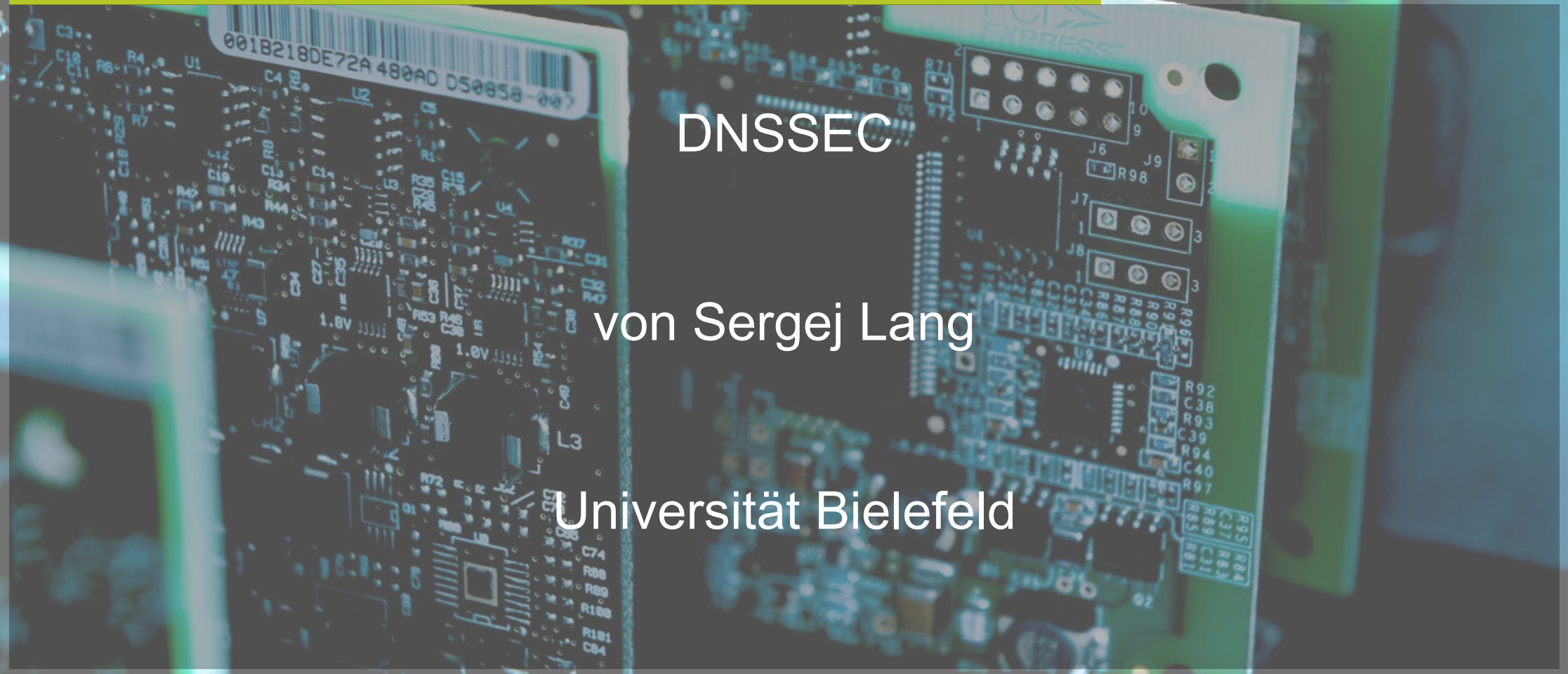
Wie funktioniert DNSSEC



DNSSEC

von Sergej Lang

Universität Bielefeld

Einleitung

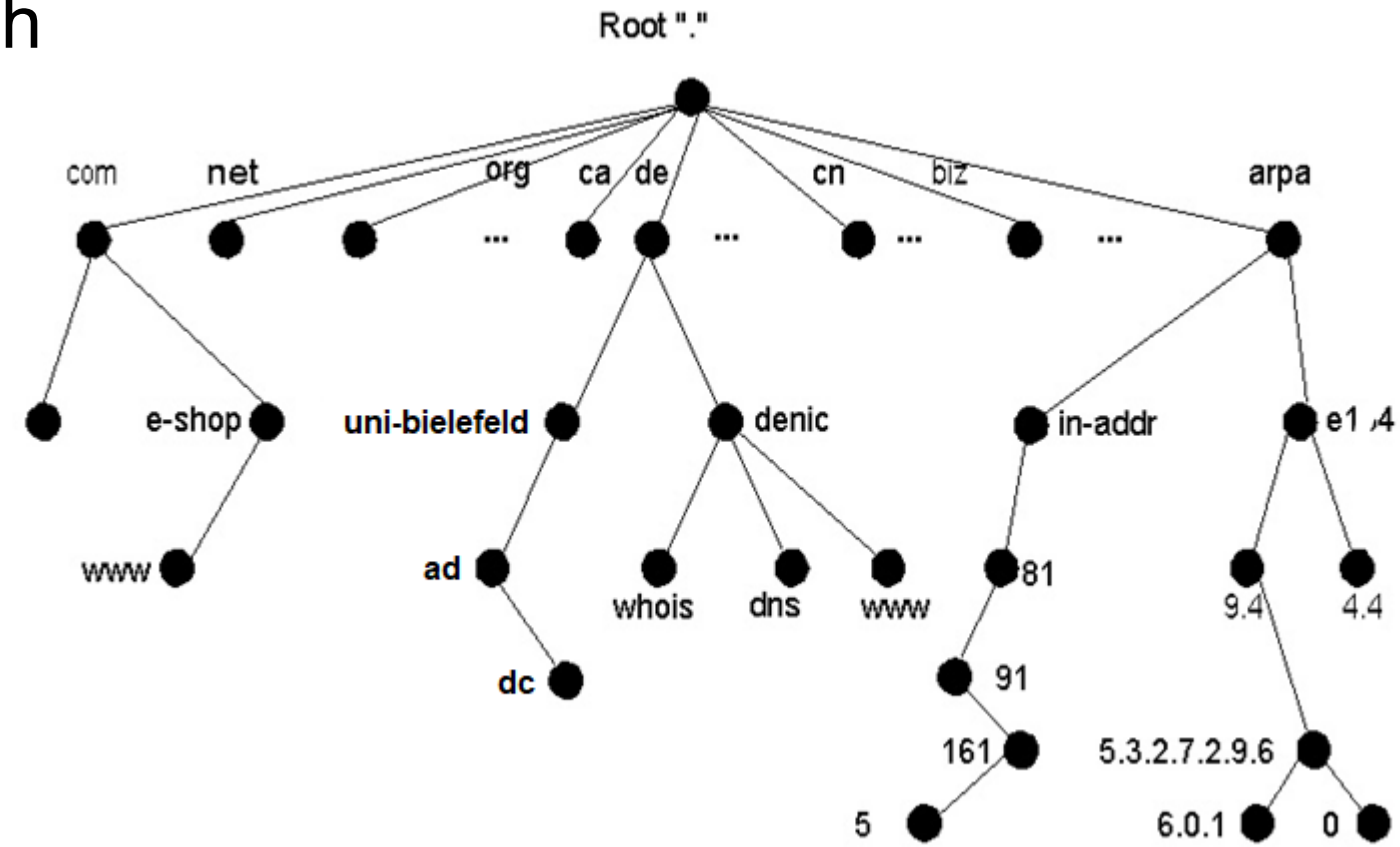
- Kurzvorstellung - DNS an der Uni-Bielefeld
- DNS - Grundlagen und Sicherheitsaspekte
- DNSSEC - Einführung
- DNSSEC - Funktionsweise
- DNSSEC - Erweiterungen (DANE/TLSA)
- DNSSEC - Fazit
- Ausblick (DoH, DoT)

