der Records
- **DNSKEY**: Public Key zur Signatur
- **NSEC/NSEC3**: Next Secure – zur Kennzeichnung von nicht vorhandenen Einträgen
- **DS**: Domain Signer – Fingerprint des Keys einer Subdomain
- **DLV**: Domain Lookaside Validation – entspricht etwa dem DS Record

Validierung mit dig

- Prüfung der Unversehrtheit

```
$ dig +trusted-key=/dev/null +sigchase a.xxx.schlittermann.de
;; RRset to chase:
a.xxx.schlittermann.de. 85719   IN      A       194.39.236.1

;; RRSIG of the RRset to chase:
a.xxx.schlittermann.de. 85719   IN      RRSIG   A 5 4 86400 20100401212456 20100302212456 50433 xxx....

Launch a query to find a RRset of type DNSKEY for zone: xxx.schlittermann.de.

;; DNSKEYset that signs the RRset to chase:
xxx.schlittermann.de.   85740   IN      DNSKEY  257 3 5 AwEAAbHQS/v8ACLTAP2Un1Q...
xxx.schlittermann.de.   85740   IN      DNSKEY  256 3 5 AwEAAb46CqKv2xV9VxIMnPd...

;; RRSIG of the DNSKEYset that signs the RRset to chase:
xxx.schlittermann.de.   85740   IN      RRSIG   DNSKEY 5 3 86400 20100401212456 20100302212456 30922 xxx....
xxx.schlittermann.de.   85740   IN      RRSIG   DNSKEY 5 3 86400 20100401212456 20100302212456 50433 xxx....

Launch a query to find a RRset of type DS for zone: xxx.schlittermann.de.
;; NO ANSWERS: no more

;; WARNING There is no DS for the zone: xxx.schlittermann.de.

;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING A RRset for a.xxx.schlittermann.de. with DNSKEY:50433: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Now, we are going to validate this DNSKEY by the DS
;; the DNSKEY isn't trusted-key and there isn't DS to validate the DNSKEY: FAILED
```

Vollständige Validierung

- Bisher nur die Signaturen angezeigt und geprüft...
- Fehlt: Validierung des verwendeten öffentlichen Schlüssels

Vollständige Validierung (dig)

- Download DNSKEY:

```
$ dig +short DNSKEY \
    xxx.schlittermann.de \
    | grep ^257 \
    >trusted-key.key
```

- Prüfung des Key (alternative Kommunikatiosnwege)
- Anpassung Keyfile trusted-key.key:

```
xxx.schlittermann.de. IN DNSKEY \
    257 3 5 Awe...
```

Vollständige Validierung (dig)

