DNS und DNSSEC

Eine Einführung

Simon Mittelberger

12. und 13. Januar, 2011

Domain Name System

Gliederung

Gliederung

Gliederung

Domain Name System

- Warum DNS?

Domain Name System

- Warum DNS?
  - 

Domain Name System

- Warum DNS?
  - 
- Aufgaben

Domain Name System

- Warum DNS?
  - 
- Aufgaben
  - Domain $\rightarrow$ IP

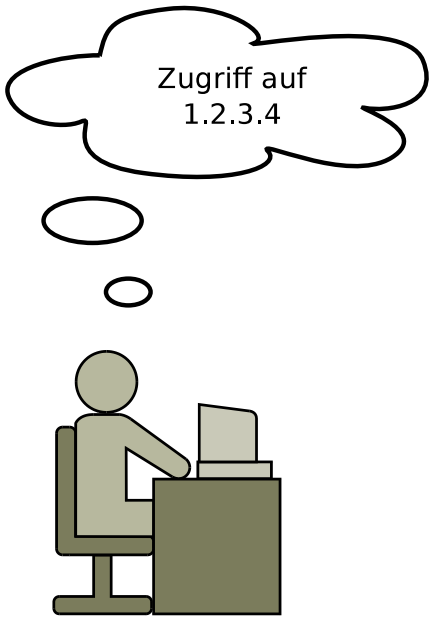
Domain Name System

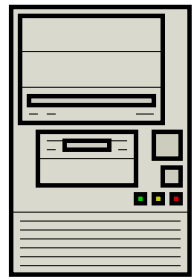
- Warum DNS?
  - 
- Aufgaben
  - Domain $\rightarrow$ IP
  - Domain $\leftarrow$ IP

Domain Name System

- Warum DNS?
  - 
- Aufgaben
  - Domain $\rightarrow$ IP
  - Domain $\leftarrow$ IP
- Ein weltweites System

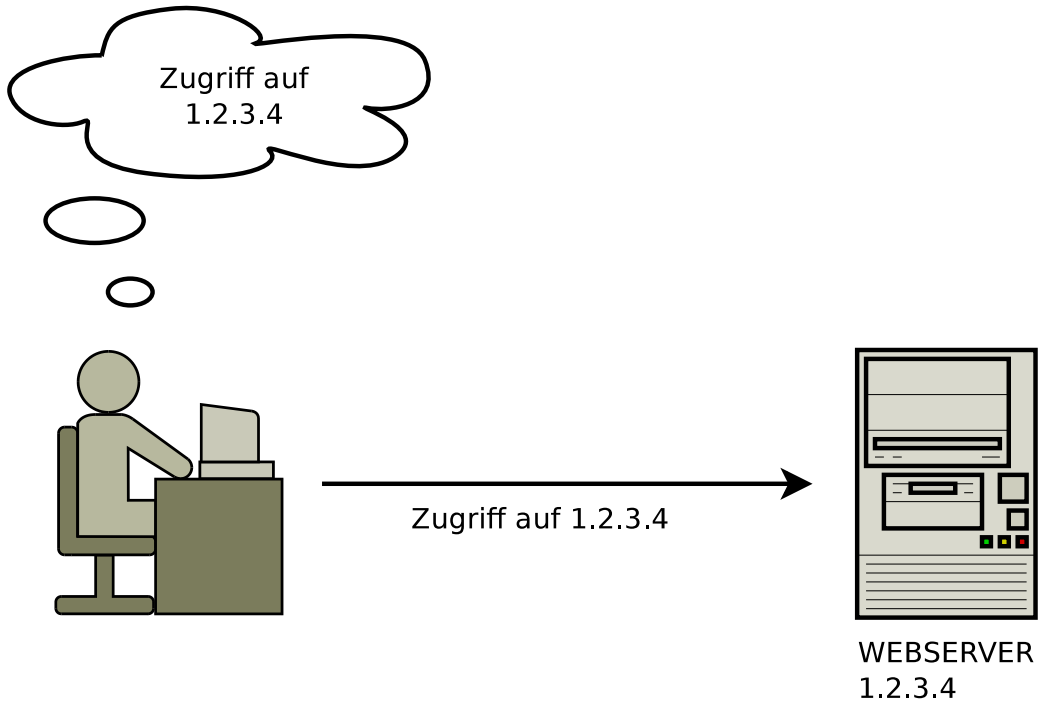
Motivation für DNS



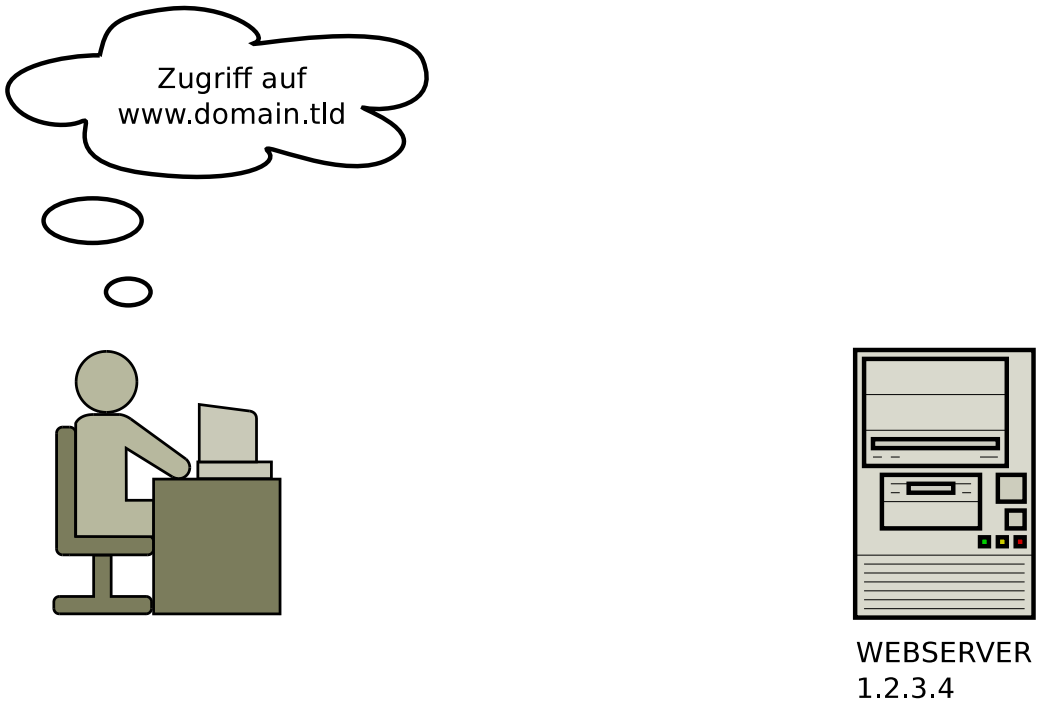


WEBSERVER
1.2.3.4

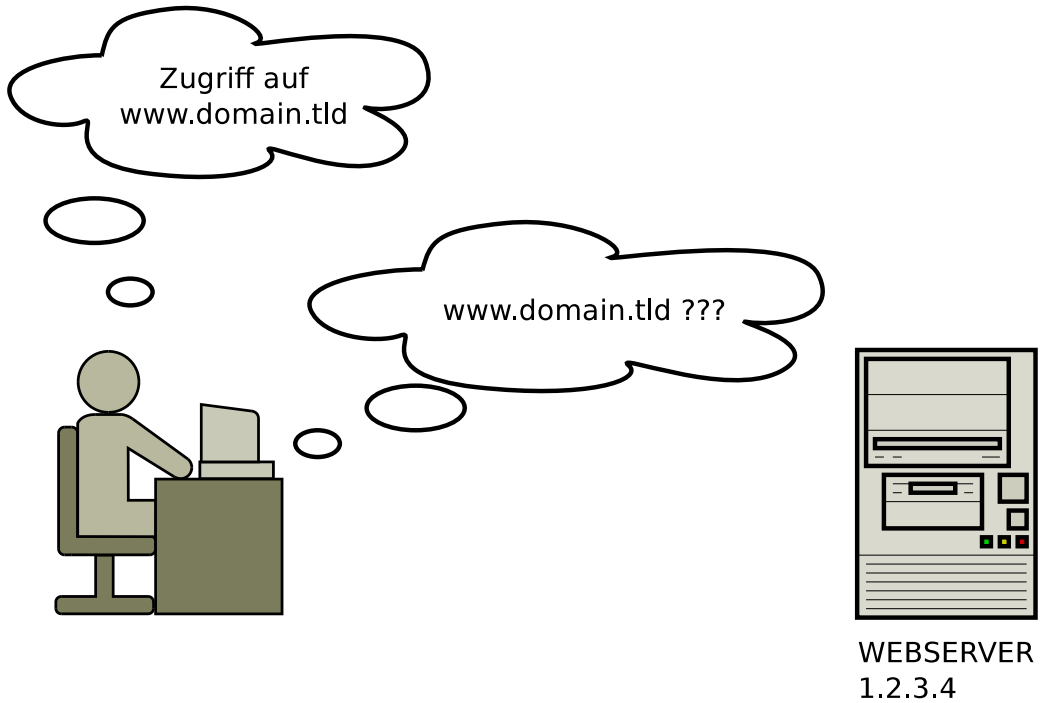
Motivation für DNS



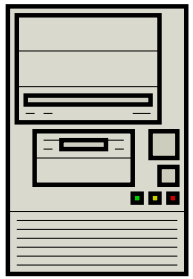
Motivation für DNS



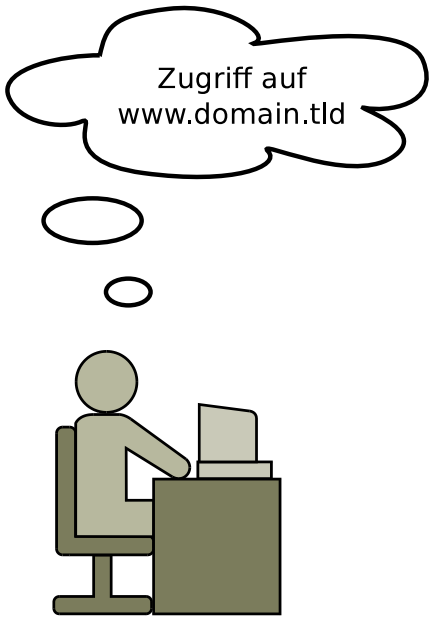
Motivation für DNS

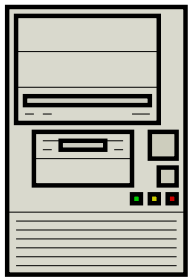


Nameserver



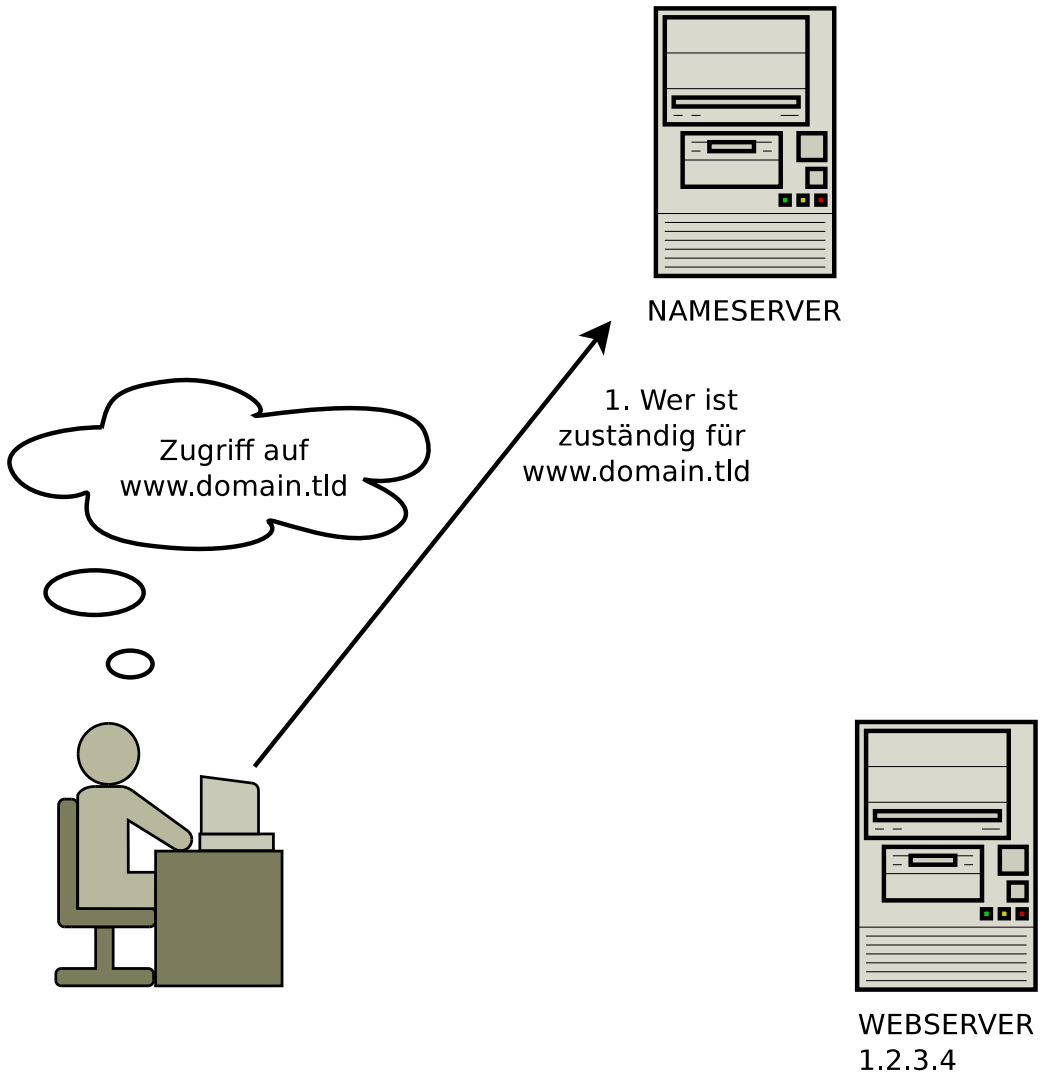
NAMESERVER



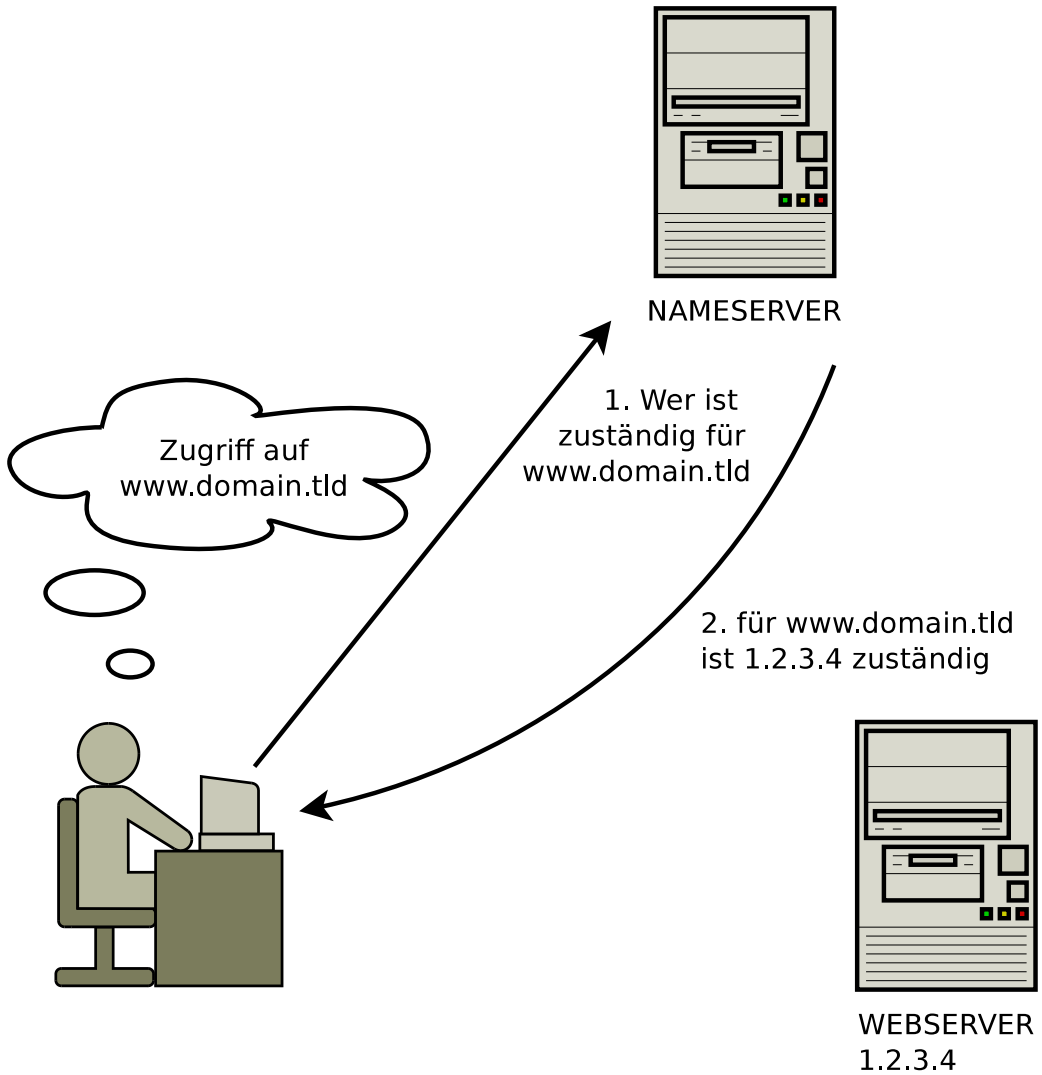


WEBSERVER
1.2.3.4

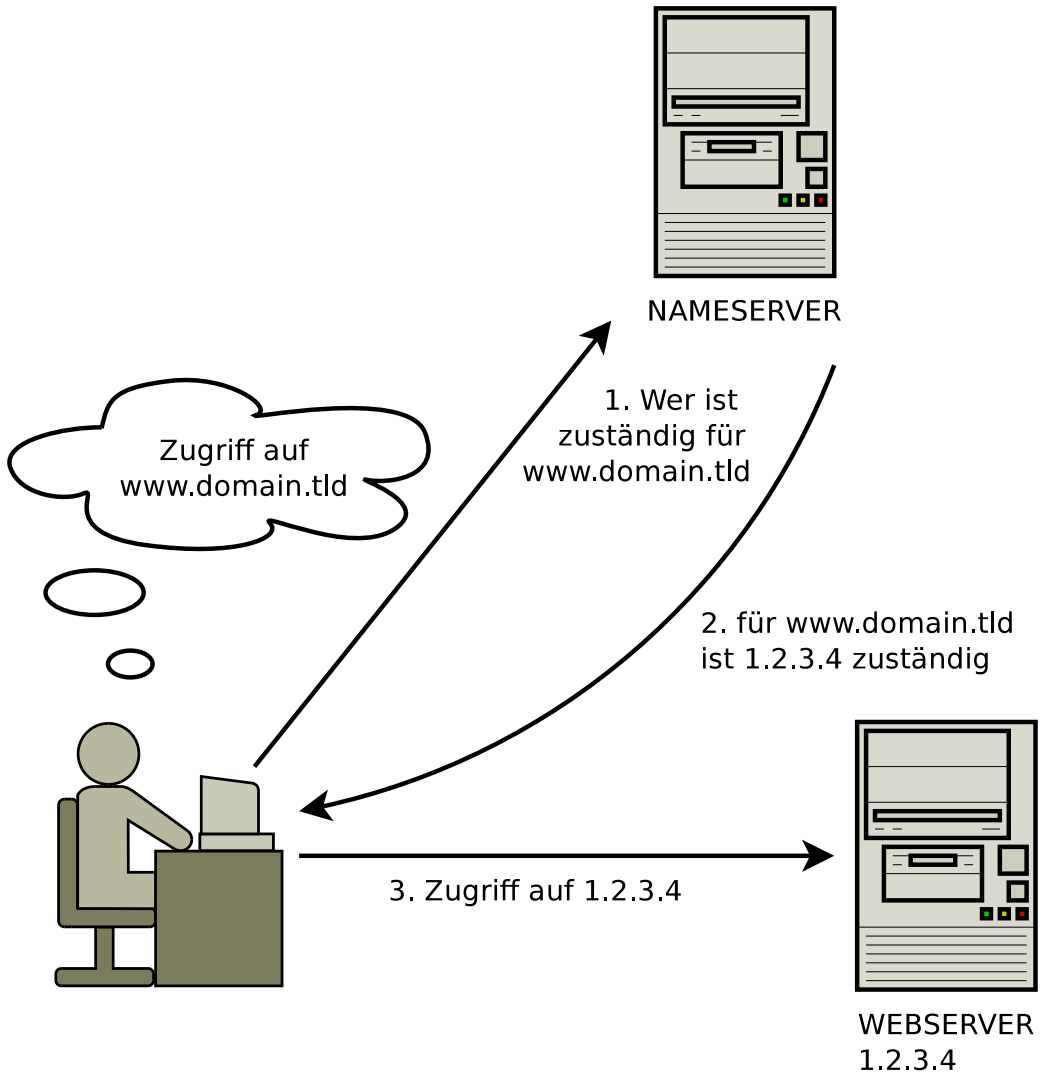
Nameserver


NAMESERVER
1. Wer ist zuständig für www.domain.tld
Zugriff auf www.domain.tld
WEBSERVER
1.2.3.4

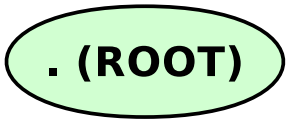
Nameserver


NAMESERVER
Zugriff auf
www.domain.tld
1. Wer ist
zuständig für
www.domain.tld
2. für www.domain.tld
ist 1.2.3.4 zuständig
WEBSERVER
1.2.3.4

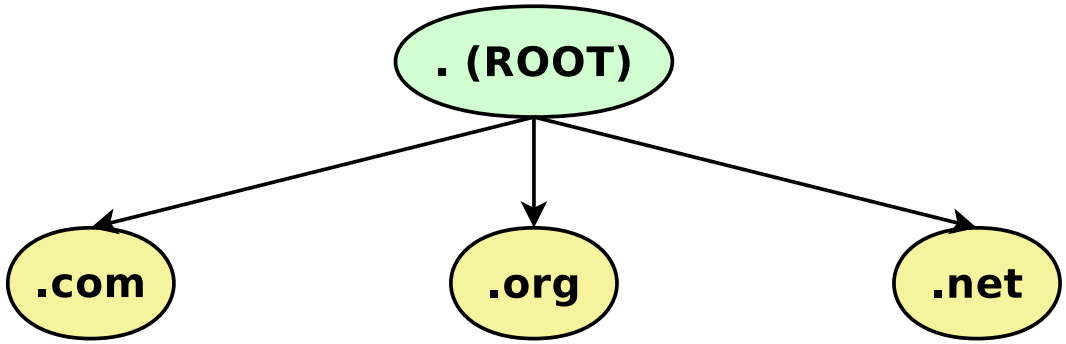
Nameserver


NAMESERVER
Zugriff auf
www.domain.tld
1. Wer ist
zuständig für
www.domain.tld
2. für www.domain.tld
ist 1.2.3.4 zuständig
3. Zugriff auf 1.2.3.4
WEBSERVER
1.2.3.4