Kurzvorstellung - DNS an der Uni-Bielefeld

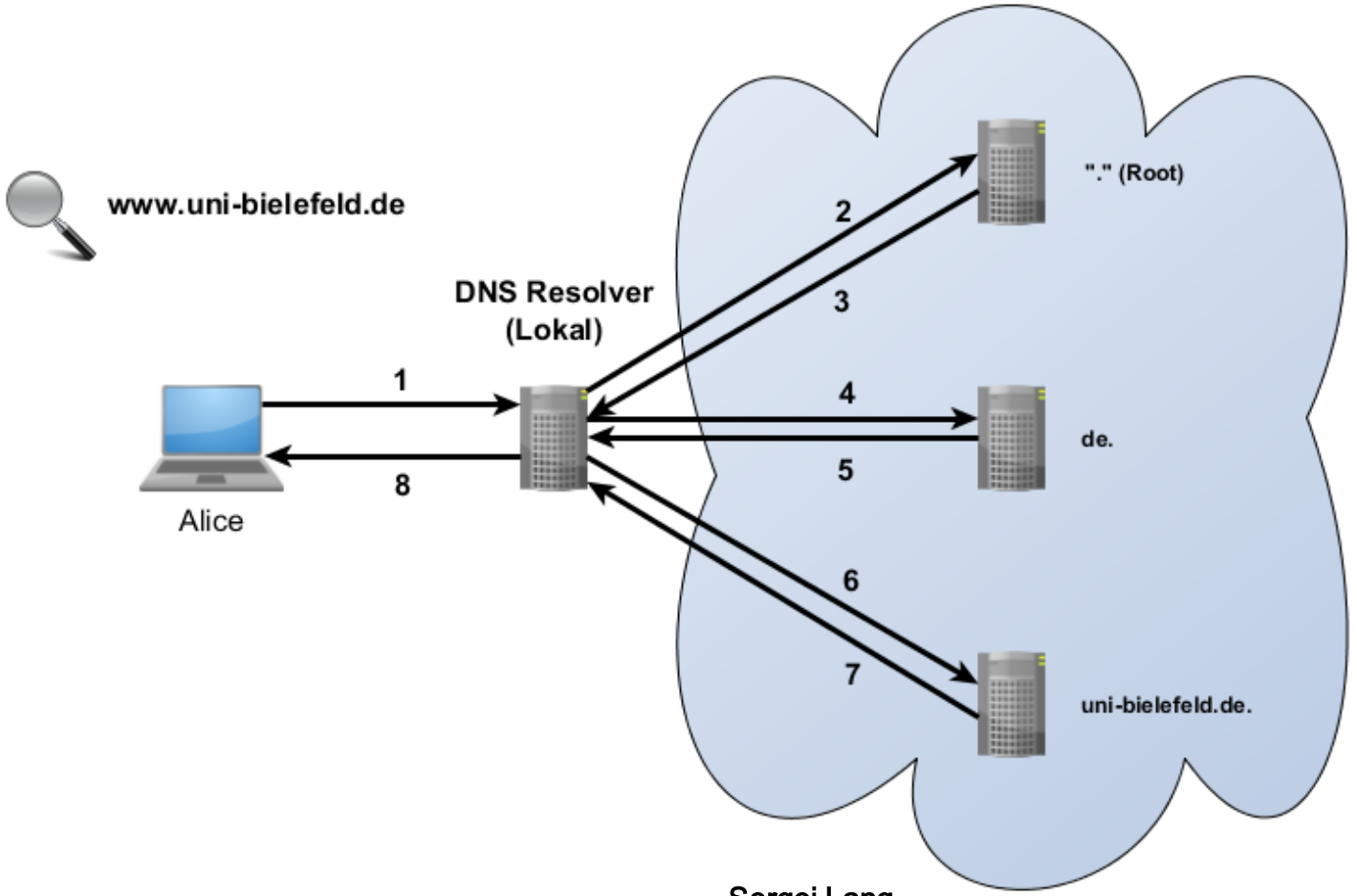
- Betrieb von Autoritativen DNS Servern
  - 128 DNS Zonen (davon 69x 2nd Level Domains)
- Betrieb von DNS Resolvern
  - Ca. 1900 Rekursive DNS Anfragen/Sek (im Peak)
- Zonendelegierung an Einrichtungen und Fakultäten
- Betrieb eines IP-Management Systems

