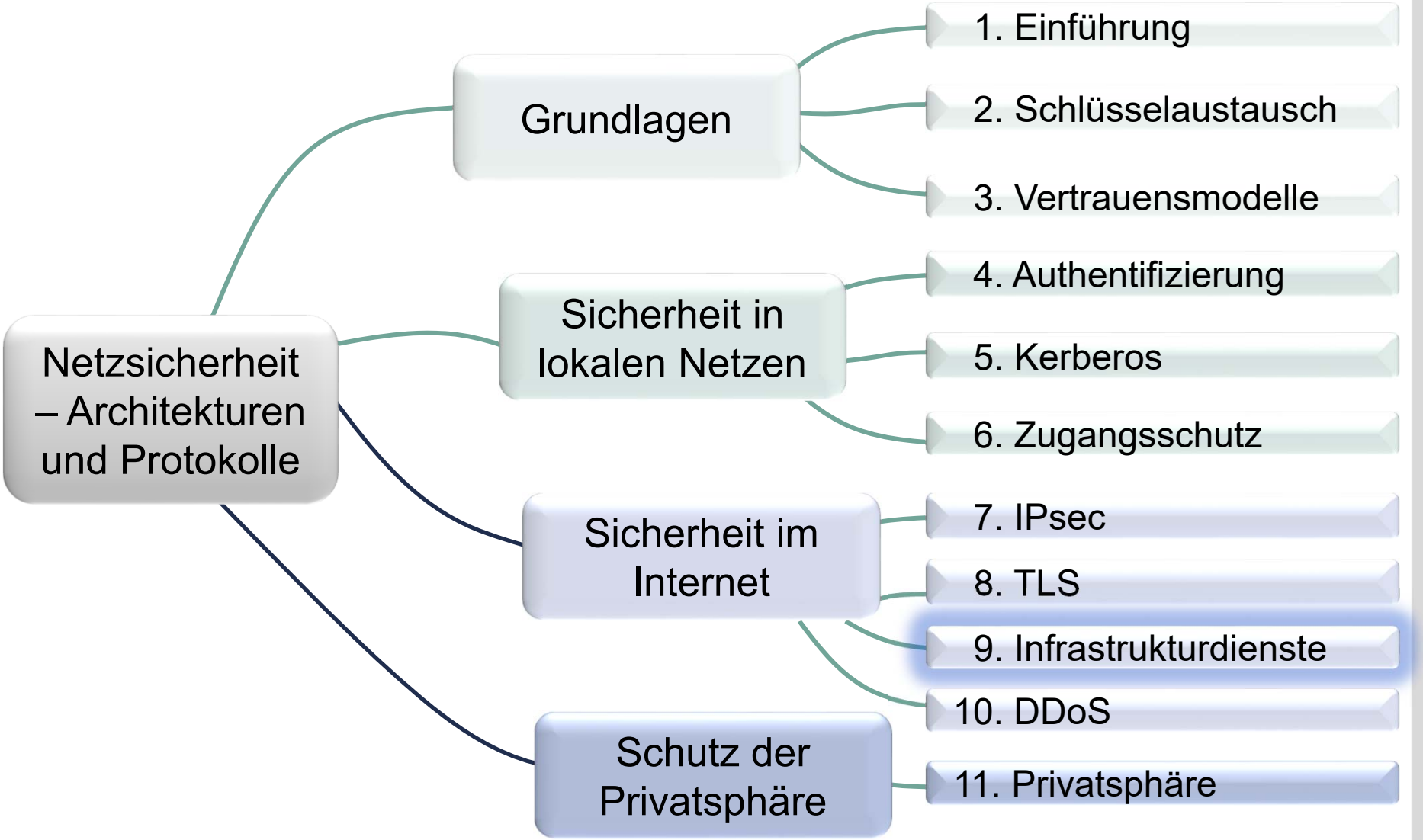
Vorlesung Netzsicherheit
Kapitel 9 – Infrastrukturdienste