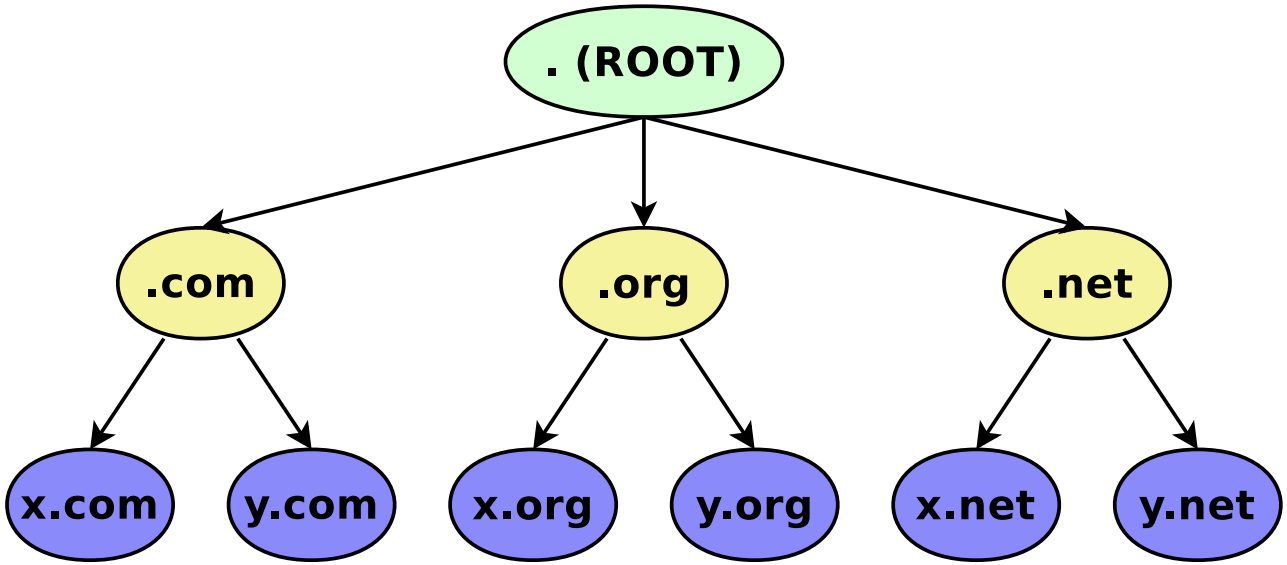
Hierarchie



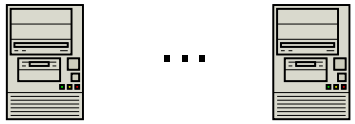
Hierarchie



Hierarchie

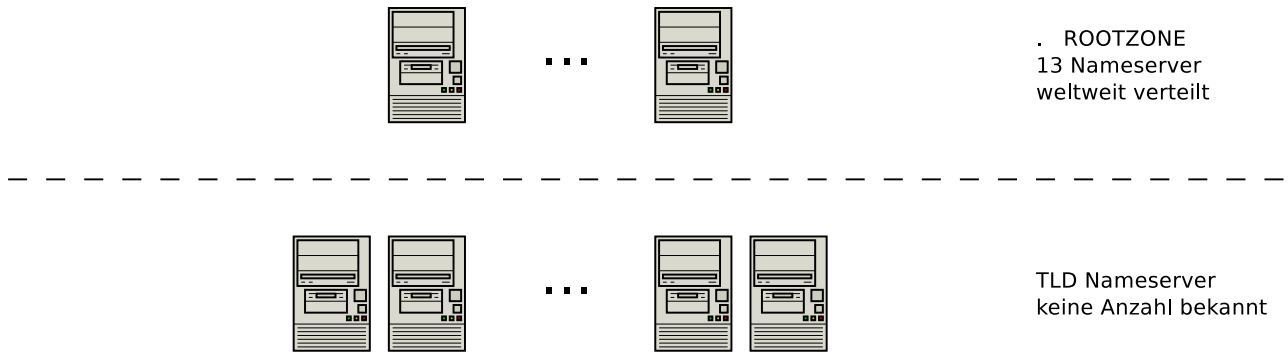


Infrastruktur

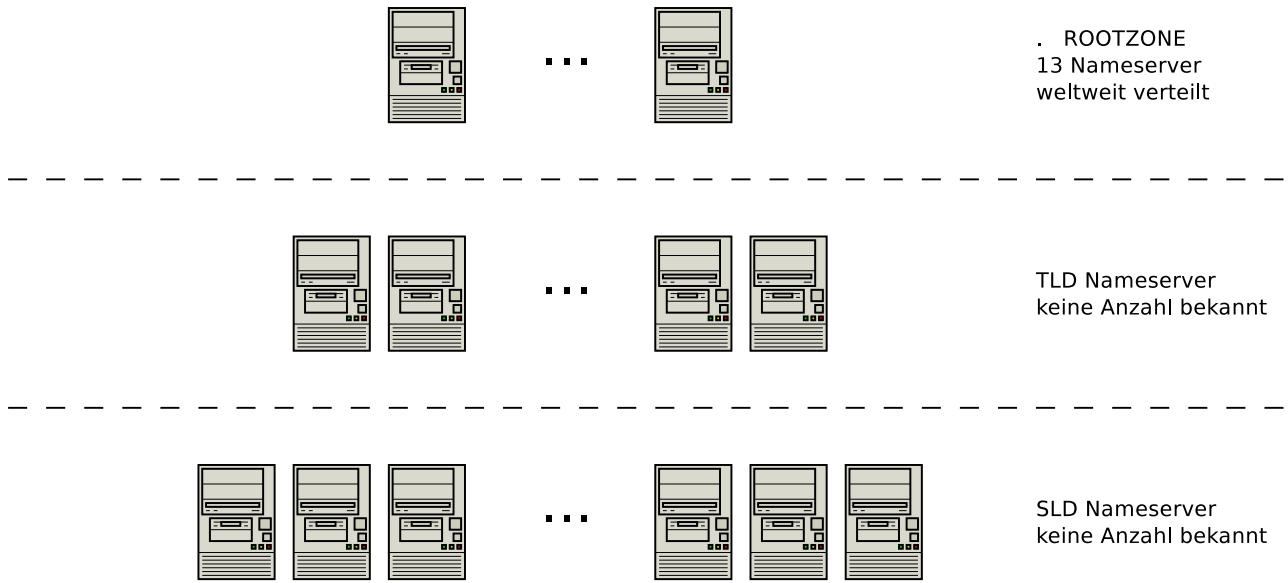


. ROOTZONE
13 Nameserver
weltweit verteilt

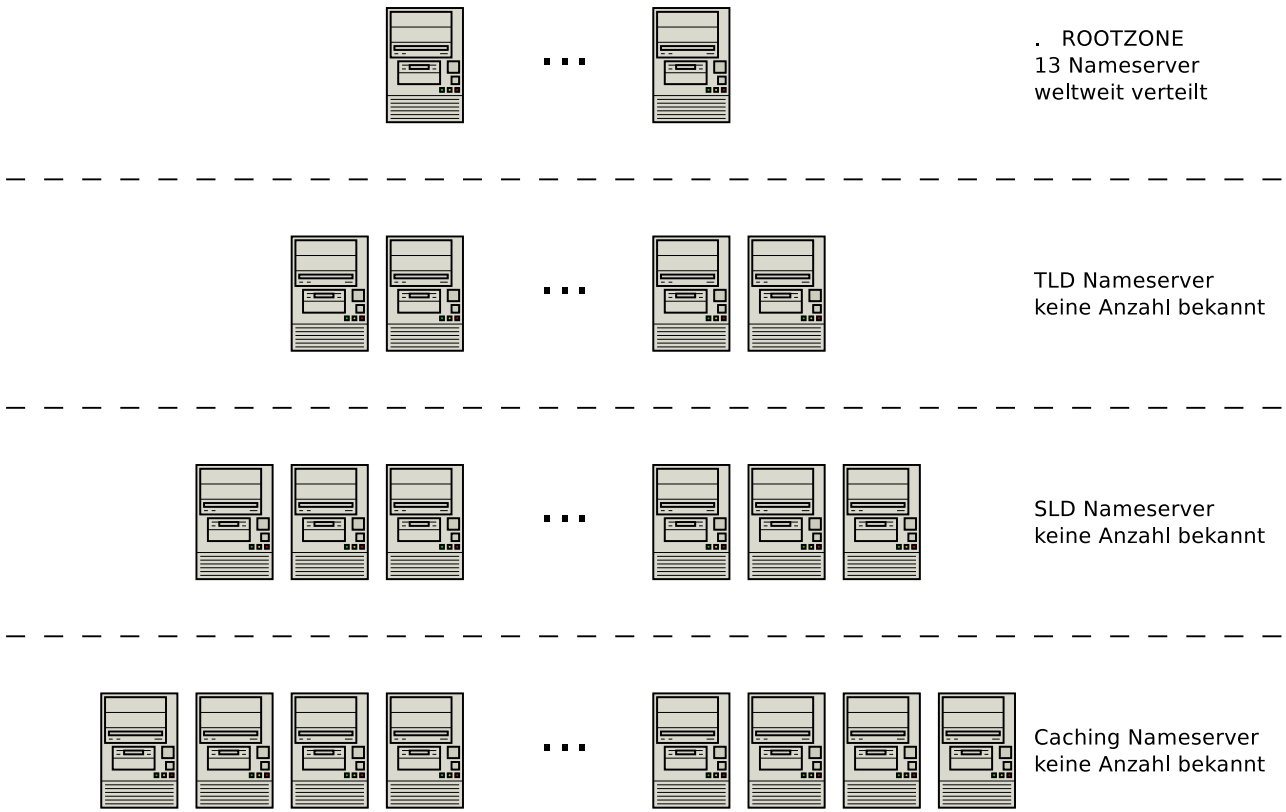
Infrastruktur



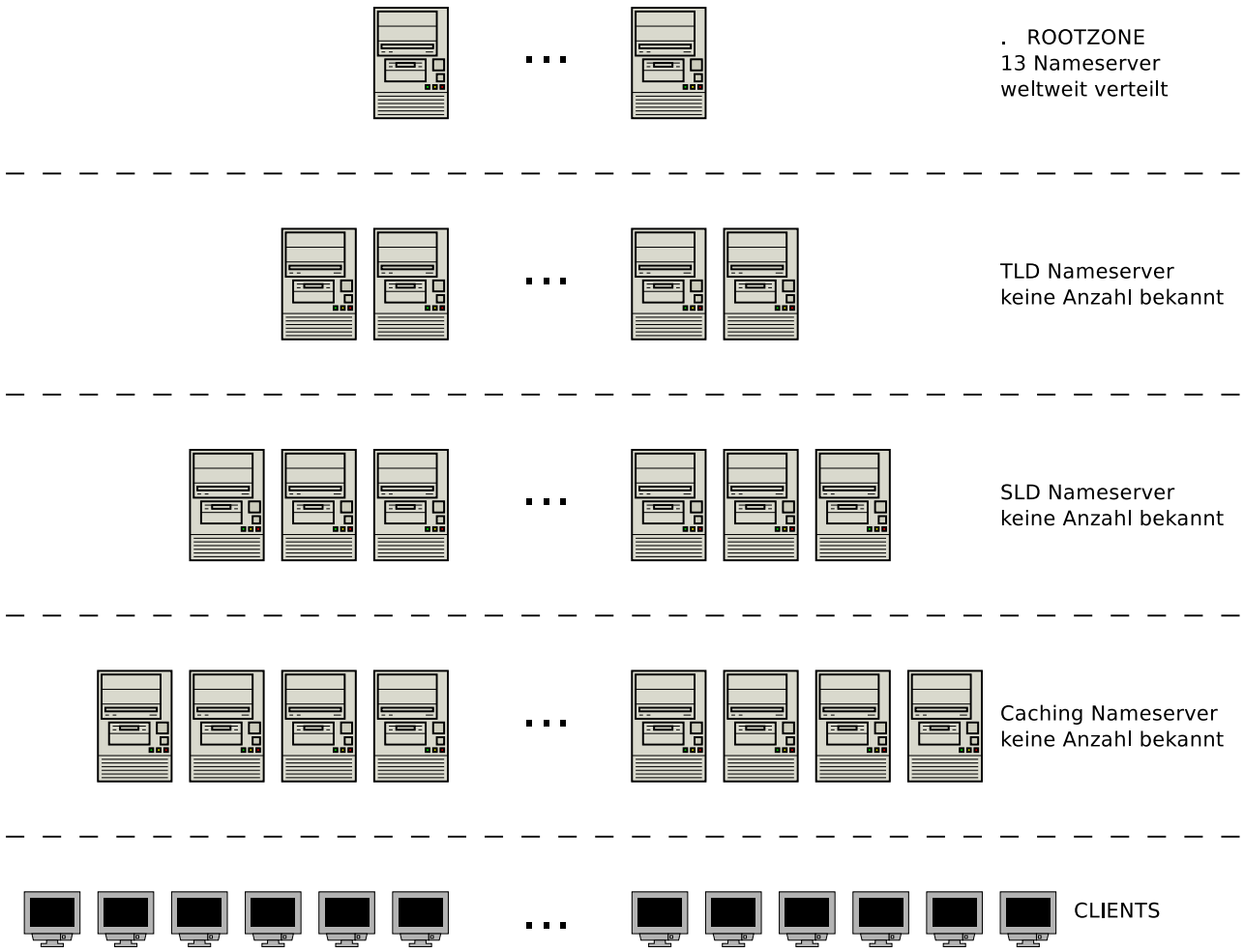
Infrastruktur



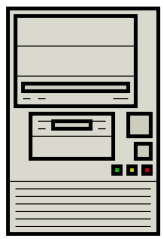
Infrastruktur

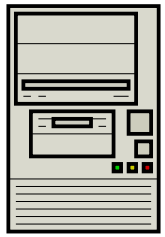


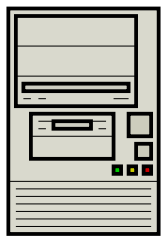
Infrastruktur

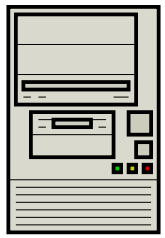


Funktionsweise

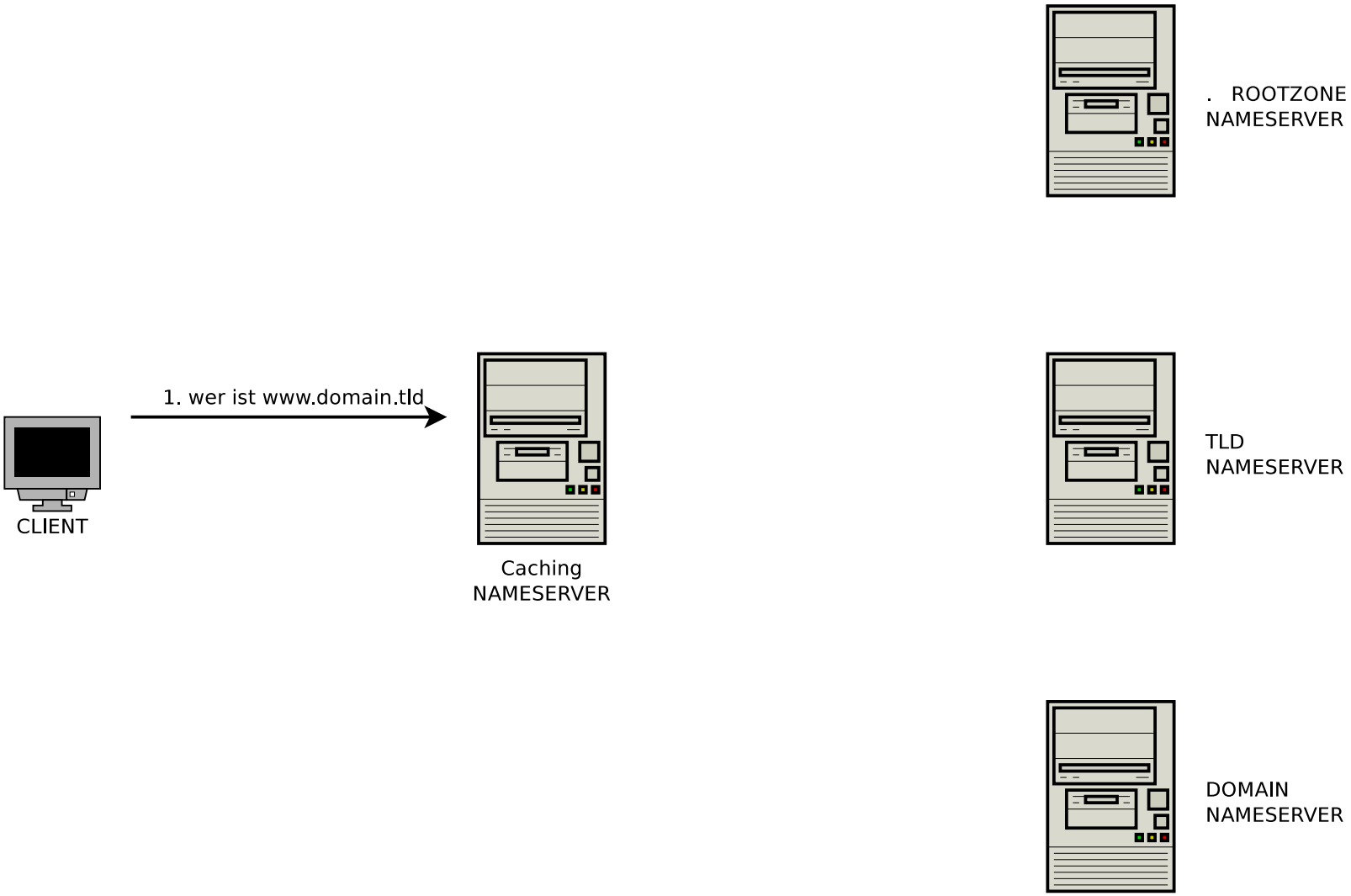




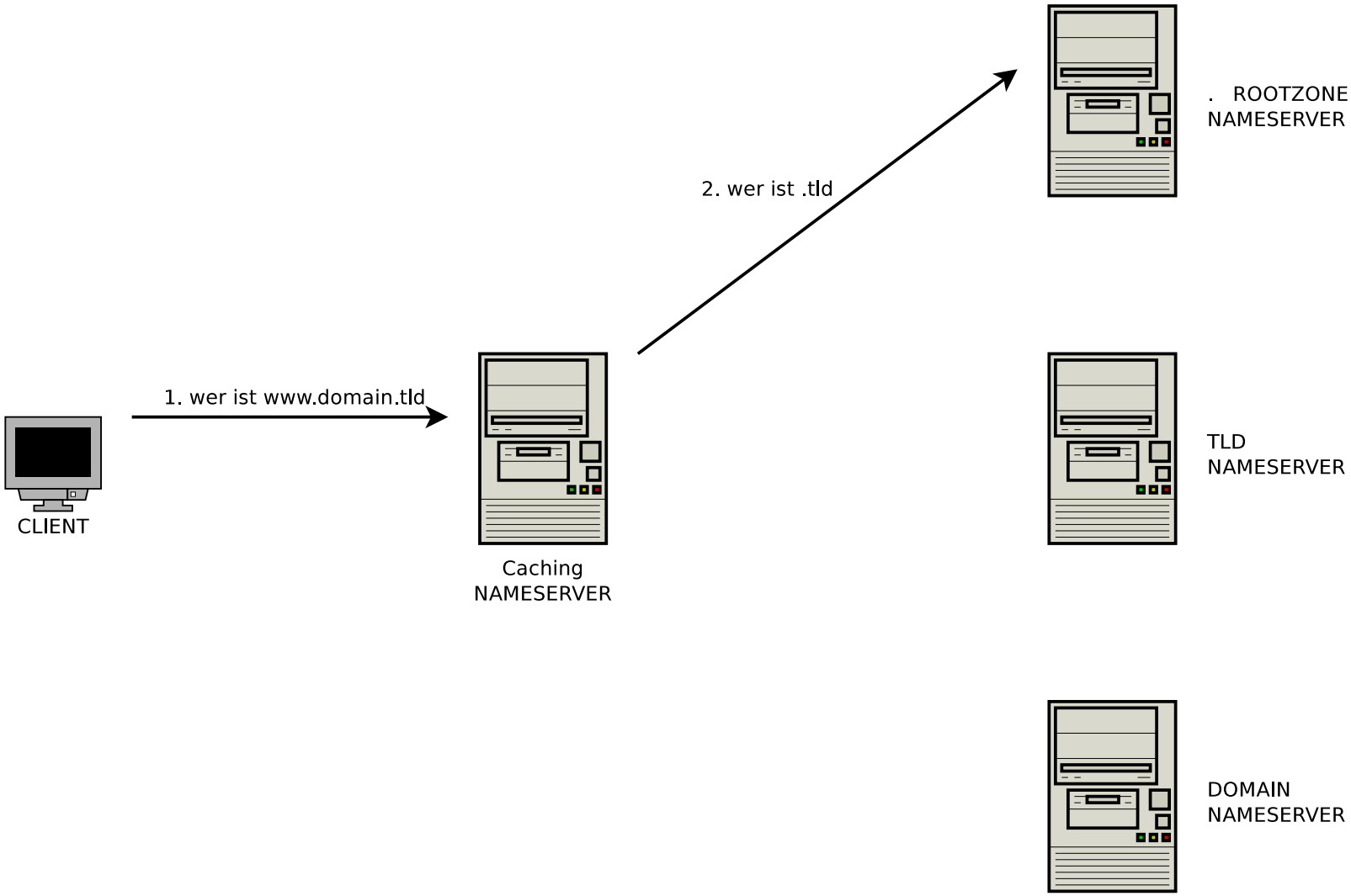




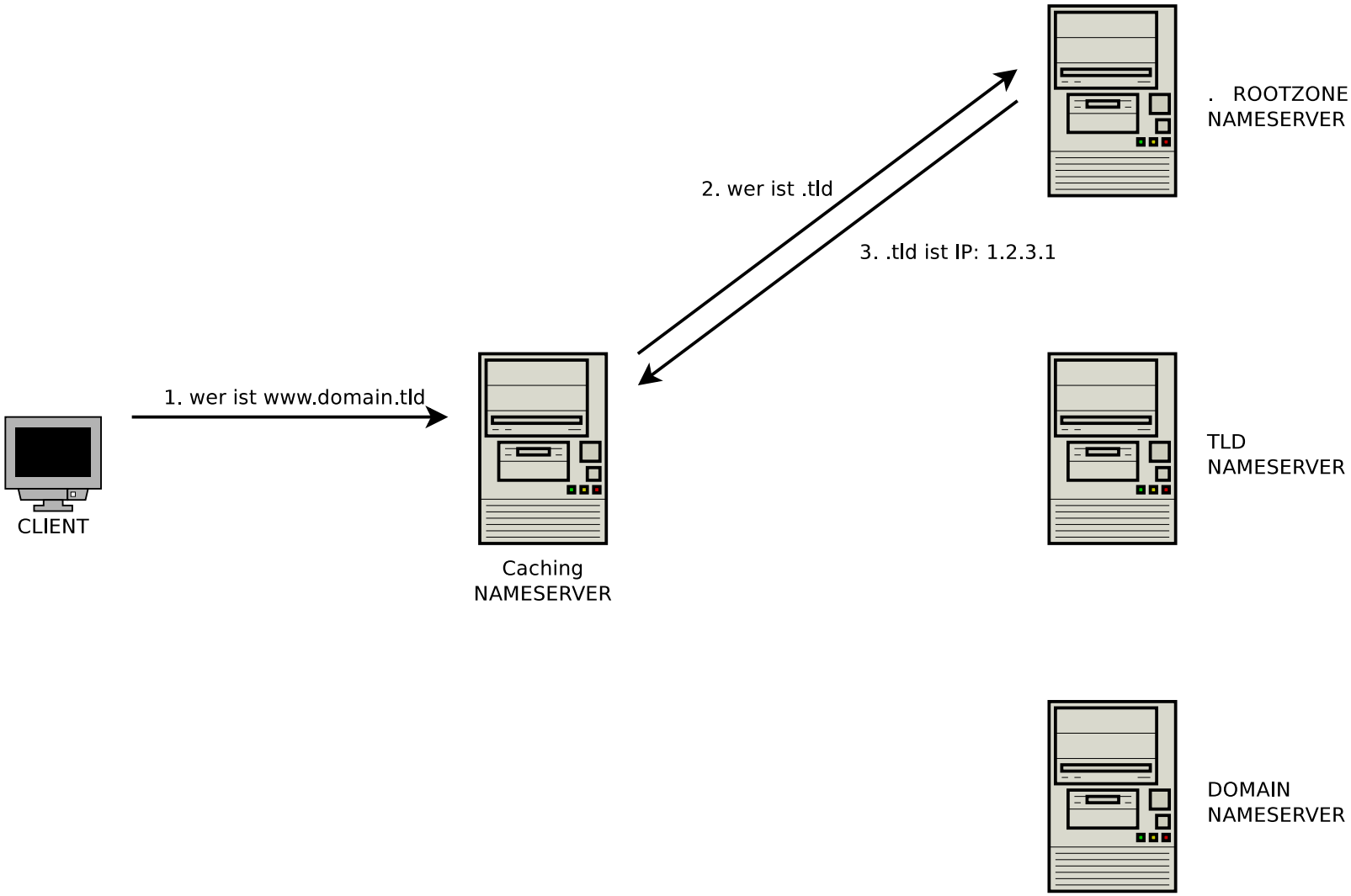
Funktionsweise



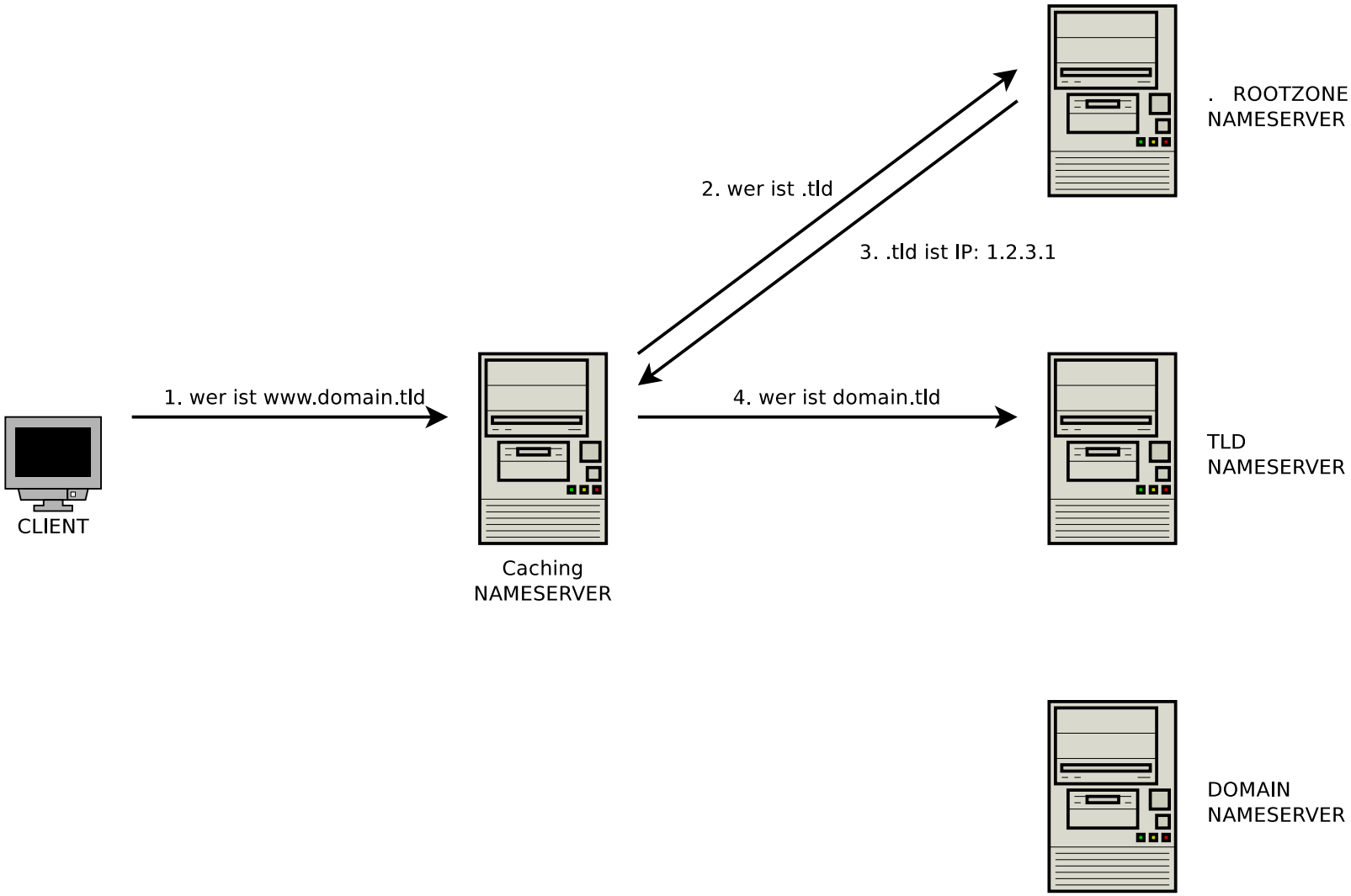
Funktionsweise



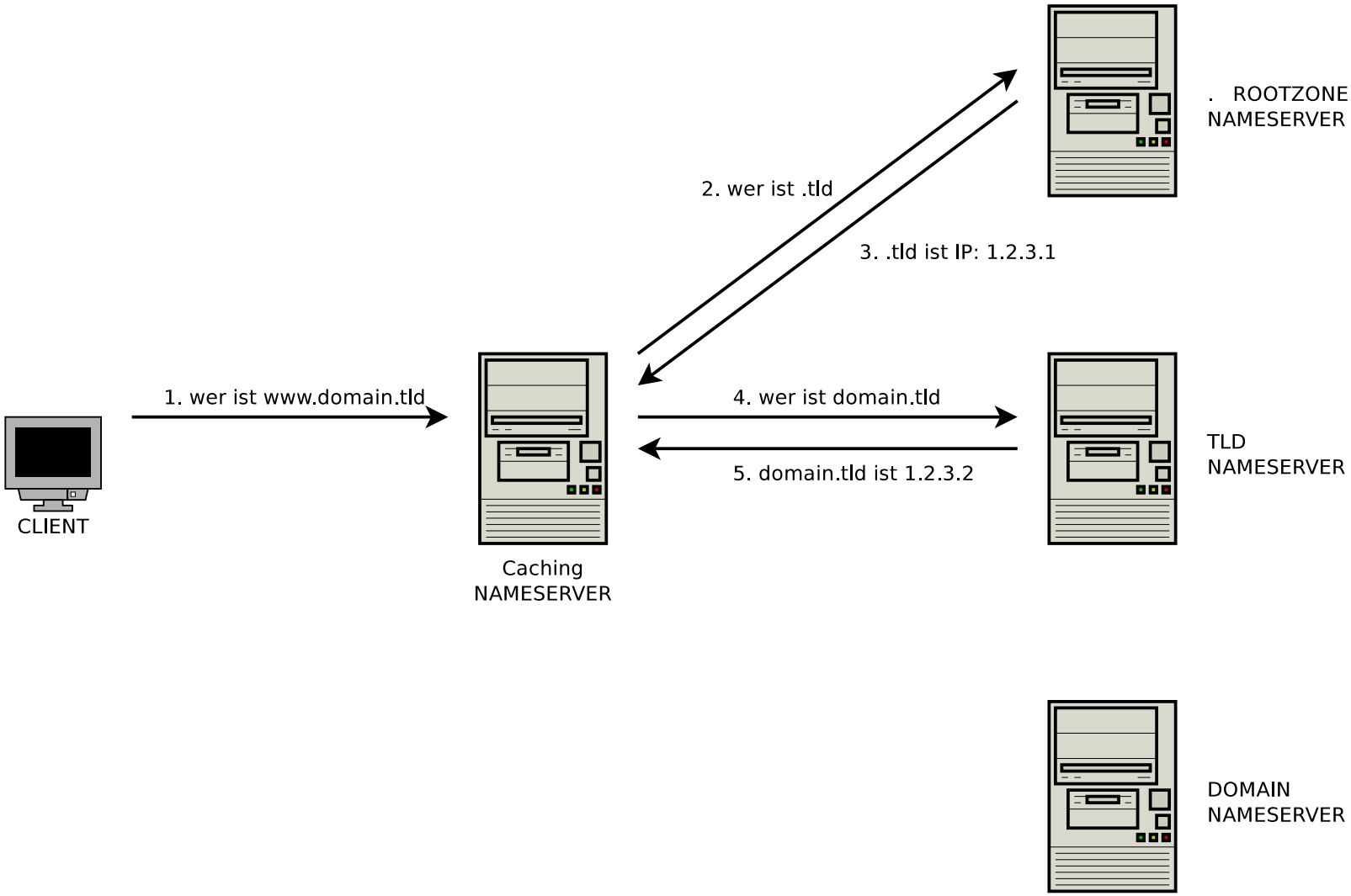
Funktionsweise



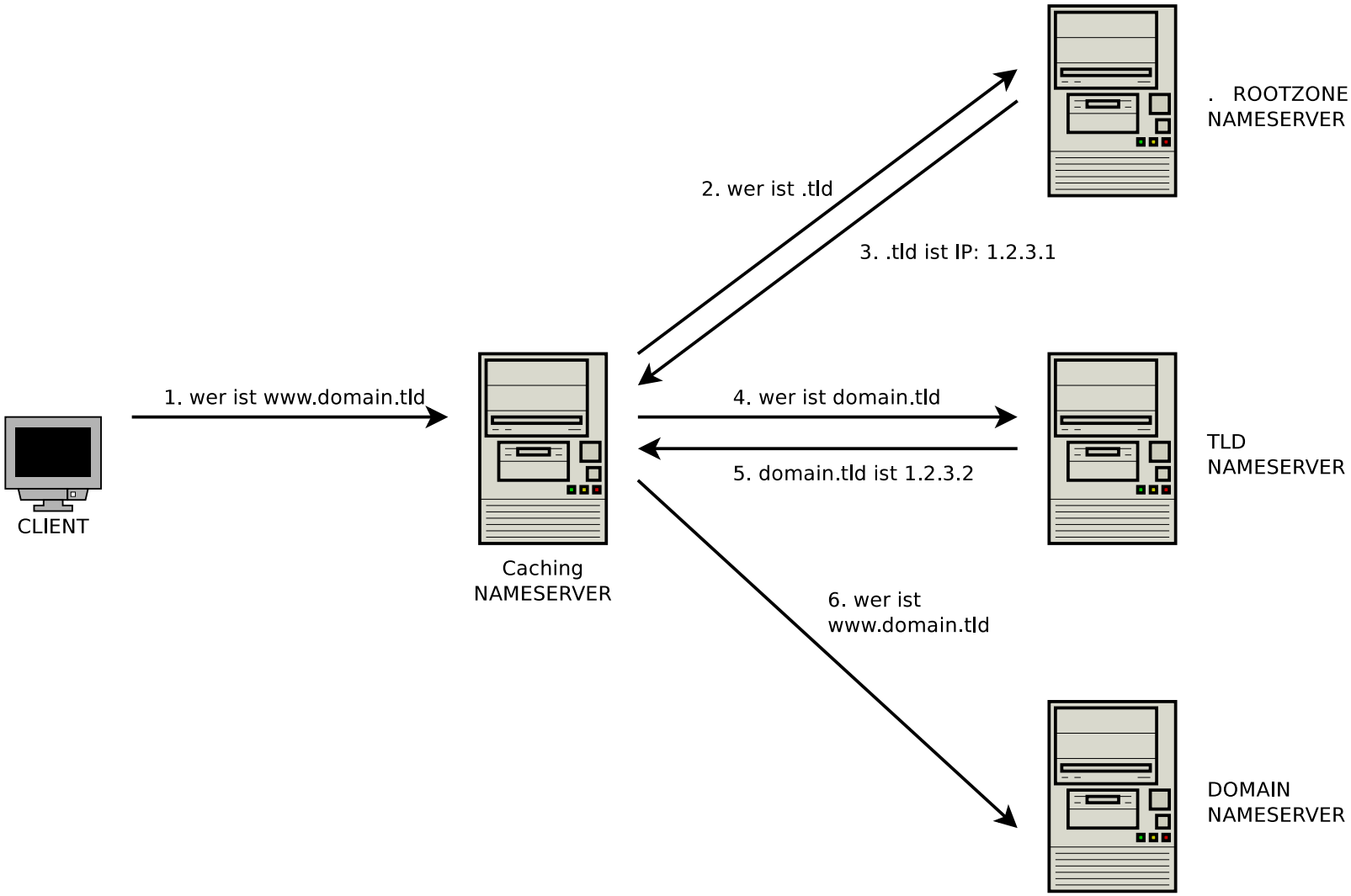
Funktionsweise



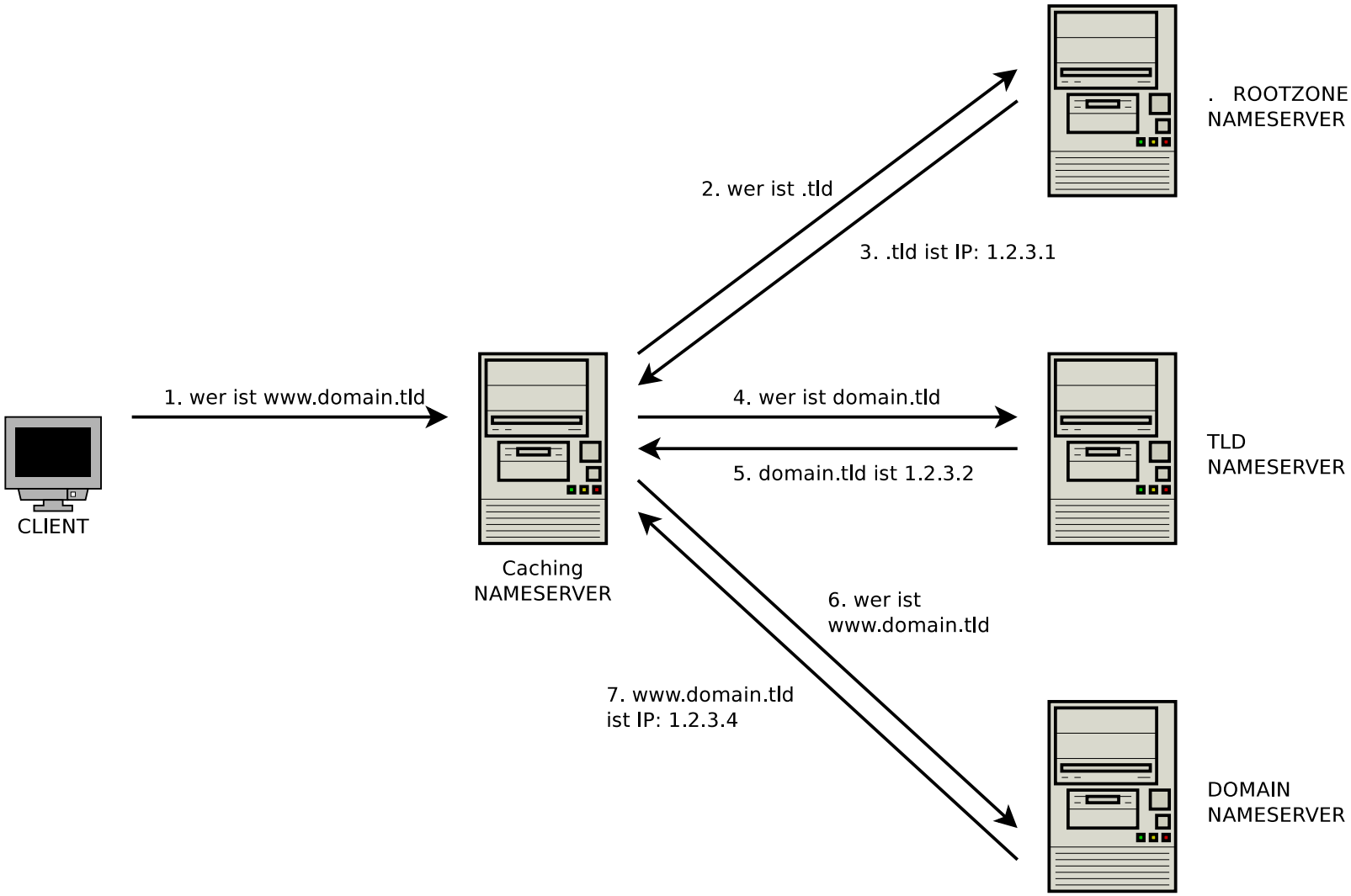
Funktionsweise



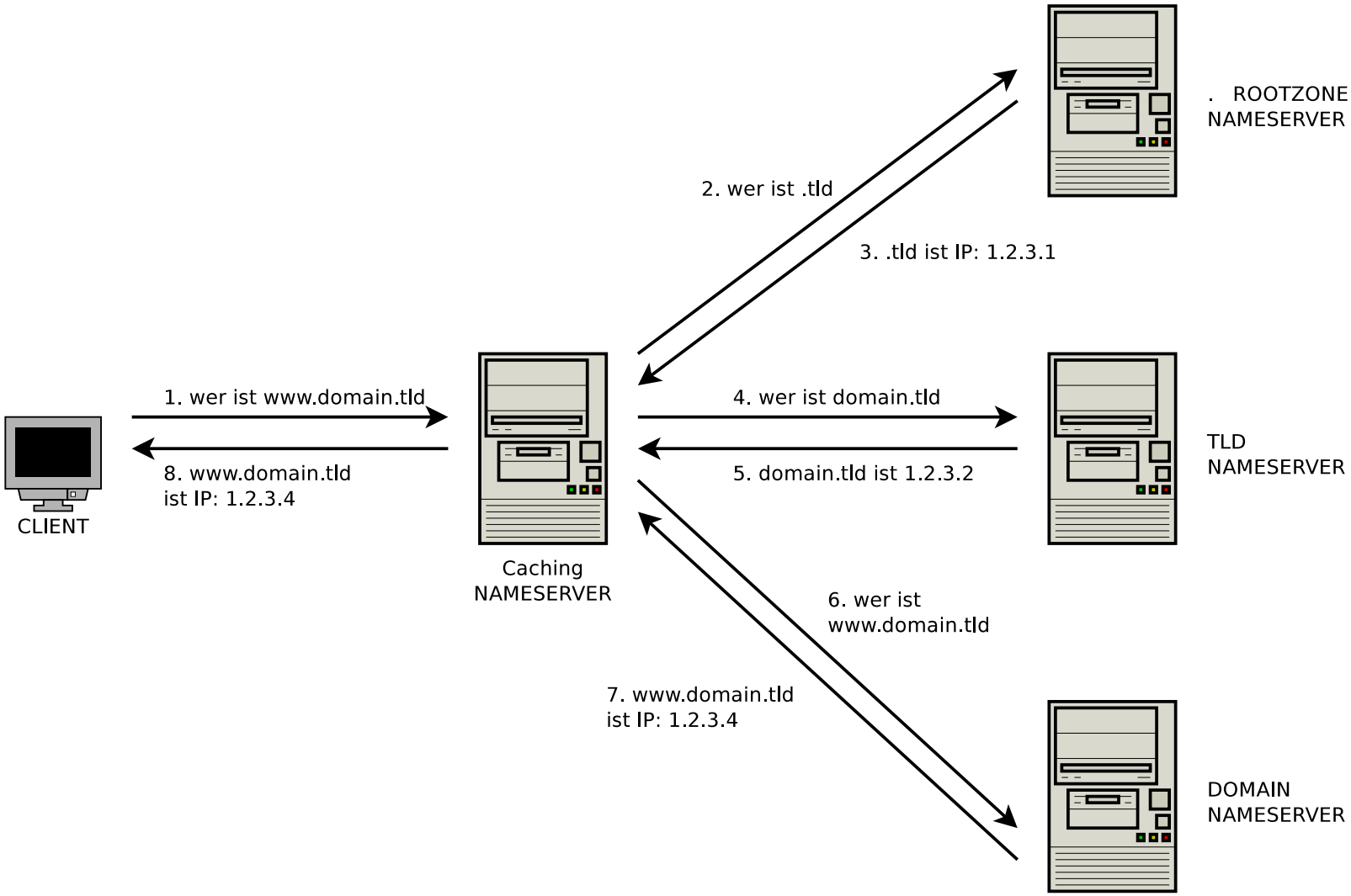
Funktionsweise



Funktionsweise



Funktionsweise



DNS Records

A	IPv4-Adresse
AAAA	IPv6-Adresse
NS	Authoritativer Nameserver
MX	Mailserver für die Domain
CNAME	Definition von Aliasen
SOA	Administrative Daten der Zone (z.B: Seriennummer, ...)
SPF	Berechtigt Mailserver zum versenden von Mails
PTR	Auflösung von IP-Adressen nach Namen

DNS Angriffe

- Ist DNS sicher?

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification

DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing

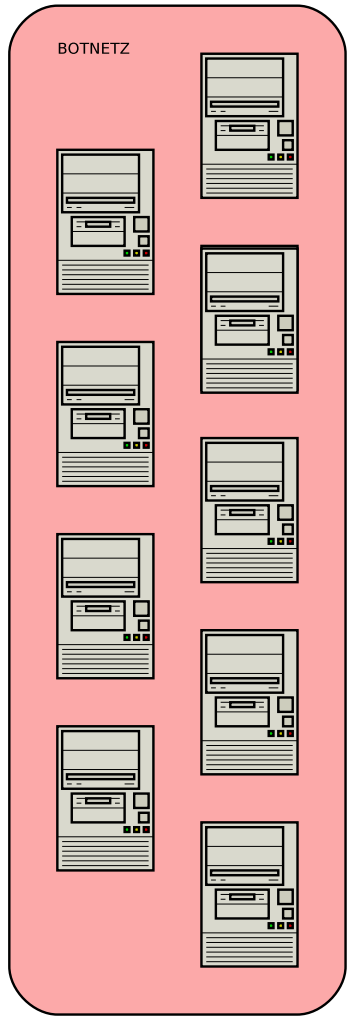
DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