DNS - Grundlagen

- DNS ist hierarchisch
- … und dezentral



DNS - Grundlagen



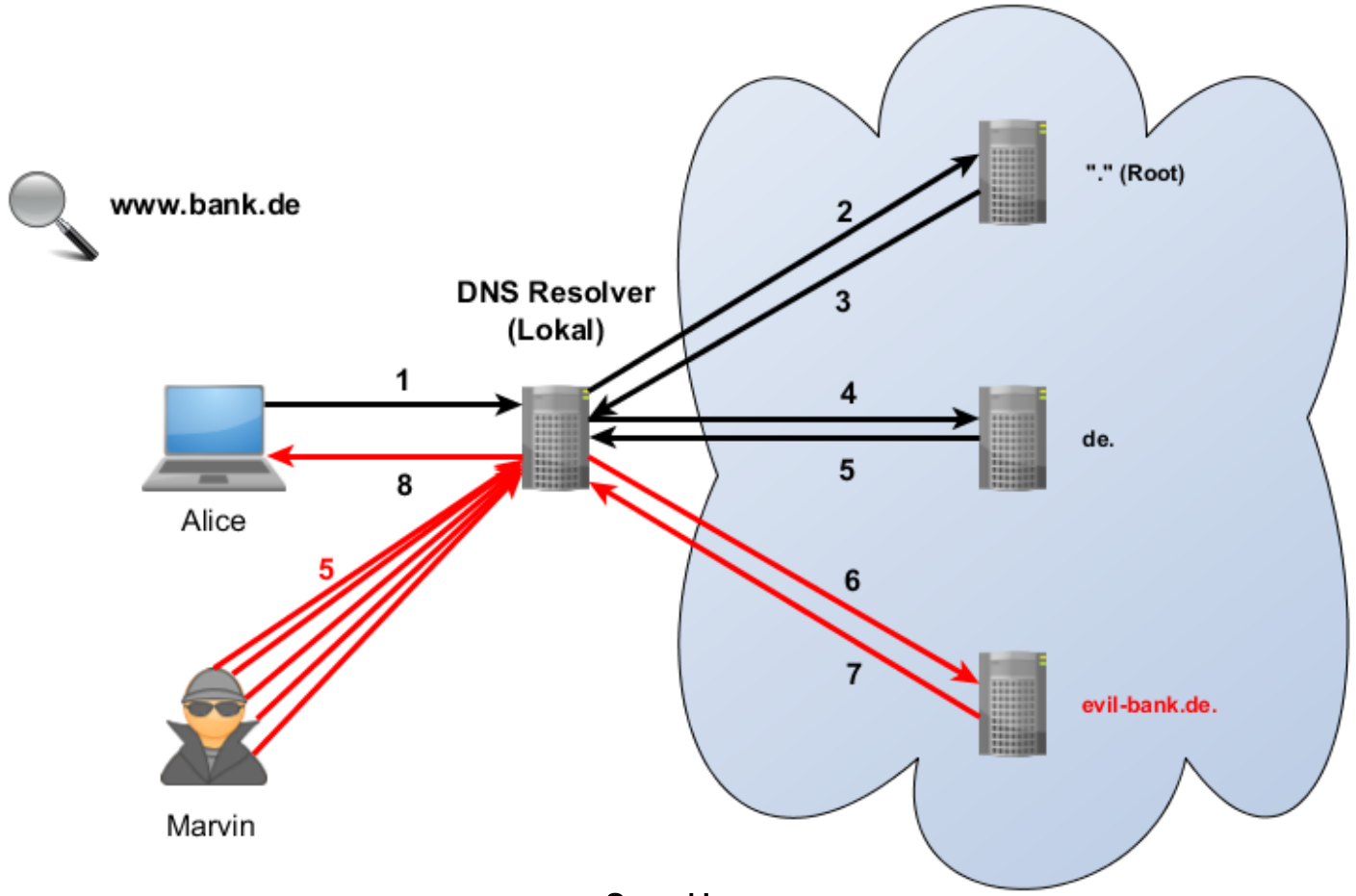
DNS - Sicherheitsaspekte

- DNS ist unverschlüsselt.
- Aus Performance Gründen meistens verbindungslos (UDP).
- Der lokale DNS Resolver hat eine zentrale Rolle im Netzwerk.
- Einer DNS Antwort wird grundsätzlich geglaubt.