- lokal abgelegter public Key des Unterzeichners

```
$ cat trusted-key.key
xxx.schlittermann.de. IN DNSKEY 257 3 5 AwEAAbHQS/v8ACLTAP2Un1Qb...

$ dig +trusted-key=trusted-key.key +sigchase a.xxx.schlittermann.de
(...)

Launch a query to find a RRset of type DS for zone: xxx.schlittermann.de.
;; NO ANSWERS: no more

;; WARNING There is no DS for the zone: xxx.schlittermann.de.


;; WE HAVE MATERIAL, WE NOW DO VALIDATION
;; VERIFYING A RRset for a.xxx.schlittermann.de. with DNSKEY:50433: success
;; OK We found DNSKEY (or more) to validate the RRset
;; Ok, find a Trusted Key in the DNSKEY RRset: 30922
;; VERIFYING DNSKEY RRset for xxx.schlittermann.de. with DNSKEY:30922: success

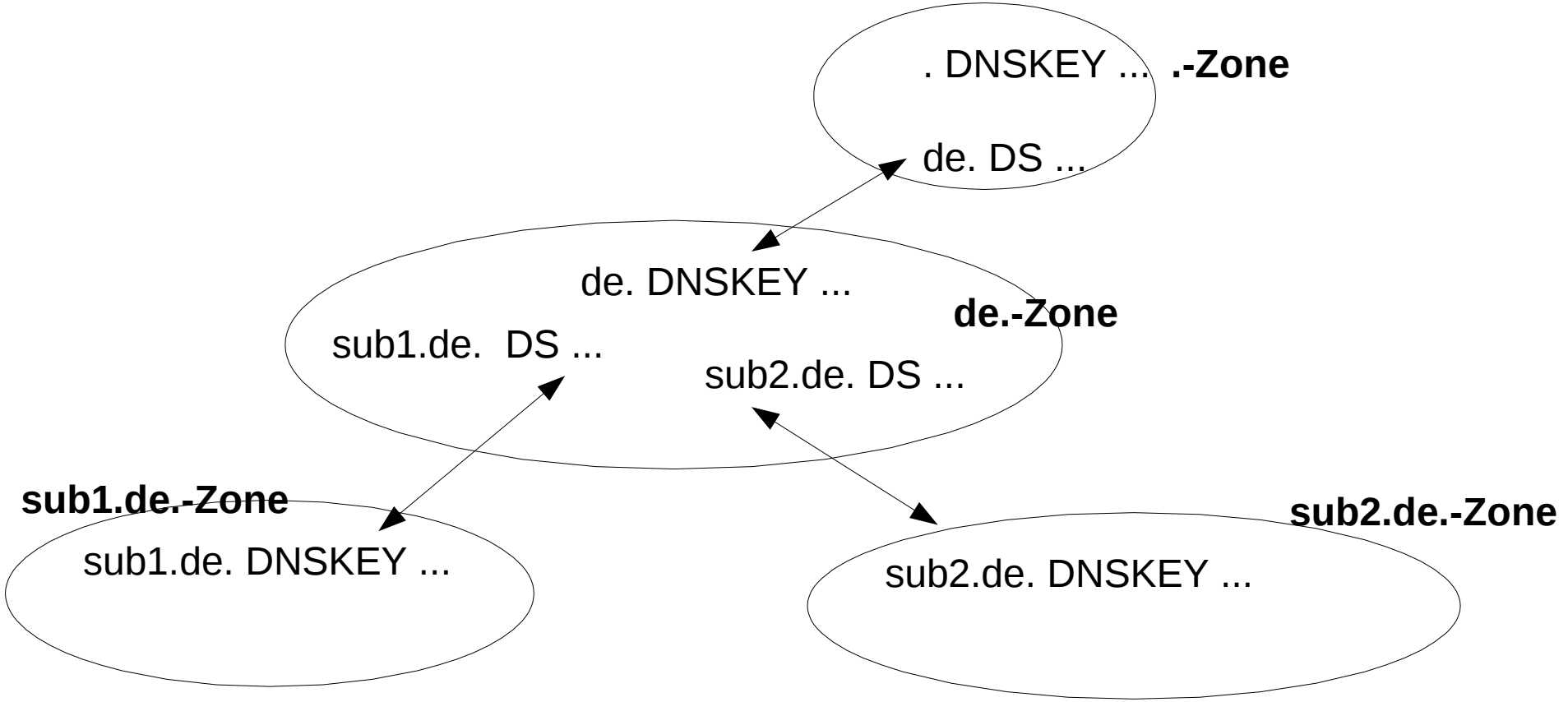
;; Ok this DNSKEY is a Trusted Key, DNSSEC validation is ok: SUCCESS
```

Vollständige Validierung im Resolver

- Prüfung der Integrität (RRSIG)
- Authentizität des öffentlichen Schlüssels
  - Chain of trust (existiert noch nicht)
  - Manuelle Schlüsselpflege – lokale Whitelist
  - Domain Lookaside Validation (dlv.isc.org)

Validierung im Resolver (Chain of Trust)

- Parent-Zone hat DS-Record (Domain Signer) – Fingerprint des DNSKEY der Child-Zone



Validierung im Resolver (Chain of Trust)

- Organisatorisches Problem und technisches Problem
- .de: Masterplan (Ende 2011)
- .cz, .bz, .se, .gov und einige andere: Production
- Fehlt: DNSKEY der Root-Zone „.“

Validierung im Resolver (manuell)

- Stub-Resolver: kein DNSSEC
- Resolver (Bind9 ab 9.3)
- ```
  options { ...
    dnssec-enable yes;
    dnssec-validation yes;
  };
  trusted-keys {
    xxx.schlittermann.de. 257 ...
  };
  ```
- Skaliert nicht!
  ```

Validierung im Resolver (manuell)

```
$ dig +dnssec a.xxx.schlittermann.de

; <<>> DiG 9.5.1-P3 <<>> +dnssec a.xxx.schlittermann.de
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61798
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;a.xxx.schlittermann.de.   IN A

;; ANSWER SECTION:
a.xxx.schlittermann.de. 84895 IN A  194.39.236.1
a.xxx.schlittermann.de. 84895 IN RRSIG A 5 4 86400 20100409210029 20100310210029 8760
xxx.schlittermann.de. i3jFrg865V3OiHZRBELzZGGTP+nk8CcJh/obNeeXeUeOFb34neAPZfsF
WefoUdM5LjKP9fxhBmMC8e4Nm04Jkg==
```

- Vertrauensfrage!
- Skaliert auch nicht

Validierung im Resolver (manuell)

- Test bei ungültiger Signatur