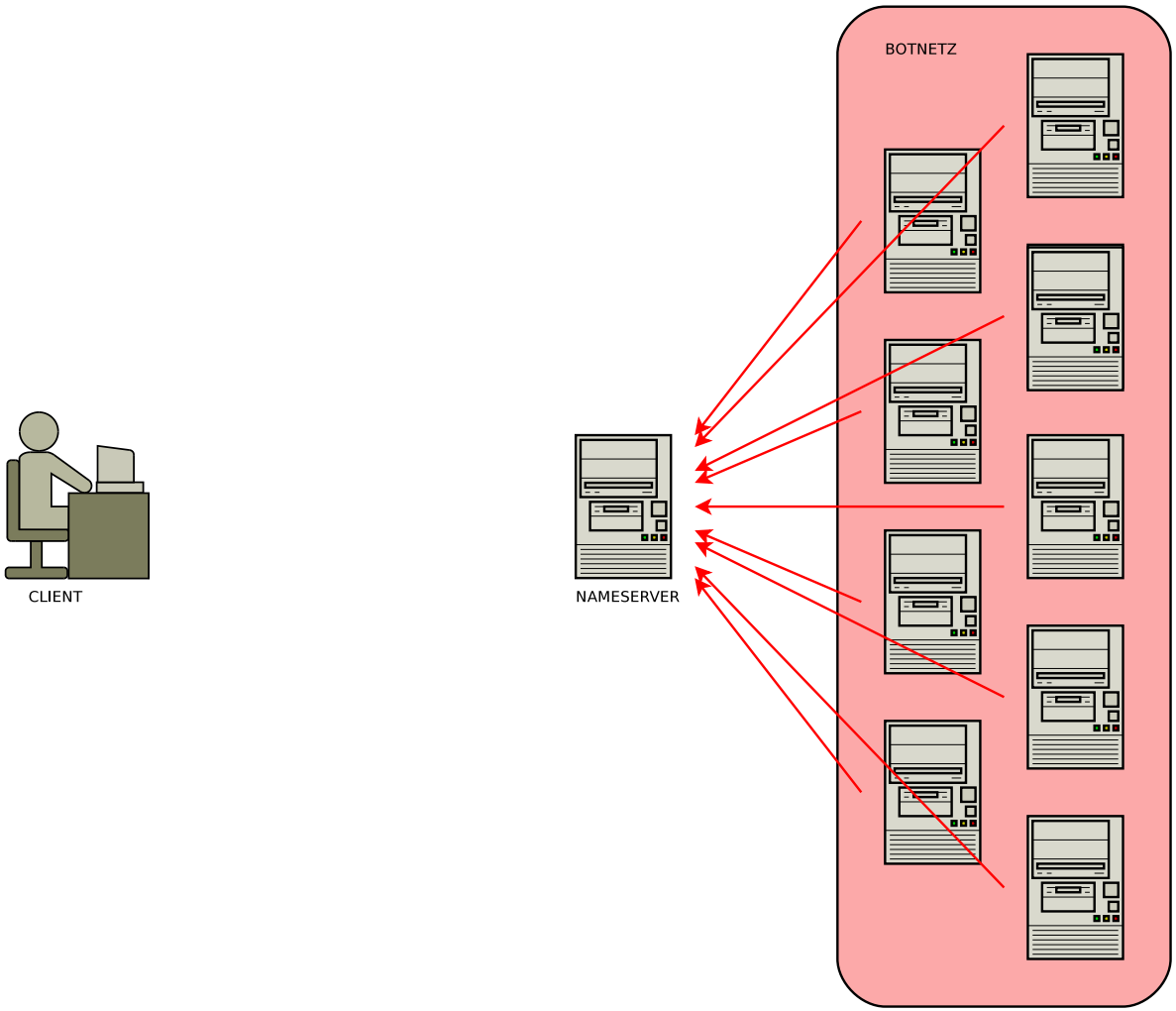
DDOS

CLIENT

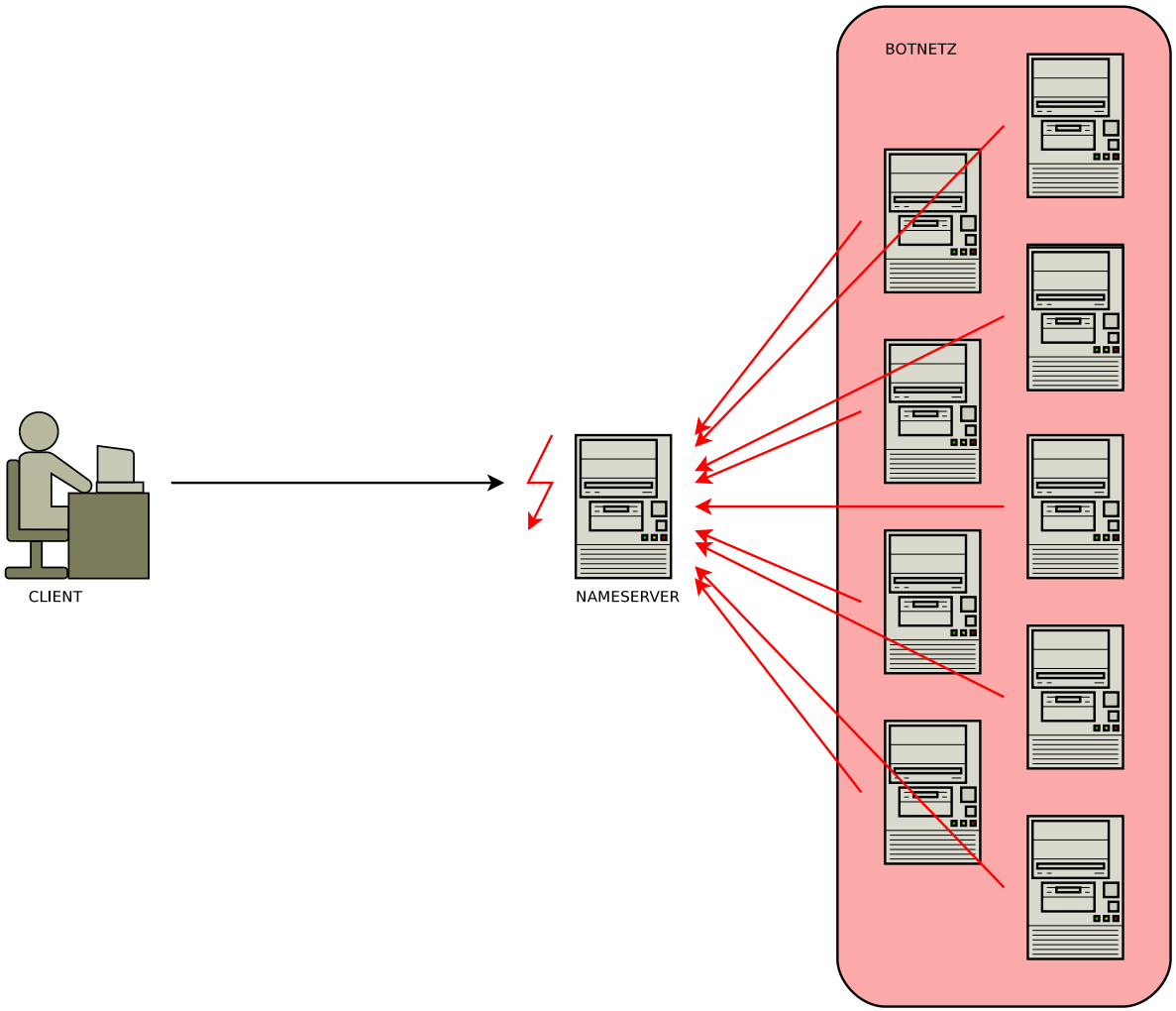
NAMESERVER



DDOS



DDOS

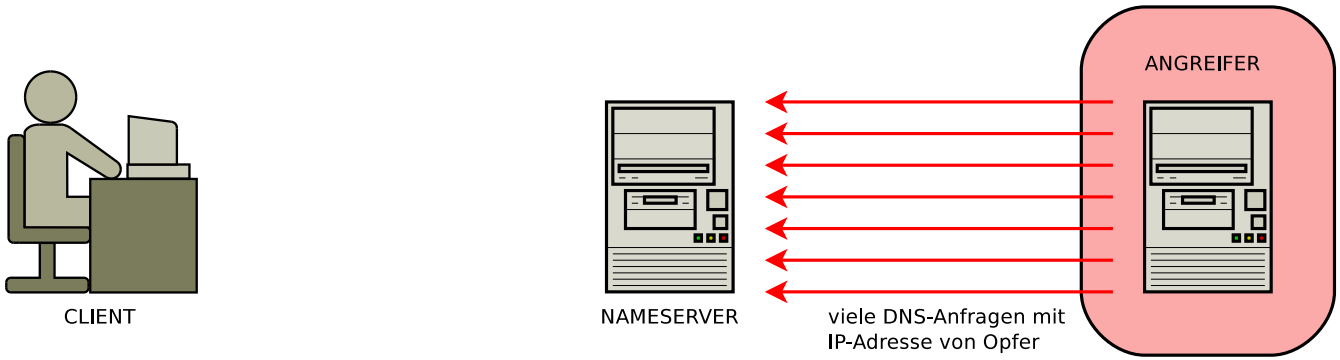


DNS Amplification

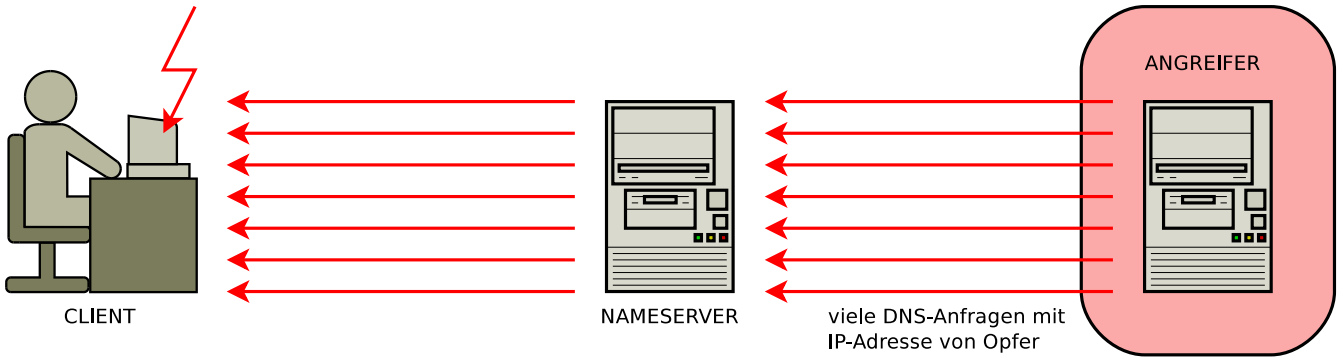
CLIENT

NAMESERVER

DNS Amplification



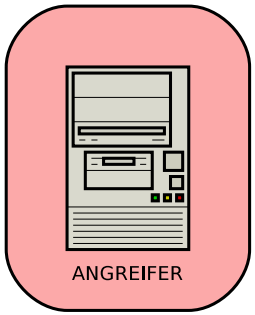
DNS Amplification



DNS-Spoofing

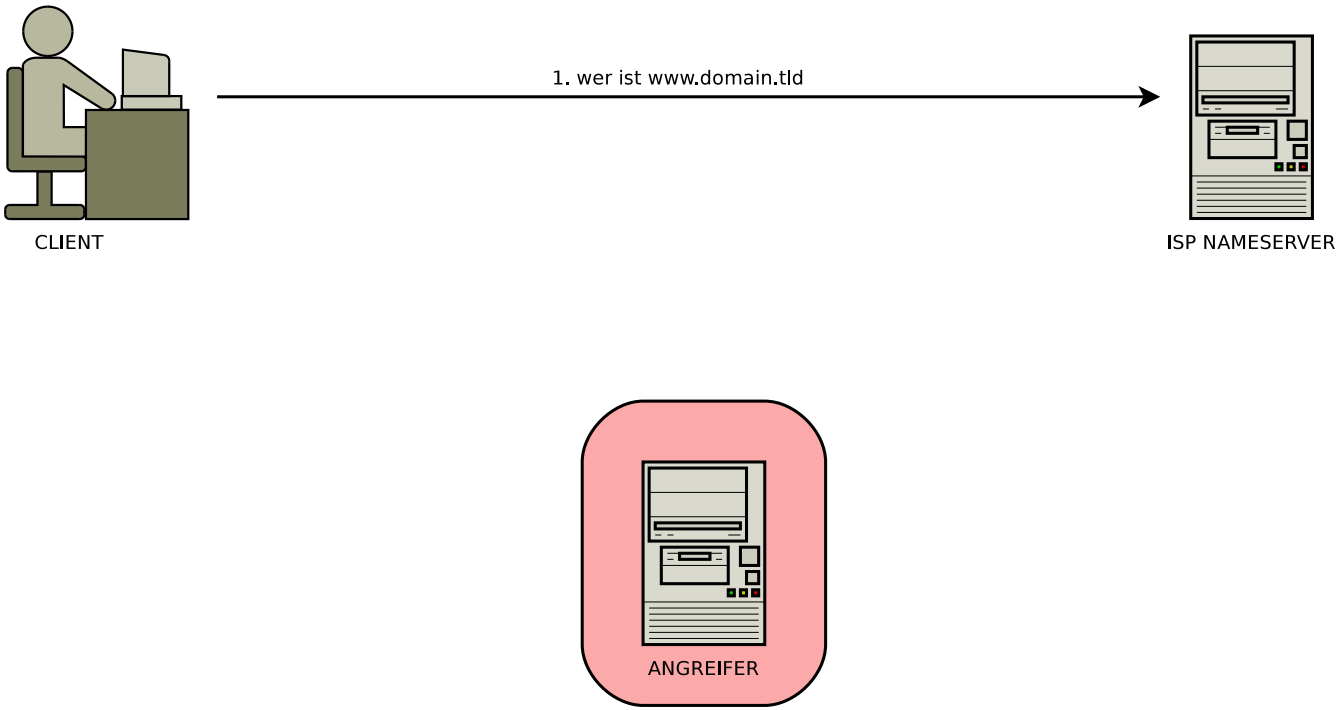
CLIENT

ISP NAMESERVER

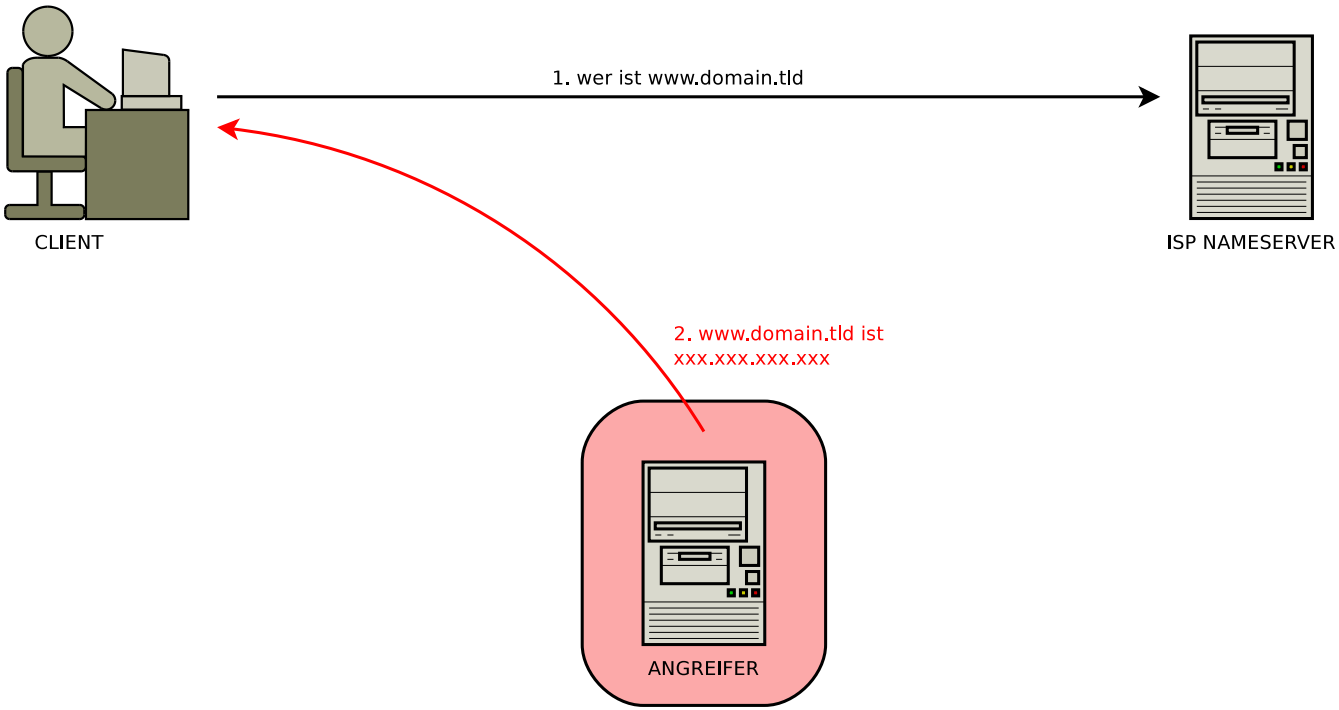


ANGREIFER

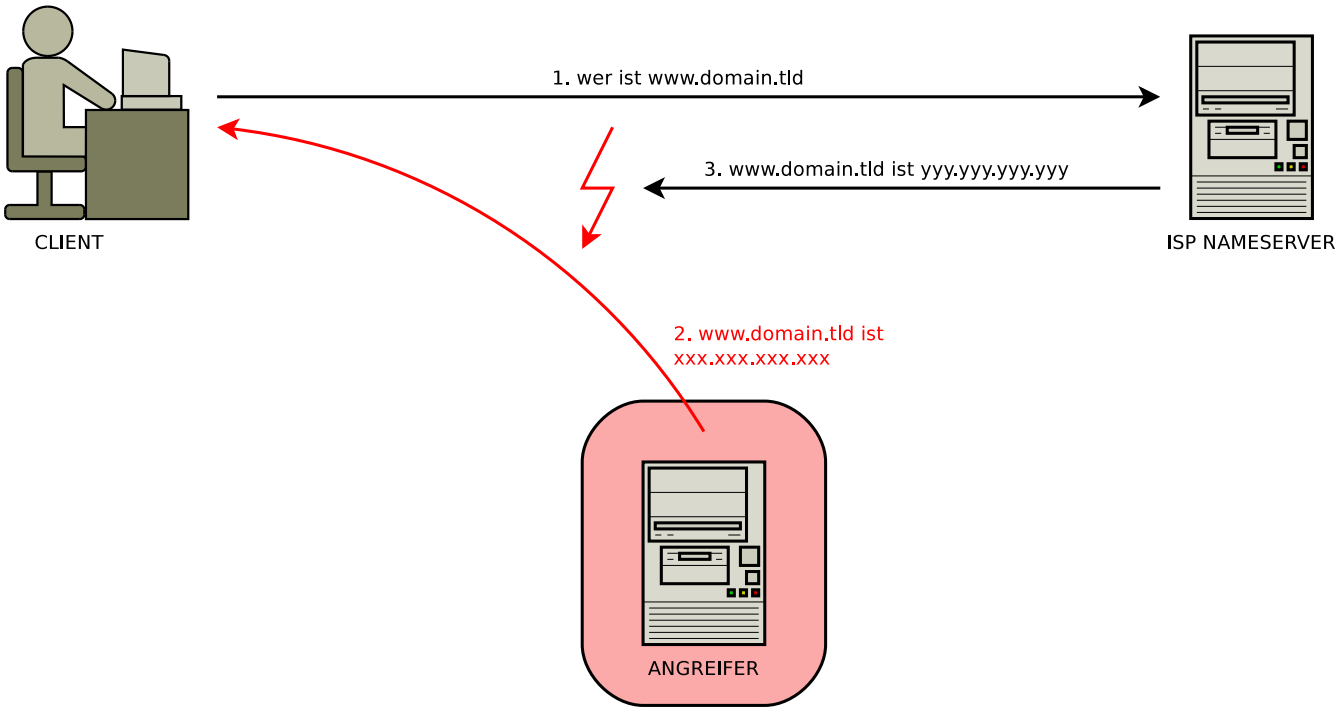
DNS-Spoofing



DNS-Spoofing



DNS-Spoofing



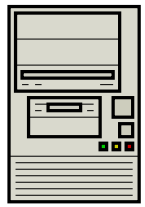
DNS-Cache-Poisoning

CLIENT 1

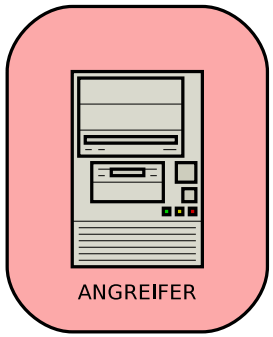
CLIENT 2

CLIENT 3

Caching NAMESERVER

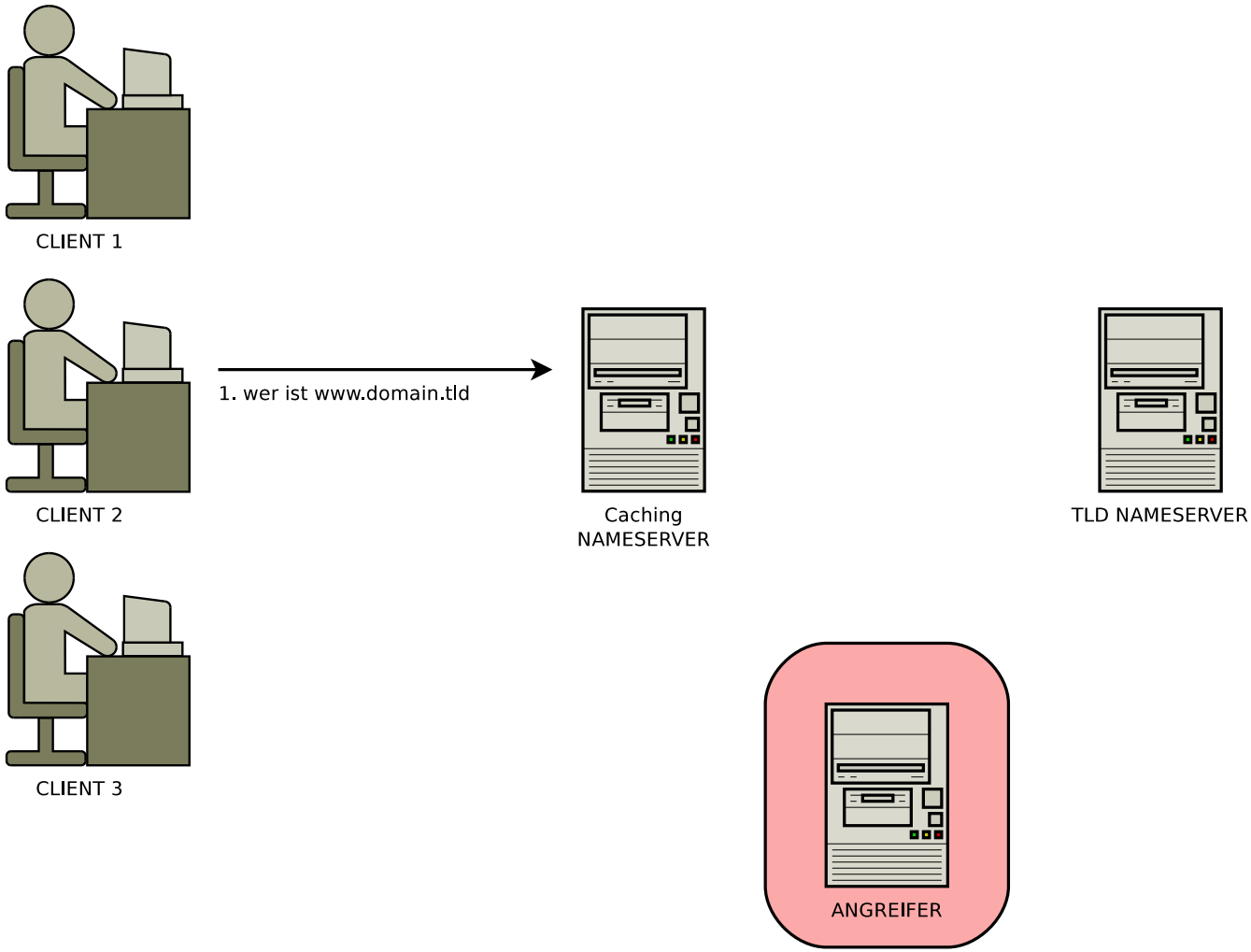


TLD NAMESERVER

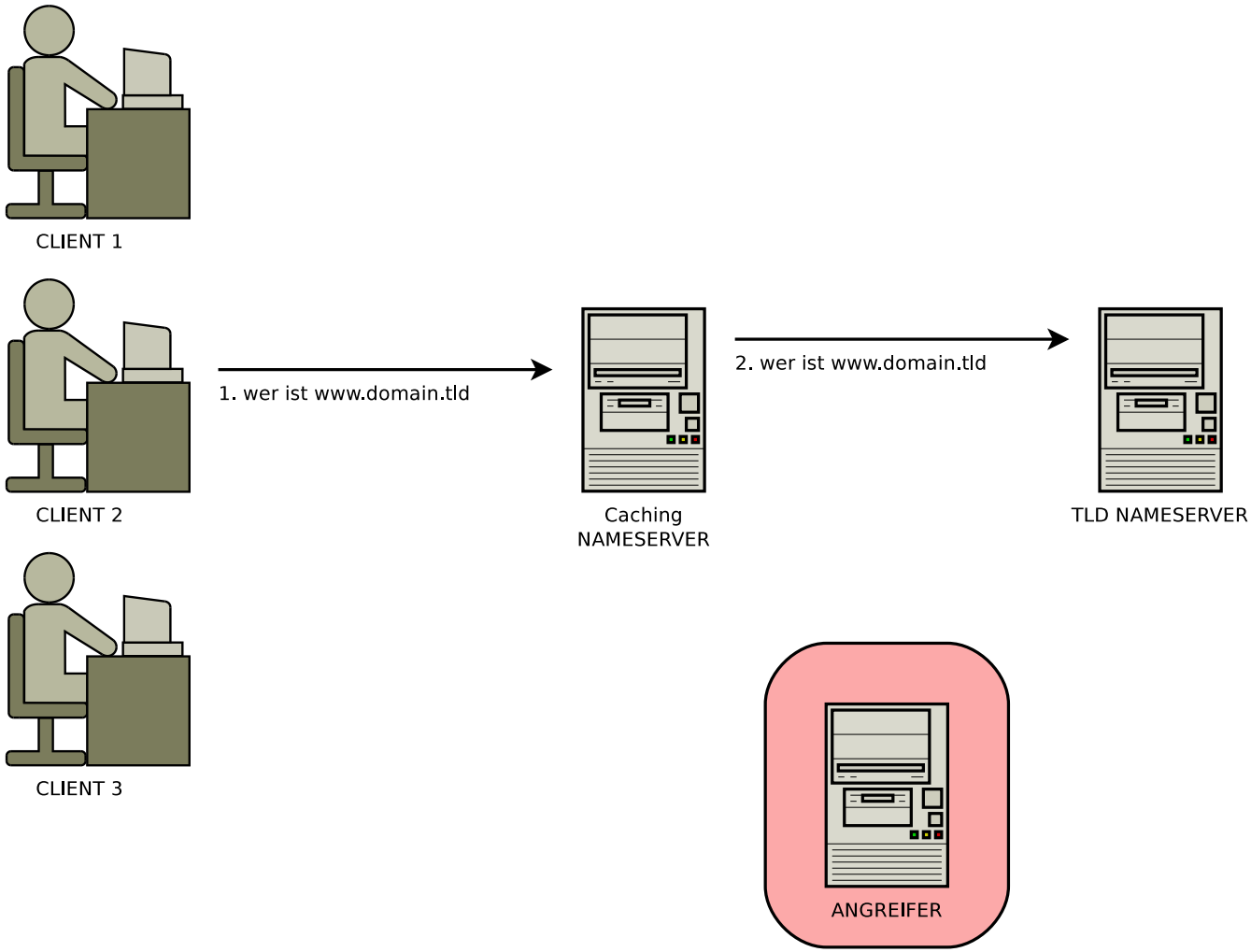


ANGREIFER

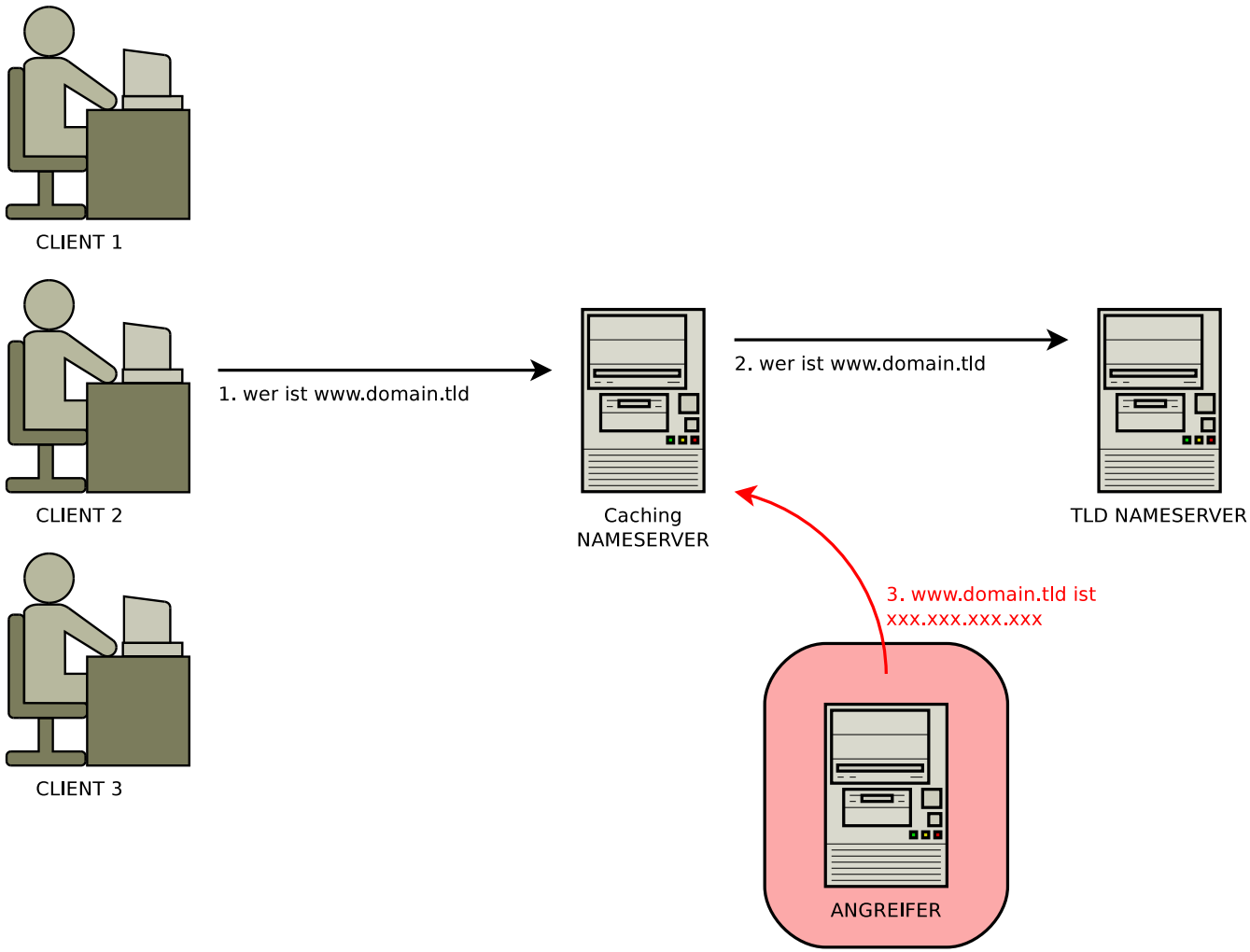
DNS-Cache-Poisoning



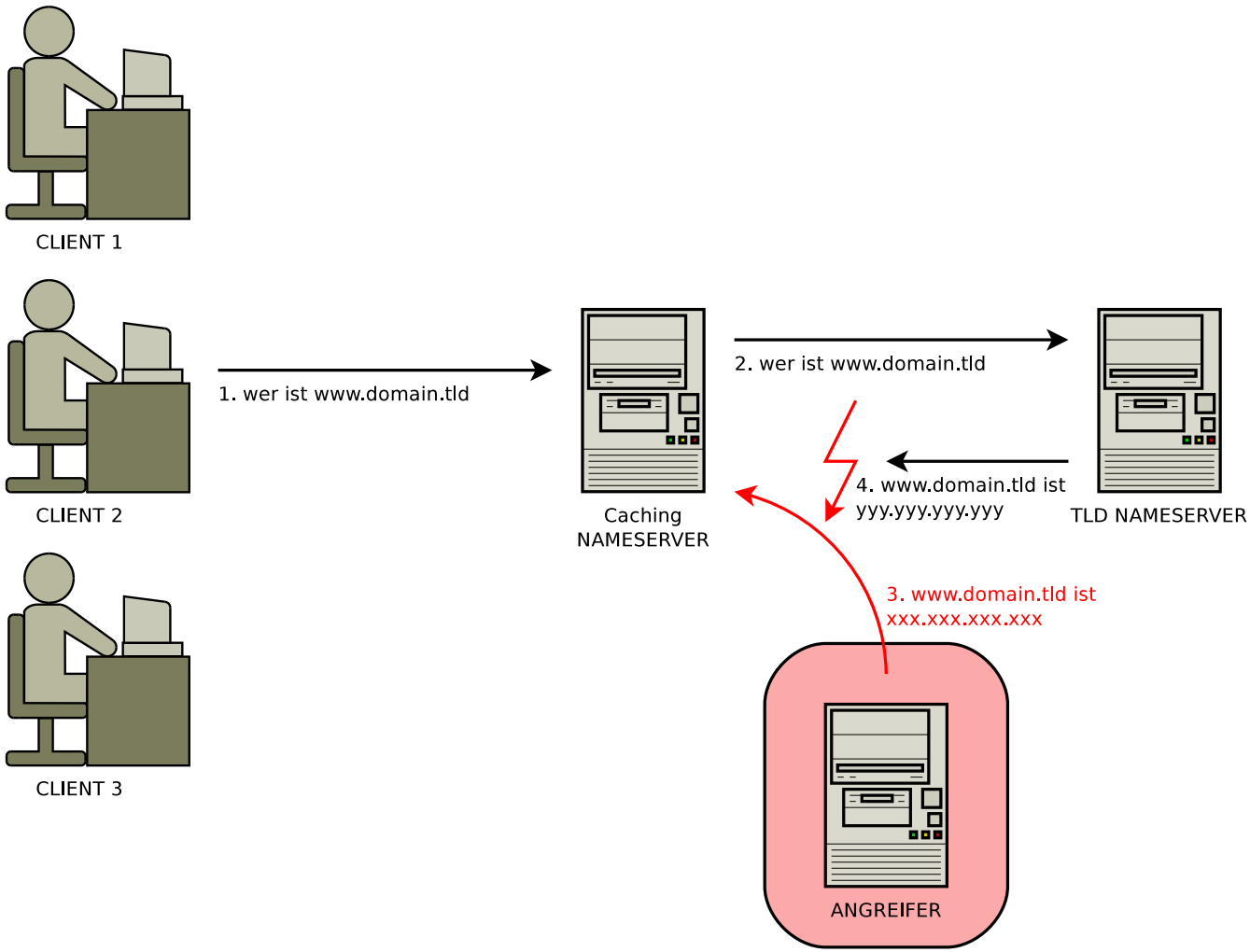
DNS-Cache-Poisoning



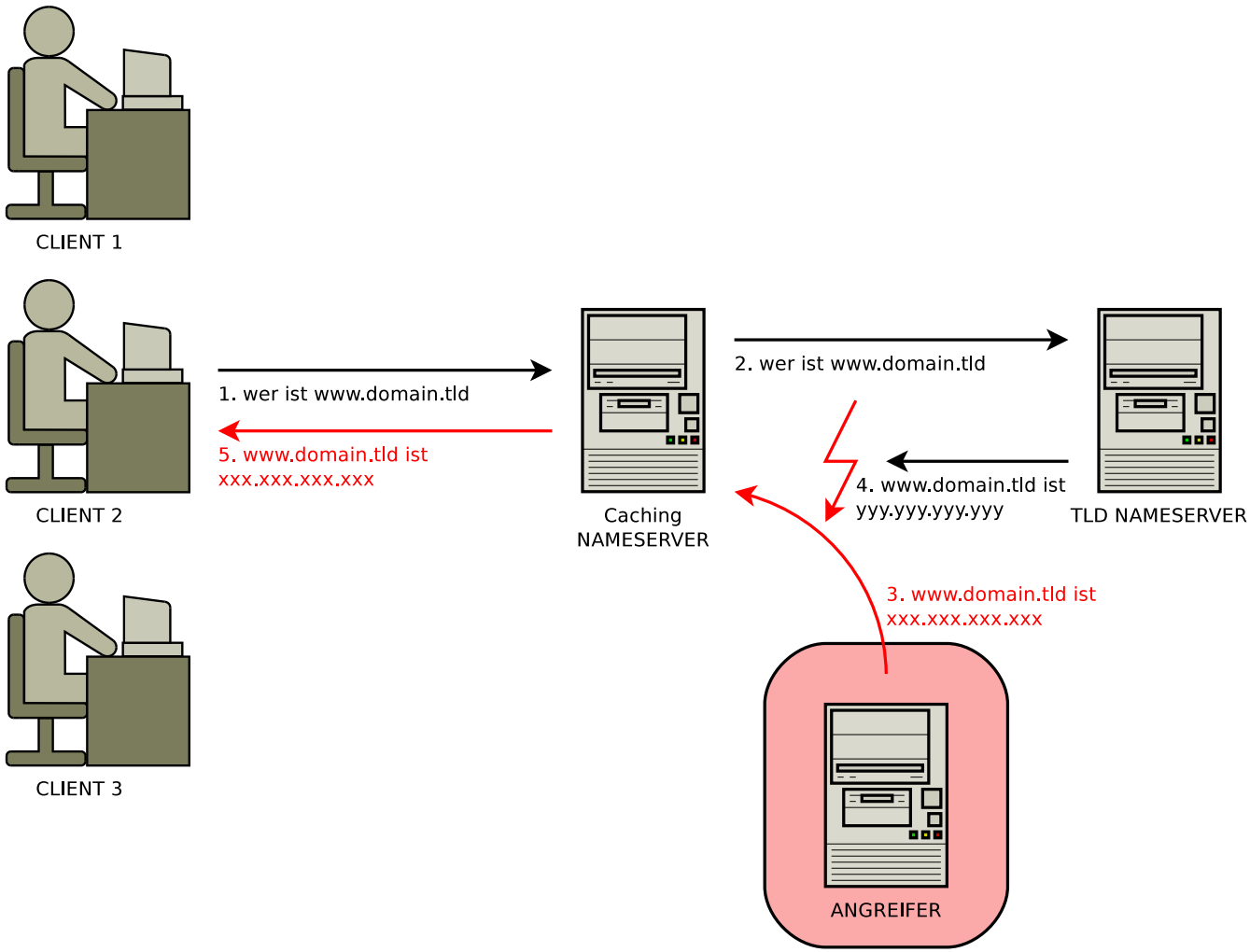
DNS-Cache-Poisoning



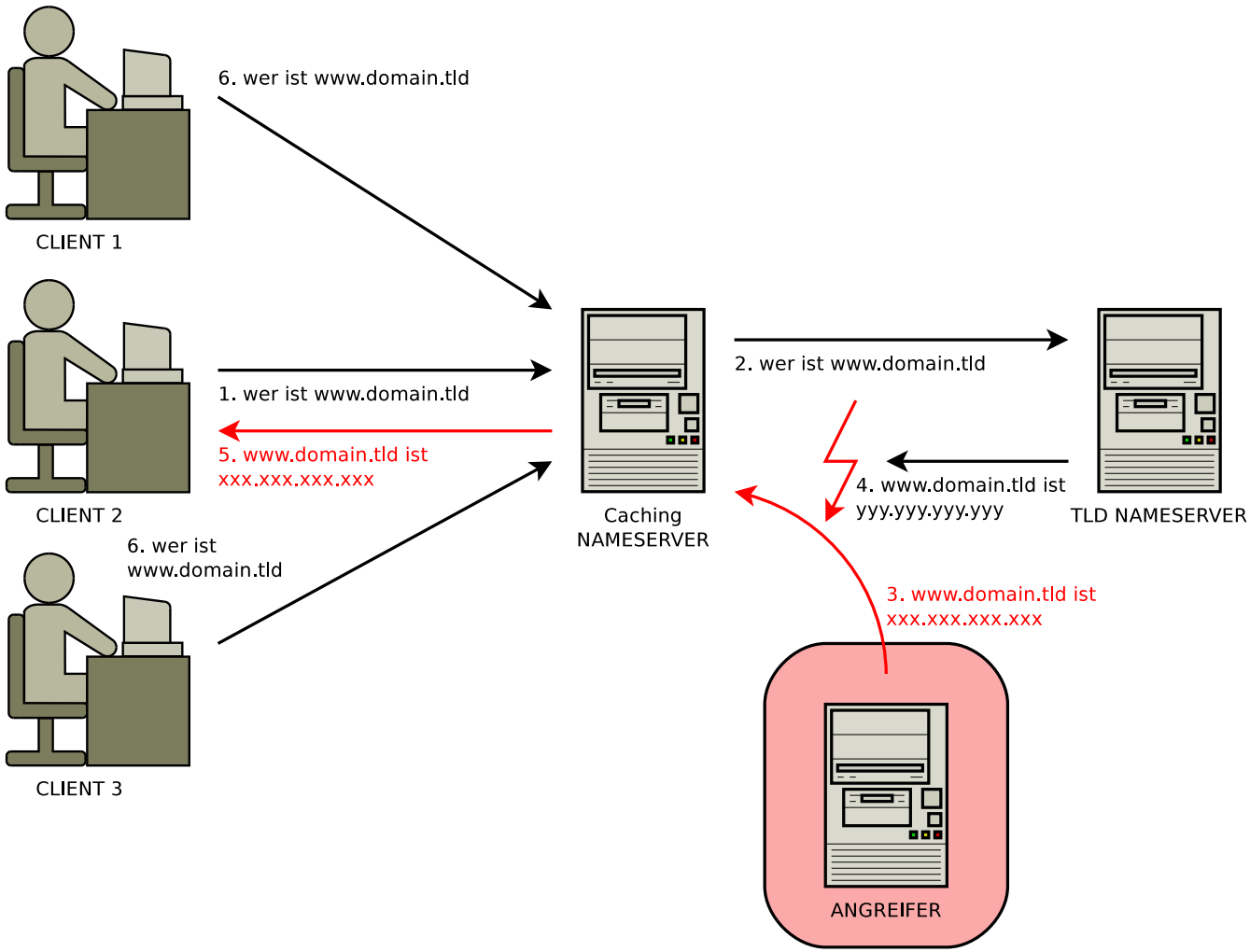
DNS-Cache-Poisoning



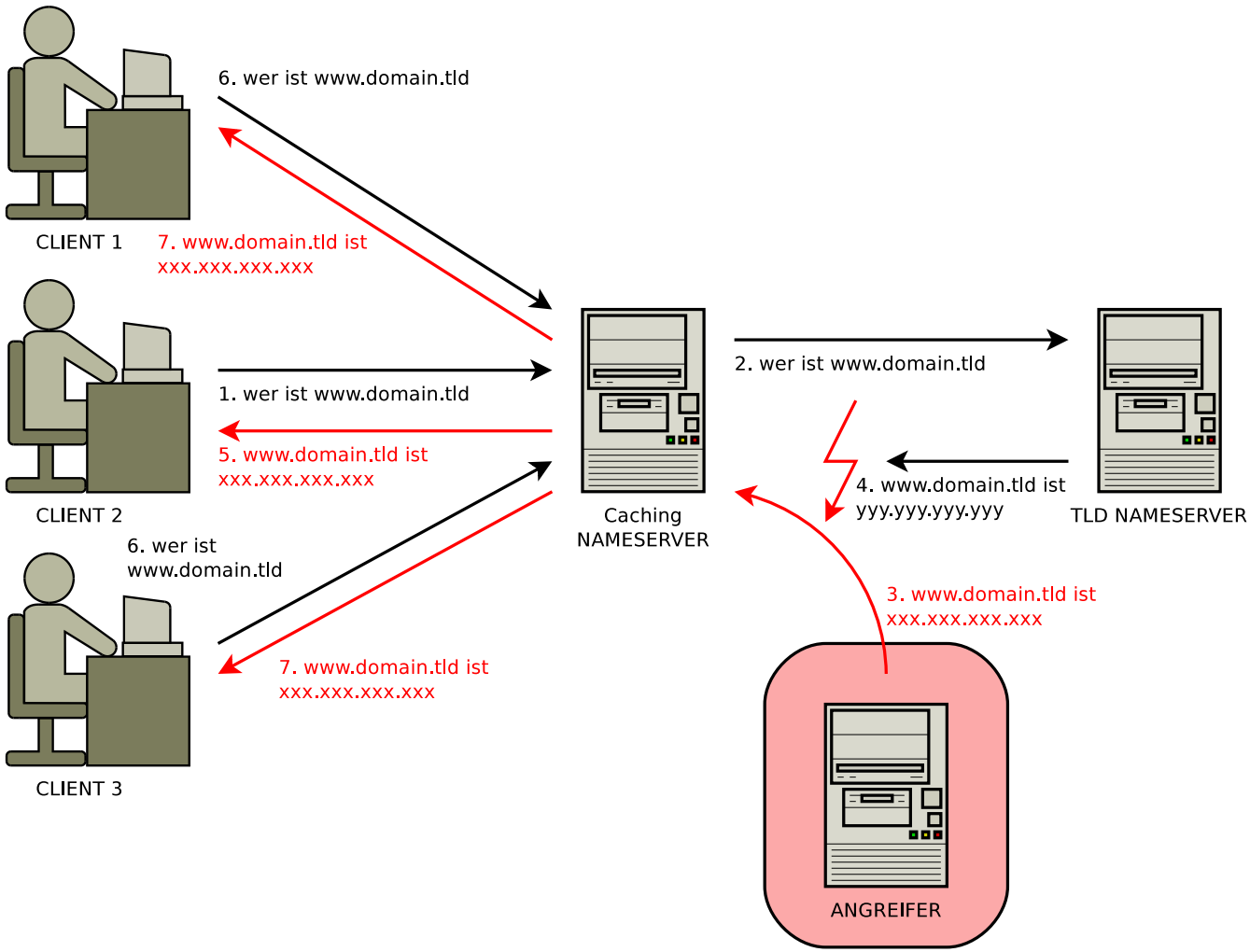
DNS-Cache-Poisoning



DNS-Cache-Poisoning



DNS-Cache-Poisoning



DNS Angriffe

- Ist DNS sicher?
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

DNS Angriffe

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

DNS Angriffe

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS - Ziel nicht erreichbar, Rechner außer Gefecht
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

DNS Angriffe

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS - Ziel nicht erreichbar, Rechner außer Gefecht
  - DNS-Amplification - Rechner außer Gefecht
  - DNS-Spoofing
  - DNS-Cache-Poisoning

DNS Angriffe

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS - Ziel nicht erreichbar, Rechner außer Gefecht
  - DNS-Amplification - Rechner außer Gefecht
  - DNS-Spoofing - Falsches Ziel wird erreicht
  - DNS-Cache-Poisoning

DNS Angriffe

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS - Ziel nicht erreichbar, Rechner außer Gefecht
  - DNS-Amplification - Rechner außer Gefecht
  - DNS-Spoofing - Falsches Ziel wird erreicht
  - DNS-Cache-Poisoning - Falsches Ziel wird erreicht

Fragen ?

Asymmetric Cryptography

Gliederung

Gliederung

Gliederung

Asymmetric Cryptography

- Warum Asymmetrische Verschlüsselung?

Asymmetric Cryptography

- Warum Asymmetrische Verschlüsselung?
  - Digitale Signatur

Asymmetric Cryptography

- Warum Asymmetrische Verschlüsselung?
  - Digitale Signatur$\rightarrow$ Authentizität

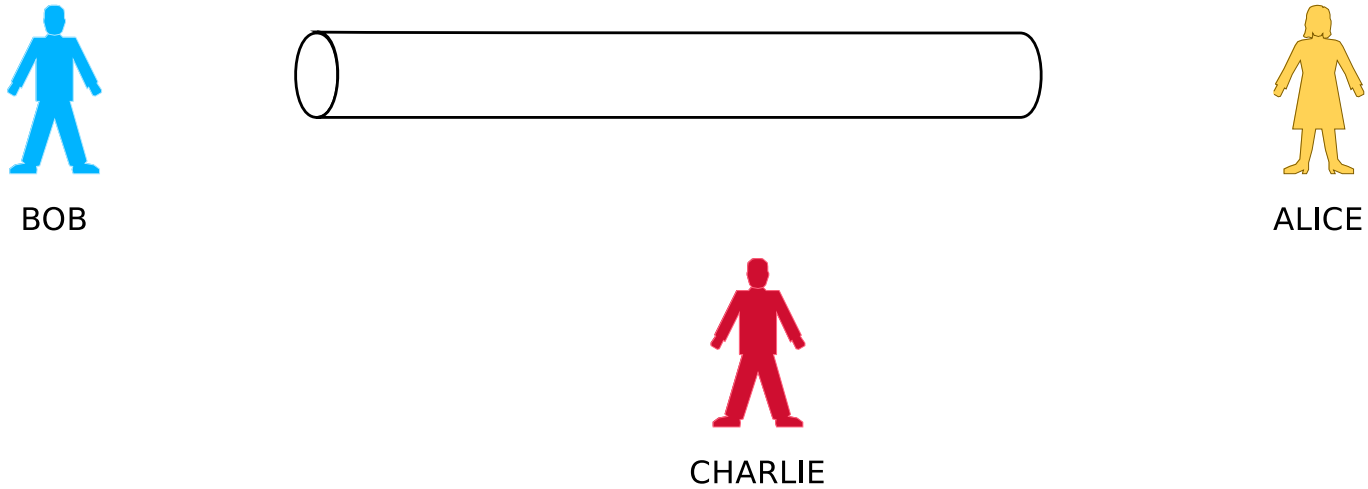
Asymmetric Cryptography

- Warum Asymmetrische Verschlüsselung?
  - Digitale Signatur$\rightarrow$ Authentizität
  - Verschlüsselung

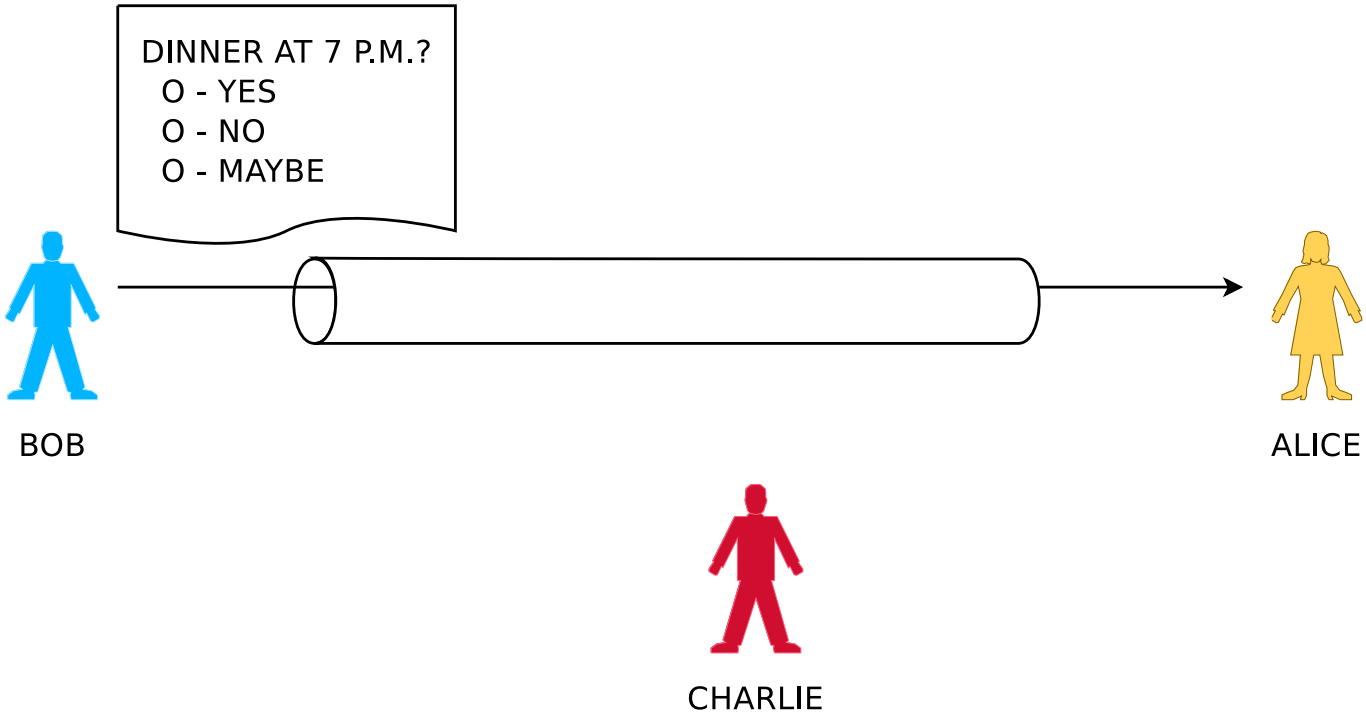
Asymmetric Cryptography

- Warum Asymmetrische Verschlüsselung?
  - Digitale Signatur$\rightarrow$ Authentizität
  - Verschlüsselung$\rightarrow$ Vetraulichkeit