DNS - Sicherheitsaspekte

- Beispiel: Cache Poisening
  - Problem: DNS Paketen wird grundsätzlich geglaubt
  - Idee: Der IP Adressauflösung wird ein falsches Ergebnis untergejubelt
  - Szenario:
    - Angreifer gibt sich als Autoritativer DNS Server aus
    - Angreifer schickt seine Antwort schneller als der echte Autoritative DNS Server
    - Angreifer kann beliebig viele Ports und Request IDs ausprobieren

DNS - Sicherheitsaspekte



DNS - Sicherheitsaspekte

- Bei Erfolg:
  - Umleiten auf eigene Server
  - Zugänge/Passwörter klauen
  - Die falsche IP Adresse verbleibt im Cache des DNS Resolvers
  - Andere Clients erhalten automatisch die selbe falsche Antwort
- Was kann man dagegen tun?
  - Der Autoritativen DNS Antwort nicht generell vertrauen

DNSSEC - Einführung

- DNSSEC sorgt für Authentizität von DNS Antworten
- Public Key Verfahren
  - DNS Server Signiert seine Zoneneinträge mit seinem Private Key
  - DNS Server stellt seinen Public Key im DNS zur Verfügung
  - Chain of Trust wird aufgebaut
    - Die übergeordneten DNS Zone enthält einen Hash des Public Key der untergeordneten DNS Zone (DS Record).
- DNS Resolver kann die Authentizität überprüfen