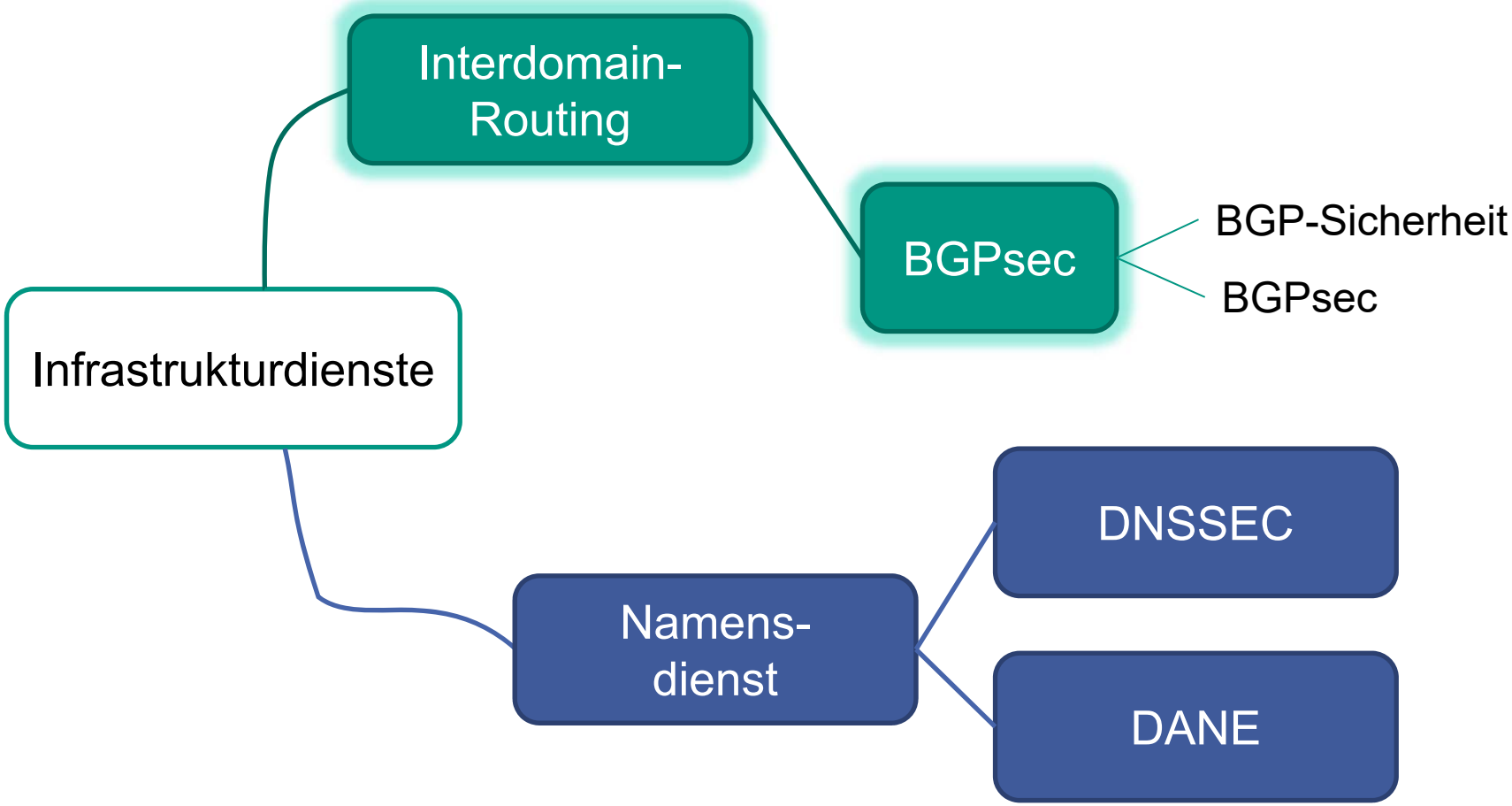
PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Institut für Telematik, Prof. Zitterbart