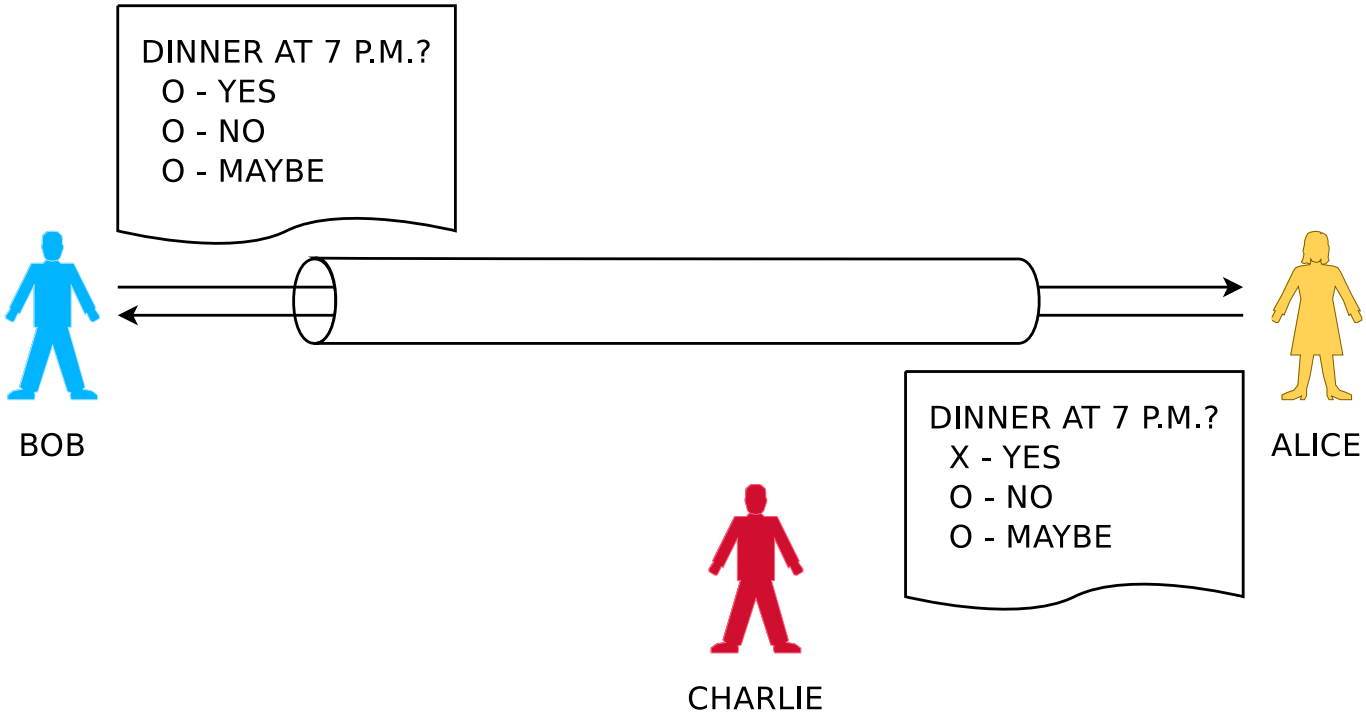
Motivation - Eavesdropping



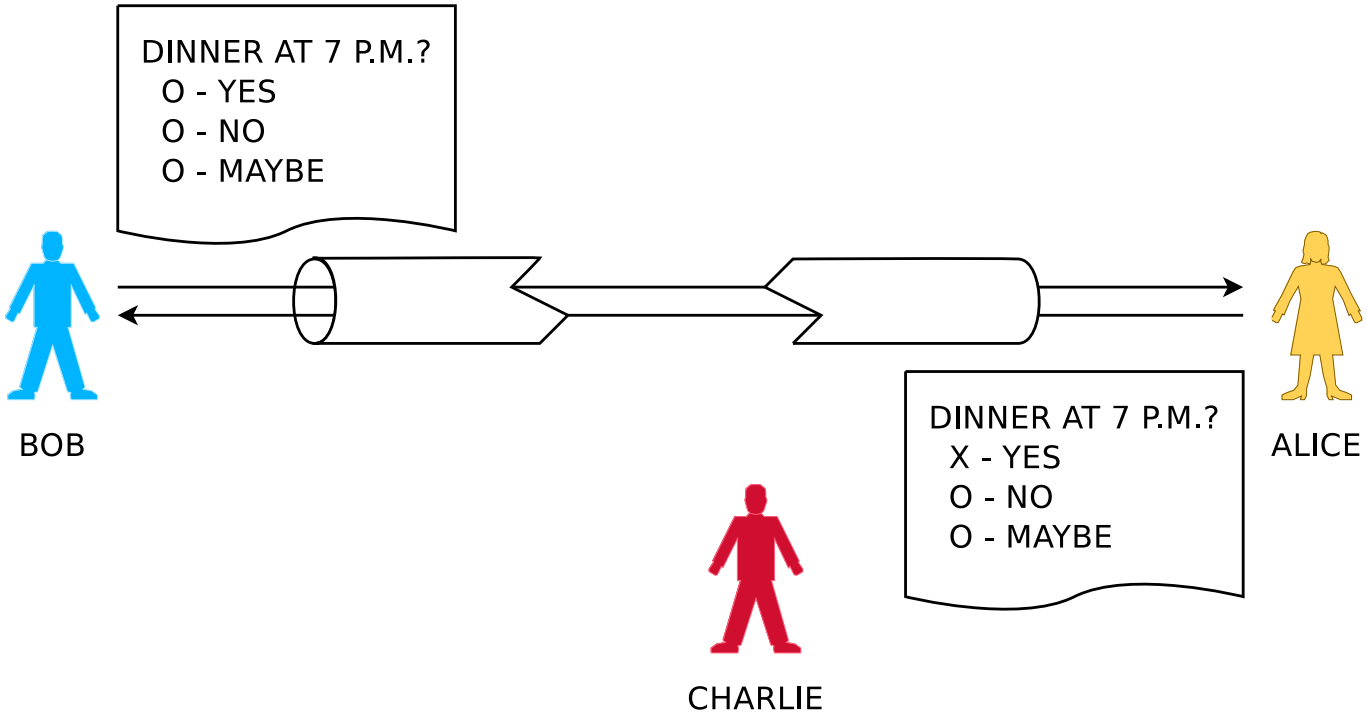
Motivation - Eavesdropping



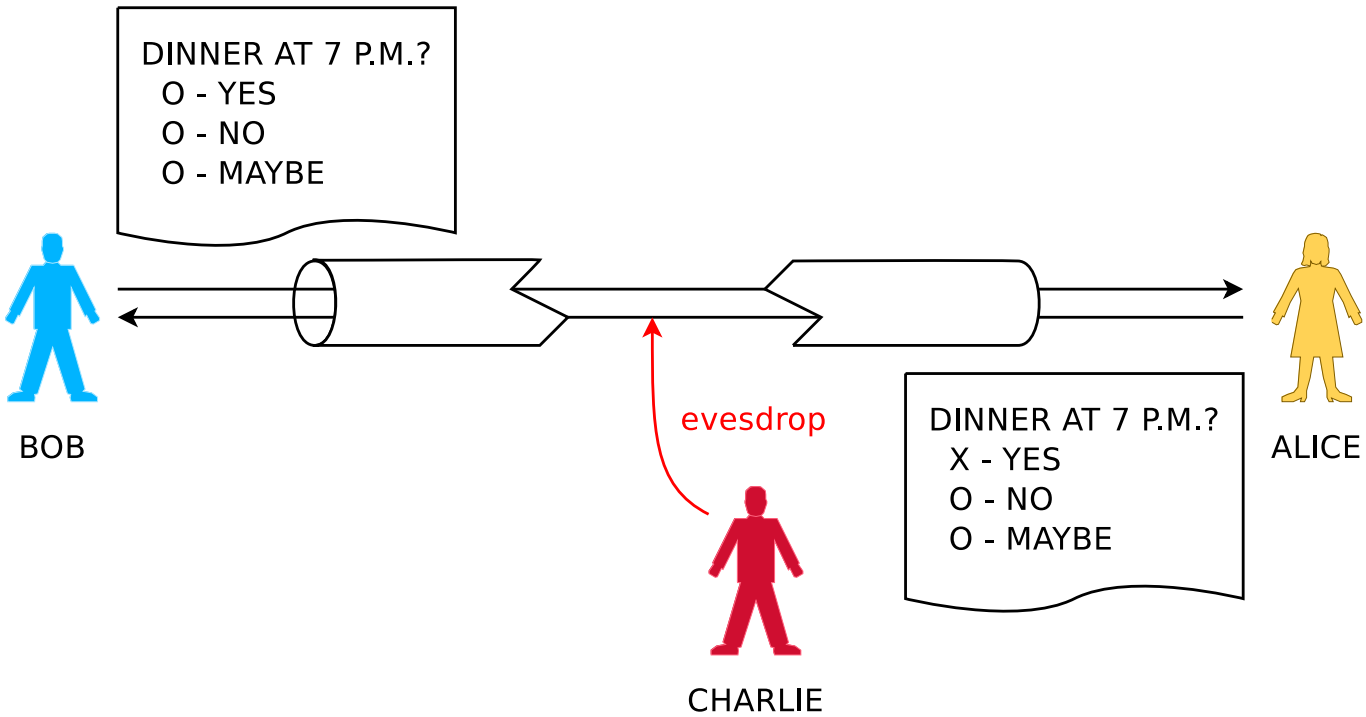
Motivation - Eavesdropping



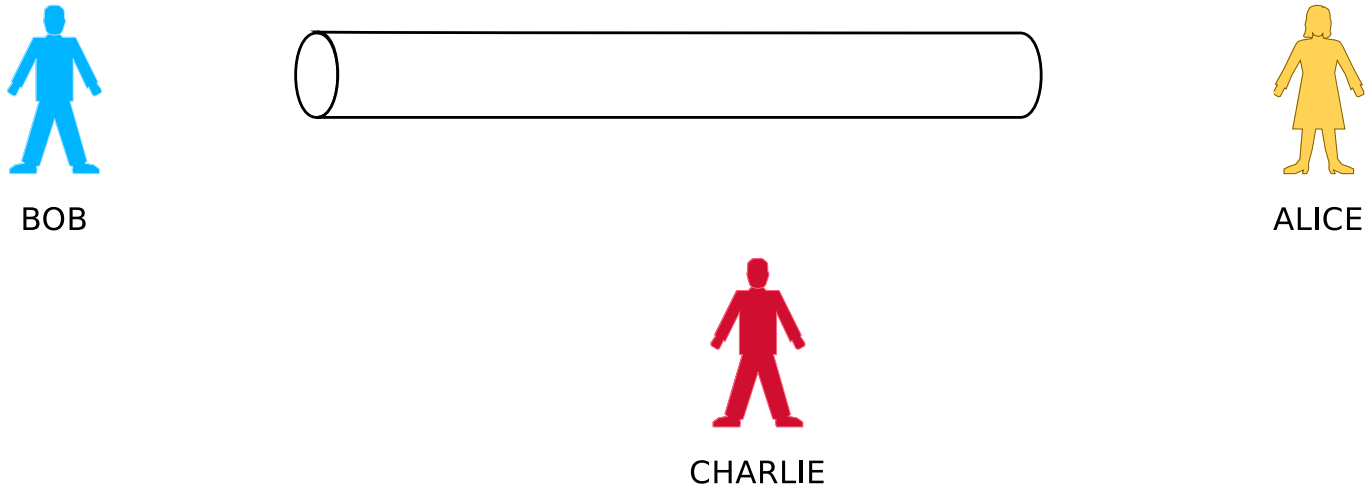
Motivation - Eavesdropping



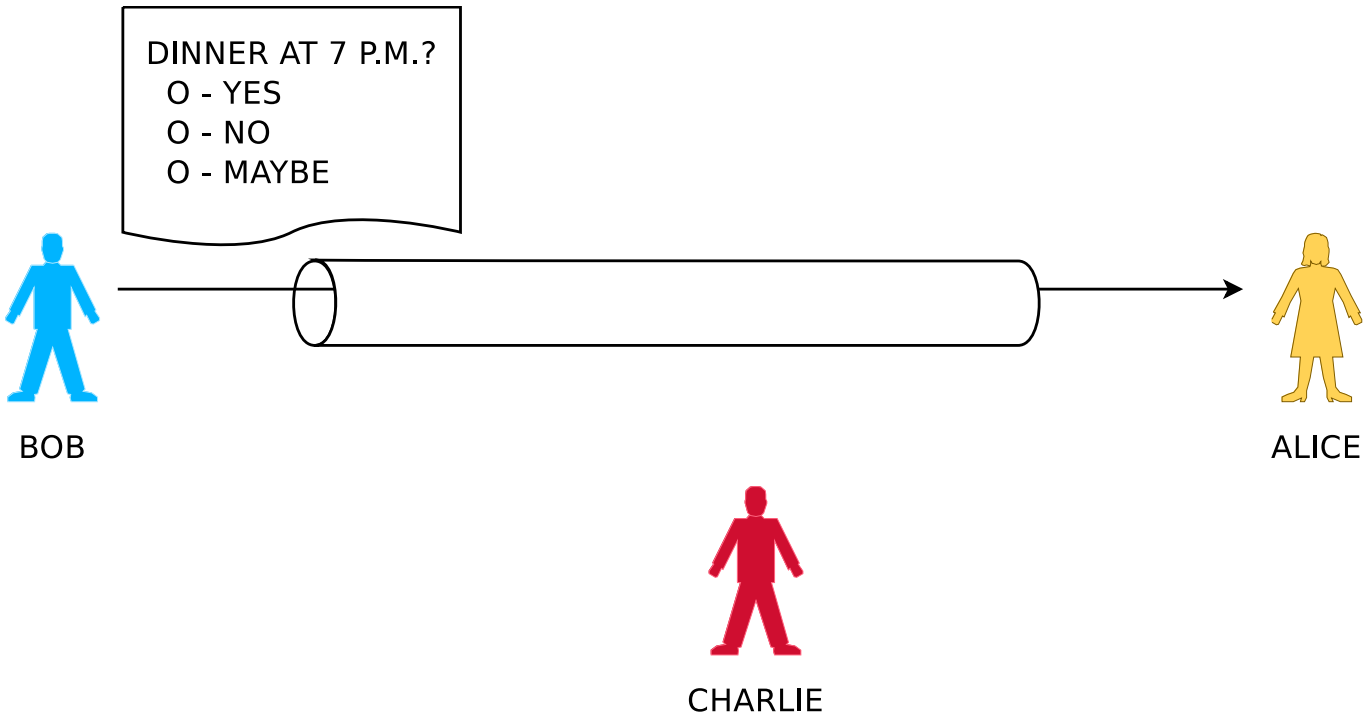
Motivation - Eavesdropping



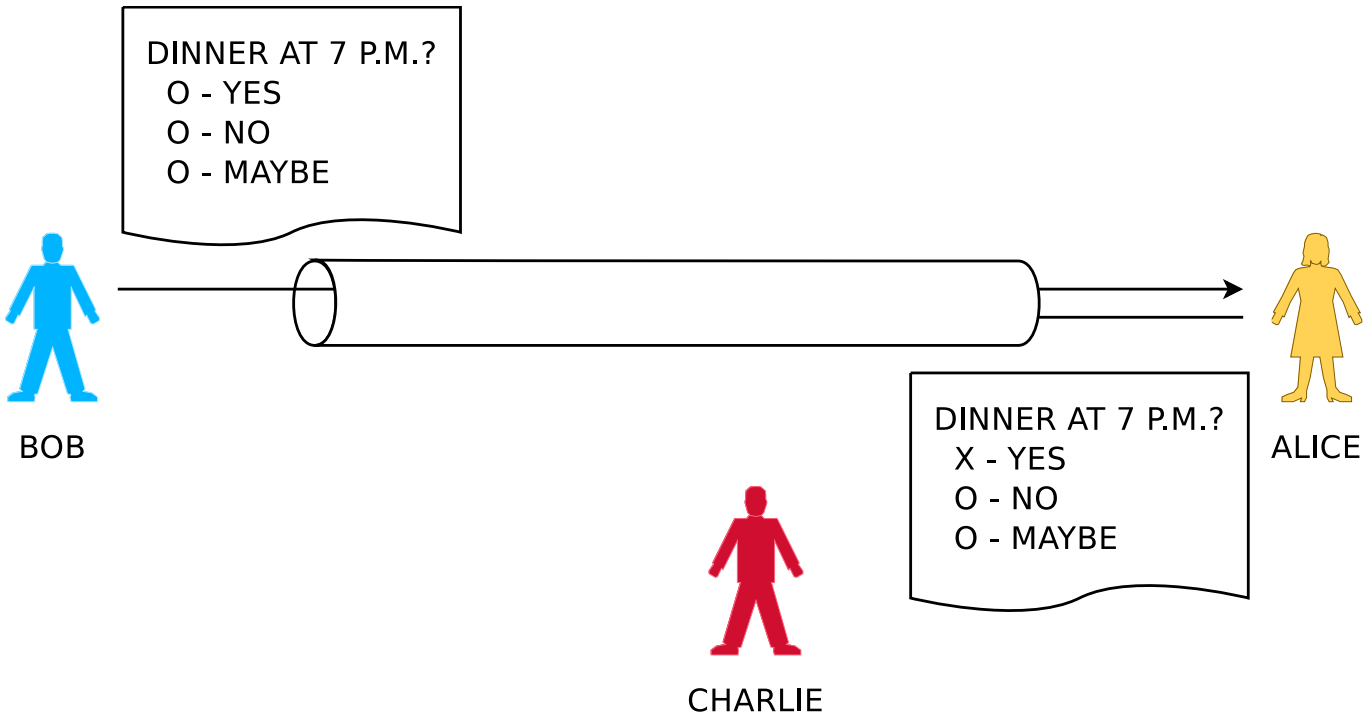
Motivation - Spoofing



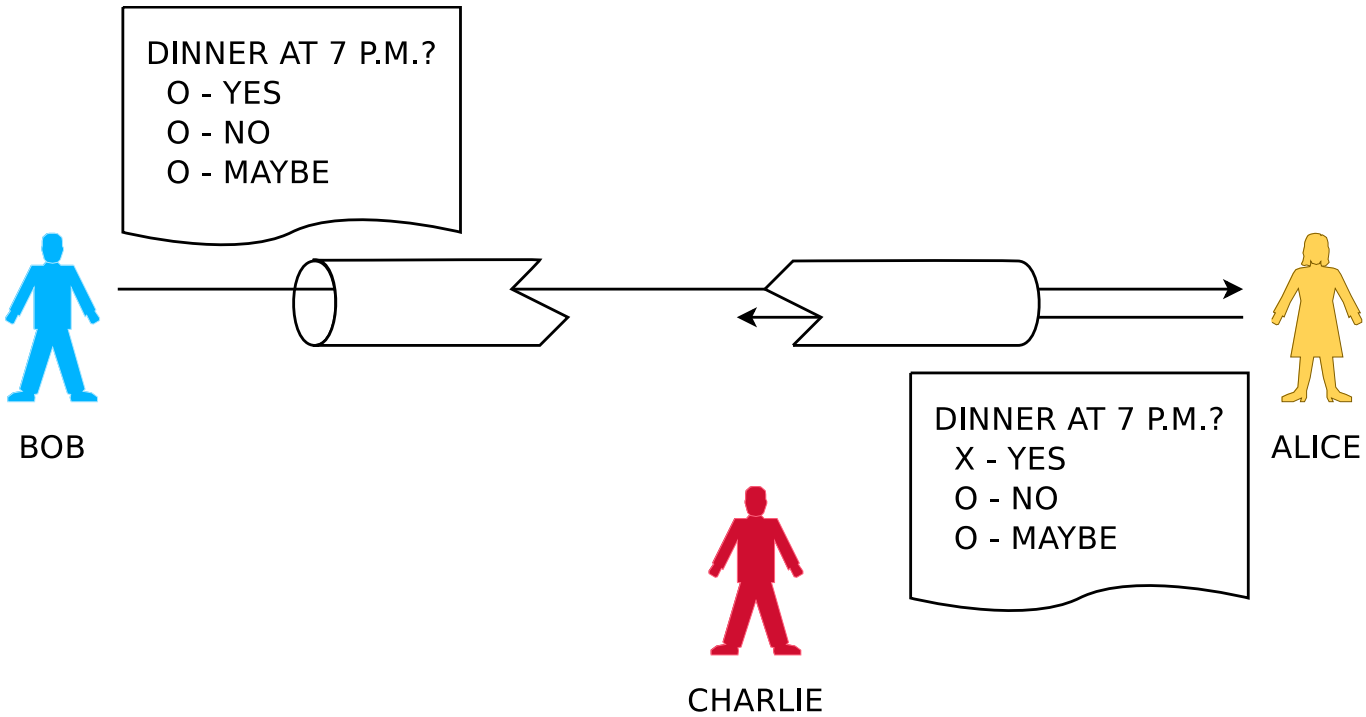
Motivation - Spoofing



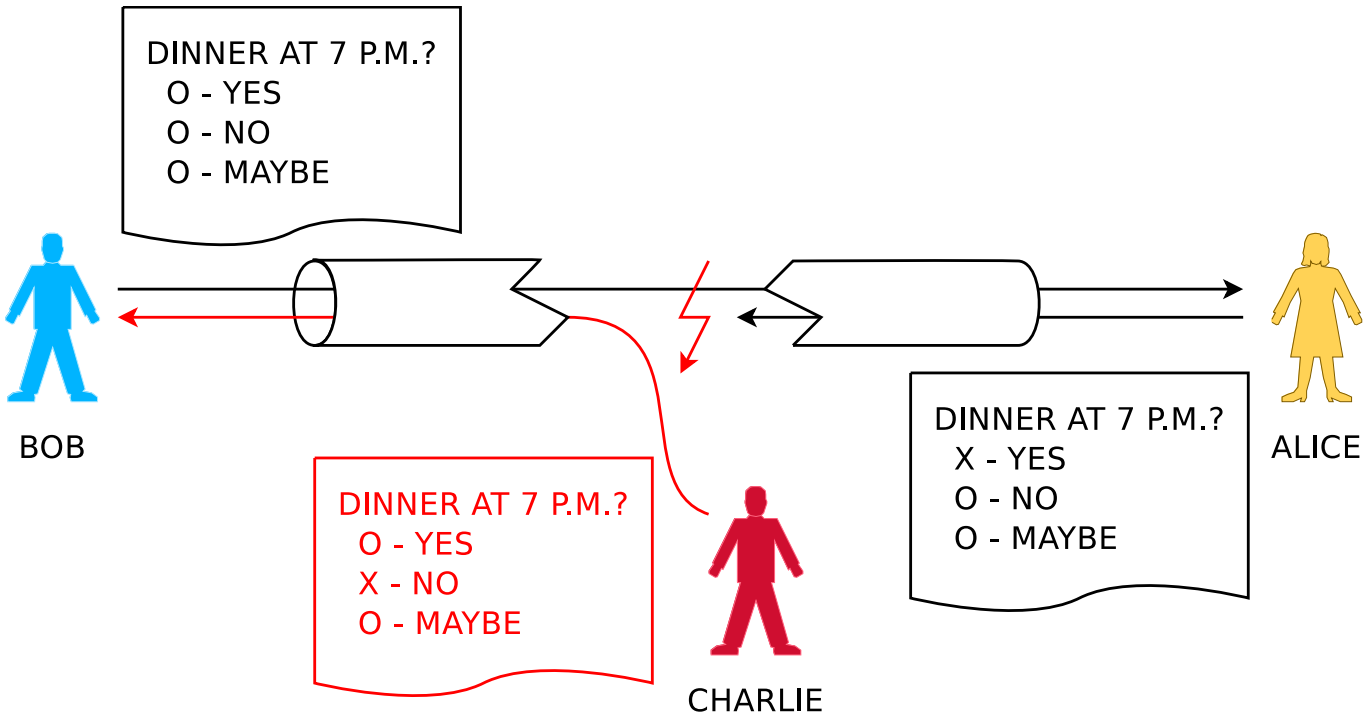
Motivation - Spoofing



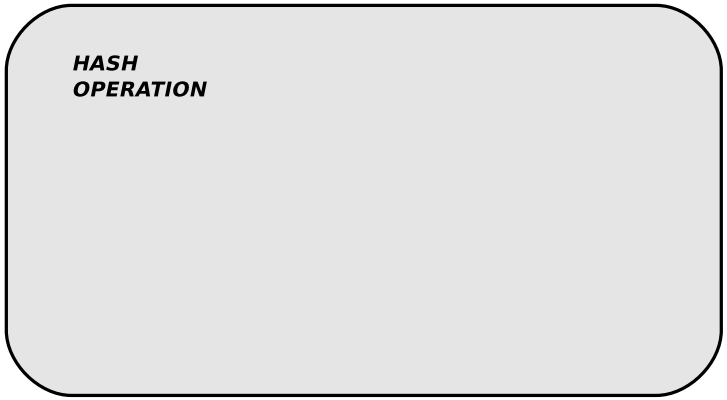
Motivation - Spoofing



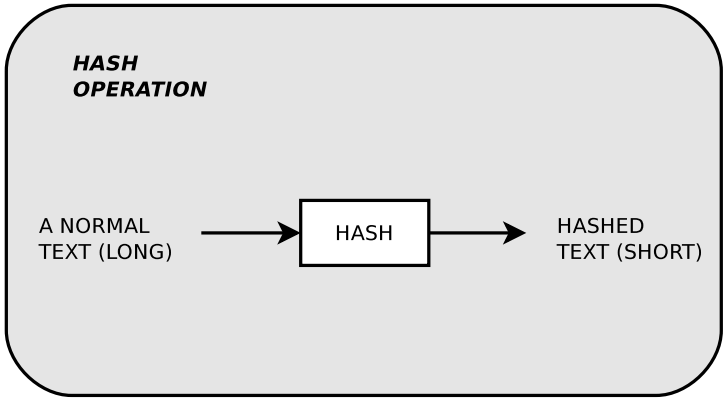
Motivation - Spoofing



Hash-Algorithmus

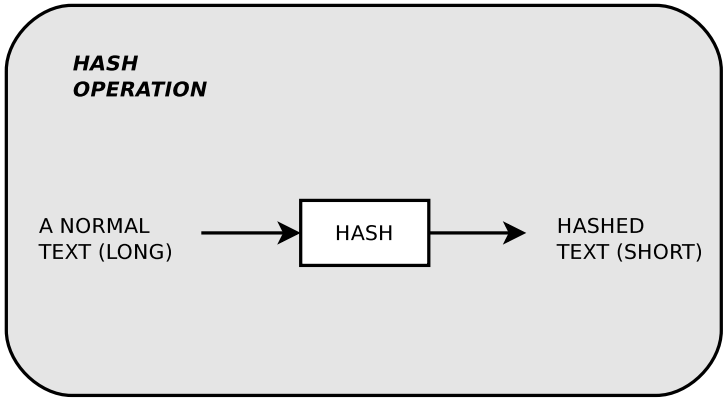


Hash-Algorithmus



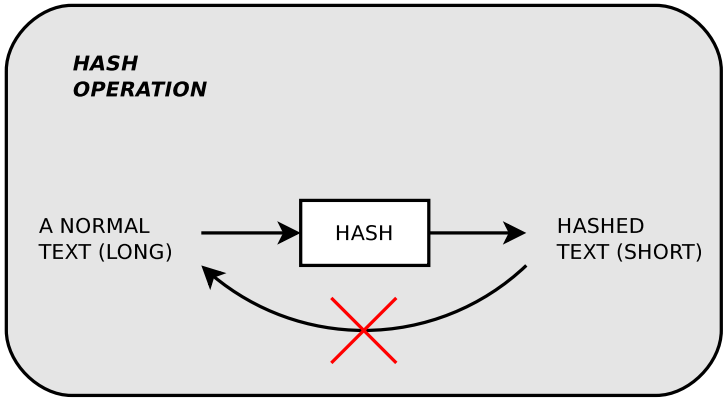
- bildet viele Bits auf wenige Bits ab

Hash-Algorithmus



- bildet viele Bits auf wenige Bits ab
- sehr einfach in Hinrichtung

Hash-Algorithmus



- bildet viele Bits auf wenige Bits ab
- sehr einfach in Hinrichtung
- sehr schwer in Rückrichtung

Funktionsweise

Schlüsselpaar:

Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser

Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser

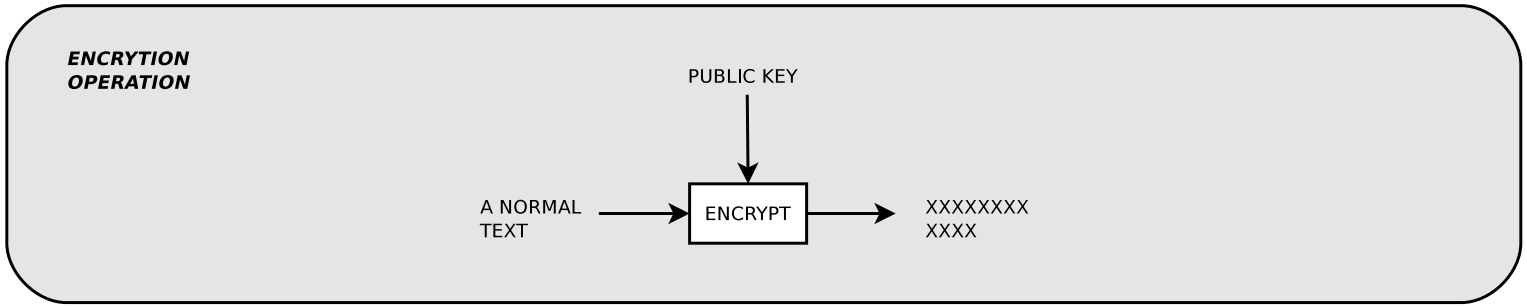
Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser



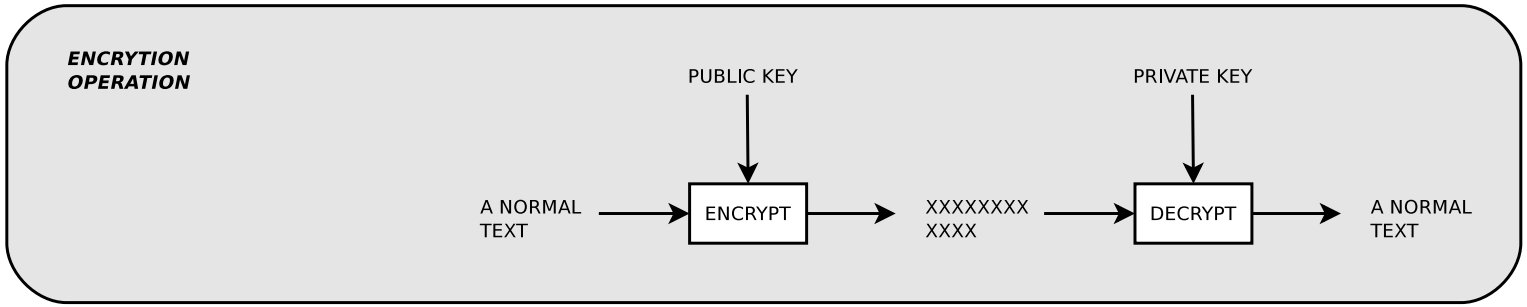
Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser



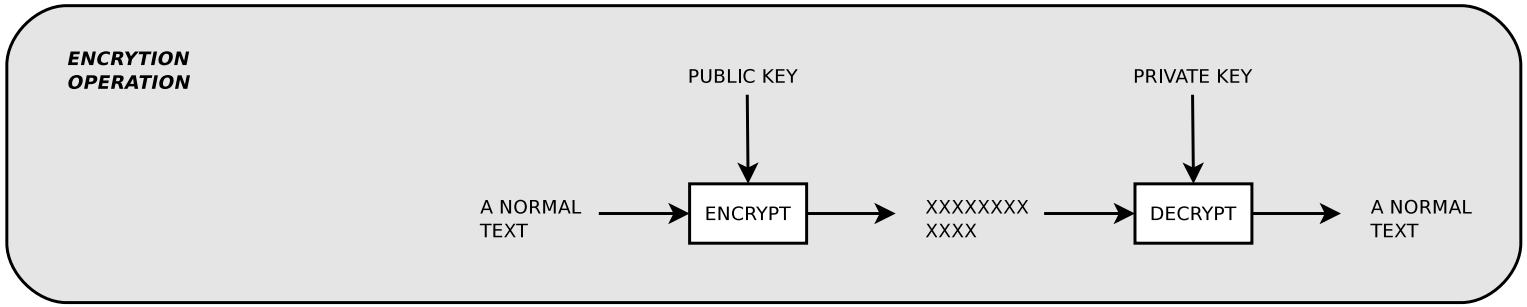
Funktionsweise

Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser



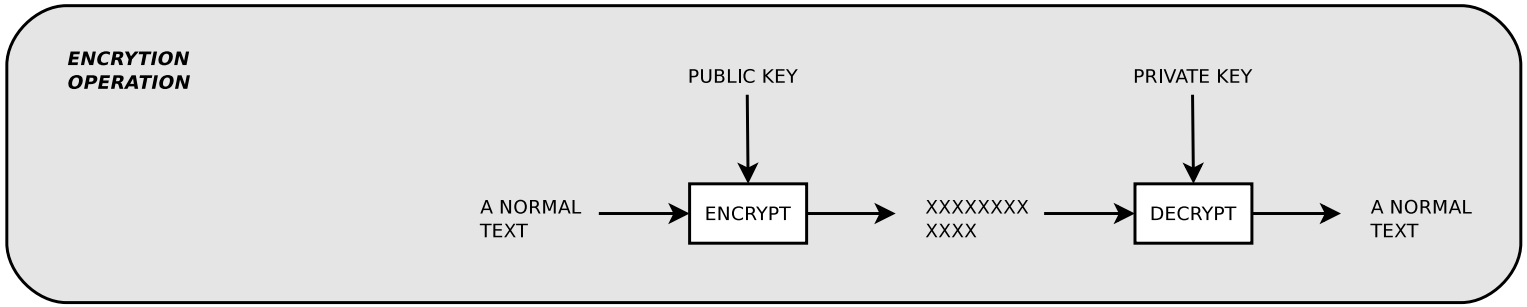
Funktionsweise

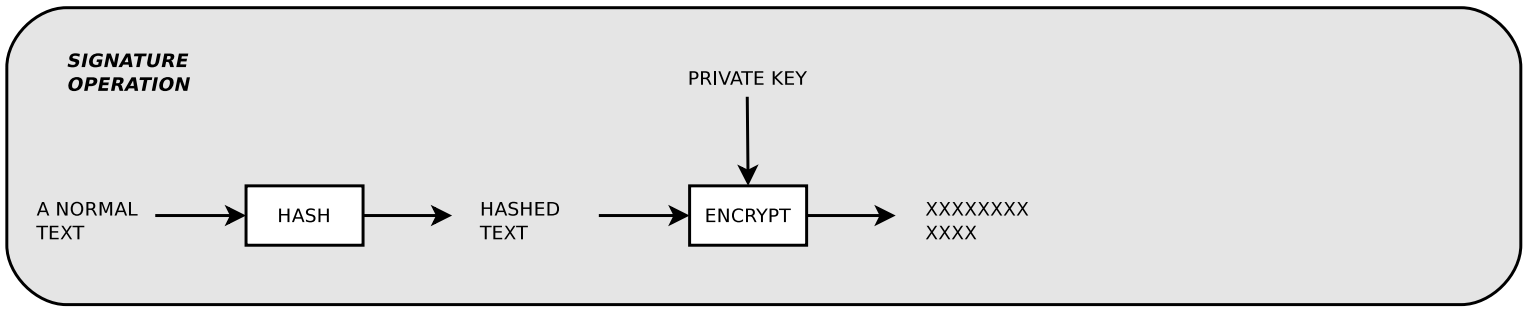
Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser





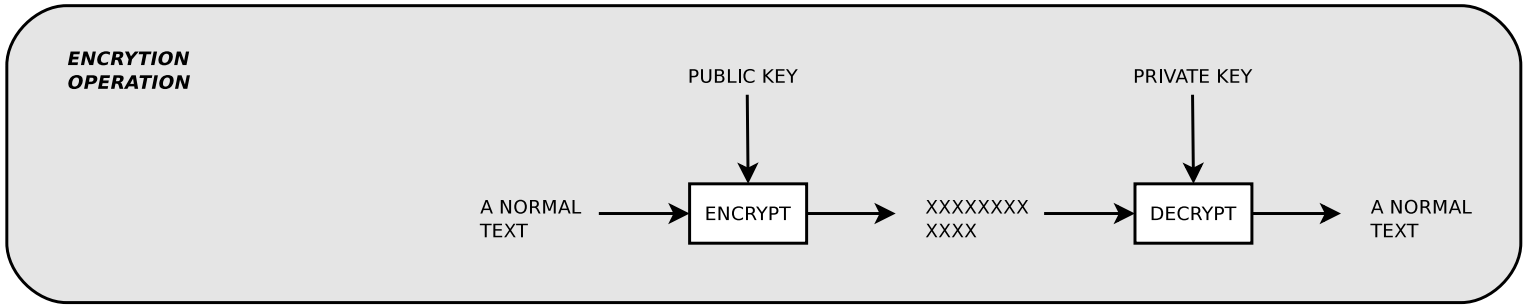
Funktionsweise

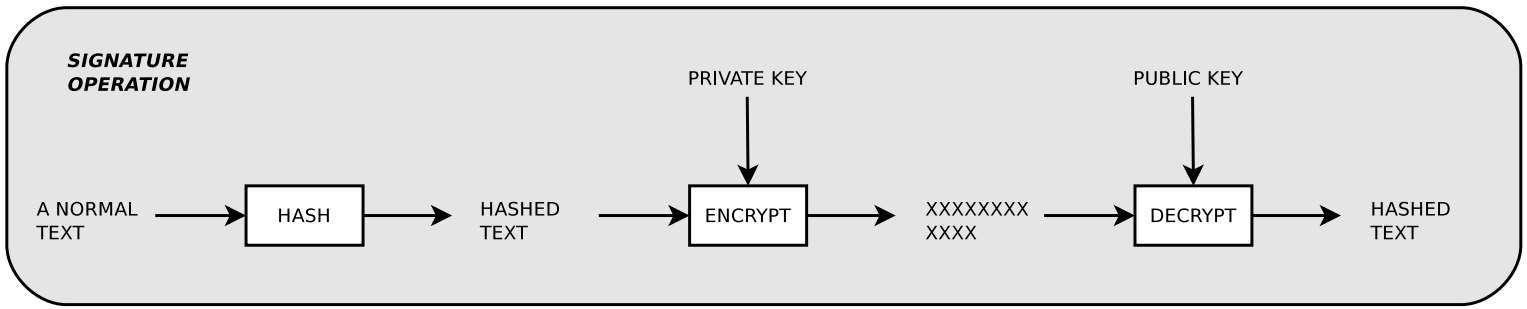
Schlüsselpaar:

privater Schlüssel geheim, nur Besitzer bekannt

öffentlicher Schlüssel für alle einsehbar

Schlüssellänge Mehr = Besser





Anwendung - Vorgaben

- Alice besitzt einen privaten Schlüssel A_{PRIV} und einen öffentlichen Schlüssel A_{PUB}

Anwendung - Vorgaben

- Alice besitzt einen privaten Schlüssel A_{PRIV} und einen öffentlichen Schlüssel A_{PUB}
- Bob besitzt einen privaten Schlüssel B_{PRIV} und einen öffentlichen Schlüssel B_{PUB}

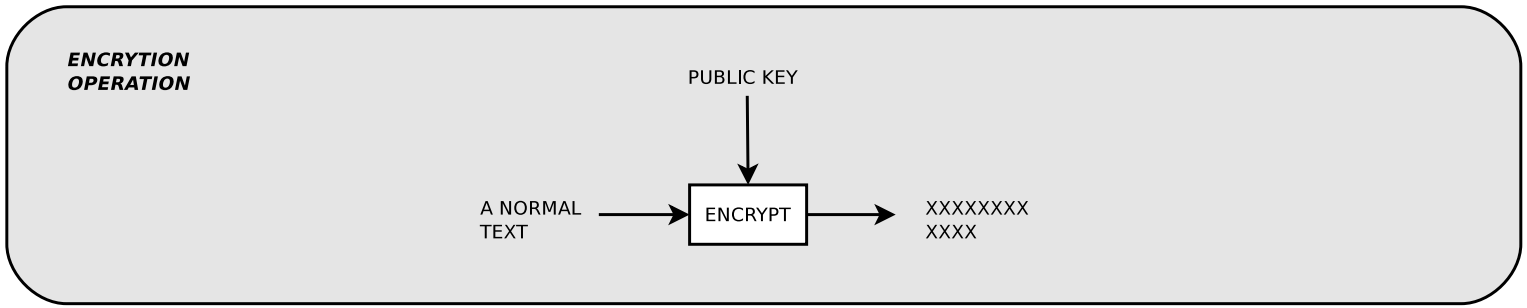
Anwendung - Vorgaben

- Alice besitzt einen privaten Schlüssel A_{PRIV} und einen öffentlichen Schlüssel A_{PUB}
- Bob besitzt einen privaten Schlüssel B_{PRIV} und einen öffentlichen Schlüssel B_{PUB}
- Öffentlicher Schlüssel ist dem jeweils Anderen bekannt

Anwendung - Vertrauliche Nachricht

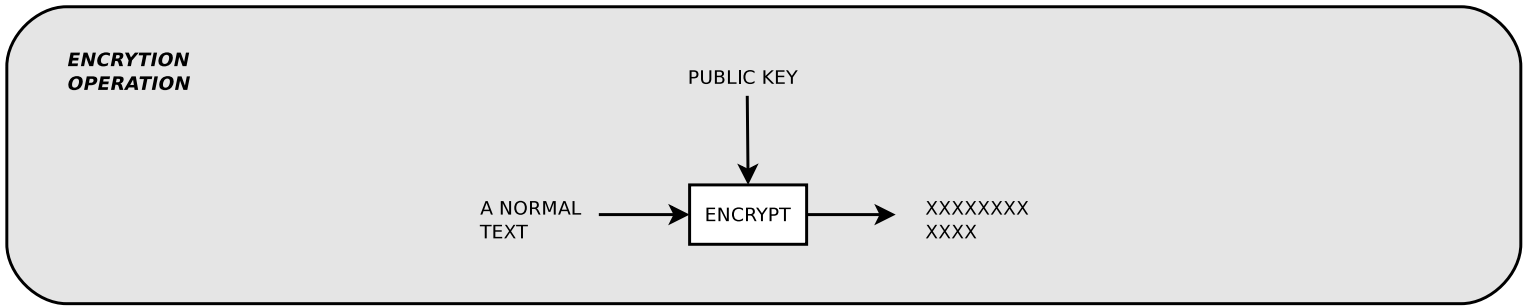
- Bob verschlüsselt Nachricht:

Anwendung - Vertrauliche Nachricht



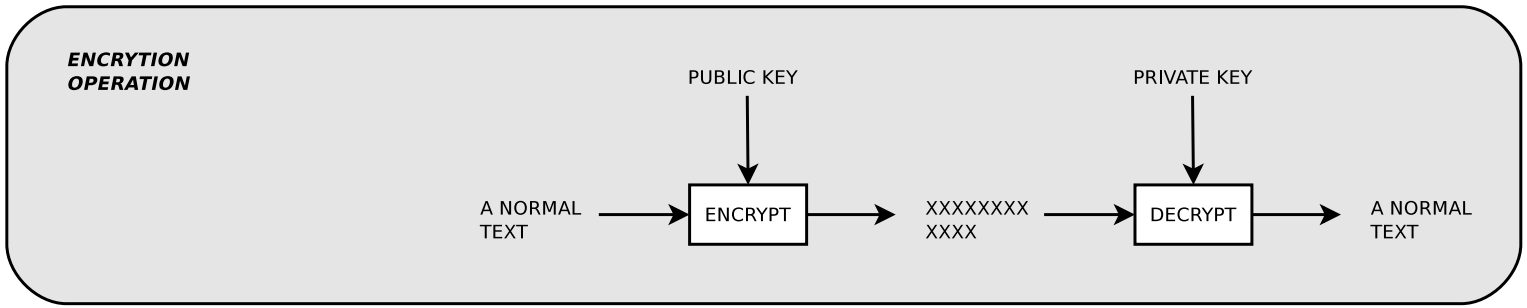
- Bob verschlüsselt Nachricht:
  - Cypher = Encryption(Text, A_{PUB})

Anwendung - Vertrauliche Nachricht



- Bob verschlüsselt Nachricht:
  - Cypher = Encryption(Text, A_{PUB})
- Alice empfängt Cypher' und entschlüsselt:

Anwendung - Vertrauliche Nachricht



- Bob verschlüsselt Nachricht:
  - Cypher = Encryption(Text, A_{PUB})
- Alice empfängt Cypher' und entschlüsselt:
  - Text' = Decryption(Cypher', A_{PRIV})

Anwendung - Authentische Nachricht

- Bob hasht Nachricht:

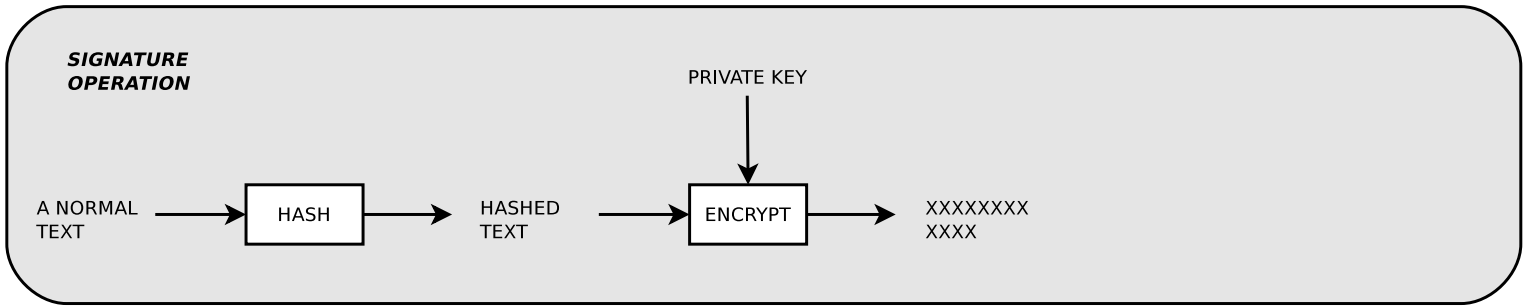
Anwendung - Authentische Nachricht

- Bob hasht Nachricht:
  - Hash = Hash(Text)

Anwendung - Authentische Nachricht

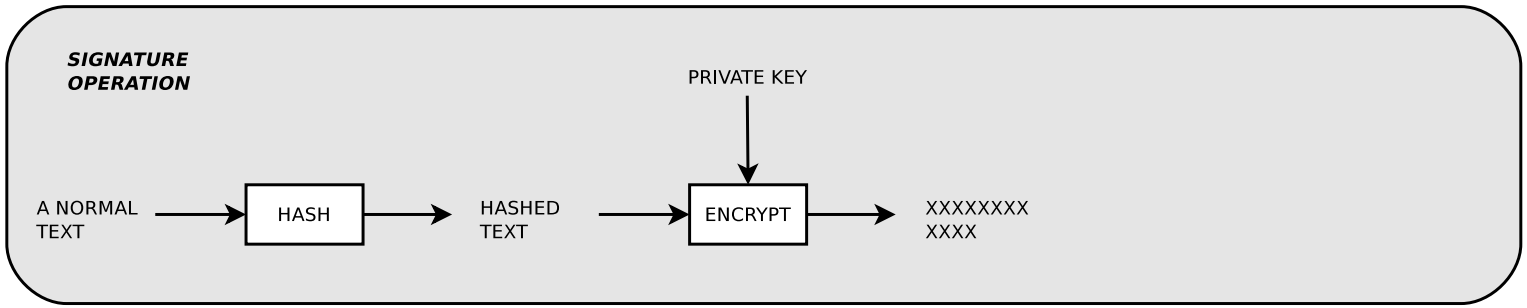
- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:

Anwendung - Authentische Nachricht



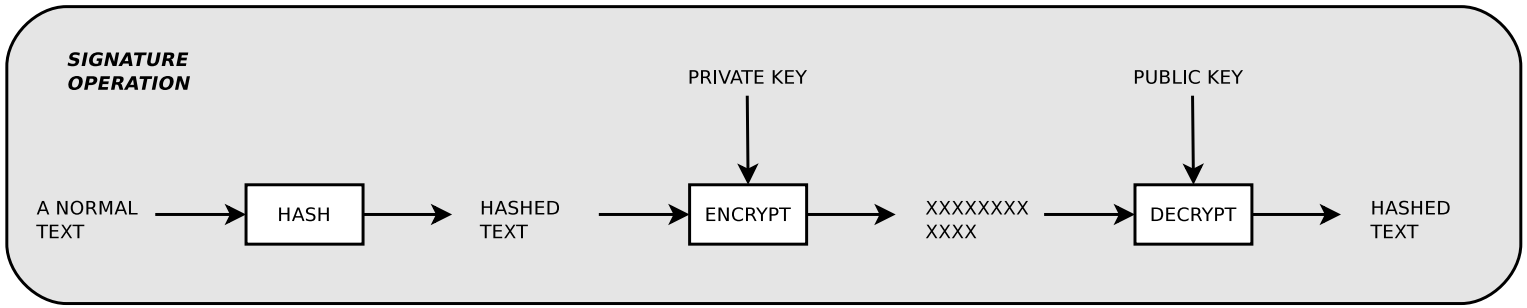
- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:
  - Signature = Encryption(Hash, B_{PRIV})

Anwendung - Authentische Nachricht



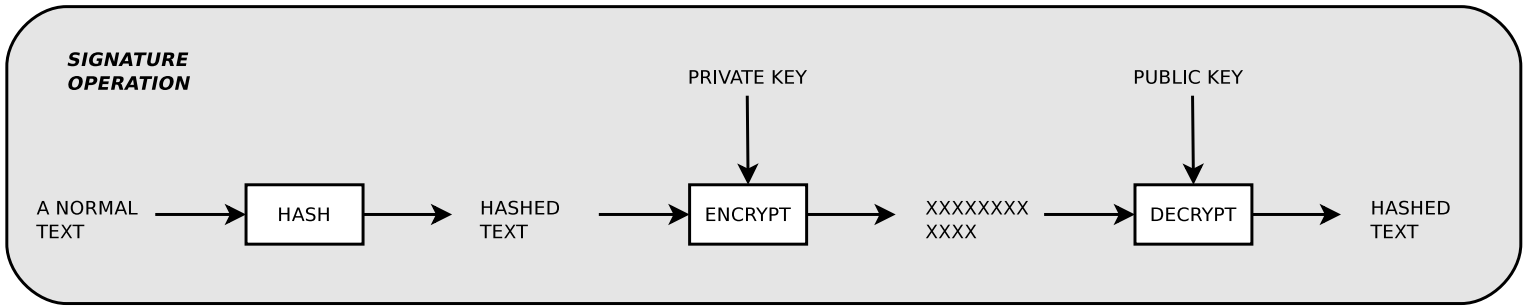
- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:
  - Signature = Encryption(Hash, B_{PRIV})
- Alice empfängt Text' und Signature' und validiert:

Anwendung - Authentische Nachricht



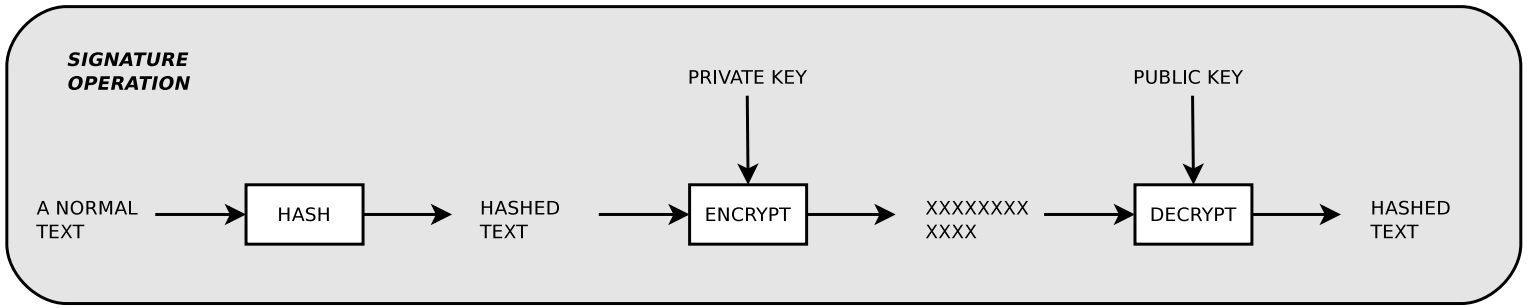
- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:
  - Signature = Encryption(Hash, B_{PRIV})
- Alice empfängt Text' und Signature' und validiert:
  - Hash' = Decryption(Signature', B_{PUB})

Anwendung - Authentische Nachricht



- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:
  - Signature = Encryption(Hash, B_{PRIV})
- Alice empfängt Text' und Signature' und validiert:
  - Hash' = Decryption(Signature', B_{PUB})
  - Hash = Hash(Text')

Anwendung - Authentische Nachricht



- Bob hasht Nachricht:
  - Hash = Hash(Text)
- Bob signiert Nachricht:
  - Signature = Encryption(Hash, B_{PRIV})
- Alice empfängt Text' und Signature' und validiert:
  - Hash' = Decryption(Signature', B_{PUB})
  - Hash = Hash(Text')
  - Hash == Hash'

Certificate

Grundlegende Idee

Nachweisen der Gültigkeit eines Schlüssels.

Certificate

Was steht in einem Zertifikat?

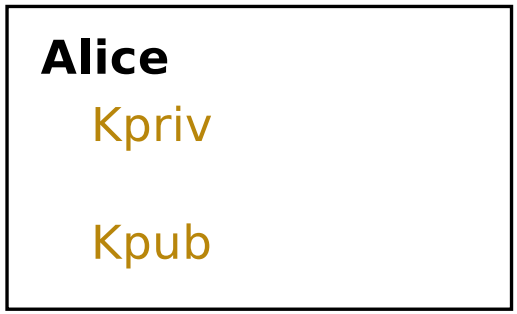
- Certificate
  - ...
  - Issuer
  - Validity
    - Not Before
    - Not After
  - Subject
  - Subject Public Key Info
    - ...
    - Subject Public Key
  - ...
- ...
- Certificate Signature

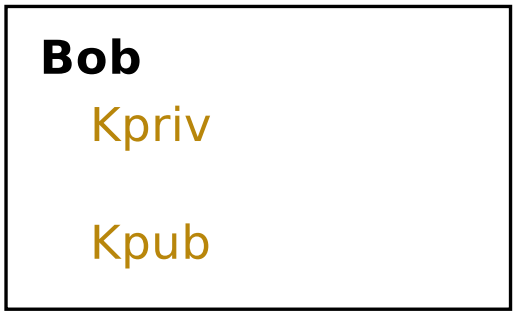
Public Key Infrastructure

Grundlegende Idee

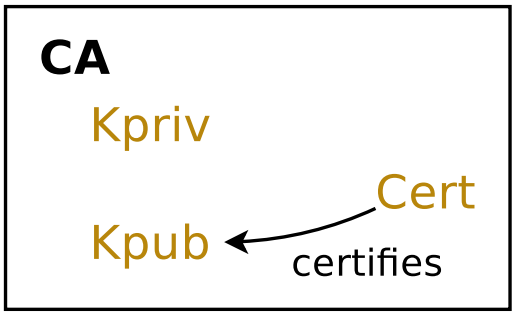
Schlüsselhierarchie mit Vertrauensanker, zur Validierung verteilter Schlüssel.

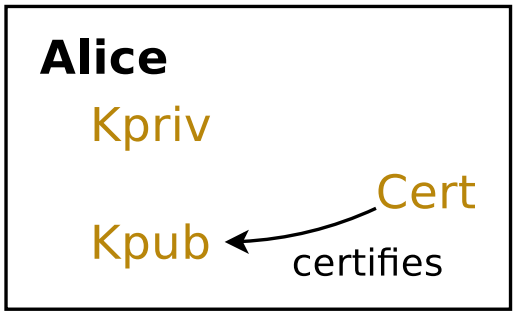
Hierarchie

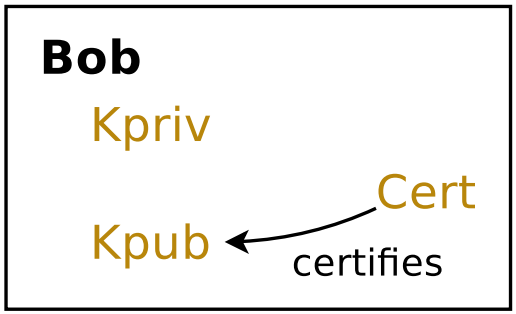




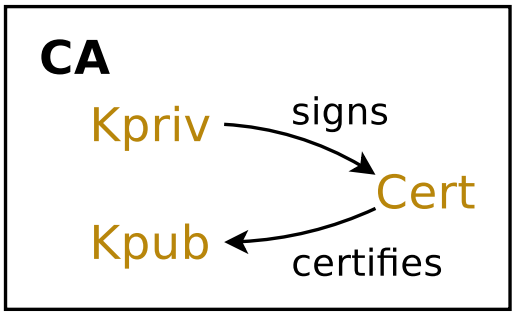
Hierarchie

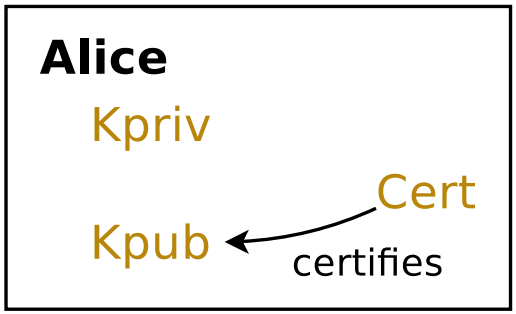

CA
Kpriv
Cert
Kpub
certifies

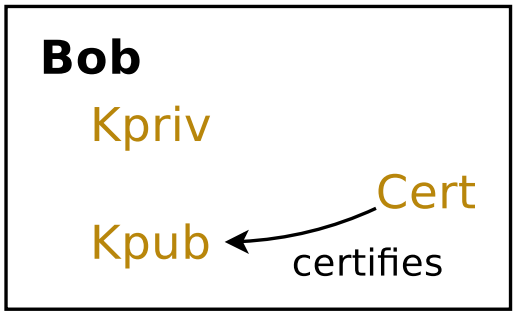

Alice
Kpriv
Cert
Kpub
certifies


Bob
Kpriv
Cert
Kpub
certifies

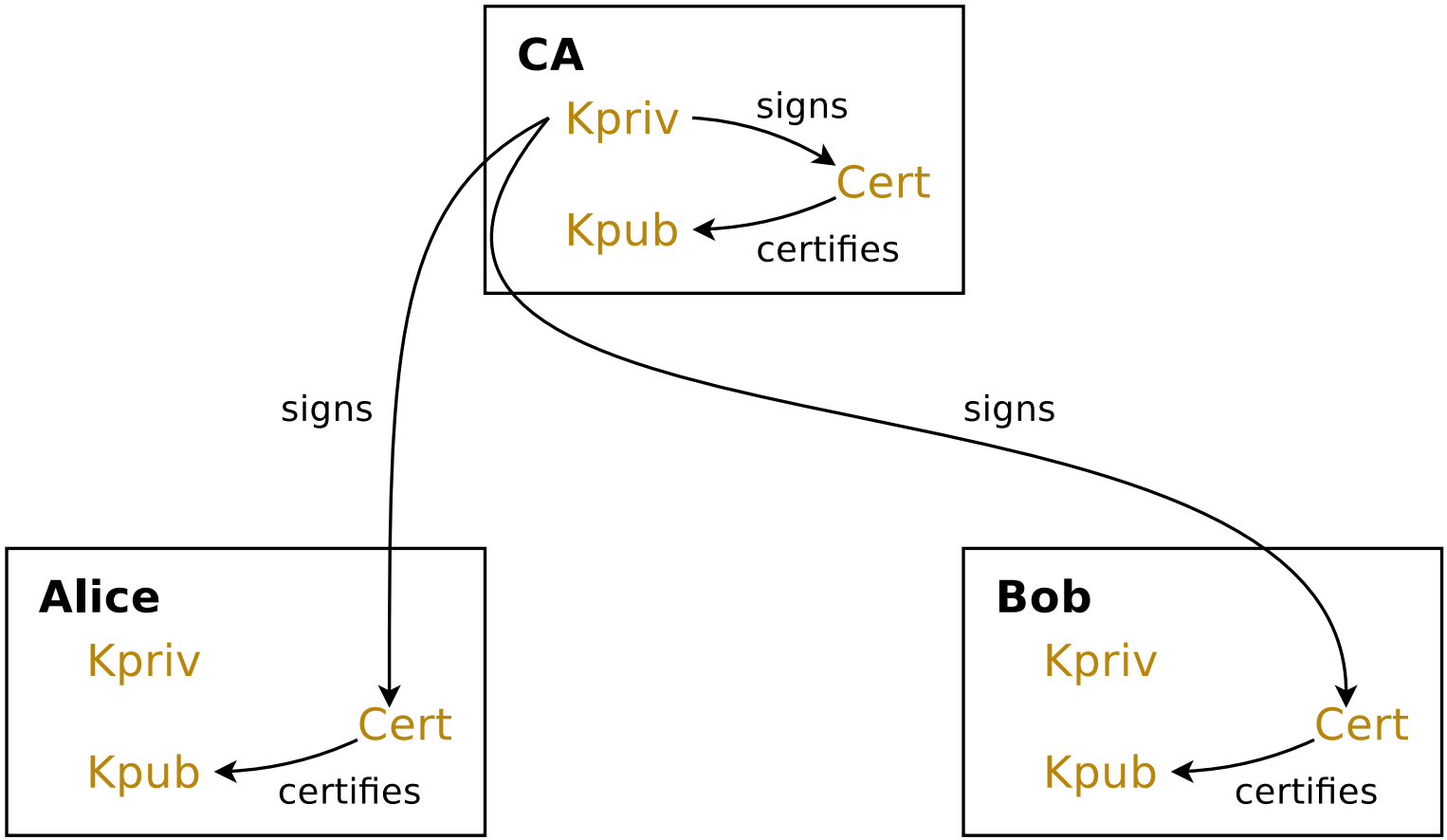
Hierarchie


CA
Kpriv
signs
Cert
Kpub
certifies

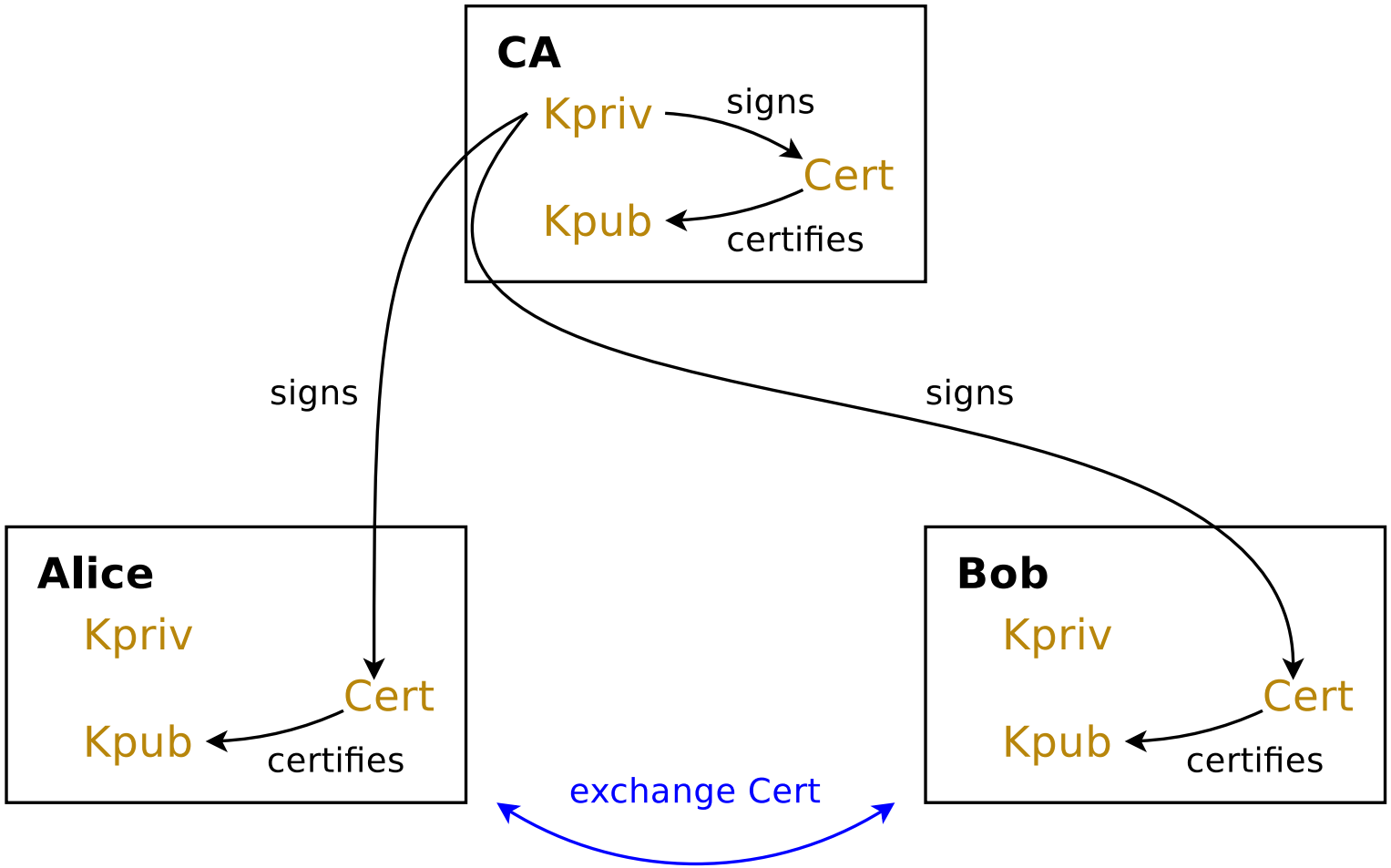

Alice
Kpriv
Cert
Kpub
certifies


Bob
Kpriv
Cert
Kpub
certifies

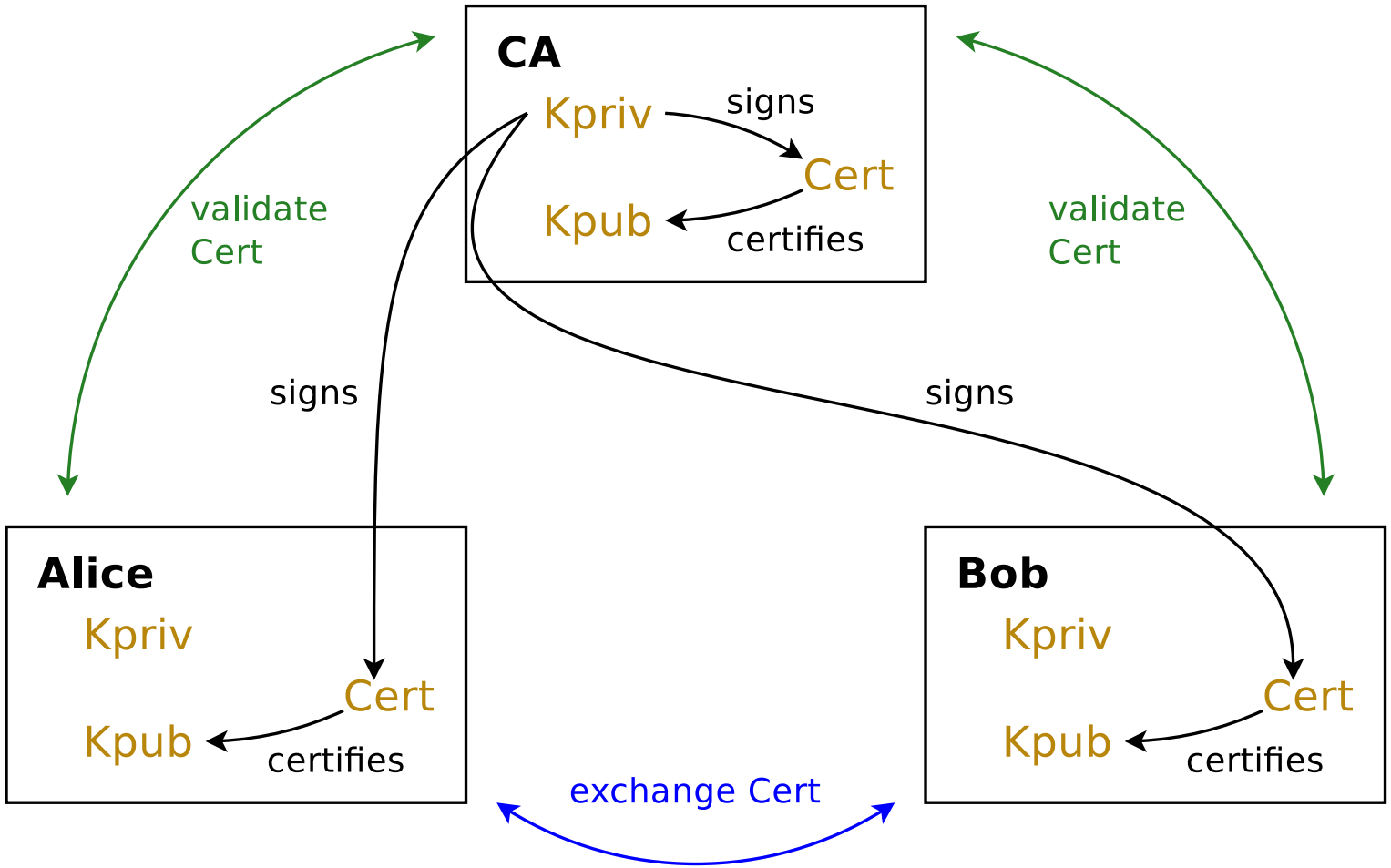
Hierarchie


CA
Kpriv
signs
Cert
Kpub
certifies
signs
signs
Alice
Kpriv
Cert
Kpub
certifies
Bob
Kpriv
Cert
Kpub
certifies

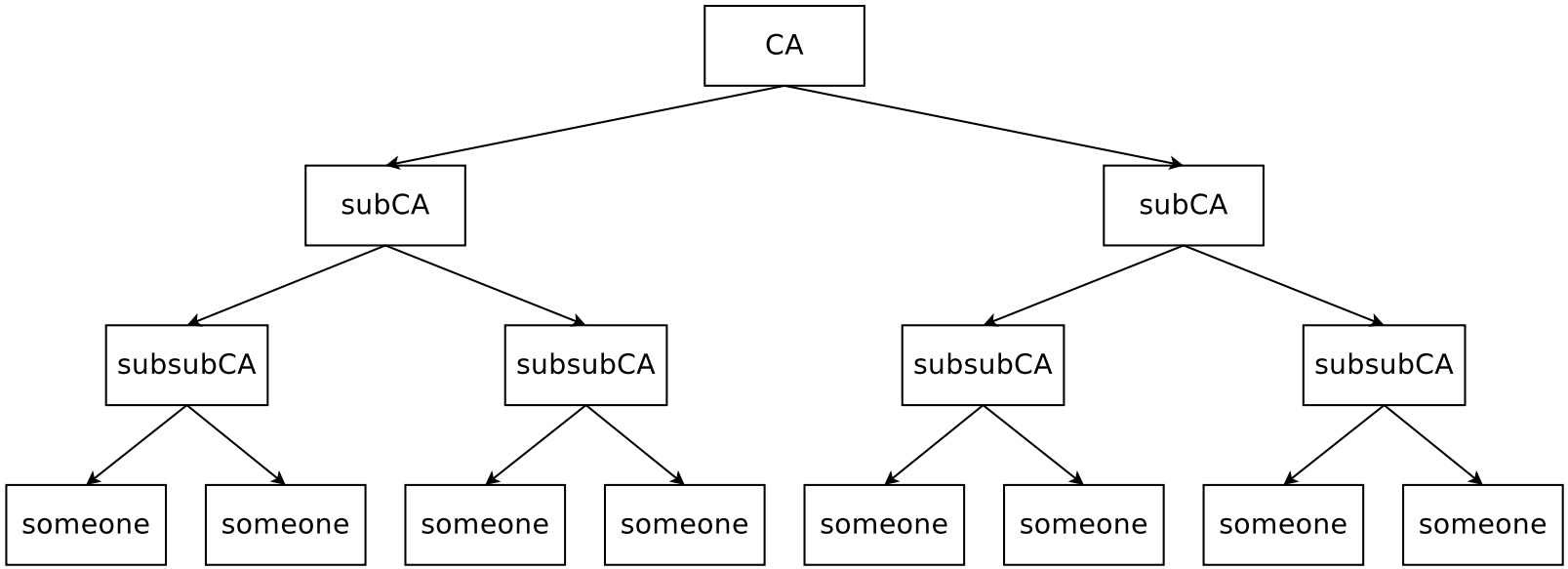
Hierarchie


CA
Kpriv
signs
Cert
Kpub
certifies
signs
signs
Alice
Kpriv
Cert
Kpub
certifies
Bob
Kpriv
Cert
Kpub
certifies
exchange Cert

Hierarchie


CA
Kpriv
signs
Cert
Kpub
certifies
validate
Cert
validate
Cert
signs
signs
Alice
Kpriv
Cert
Kpub
certifies
Bob
Kpriv
Cert
Kpub
certifies
exchange Cert

Hierarchie


CA
subCA
subCA
subsubCA
subsubCA
subsubCA
subsubCA
someone
someone
someone
someone
someone
someone
someone
someone

Überblick

- Asymmetrische Kryptografie

Überblick

- Asymmetrische Kryptografie
  - Authentizität

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit
- Certificate

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit
- Certificate
  - Gültigkeit der Schlüssel

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit
- Certificate
  - Gültigkeit der Schlüssel
- Public Key Infrastructure

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit
- Certificate
  - Gültigkeit der Schlüssel
- Public Key Infrastructure
  - Vertrauensanker

Überblick

- Asymmetrische Kryptografie
  - Authentizität
  - Vertraulichkeit
- Certificate
  - Gültigkeit der Schlüssel
- Public Key Infrastructure
  - Vertrauensanker
  - Verteilung der Schlüssel vereinfacht

Fragen ?

Domain Name System Security Extensions

Gliederung

Gliederung

Domain Name System Security Extensions

- Warum DNSSEC?

Domain Name System Security Extensions

- Warum DNSSEC?
  - Verhinderung von Angriffen

Domain Name System Security Extensions

- Warum DNSSEC?
  - Verhinderung von Angriffen
- Aufgaben

Domain Name System Security Extensions

- Warum DNSSEC?
  - Verhinderung von Angriffen
- Aufgaben
  - Schützen der DNS-Antworten der Nameserver

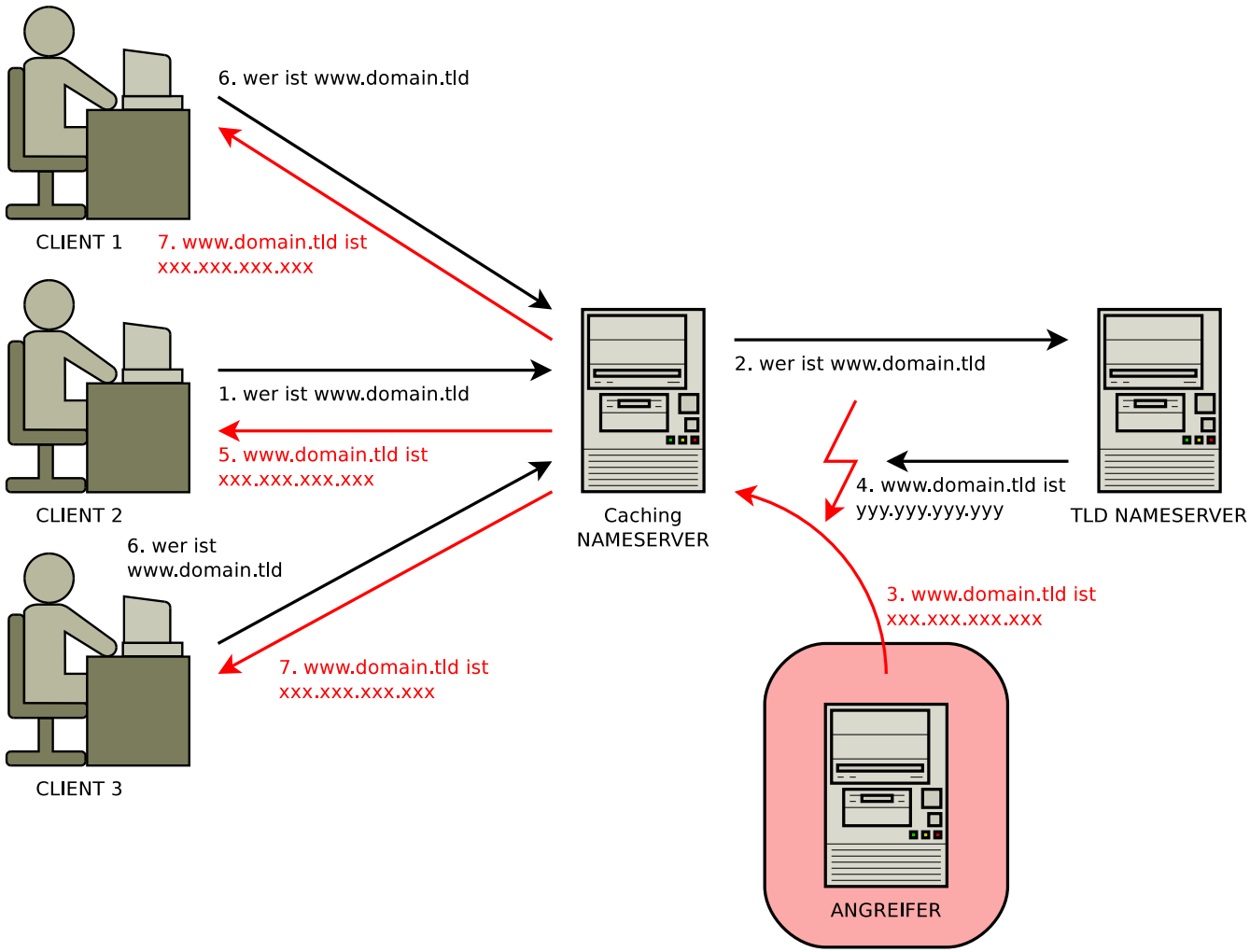
Domain Name System Security Extensions

- Warum DNSSEC?
  - Verhinderung von Angriffen
- Aufgaben
  - Schützen der DNS-Antworten der Nameserver
- Muss global angewandt werden

Motivation

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

DNS-Cache-Poisoning



Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

- Was bedeutet das?

Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

- Was bedeutet das?
  - asymmetrische Kryptografie

Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

- Was bedeutet das?
  - asymmetrische Kryptografie
    - Private Schlüssel

Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

- Was bedeutet das?
  - asymmetrische Kryptografie
    - Private Schlüssel
    - Öffentliche Schlüssel

Idee

Grundlegende Idee

Schützen der DNS-Antworten bzw. Resource Records durch digitale Signatur

- Was bedeutet das?
  - asymmetrische Kryptografie
    - Private Schlüssel
    - Öffentliche Schlüssel
  - Schlüsselhierarchie

Was wird signiert?

Zwei Möglichkeiten:

Was wird signiert?

Zwei Möglichkeiten:

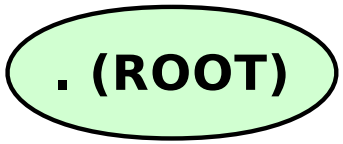
- Signieren der DNS-Antwort

Was wird signiert?

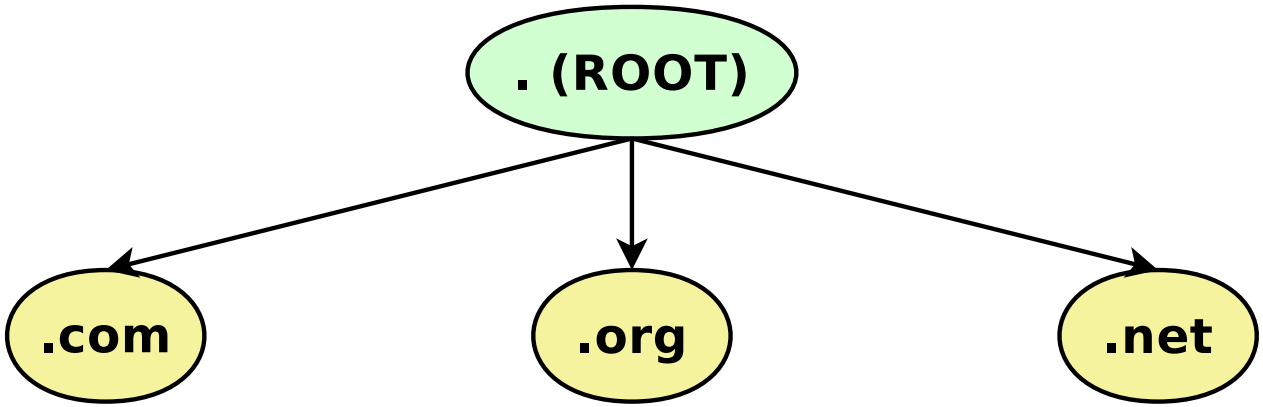
Zwei Möglichkeiten:

- Signieren der DNS-Antwort
- Signieren der Records

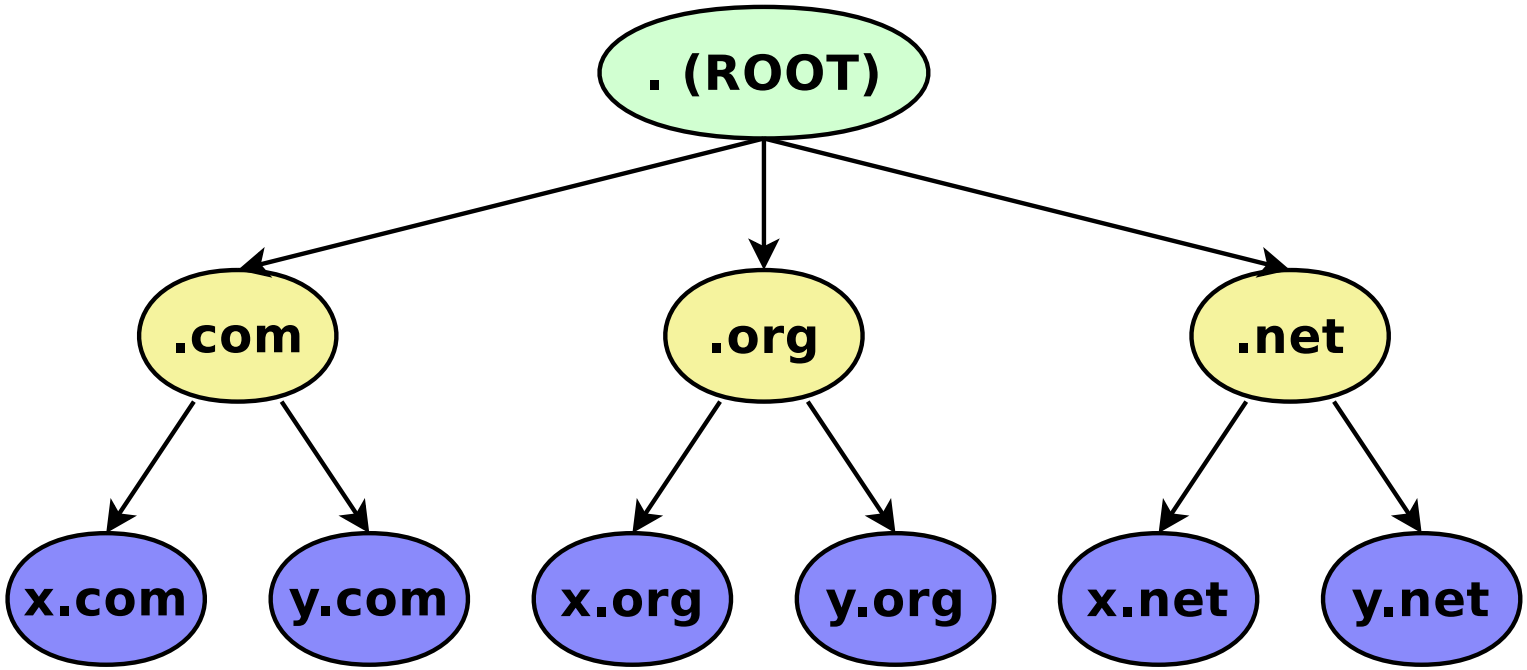
Schlüsselhierarchie



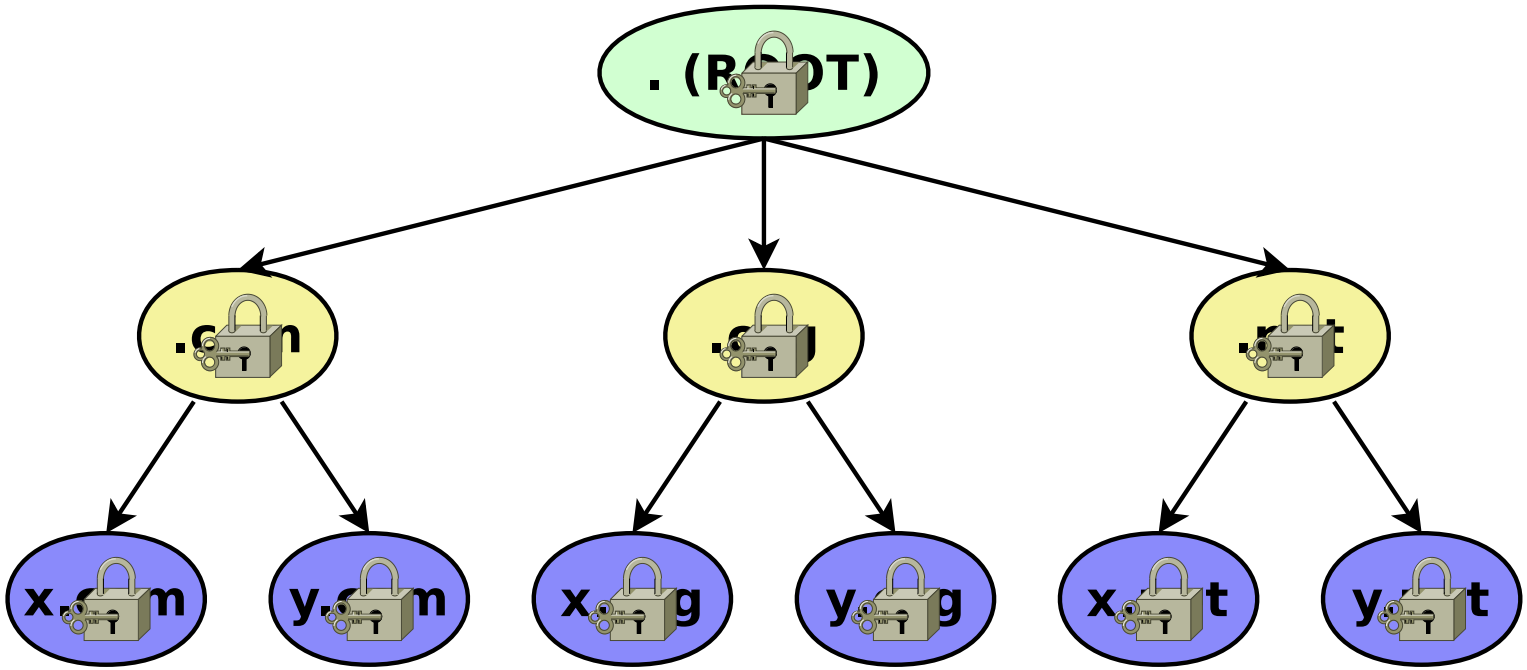
Schlüsselhierarchie



Schlüsselhierarchie



Schlüsselhierarchie



Neue Records

DNSKEY Öffentlicher Schlüssel

Neue Records

DNSKEY Öffentlicher Schlüssel

RRSIG Signatur

Neue Records

DNSKEY Öffentlicher Schlüssel

RRSIG Signatur

IST DOCH EINFACH!