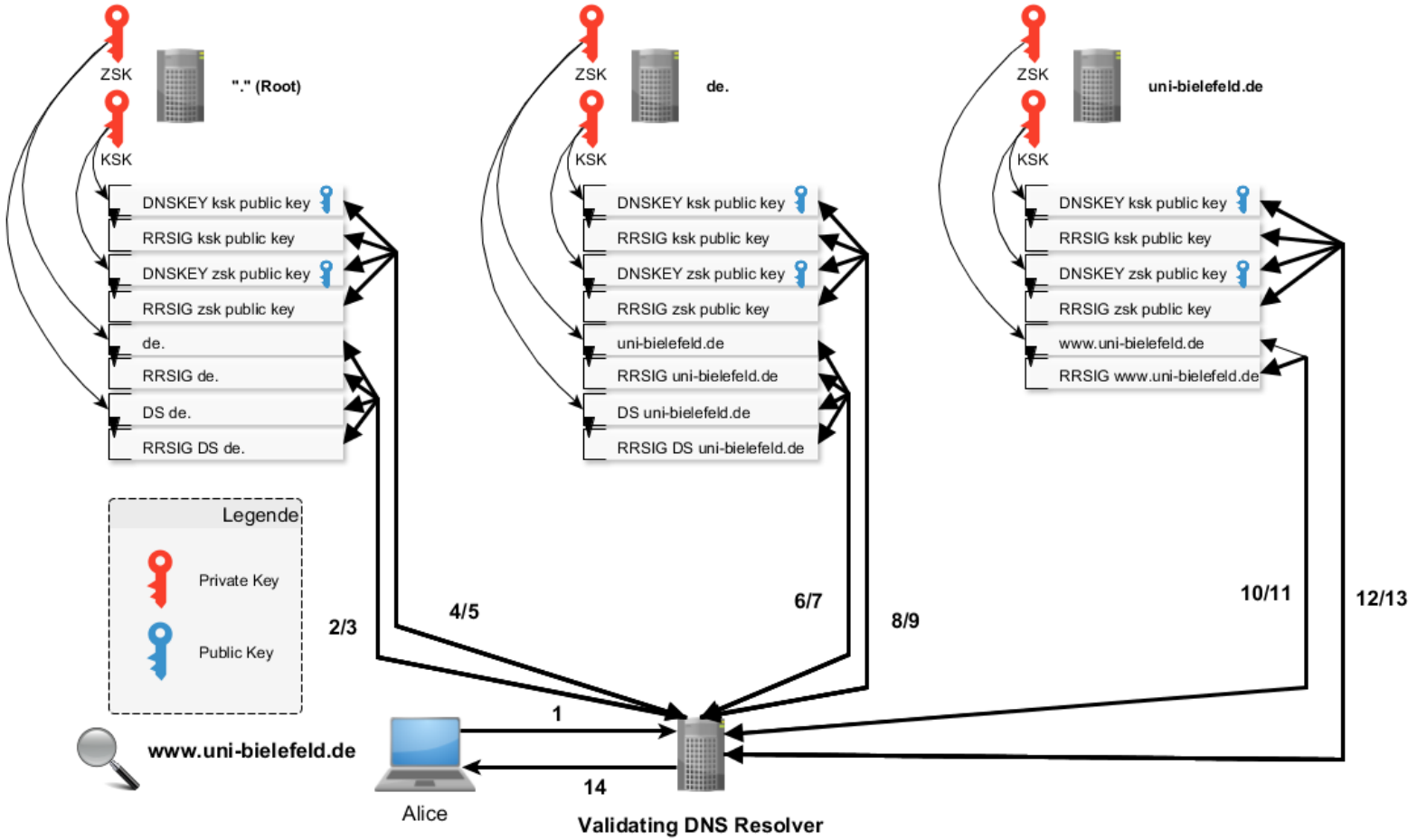
DNSSEC - Funktionsweise

- Zone Signing Key (ZSK)
  - Kurze Lebensdauer (wenige Wochen)
  - Signiert die eigentlichen DNS Records
- Key Signing Key (KSK)
  - Lange Lebensdauer (1 - 5 Jahre)
  - Signiert den ZSK (und sich selbst)
  - Hashwert vom KSK Public Key wird in der übergeordneten DNS Zone hinterlegt

DNSSEC - Funktionsweise

- Neue Resource Records
  - DNSKEY
  - RRSIG
  - DS
  - NSEC/NSEC3

DNSSEC - Funktionsweise



DNSSEC - Erweiterungen (DANE/TLSA)

- Problem: Jede CA kann jeder Domain ein Zertifikat ausstellen.
  - Der Client muss einer CA vertrauen.
  - Nicht alle CA arbeiten sauber.
- Idee: Informationen welcher CA vertraut werden darf im DNS hinterlegen.
- Lösung: DNS-Based Authentication of Named Entities (DANE)
  - Informationen zum gültigen TLS/SSL Zertifikat werden zusätzlich im DNS hinterlegt.
  - Andere Zertifikate als im DNS hinterlegt sind ungültig, egal von welcher CA.

DNSSEC - Erweiterungen (DANE/TLSA)

- Neuer Record: Transport Layer Security Associate (TLSA)
  - Service Port für das ein Zertifikat gilt
  - Transport Protokoll, dass vom Service genutzt wird. (z.B. TCP, UDP, SCTP)
  - TLSA Certificate Usage Parameter z.B:
    - Zertifikat muss von angegebenen CA stammen.
    - x509 Trust Chain muss gültig sein.
    - Nur das angegebene Zertifikat darf mit der Domain eingesetzt werden.
  - Hashwert vom Public Zertifikat des Webservers/CA

DNSSEC - Fazit

- Nachteile:
  - Langsamere DNS Auflösung (hängt noch stärker vom Cache ab)
  - Risiko einer Unerreichbarkeit beim Schlüsselwechsel.
  - DNS Betrieb wird insgesamt komplexer.
  - (DNS Datenverkehr ist immer noch nicht verschlüsselt!)
- Vorteile:
  - Für den Anwender keine Aktion erforderlich.
  - Schützt vor Angriffen auf die Identität des Autoritativen DNS Servers
  - DNS Antworten können auf ihre Echtheit überprüft werden.

Ausblick (DoH, DoT)

- Idee: Vertrauliches übertragen von DNS Datenverkehr
- DOT - DNS over TLS
  - Datenverkehr wird Verschlüsselt
  - Eigener TCP Port 853
  - DNS Verkehr kann als solcher erkannt werden und speziell behandelt werden.
- DOH - DNS over HTTPS
  - Datenverkehr wird Verschlüsselt
  - TCP Port 443 (HTTPS)
  - DNS Datenverkehr wird als HTTPS Verkehr getarnt und kann nicht gefiltert werden.

Fragen?

Quellen:

https://www.pexels.com/de-de/foto/beraten-brett-fokus-fragen-208494/

https://blog.apnic.net/2018/10/12/doh-dns-over-https-explained/

https://ftp.isc.org/isc/dnssec-guide/html/dnssec-guide.html

https://www.heise.de/ct/artikel/Domain-Name-System-absichern-mit-DNSSEC-903318.html

https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server--2

https://blog.webernetz.net/how-to-use-danetlsa/

https://thomas-leister.de/dane-tlsa-records-erklaert/

DNSSEC Analyszer Tools:

https://dnssec-analyzer.verisignlabs.com/

http://dnsviz.net/d/xyz.uni-owl.de/analyze/