```
$ dig +dnssec c.xxx.schlittermann.de

; <<>> DiG 9.5.1-P3 <<>> +dnssec c.xxx.schlittermann.de
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 37402
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;c.xxx.schlittermann.de.    IN A

;; Query time: 138 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Mar 11 23:33:39 2010
```

Domain Lookaside Validation - DLV

- Zonen-Keys werden bei dlv.isc.org hinterlegt
- ISC bestätigt die Glaubwürdigkeit der hinterlegten Keys
- „künstlicher“ Einstiegspunkt (Security Entry Point)
- je Zone eine DLV-Query zu *zone.*dlv.isc.org
- Resolver kennt nur noch den DNSKEY von dlv.isc.org

Domain Lookaside Validation - DLV

```
options {
    ...
    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside
      . trust-anchor dlv.isc.org.;
};
trusted-keys {
    dlv.isc.org. 257 3 5 ...
};
```

Domain Lookaside Validation - DLV

```
$ dig +dnssec soa cz.

; <<>> DiG 9.5.1-P3 <<>> +dnssec soa cz.
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1011
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;cz.                IN SOA

;; ANSWER SECTION:
cz.             3215  IN SOA   a.ns.nic.cz. hostmaster.nic.cz. 1268339669 900 300 604800 900
cz.             3215  IN RRSIG SOA 5 1 18000 20100324015341 20100311193429 50825 cz.
H2QowfdoImRqq6kMvlLbrIvAQfIOUyflJmw863OXyfIzqX22Z1kYIHcZ
acb5JOrMXJraRQPVYBcl4la4GXTp4dwQ+CgiSCFrtgTBLIf2gq+NRCn+
xjb1KB6OZVBDqKmkl4iOT6acIIwyfhq0DxW0q/cQCR52M7Cz15NvGH5z jzk=

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Mar 11 22:13:50 2010
```

Risiken und Nebenwirkungen

- Forwarder ohne DNSSEC-Unterstützung (dnsmasq u.a.): SERVFAIL
- ungültige Signaturen (veraltet/kaputt): SERVFAIL
- SERVFAIL => **no such host**
- mehr Traffic (UDP bis 4k statt 512B)
- Wir können nicht alles haben!

Schmerzlinderung

- options {
  ...
  dnssec-accept-expired yes;
  };
- Flag: checking disabled

```
$ dig +cdflag +dnssec c.xxx.schlittermann.de
...
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58295
;; flags: qr rd ra cd; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;c.xxx.schlittermann.de.      IN A

;; ANSWER SECTION:
c.xxx.schlittermann.de.    86400  IN A   194.39.236.33
c.xxx.schlittermann.de.    86400  IN RRSIG  A 5 4 86400 20100410212459 20100311212459 8760 xxx.schlittermann.de.
qCFL2ECNFh+gZLGyqflOzG7buDbVQJ9gje6/9VKZbg987SJqs0vRtuLu HUjD6NXBs/PSB4o701iWgzFdPLNm4A==
```

Was bleibt?

- Vertrauen Stub-Resolver <--> Resolver oder eigener Resolver für jeden? (s.a. unbound)
- NSEC: Zonewalking möglich (s.a. NSEC3)
- DLV-Trusted-Key besorgen (www.isc.org), bind-Konfiguration anpassen und DNSSec nutzen

Aufgaben für den Zonenverwalter

- Schlüssel für Zone erzeugen (ZSK und KSK)

```
$ dnssec-keygen -a RSASHA1 \
  -b 512 -n ZONE example.org

$ dnssec-keygen -a RSASHA1 \
  -b 4096 -n ZONE -f KSK \
  example.org
```

Aufgaben für den Zonenverwalter

- Schlüssel in die Zone aufnehmen

```
$ cat Kexample.org.*key \
    >>example.org
```

Aufgaben für den Zonenverwalter

- Zone signieren

```
$ dnssec-signzone example.org
```

Aufgaben für den Zonenverwalter

- Bind konfigurieren

```
options {
  ...
  dnssec-enable yes;
};
zone „example.org“ {
  file „example.org.signed“;
  ...
};
```

Aufgaben für den Zonenverwalter

- Anmelden bei http://dlv.isc.org
- Maintenance
  - regelmäßige Re-Signieren
  - regelmäßig Wechsel des ZSK
- Infrastruktur?

Danke

schlittermann – internet und unix support
Heiko Schlittermann
Tannenstraße 2
01099 Dresden
http://www.schlittermann.de

Anfragen zum Thema bitte an hs@schlittermann.de

Linux User Group Dresden
http://lug-dd.schlittermann.de