Schwierigkeiten

- Schlüssellänge

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit
- Rechenaufwand für Signatur

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit
- Rechenaufwand für Signatur
- öffentliche Schlüssel durch Parent Zone signiert

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit
- Rechenaufwand für Signatur
- öffentliche Schlüssel durch Parent Zone signiert
- Sehr, sehr viele Schlüssel

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit
- Rechenaufwand für Signatur
- öffentliche Schlüssel durch Parent Zone signiert
- Sehr, sehr viele Schlüssel
- Signaturen mitliefern: UDP $\rightarrow$ TCP

Schwierigkeiten

- Schlüssellänge
- Schlüsselgültigkeit
- Rechenaufwand für Signatur
- öffentliche Schlüssel durch Parent Zone signiert
- Sehr, sehr viele Schlüssel
- Signaturen mitliefern: UDP $\rightarrow$ TCP
- Antwort für nicht-existente Domains?

Key Rollover

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Vorteile:

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Vorteile:

- ZSK Rollover vereinfacht

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Vorteile:

- ZSK Rollover vereinfacht
- ZSK weniger Bits

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Vorteile:

- ZSK Rollover vereinfacht
- ZSK weniger Bits
- Schnelleres Signieren

Key Rollover

ZSK Zone Signing Key: signiert alle Resource Records der Zone

KSK Key Signing Key: signiert alle ZSK der eigenen Zone

Vorteile:

- ZSK Rollover vereinfacht
- ZSK weniger Bits
- Schnelleres Signieren
- Sicherer

Key Rollover

- Rollover von KSK(12 Monate) und ZSK(1 Monat)

Key Rollover

- Rollover von KSK(12 Monate) und ZSK(1 Monat)
- Probleme:

Key Rollover

- Rollover von KSK(12 Monate) und ZSK(1 Monat)
- Probleme:
  - Schlüsselpublizierung in Zone und in TLD benötigt Zeit

Key Rollover

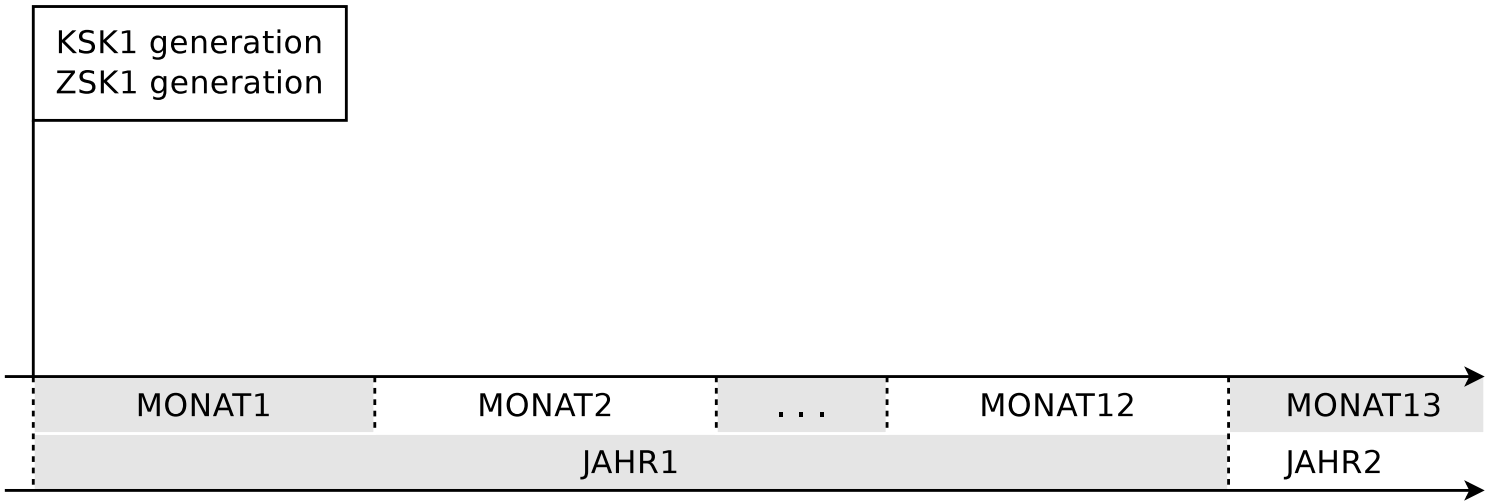
- Rollover von KSK(12 Monate) und ZSK(1 Monat)
- Probleme:
  - Schlüsselpublizierung in Zone und in TLD benötigt Zeit
  - Alte Schlüssel noch unterwegs

Key Rollover

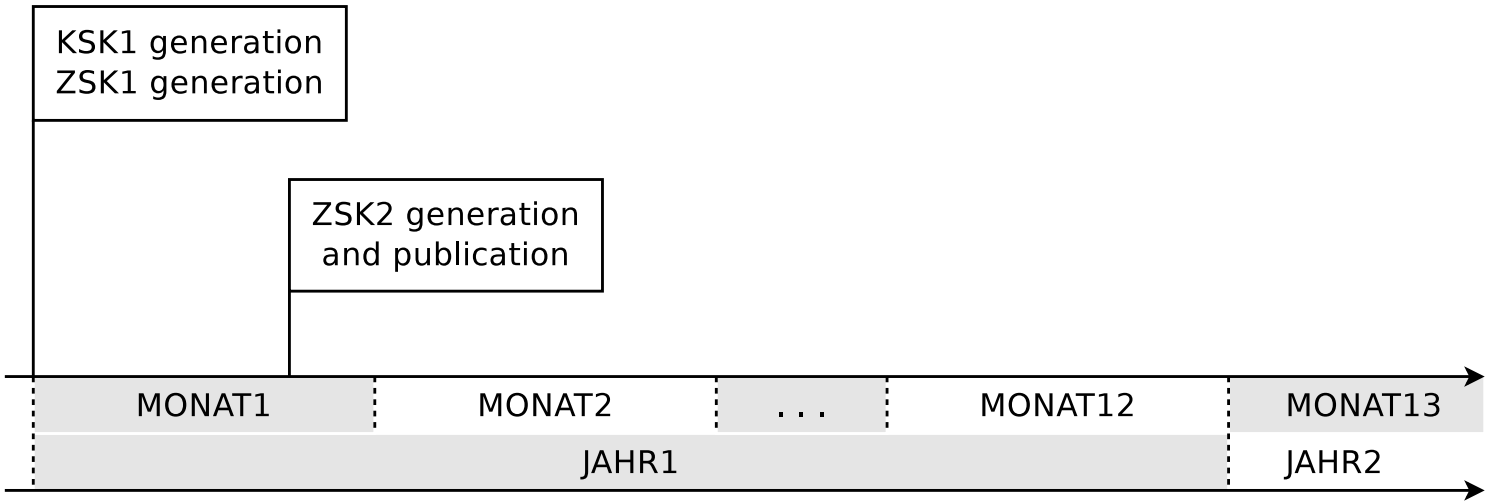
- Rollover von KSK(12 Monate) und ZSK(1 Monat)
- Probleme:
  - Schlüsselpublizierung in Zone und in TLD benötigt Zeit
  - Alte Schlüssel noch unterwegs
  - Records mit alten Signaturen noch unterwegs

Key Rollover (pre-publish-Verfahren)

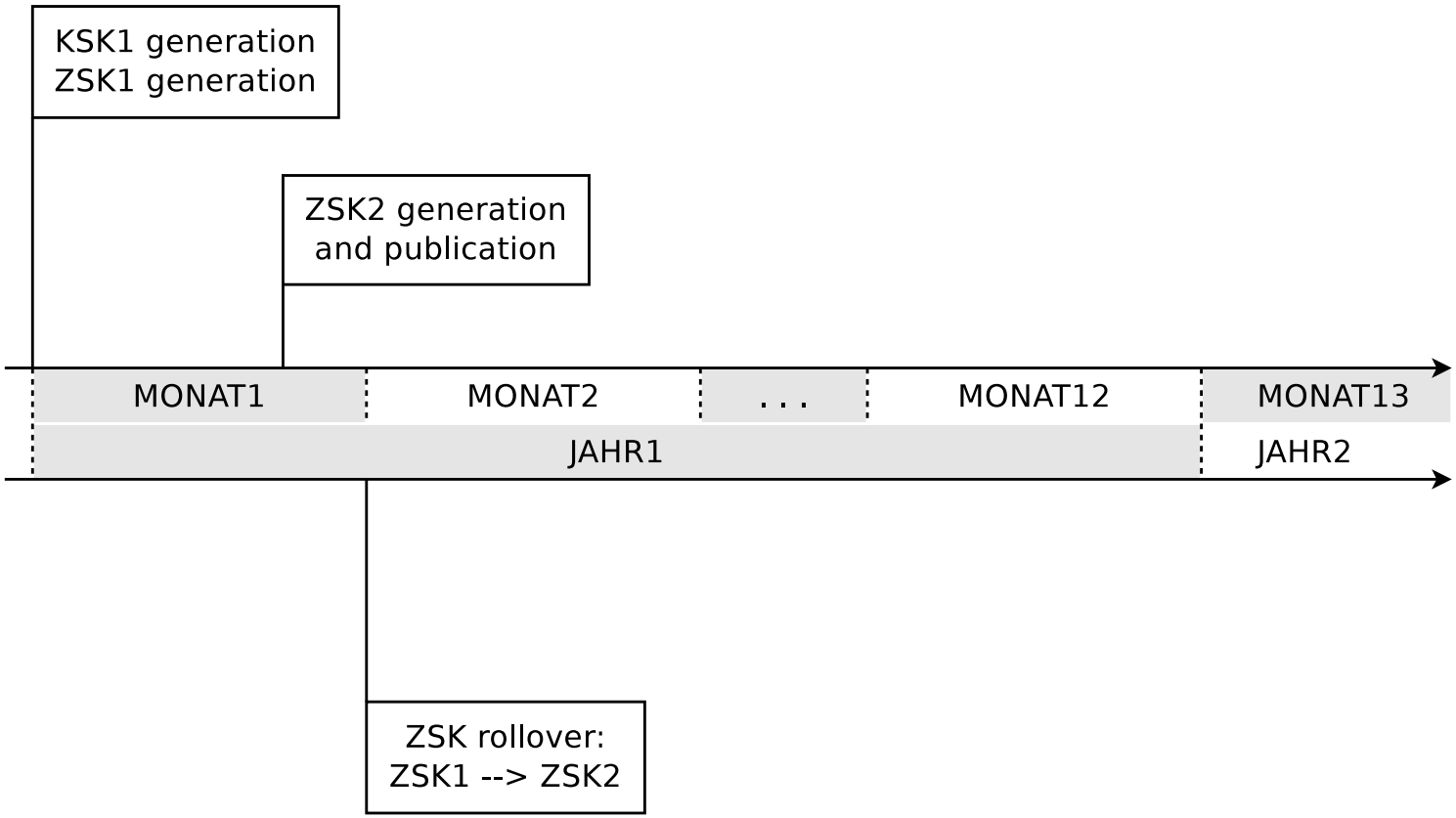
Key Rollover (pre-publish-Verfahren)



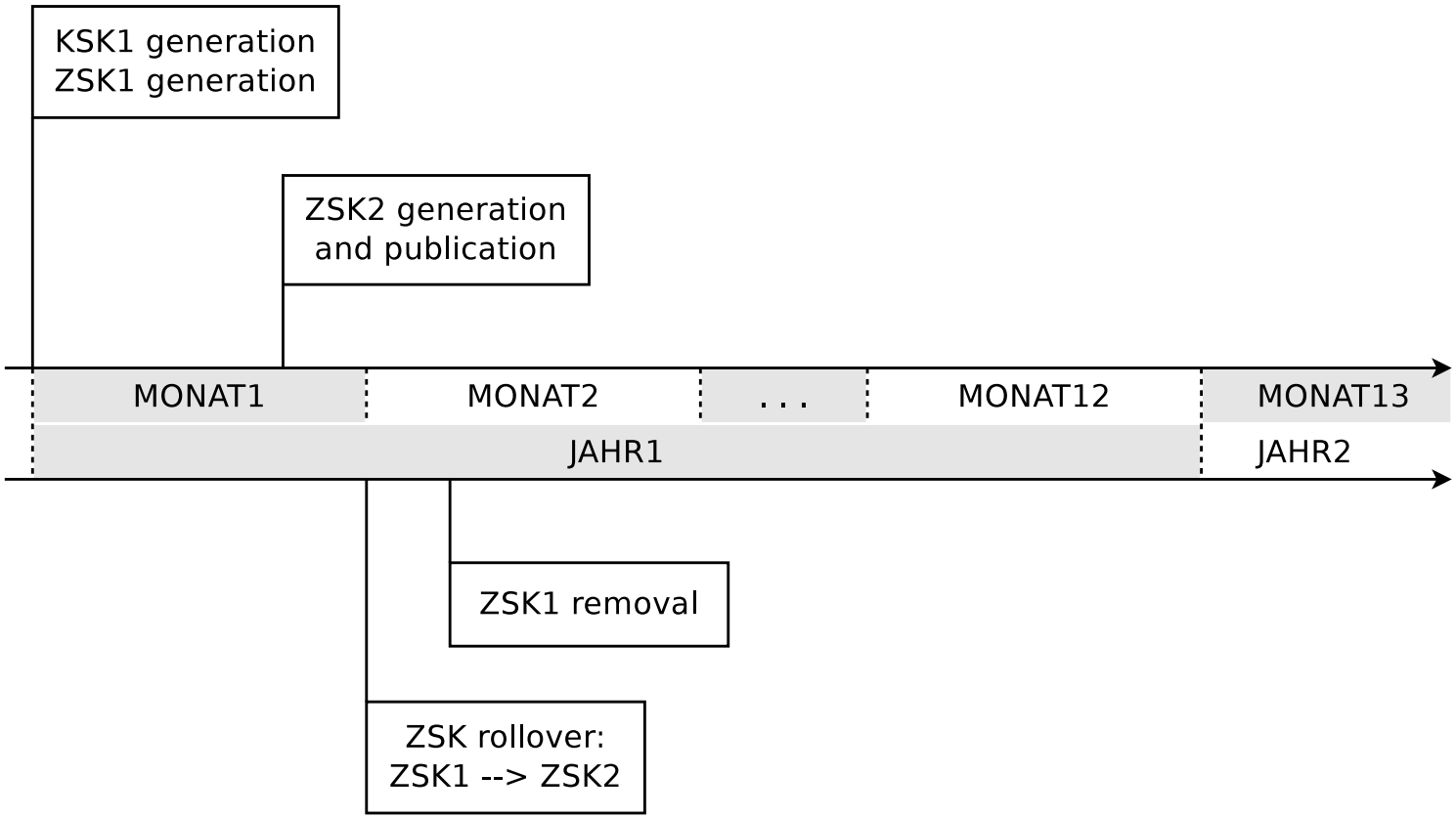
Key Rollover (pre-publish-Verfahren)



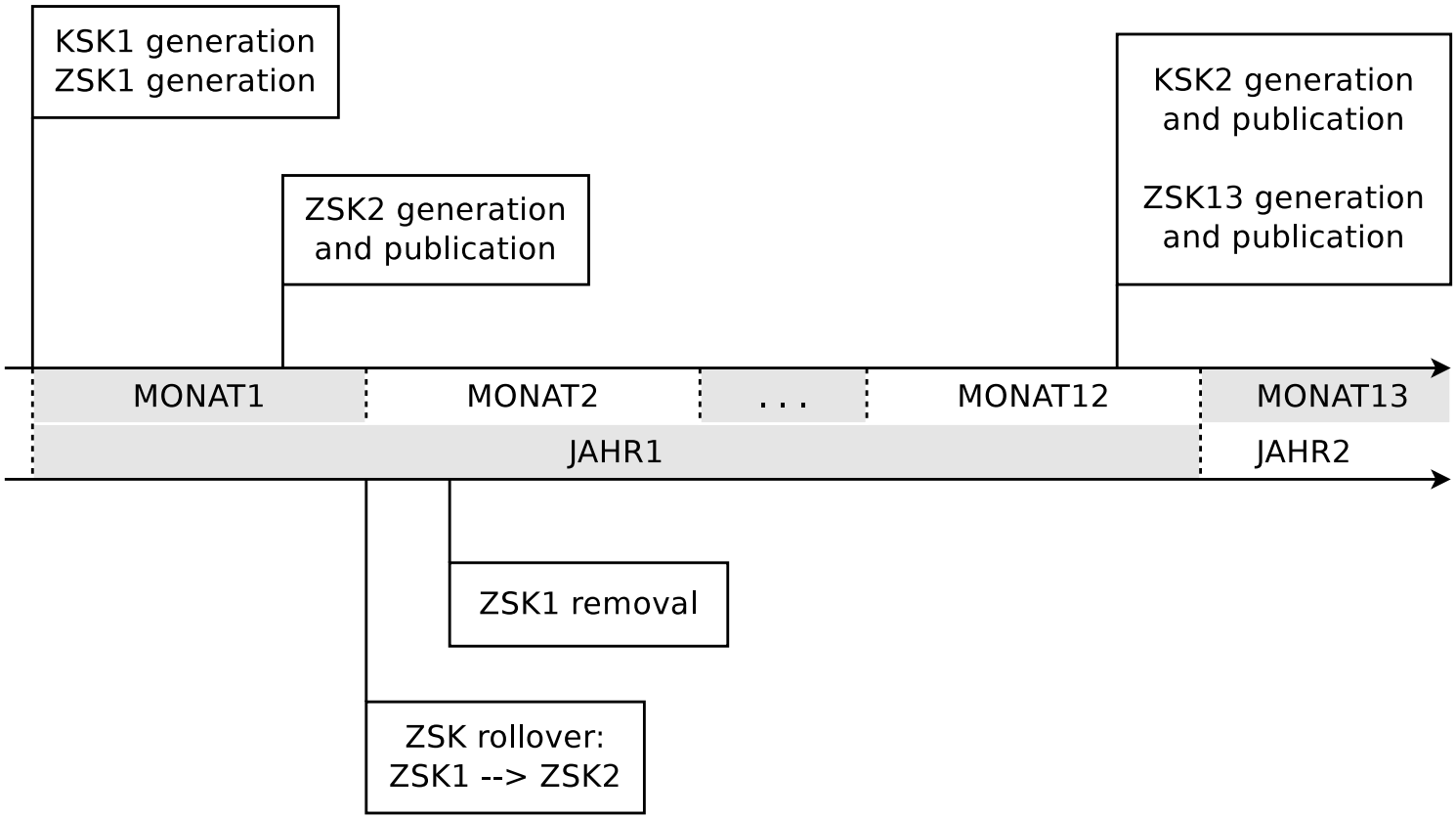
Key Rollover (pre-publish-Verfahren)



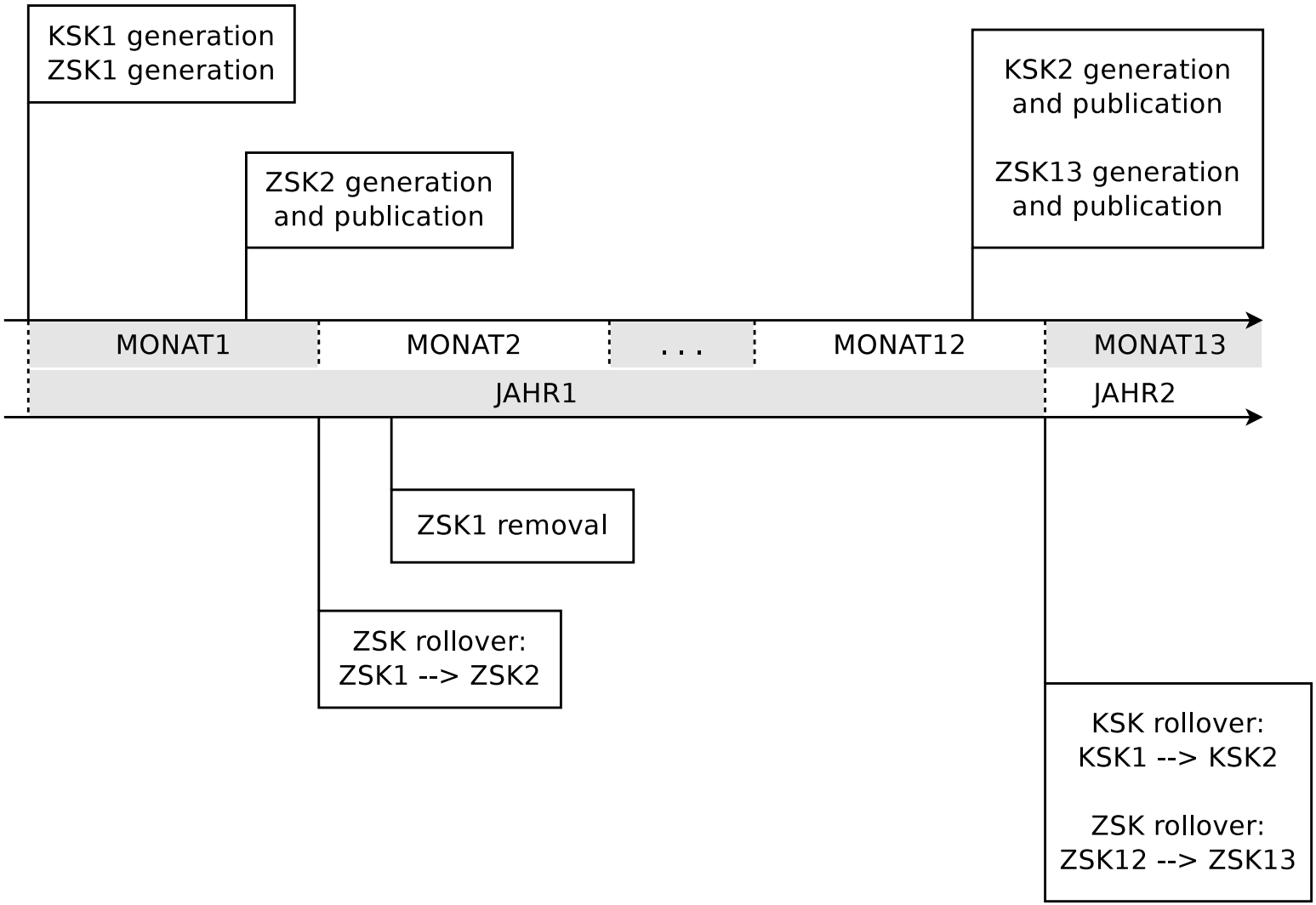
Key Rollover (pre-publish-Verfahren)



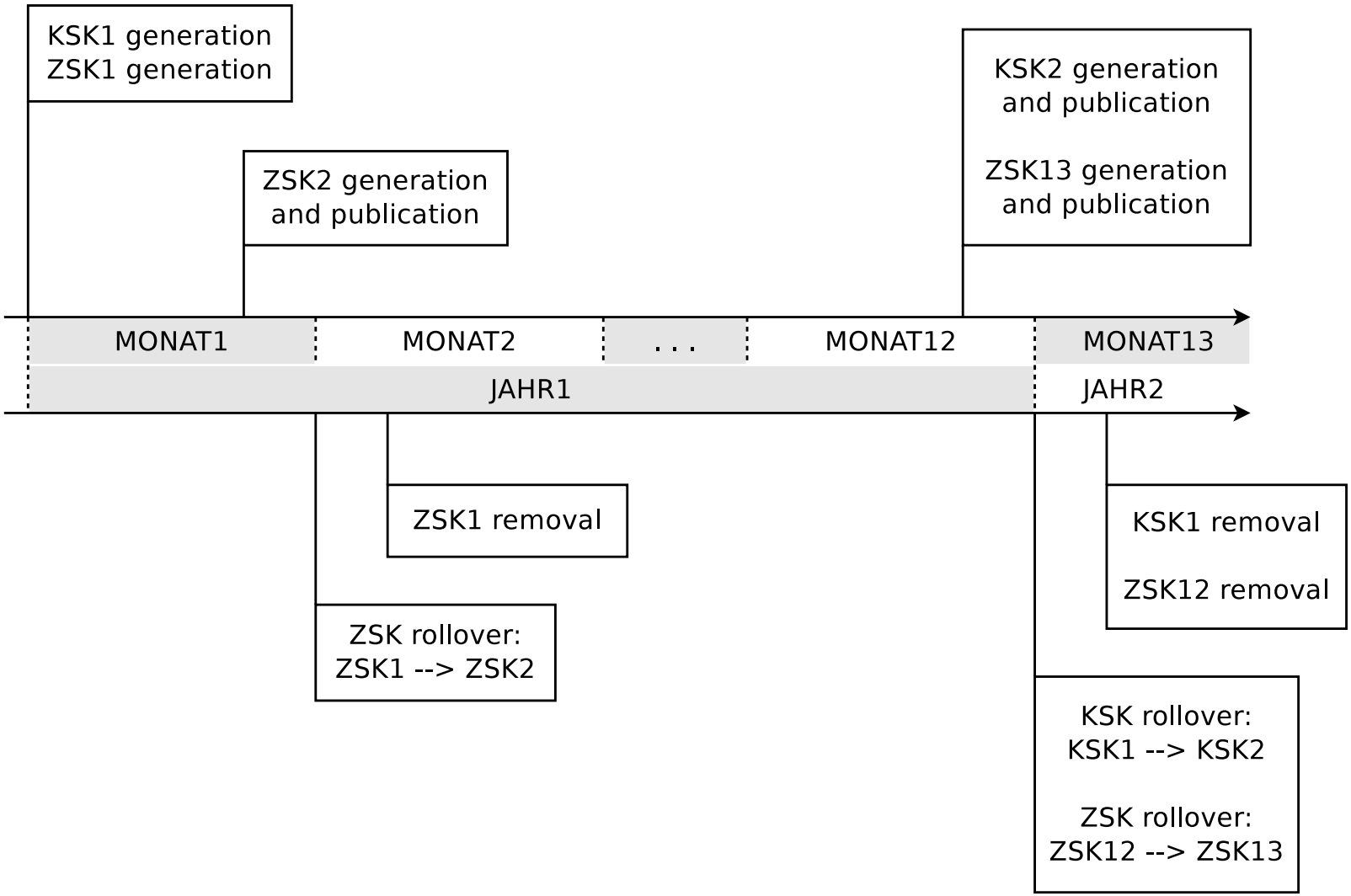
Key Rollover (pre-publish-Verfahren)



Key Rollover (pre-publish-Verfahren)



Key Rollover (pre-publish-Verfahren)



Viele Schlüssel

- 4 KB Schlüssel pro Zone

Viele Schlüssel

- 4 KB Schlüssel pro Zone
- 14 Millionen Zonen (.de)

Viele Schlüssel

- 4 KB Schlüssel pro Zone
- 14 Millionen Zonen (.de)
- ca. 53 GB Daten

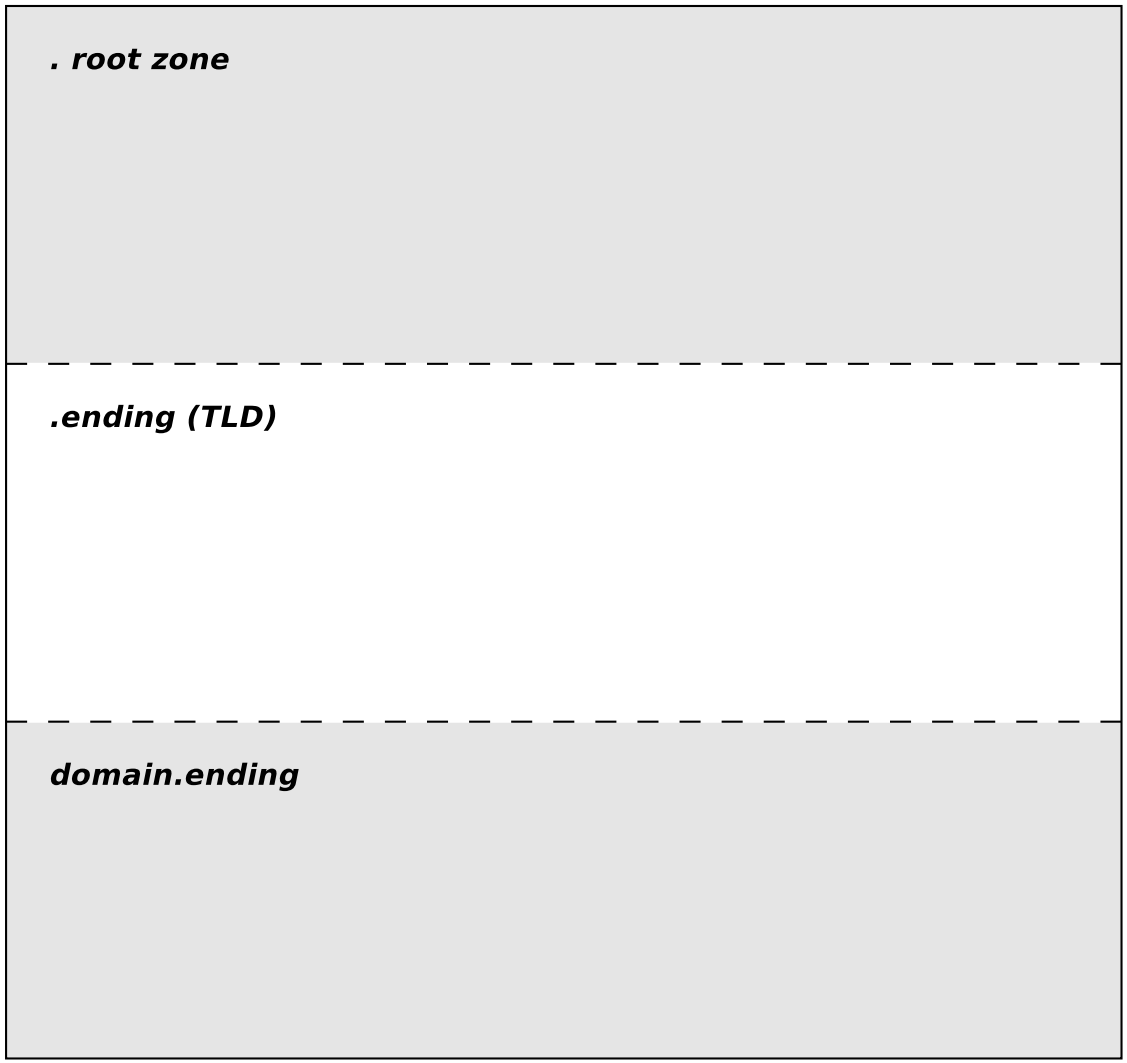
Viele Schlüssel

- 4 KB Schlüssel pro Zone
- 14 Millionen Zonen (.de)
- ca. 53 GB Daten
- Lösung: Hash statt Schlüssel $\rightarrow$ ca. 2 GB Daten

Records

DNSKEY	Öffentlicher Schlüssel
RRSIG	Signatur eines Records
DS	Delegation Signer, Hash eines öffentlichen Schlüssels

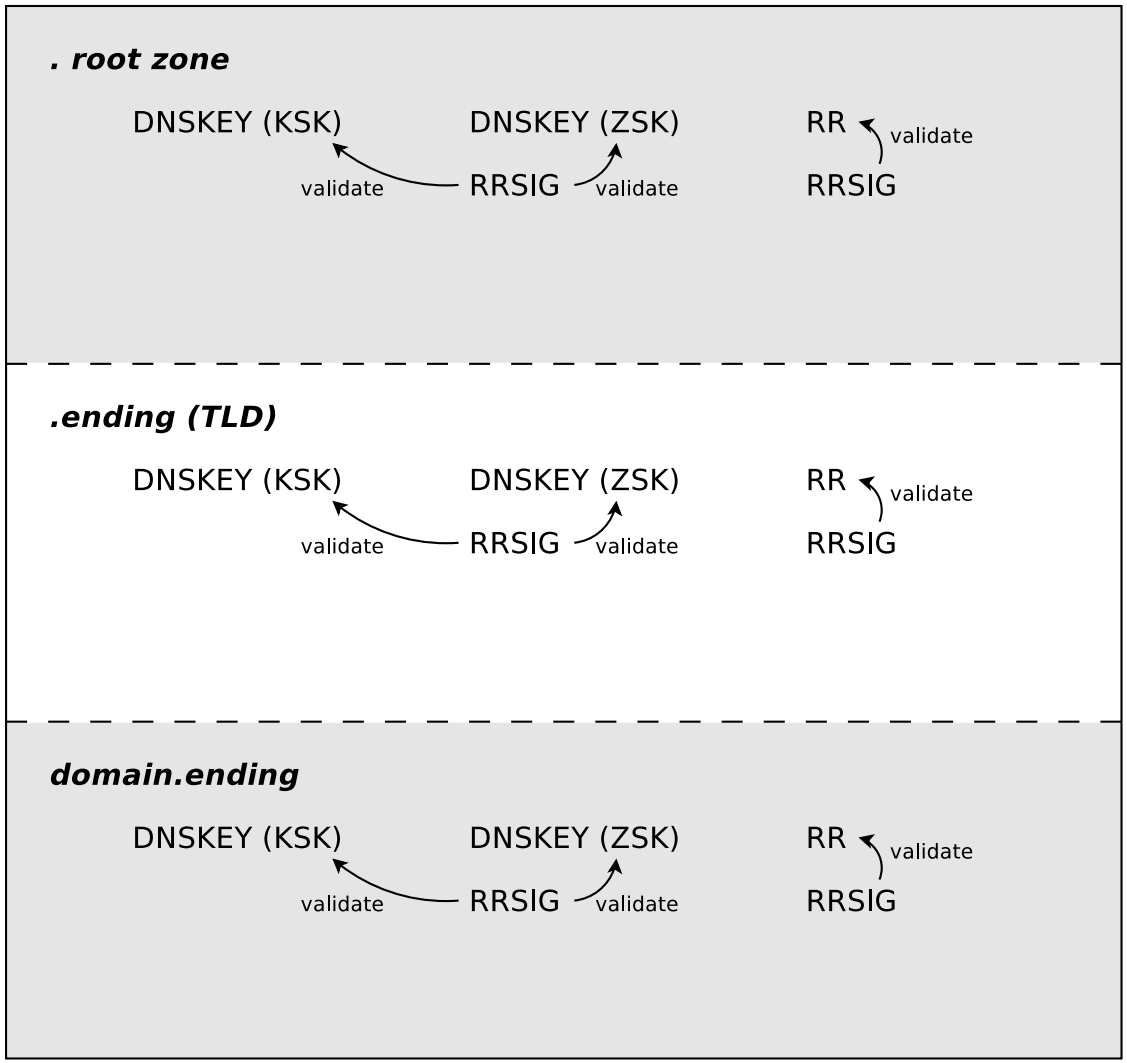
Records



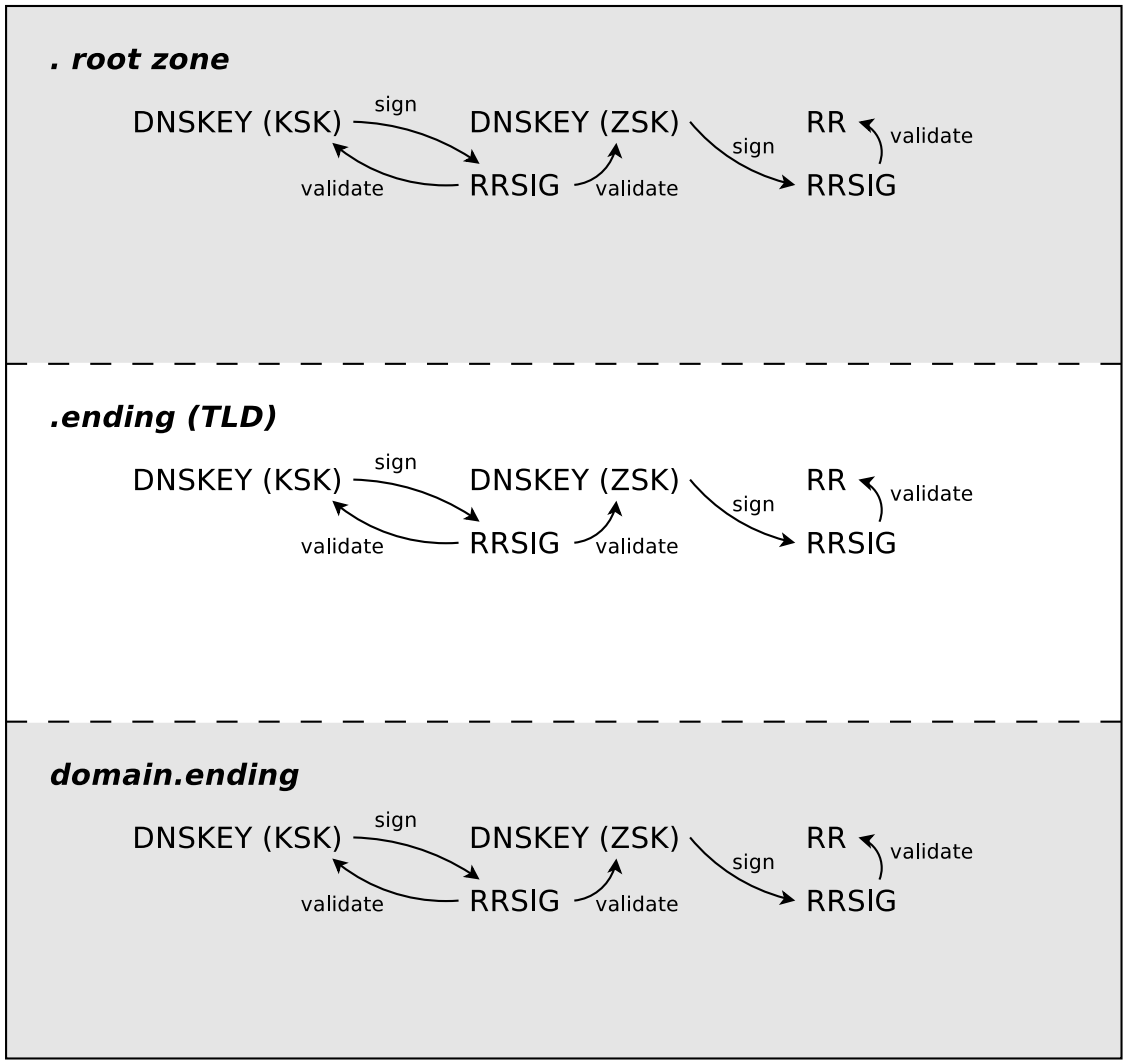
Records


. root zone
DNSKEY (KSK)
DNSKEY (ZSK)
RR
.ending (TLD)
DNSKEY (KSK)
DNSKEY (ZSK)
RR
domain.ending
DNSKEY (KSK)
DNSKEY (ZSK)
RR

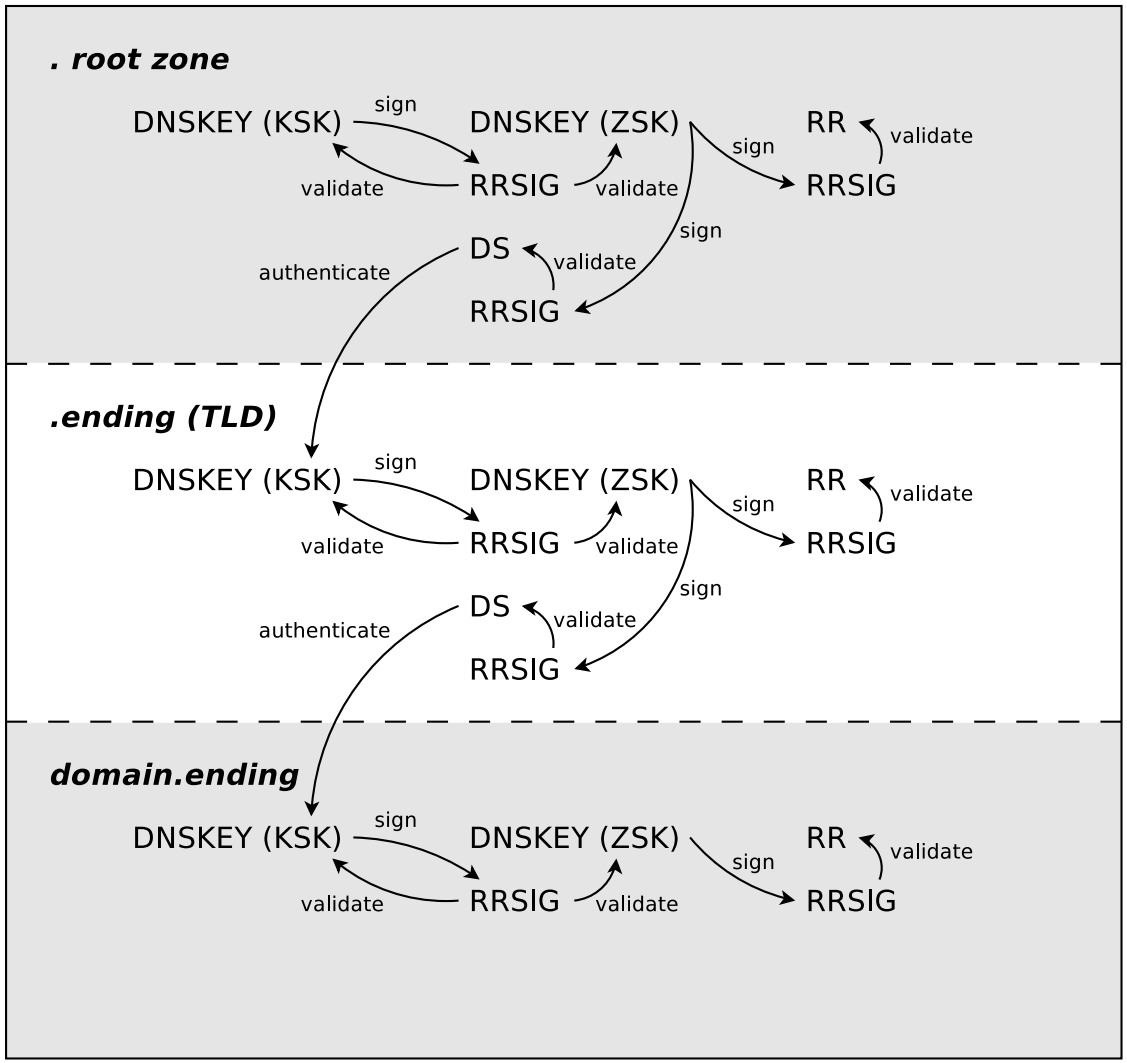
Records


. root zone
DNSKEY (KSK)
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
RRSIG
.ending (TLD)
DNSKEY (KSK)
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
RRSIG
domain.ending
DNSKEY (KSK)
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
RRSIG

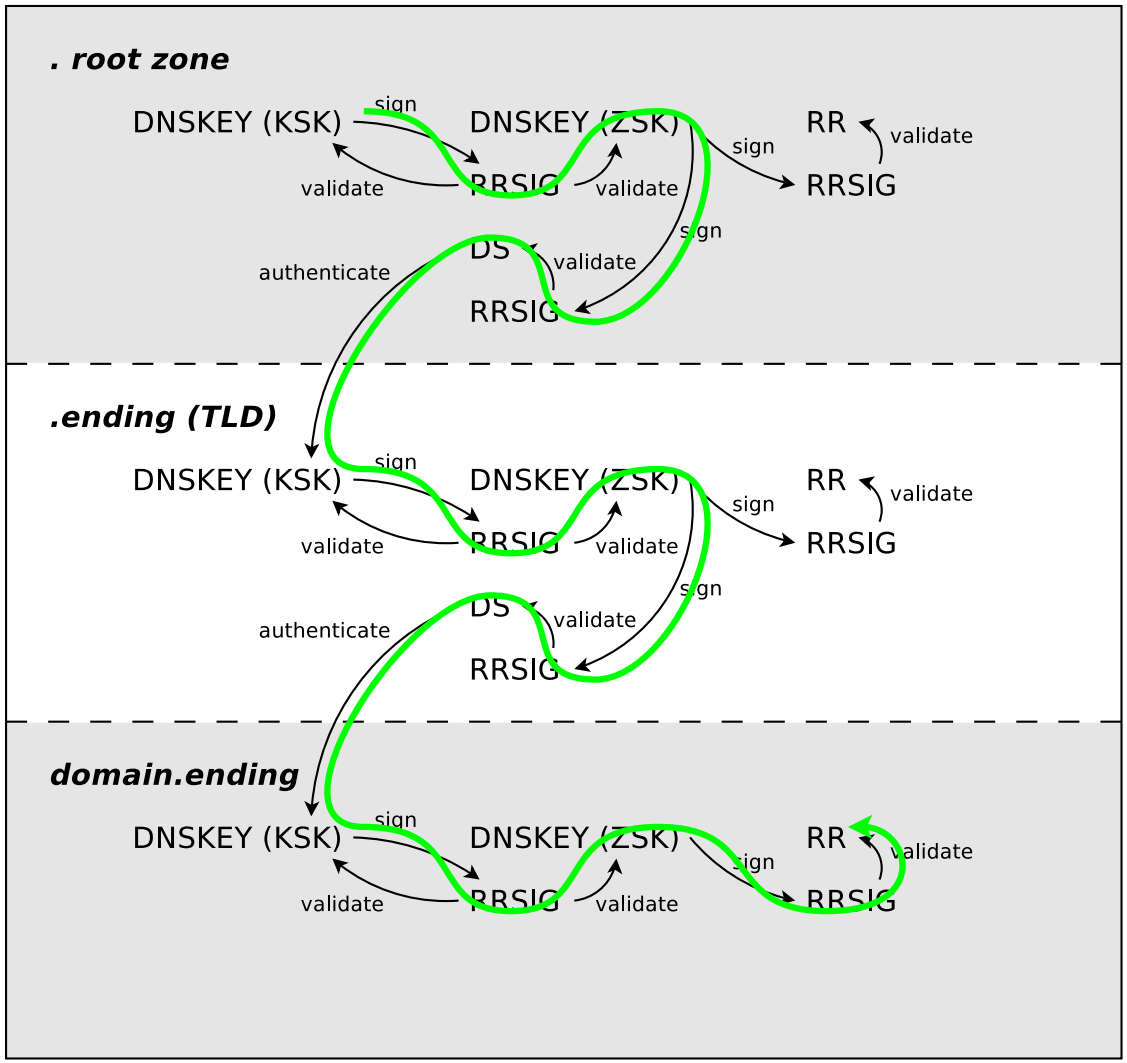
Records


. root zone
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
sign
validate
RRSIG
validate
RRSIG
.ending (TLD)
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
sign
validate
RRSIG
validate
RRSIG
domain.ending
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
sign
validate
RRSIG
validate
RRSIG

Records


. root zone
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
RRSIG
sign
DS
validate
authenticate
RRSIG
.ending (TLD)
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
RRSIG
sign
DS
validate
authenticate
RRSIG
domain.ending
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
RRSIG

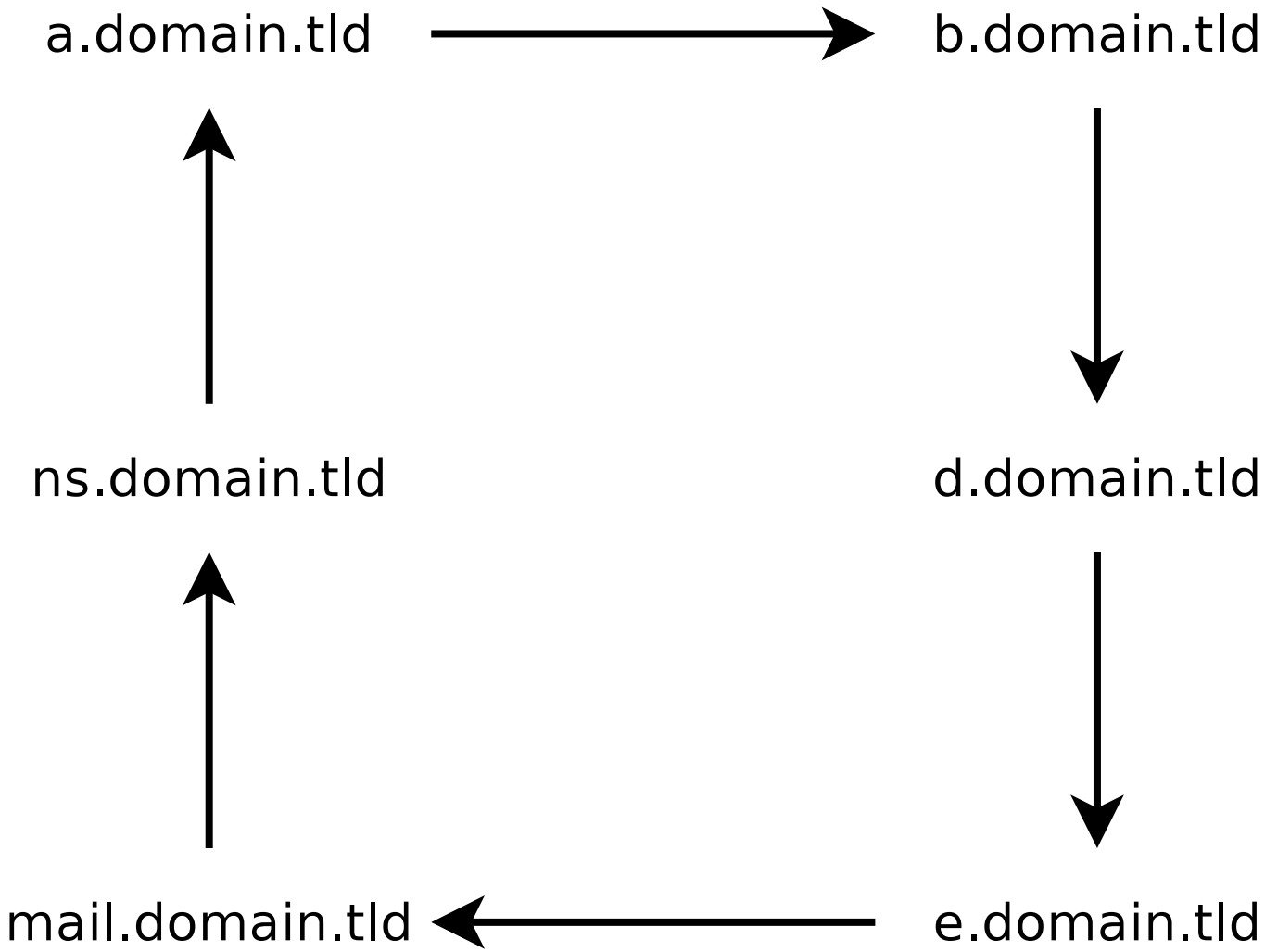
Records


. root zone
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
sign
RRSIG
DS
validate
authenticate
RRSIG
.ending (TLD)
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
sign
RRSIG
DS
validate
authenticate
RRSIG
domain.ending
DNSKEY (KSK)
sign
DNSKEY (ZSK)
RR
validate
validate
RRSIG
validate
sign
RRSIG

NSEC - Next Secure


```
a.domain.tld. IN A 172.16.1.11

b.domain.tld. IN A 172.16.1.11

d.domain.tld. IN A 172.16.1.11

e.domain.tld. IN A 172.16.1.11

mail.domain.tld. IN A 172.16.1.11

ns.domain.tld. IN A 172.16.1.11
```

NSEC - Next Secure



NSEC - Next Secure


```
a.domain.tld NSEC b.domain.tld

b.domain.tld NSEC d.domain.tld

d.domain.tld NSEC e.domain.tld

e.domain.tld NSEC mail.domain.tld

mail.domain.tld NSEC ns.domain.tld

ns.domain.tld NSEC a.domain.tld
```

NSEC - Next Secure

Suche nach c.domain.tld

```
a.domain.tld NSEC b.domain.tld

b.domain.tld NSEC d.domain.tld

d.domain.tld NSEC e.domain.tld

e.domain.tld NSEC mail.domain.tld

mail.domain.tld NSEC ns.domain.tld

ns.domain.tld NSEC a.domain.tld
```

NSEC - Next Secure

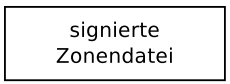
Suche nach c.domain.tld

```
a.domain.tld NSEC b.domain.tld

b.domain.tld NSEC d.domain.tld

d.domain.tld NSEC e.domain.tld

e.domain.tld NSEC mail.domain.tld

mail.domain.tld NSEC ns.domain.tld

ns.domain.tld NSEC a.domain.tld
```

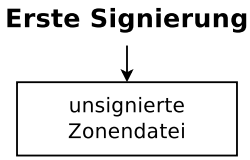
Records

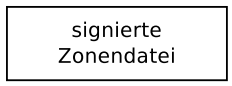
DNSKEY	Öffentlicher Schlüssel
RRSIG	Signatur eines Records
DS	Delegation Signer, Hash eines öffentlichen Schlüssels
NSEC	Nicht-Existenz-Beweis einer Domain

Erste Signierung

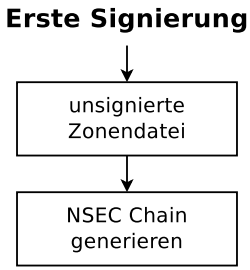


DNSSECify


Erste Signierung
unsignierte Zonendatei

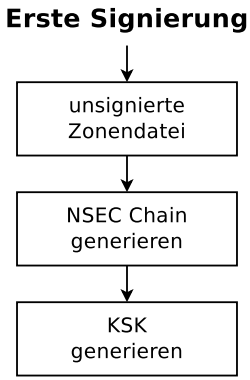

signierte Zonendatei

DNSSECify



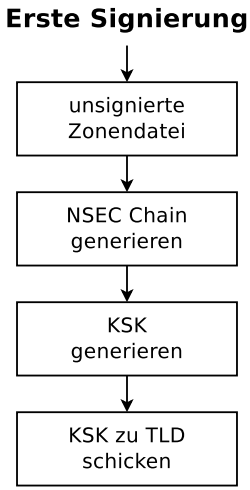
signierte Zonendatei

DNSSECify



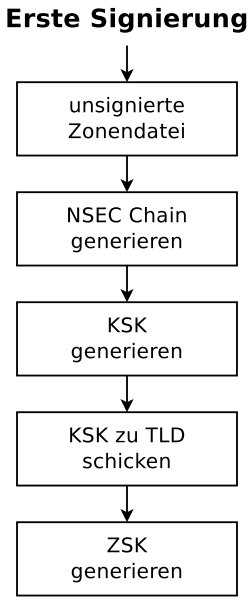
signierte Zonendatei

DNSSECify



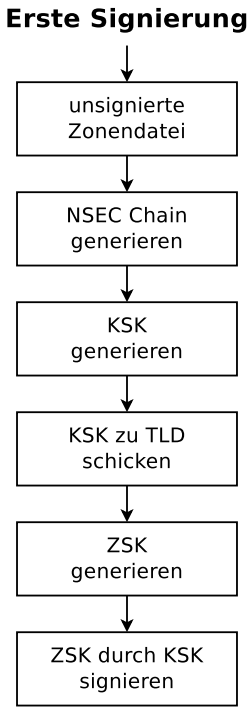
signierte Zonendatei

DNSSECify



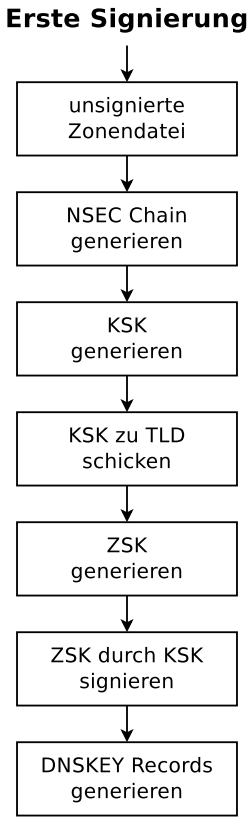
signierte Zonendatei

DNSSECify



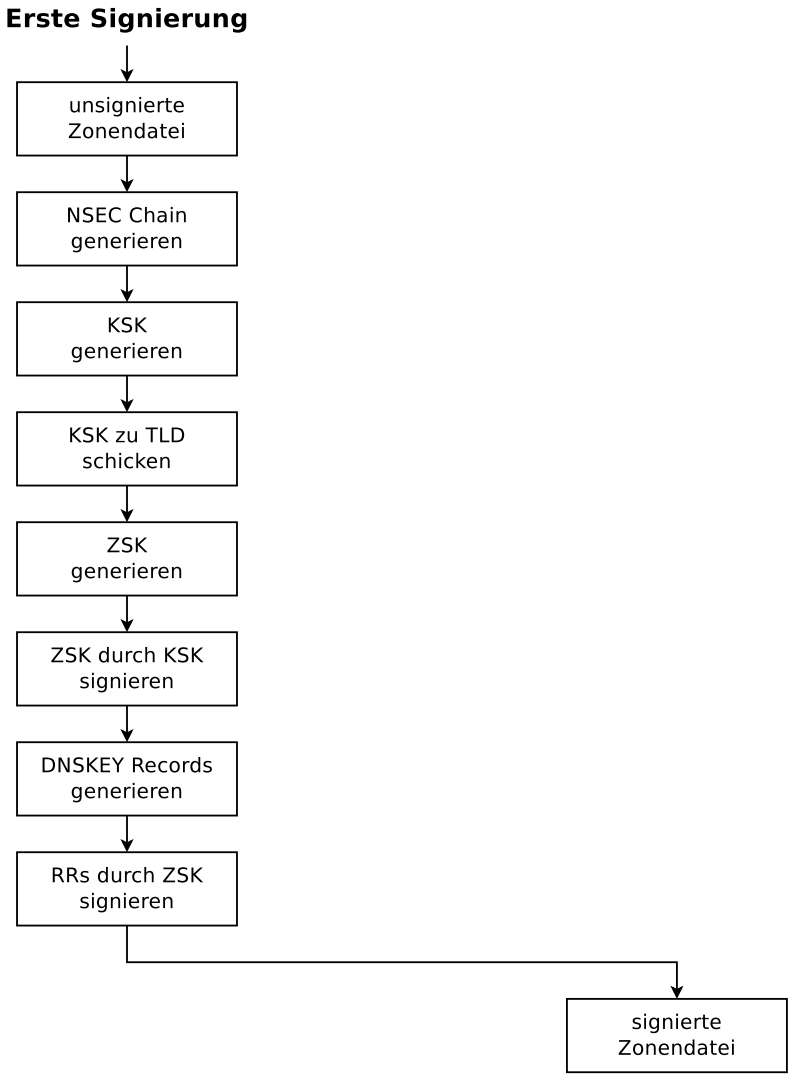
signierte Zonendatei

DNSSECify

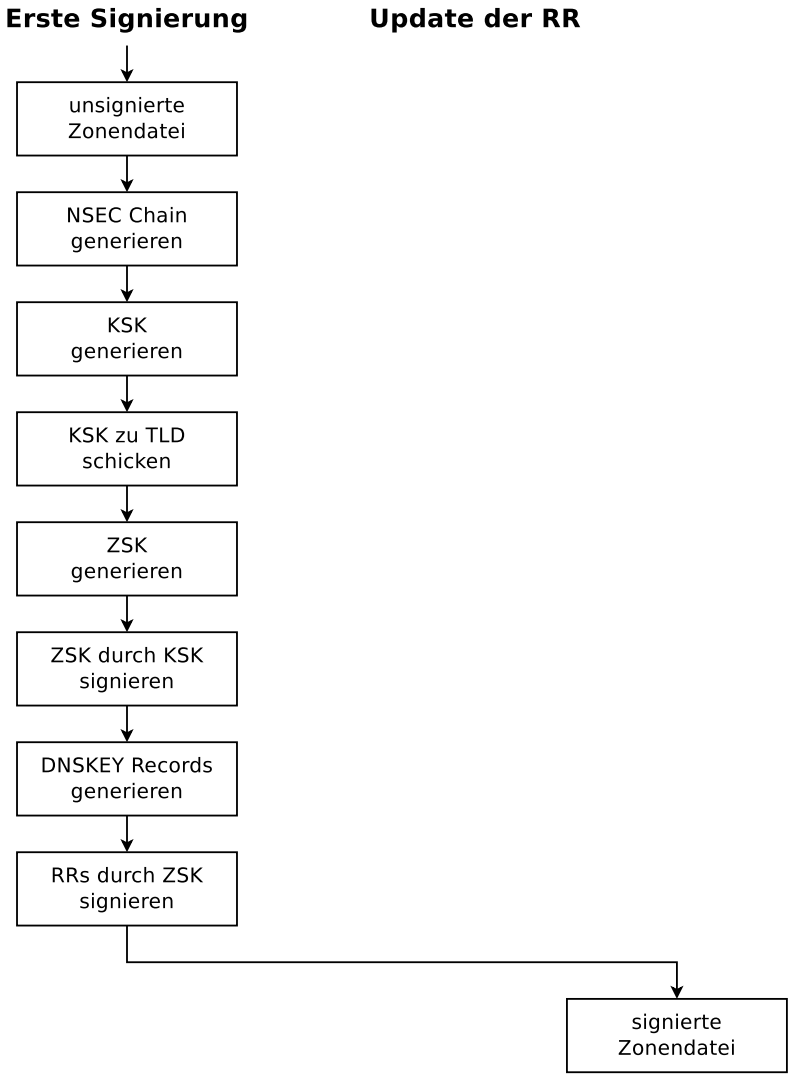


signierte Zonendatei

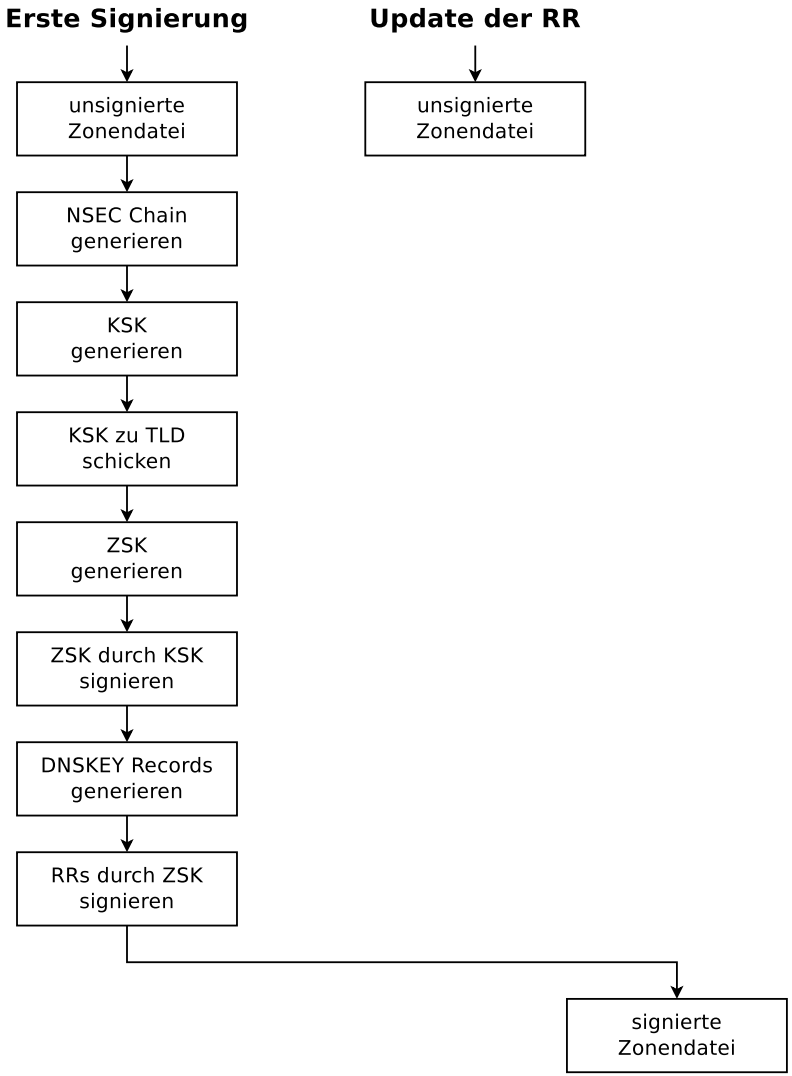
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
signierte Zonendatei

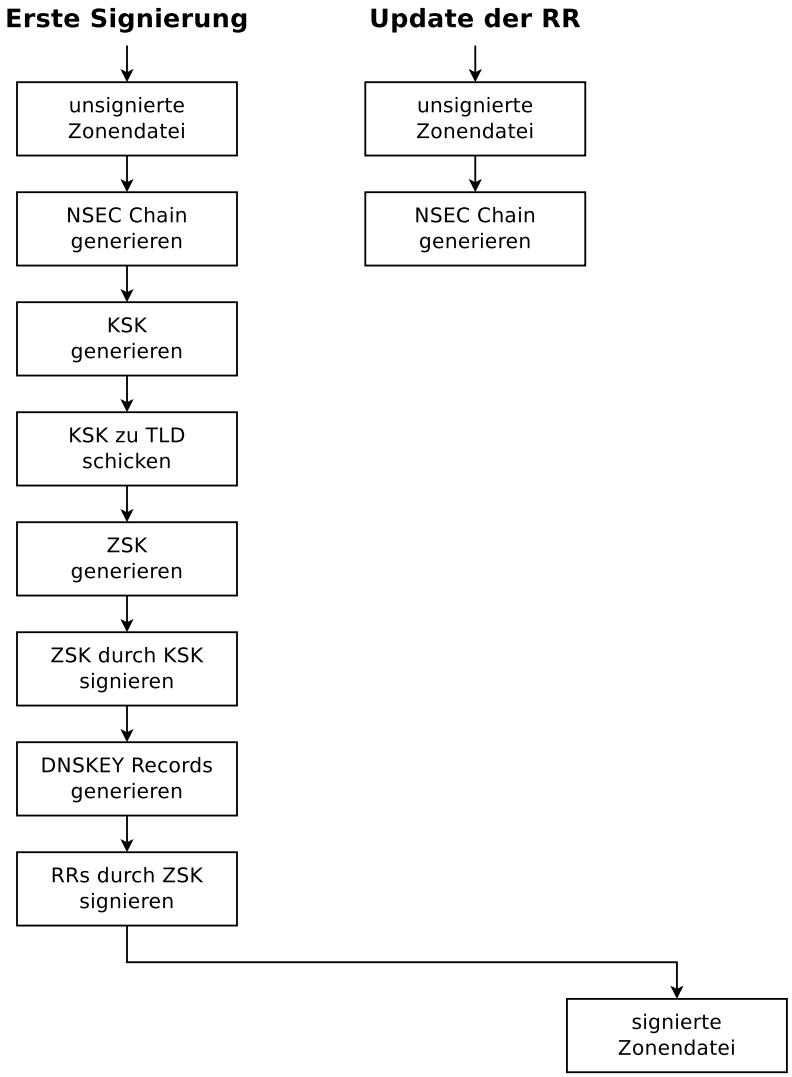
DNSSECify


Erste Signierung
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
signierte Zonendatei

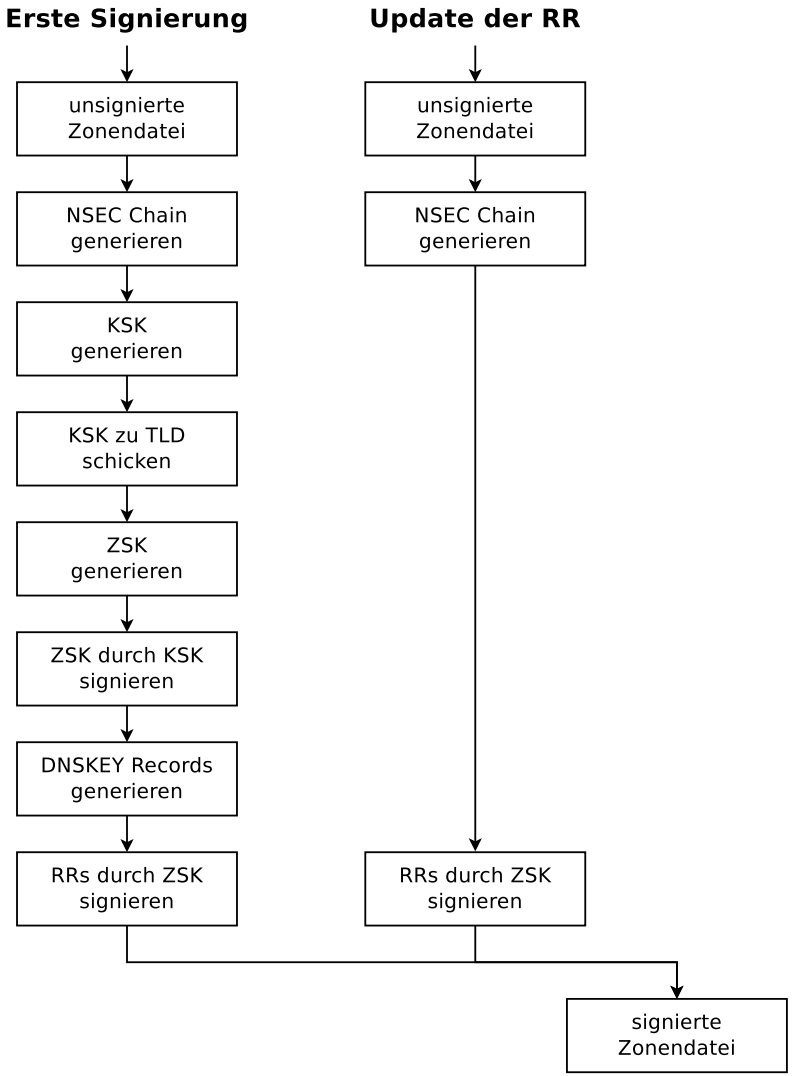
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
signierte Zonendatei

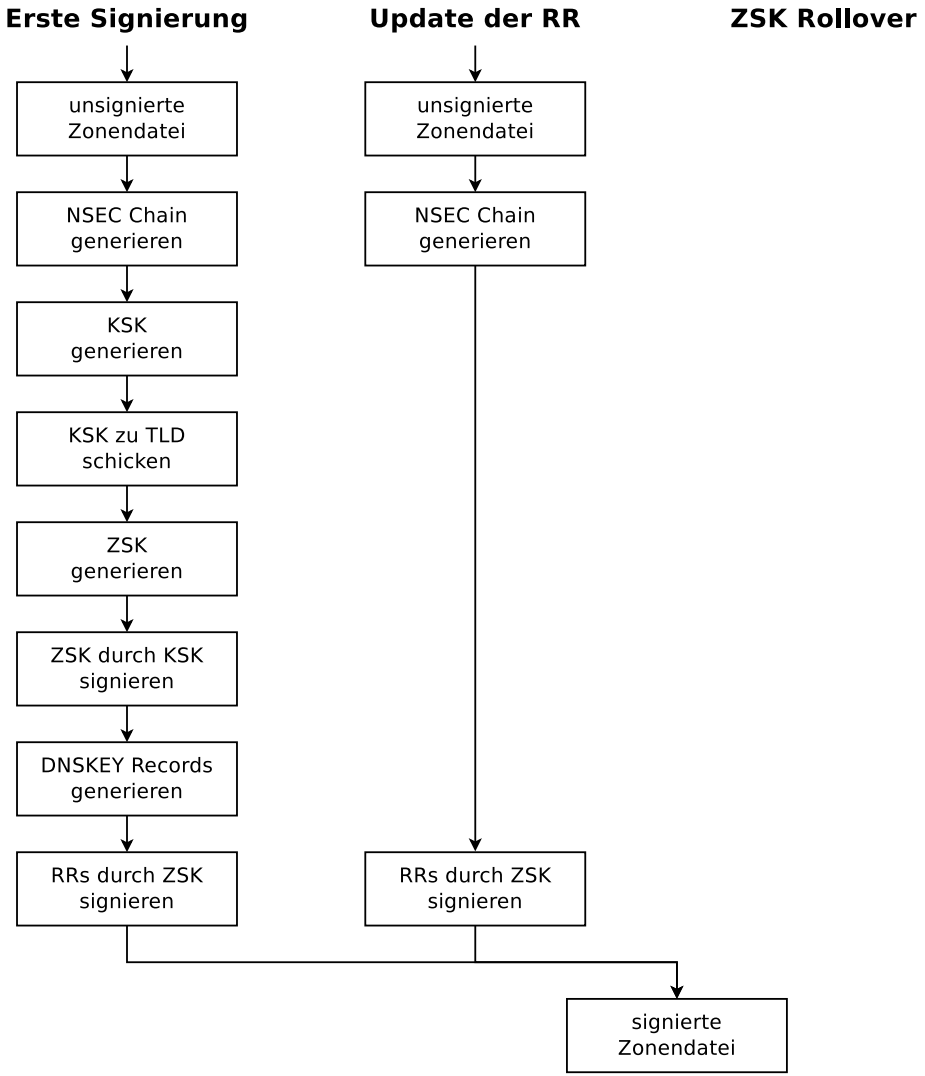
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
signierte Zonendatei

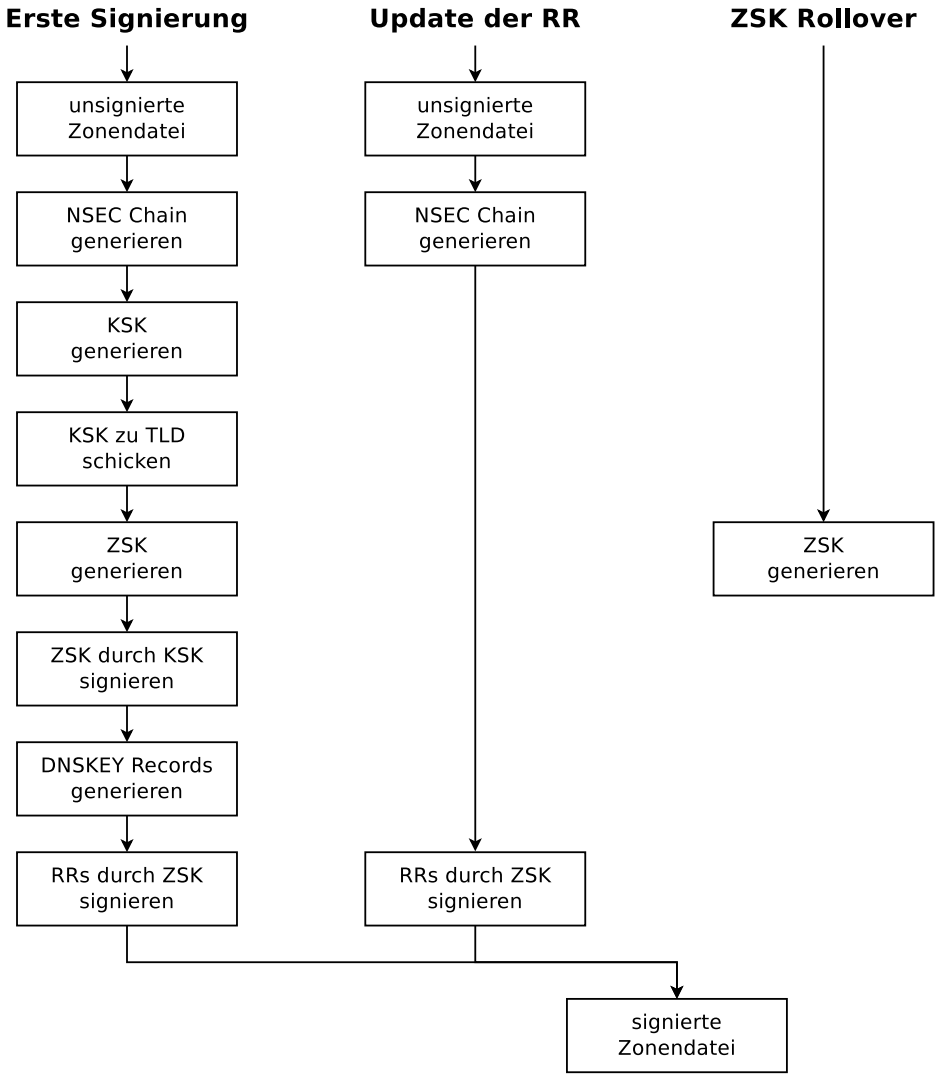
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
signierte Zonendatei

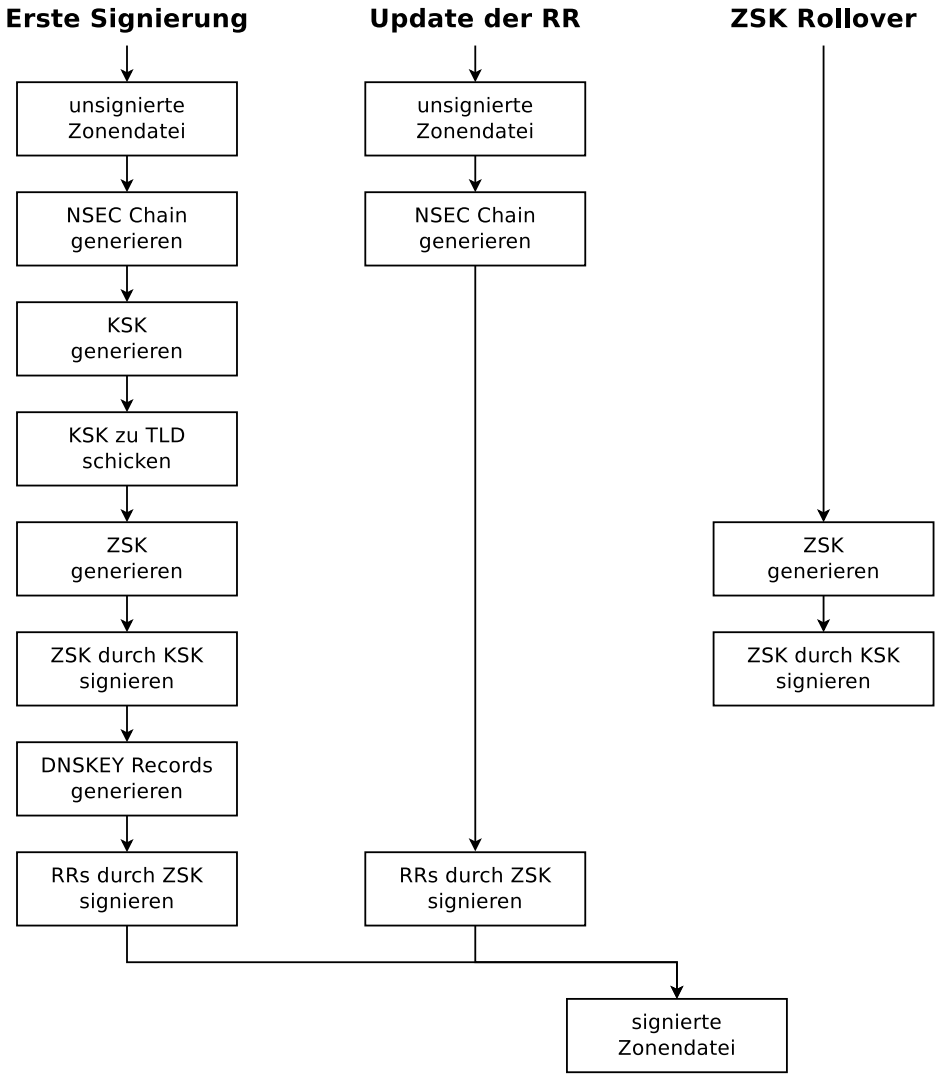
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
signierte Zonendatei

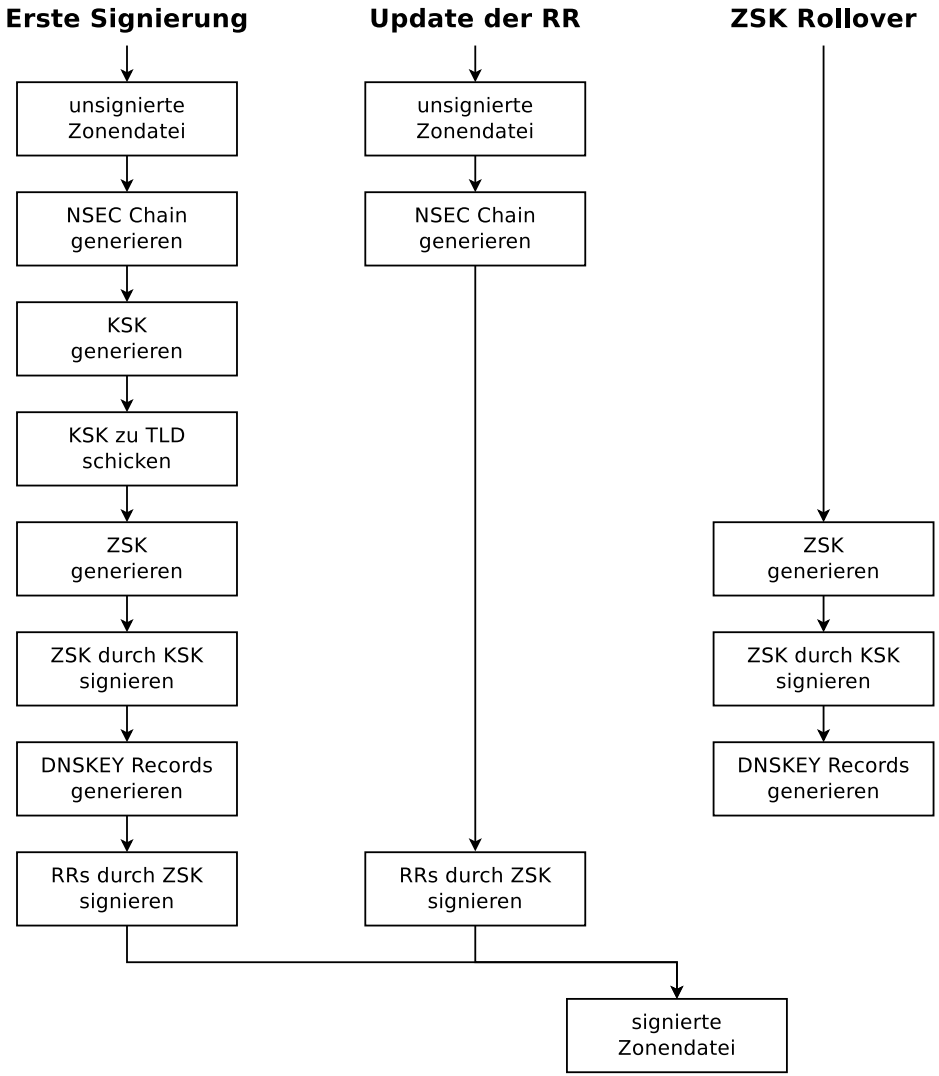
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
signierte Zonendatei

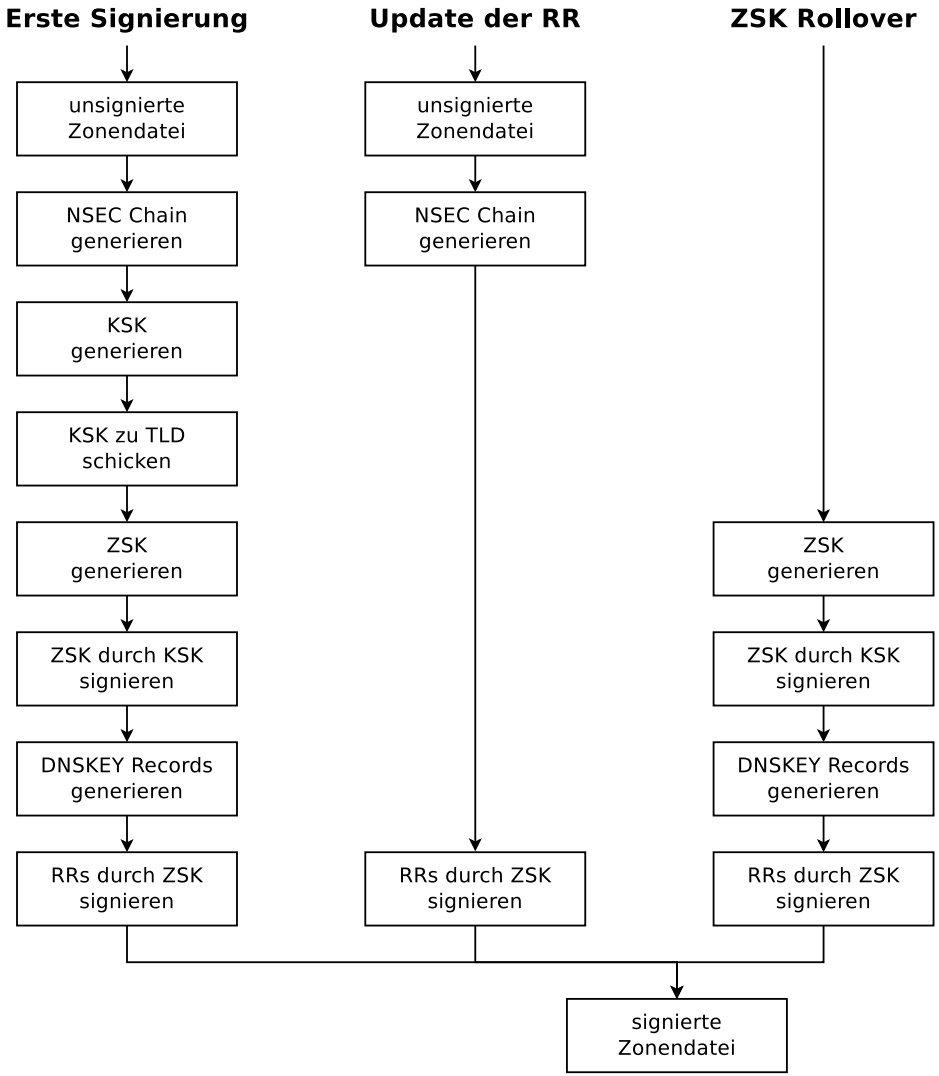
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
signierte Zonendatei

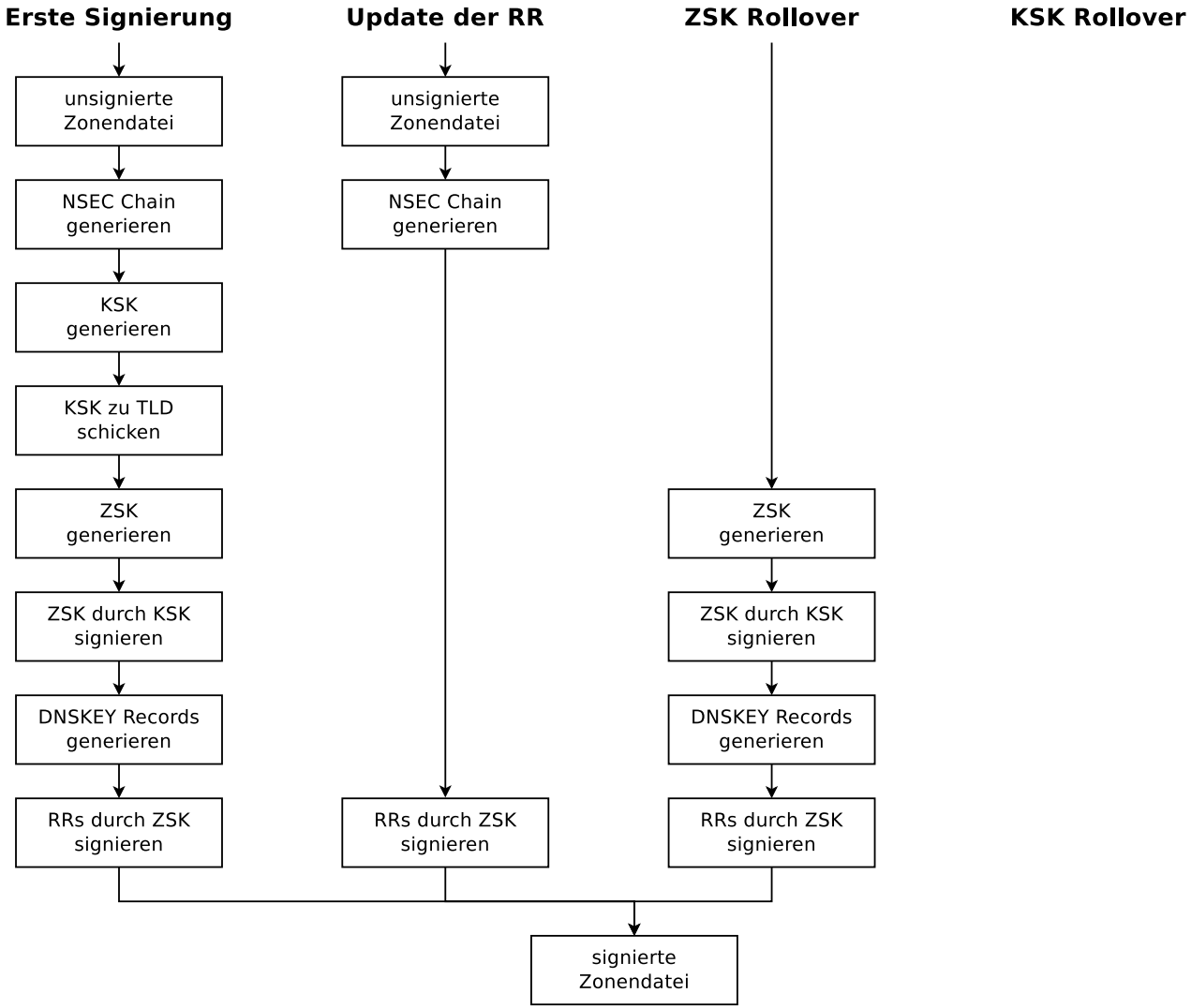
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
signierte Zonendatei

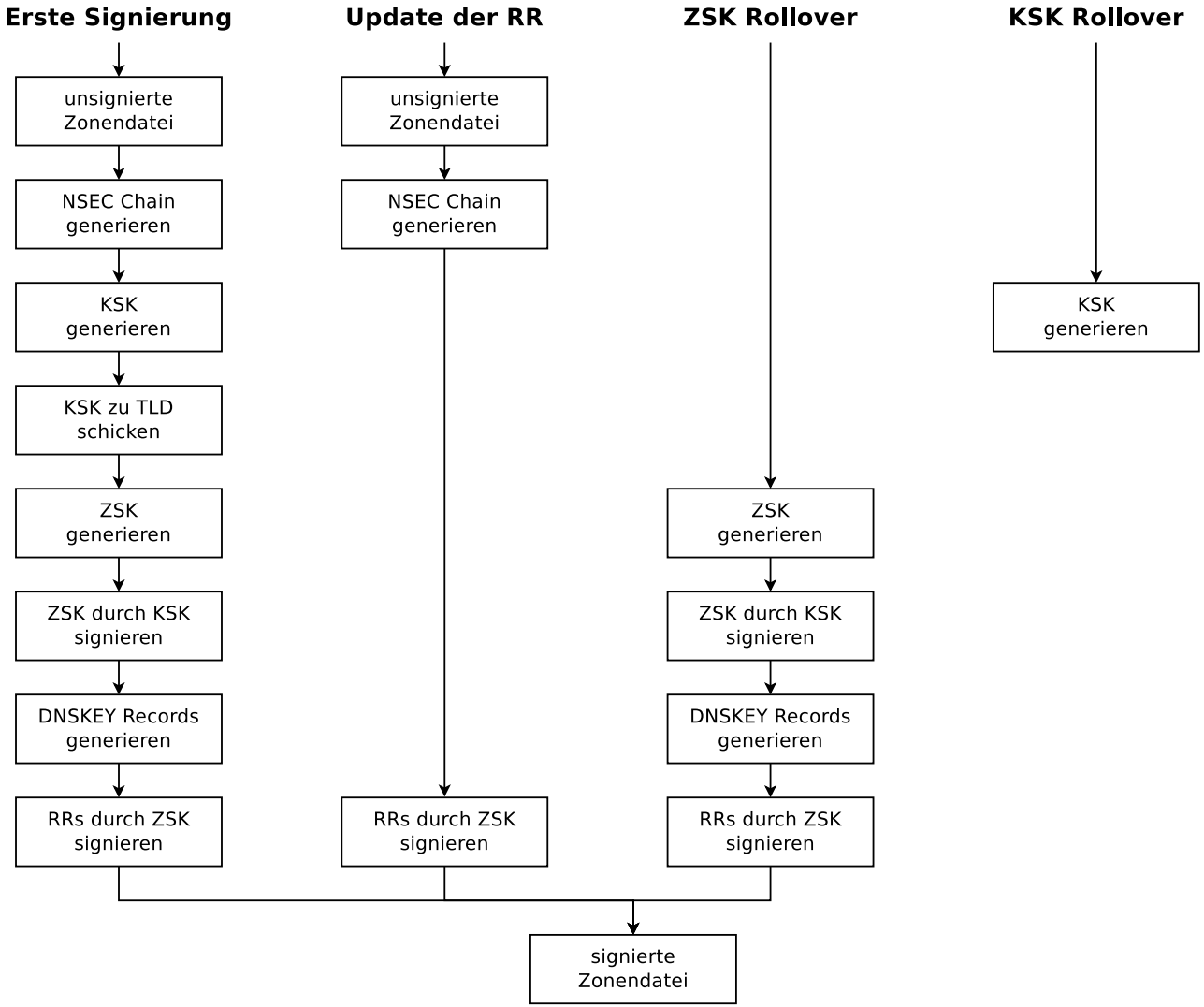
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
signierte Zonendatei

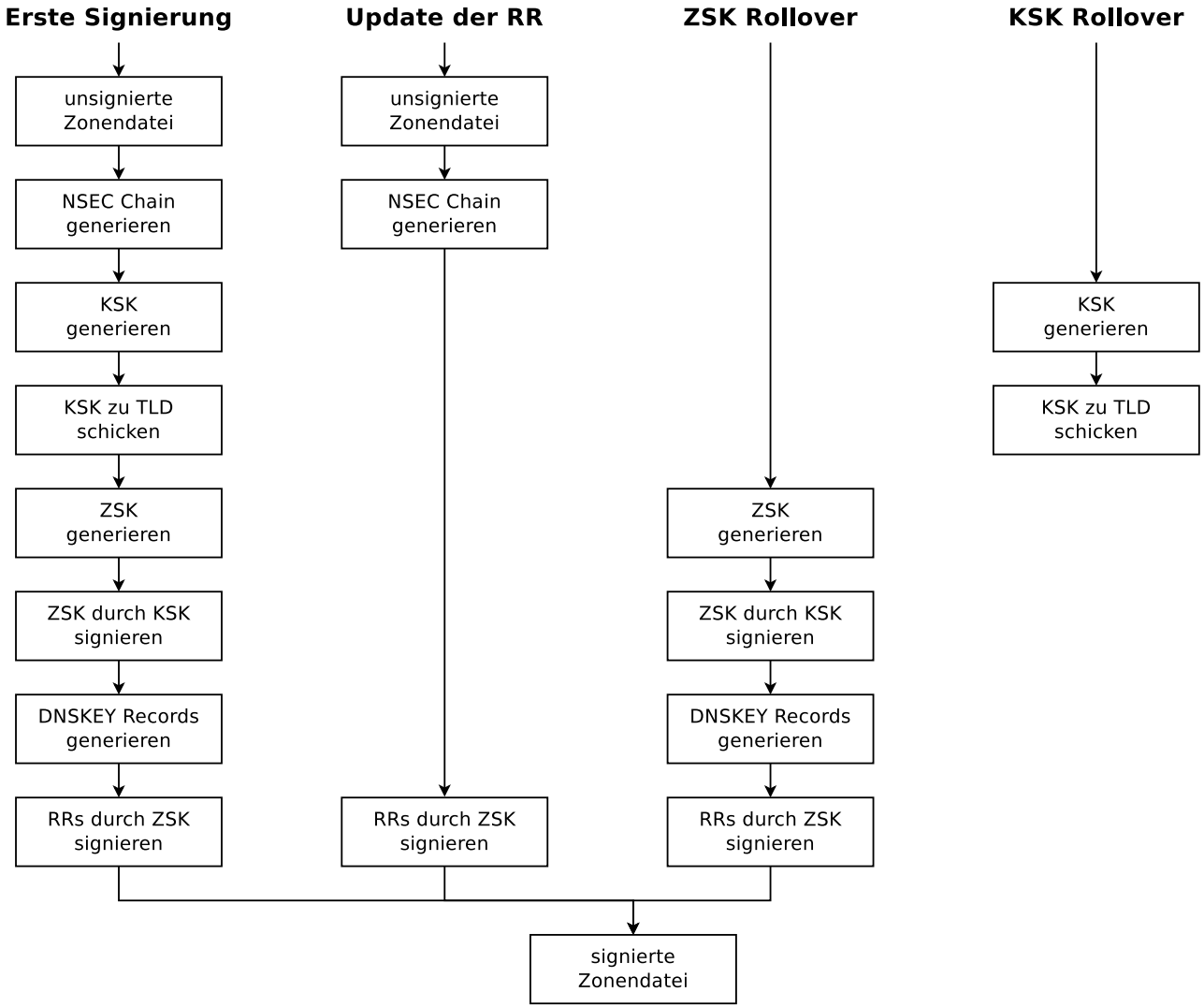
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
signierte Zonendatei

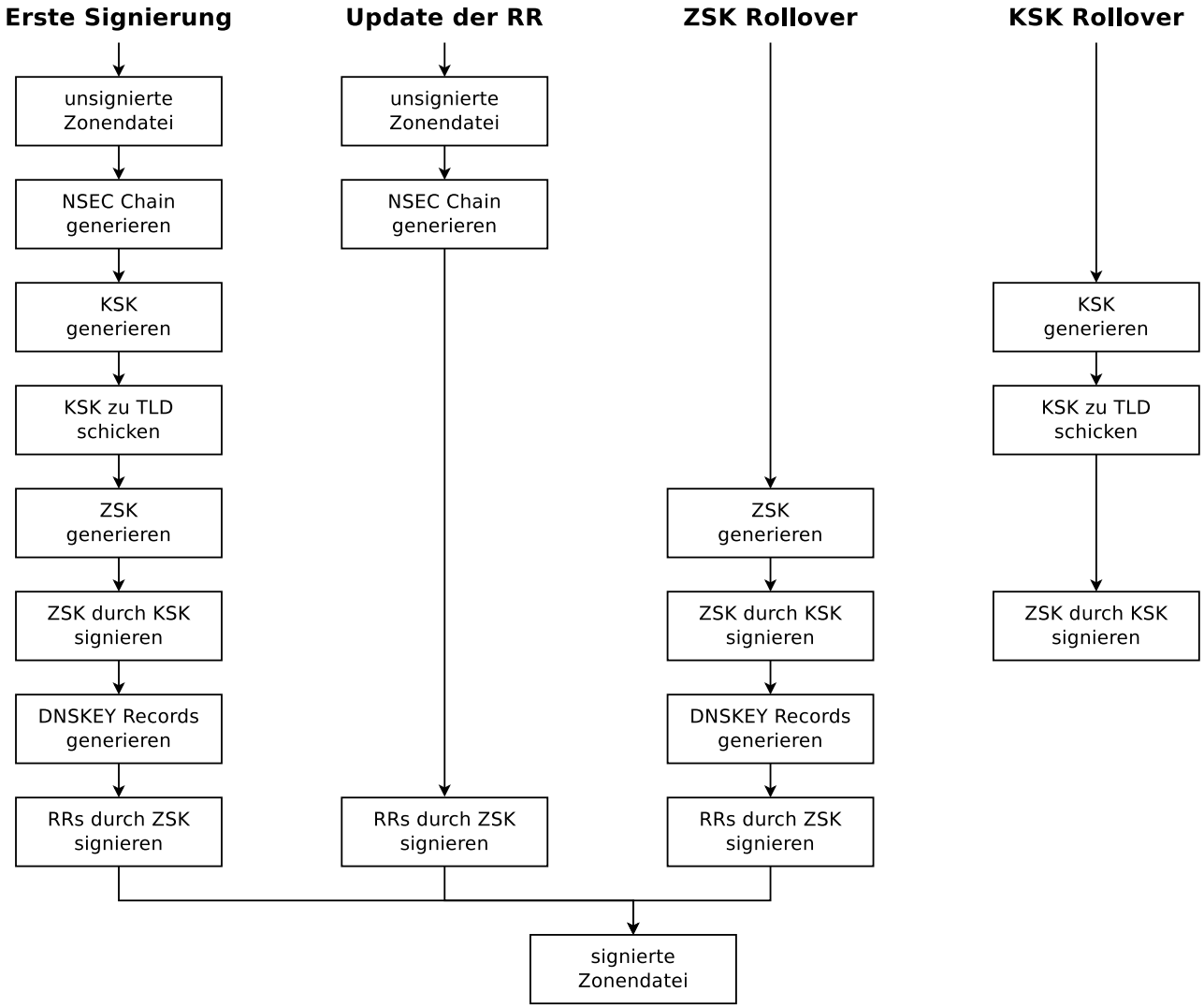
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
KSK generieren
signierte Zonendatei

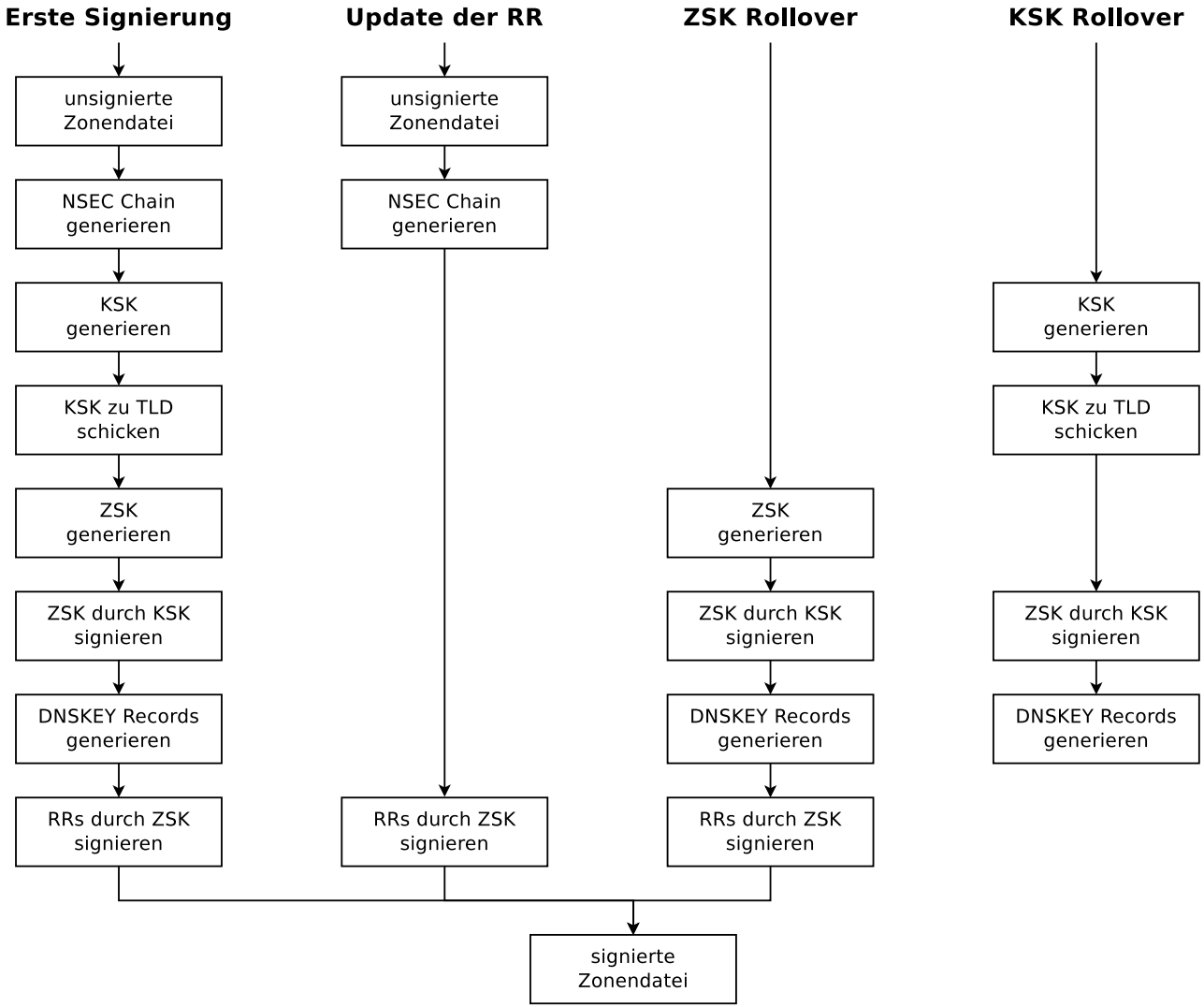
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
KSK generieren
KSK zu TLD schicken
signierte Zonendatei

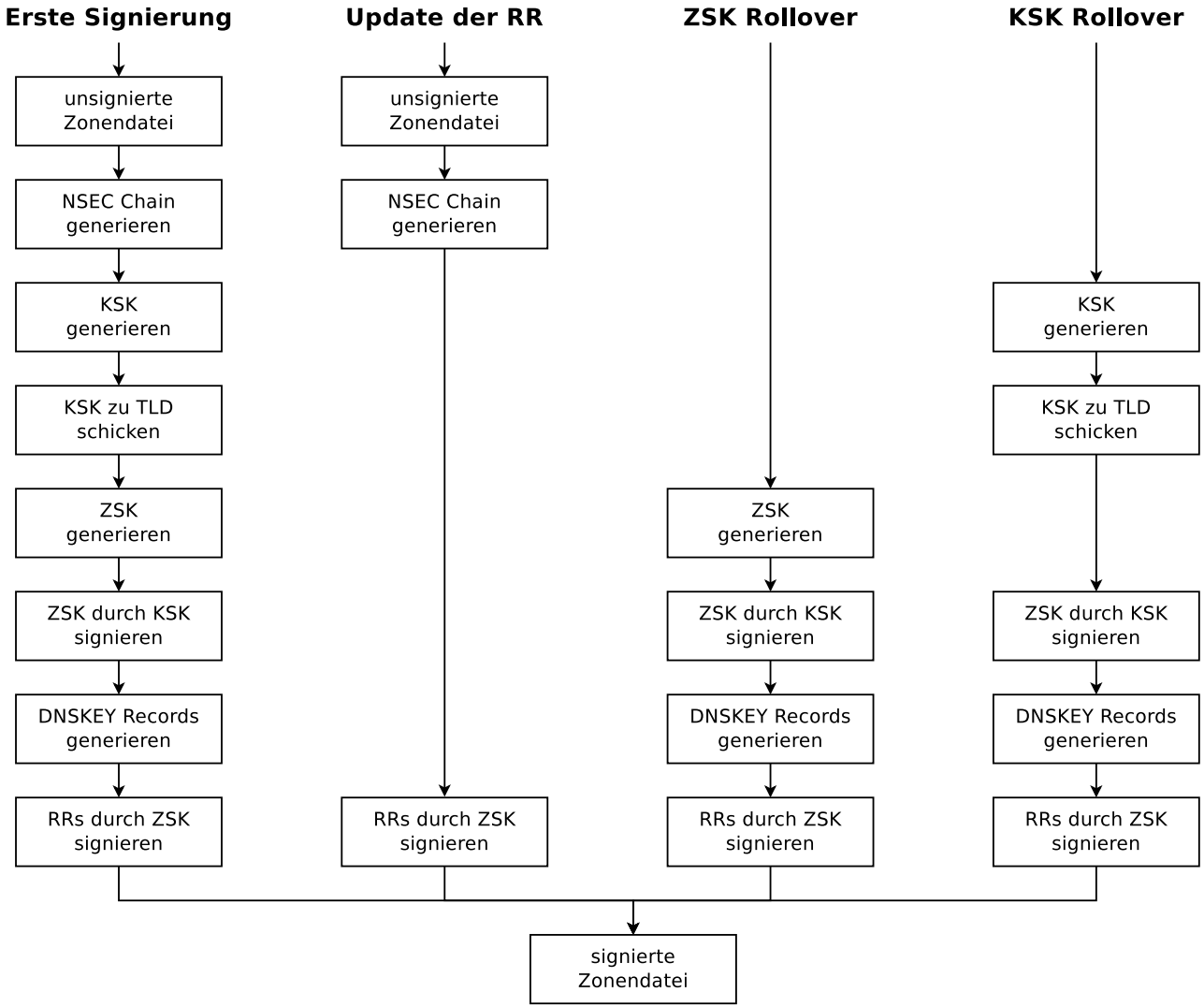
DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
KSK generieren
KSK zu TLD schicken
ZSK durch KSK signieren
signierte Zonendatei

DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
KSK generieren
KSK zu TLD schicken
ZSK durch KSK signieren
DNSKEY Records generieren
signierte Zonendatei

DNSSECify


Erste Signierung
unsignierte Zonendatei
NSEC Chain generieren
KSK generieren
KSK zu TLD schicken
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
Update der RR
unsignierte Zonendatei
NSEC Chain generieren
RRs durch ZSK signieren
ZSK Rollover
ZSK generieren
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
KSK Rollover
KSK generieren
KSK zu TLD schicken
ZSK durch KSK signieren
DNSKEY Records generieren
RRs durch ZSK signieren
signierte Zonendatei

Transfers

DNS $\rightarrow$ DNS

DNS $\rightarrow$ DNSSEC

DNSSEC $\rightarrow$ DNS

DNSSEC $\rightarrow$ DNSSEC

Transfers

DNS $\rightarrow$ DNS wie bisher

DNS $\rightarrow$ DNSSEC

DNSSEC $\rightarrow$ DNS

DNSSEC $\rightarrow$ DNSSEC

Transfers

DNS $\rightarrow$ DNS wie bisher

DNS $\rightarrow$ DNSSEC umziehen, dann signieren

DNSSEC $\rightarrow$ DNS

DNSSEC $\rightarrow$ DNSSEC

Transfers

DNS $\rightarrow$ DNS wie bisher

DNS $\rightarrow$ DNSSEC umziehen, dann signieren

DNSSEC $\rightarrow$ DNS Spezialfall 1

DNSSEC $\rightarrow$ DNSSEC

Transfers

DNS → DNS wie bisher

DNS → DNSSEC umziehen, dann signieren

DNSSEC → DNS Spezialfall 1

DNSSEC → DNSSEC Spezialfall 2

Transfers: DNSSEC → DNS

- neuer NS in TLD

Transfers: DNSSEC → DNS

- neuer NS in TLD
- alten NS und DS aus TLD entfernen

Transfers: DNSSEC → DNS

- neuer NS in TLD
- alten NS und DS aus TLD entfernen
- alte RRSIGs, DNSKEYs müssen weiterhin ausgeliefert werden

Transfers: DNSSEC → DNS

- neuer NS in TLD
- alten NS und DS aus TLD entfernen
- alte RRSIGs, DNSKEYs müssen weiterhin ausgeliefert werden
- alte DNSSEC records in allen Caches verloschen: Zone nur mehr als DNS ausliefern

Transfers: DNSSEC → DNS

- neuer NS in TLD
- alten NS und DS aus TLD entfernen
- alte RRSIGs, DNSKEYs müssen weiterhin ausgeliefert werden
- alte DNSSEC records in allen Caches verloschen: Zone nur mehr als DNS ausliefern
- Problem: Zone benötigt Resign, wenn Caches noch nicht verloschen

Transfers: DNSSEC → DNS

- neuer NS in TLD
- alten NS und DS aus TLD entfernen
- alte RRSIGs, DNSKEYs müssen weiterhin ausgeliefert werden
- alte DNSSEC records in allen Caches verloschen: Zone nur mehr als DNS ausliefern
- Problem: Zone benötigt Resign, wenn Caches noch nicht verloschen
- Alter Registrar müsste Resign machen

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD
- alten NS und DS aus TLD entfernen

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD
- alten NS und DS aus TLD entfernen
- alte und neue RRSIGs, DNSKEYs müssen ausgeliefert werden

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD
- alten NS und DS aus TLD entfernen
- alte und neue RRSIGs, DNSKEYs müssen ausgeliefert werden
- alte DNSSEC Records in allen Caches verloschen: nur mehr neue DNSSEC Records ausliefern

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD
- alten NS und DS aus TLD entfernen
- alte und neue RRSIGs, DNSKEYs müssen ausgeliefert werden
- alte DNSSEC Records in allen Caches verloschen: nur mehr neue DNSSEC Records ausliefern
- Problem: Zone benötigt Resign, wenn Caches noch nicht verloschen

Transfers: DNSSEC → DNSSEC

- neuer Registrar signiert Zone
- neuer NS und neuer DS in TLD
- alten NS und DS aus TLD entfernen
- alte und neue RRSIGs, DNSKEYs müssen ausgeliefert werden
- alte DNSSEC Records in allen Caches verloschen: nur mehr neue DNSSEC Records ausliefern
- Problem: Zone benötigt Resign, wenn Caches noch nicht verloschen
- Alter Registrar müsste Resign machen

Status

- Rootzone signiert seit 15. Juli 2010

Status

- Rootzone signiert seit 15. Juli 2010
- 249 TLDs insgesamt

Status

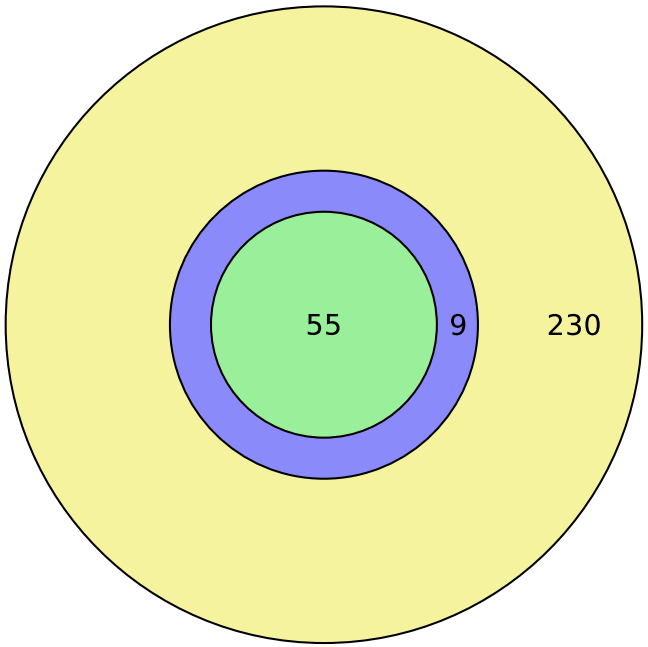
- Rootzone signiert seit 15. Juli 2010
- 249 TLDs insgesamt
- 64 signiert

Status

- Rootzone signiert seit 15. Juli 2010
- 249 TLDs insgesamt
- 64 signiert
  - 9 signiert, aber kein DS in ROOT

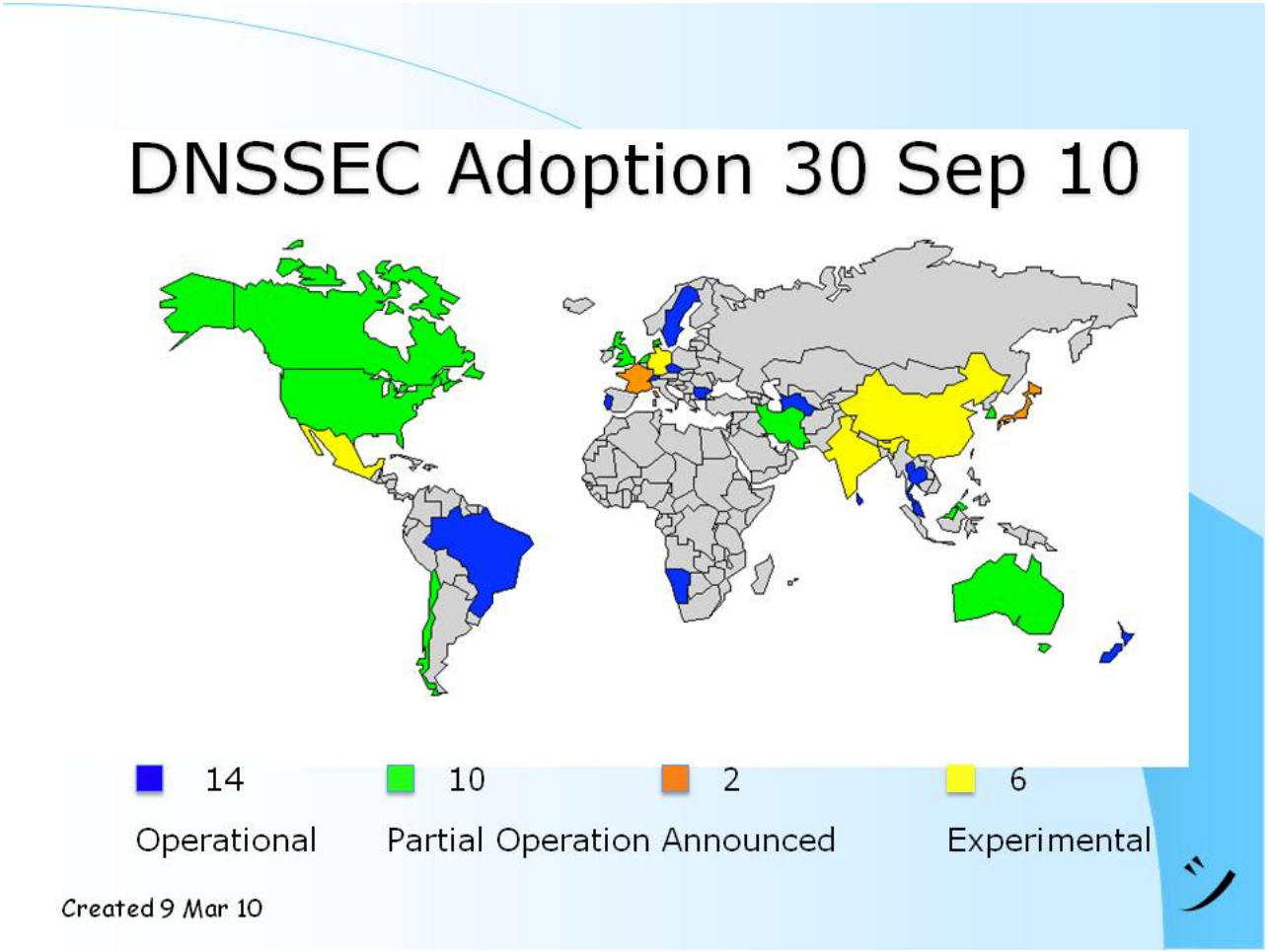
Status

- Rootzone signiert seit 15. Juli 2010
- 249 TLDs insgesamt
- 64 signiert
  - 9 signiert, aber kein DS in ROOT
  - 55 signiert mit DS in ROOT



[http://stats.research.icann.org]

Status



[http://www.dnssec-deployment.org]

Bedeutung für Registrare

- jede Domain ist eigene Zone

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat
- jede Zone muss monatlich signiert werden

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat
- jede Zone muss monatlich signiert werden
- eine Million Domains theoretisch folgender Aufwand:

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat
- jede Zone muss monatlich signiert werden
- eine Million Domains theoretisch folgender Aufwand:
  - 4 Millionen Schlüssel

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat
- jede Zone muss monatlich signiert werden
- eine Million Domains theoretisch folgender Aufwand:
  - 4 Millionen Schlüssel
  - 23 Schlüssel generieren pro Minute

Bedeutung für Registrare

- jede Domain ist eigene Zone
- jede Zone 2-4 Schlüssel
- mindestens ein neuer Schlüssel pro Zone pro Monat
- jede Zone muss monatlich signiert werden
- eine Million Domains theoretisch folgender Aufwand:
  - 4 Millionen Schlüssel
  - 23 Schlüssel generieren pro Minute
  - 23 Zonen signieren pro Minute

Überblick

- Schutz der Records durch digitale Signatur

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)
- Schlüsselhierachie (KSK $\rightarrow$ ZSK)

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)
- Schlüsselhierachie (KSK $\rightarrow$ ZSK)
- Key Rollover

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)
- Schlüsselhierachie (KSK $\rightarrow$ ZSK)
- Key Rollover
- Viele Schlüssel

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)
- Schlüsselhierachie (KSK $\rightarrow$ ZSK)
- Key Rollover
- Viele Schlüssel
- Nicht-Existenz-Beweiß

Überblick

- Schutz der Records durch digitale Signatur
- neue Records (DNSKEY, RRSIG, DS, NSEC)
- Schlüsselhierachie (KSK $\rightarrow$ ZSK)
- Key Rollover
- Viele Schlüssel
- Nicht-Existenz-Beweiß
- UDP $\rightarrow$ TCP

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten? Lösbar durch DNSSEC?
  - DDOS
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten? Lösbar durch DNSSEC?
  - DDOS - NEIN, Gefahr sogar erhöht
  - DNS-Amplification
  - DNS-Spoofing
  - DNS-Cache-Poisoning

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten? Lösbar durch DNSSEC?
  - DDOS - NEIN, Gefahr sogar erhöht
  - DNS-Amplification - NEIN, zur Zeit nicht lösbar
  - DNS-Spoofing
  - DNS-Cache-Poisoning

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten? Lösbar durch DNSSEC?
  - DDOS - NEIN, Gefahr sogar erhöht
  - DNS-Amplification - NEIN, zur Zeit nicht lösbar
  - DNS-Spoofing - JA, lösbar mit DNSSEC
  - DNS-Cache-Poisoning

Überblick

- Ist DNS sicher? - NEIN!
- Was passiert bei einem Angriff?
  - Ziel nicht erreichbar
  - Rechner außer Gefecht
  - Falsches Ziel wird erreicht
- Angriffsarten? Lösbar durch DNSSEC?
  - DDOS - NEIN, Gefahr sogar erhöht
  - DNS-Amplification - NEIN, zur Zeit nicht lösbar
  - DNS-Spoofing - JA, lösbar mit DNSSEC
  - DNS-Cache-Poisoning - JA, lösbar mit DNSSEC

Fragen ?