Inhalte der Vorlesung

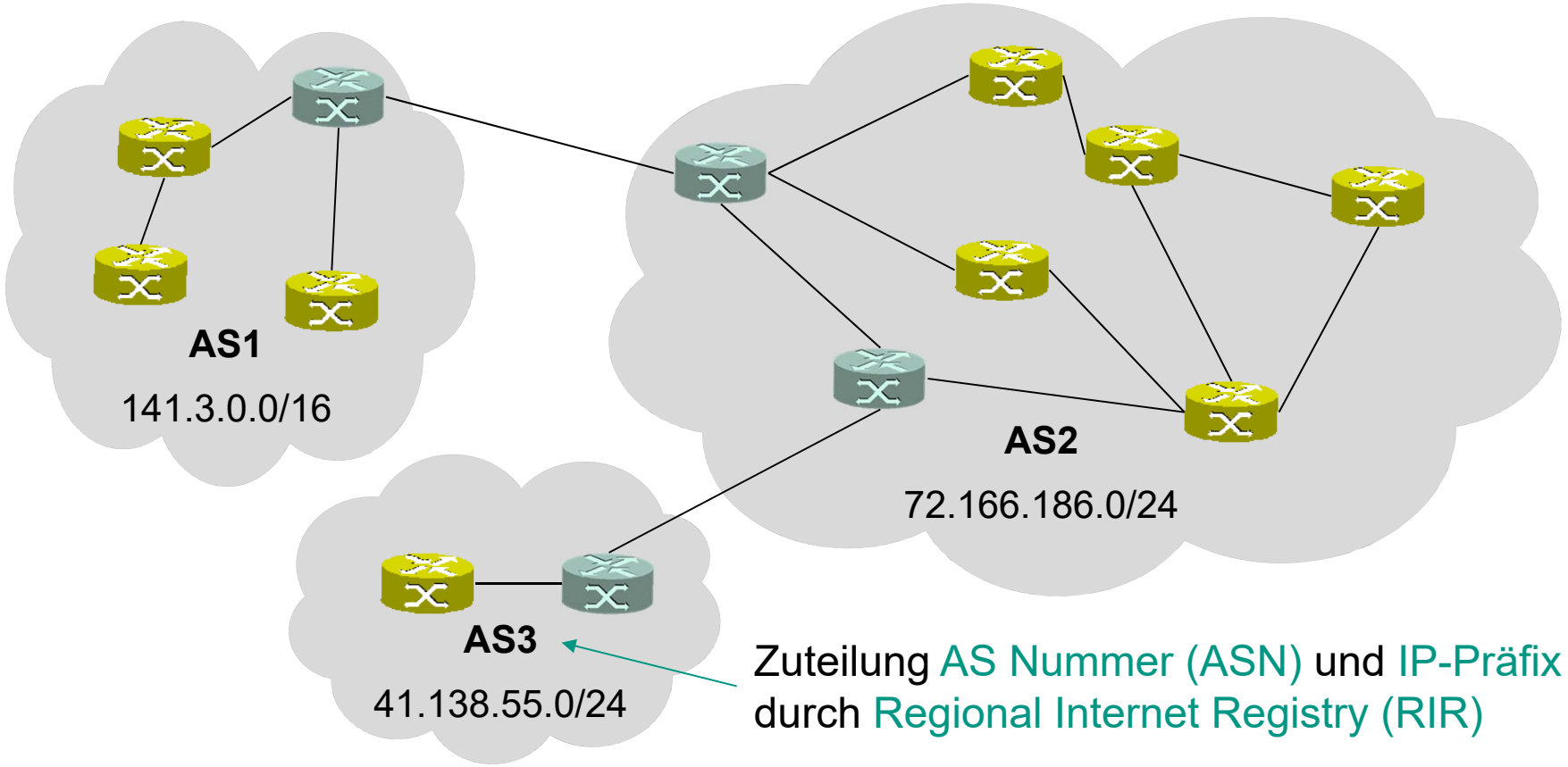


Überblick


Interdomain-
Routing
BGPsec
BGP-Sicherheit
BGPsec
Infrastrukturdienste
Namens-
dienst
DNSSEC
DANE

Internet: Netz von Netzen

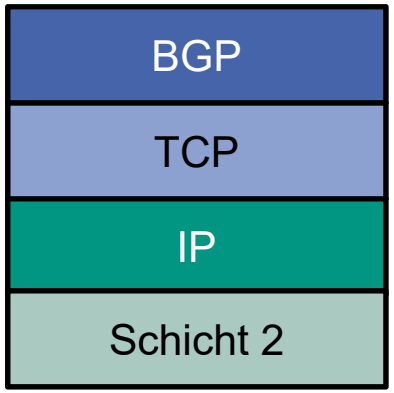
- Routing innerhalb eines autonomen Systems
  - Interior Gateway Protocol
- Routing zwischen autonomen Systemen
  - Exterior Gateway Protocol

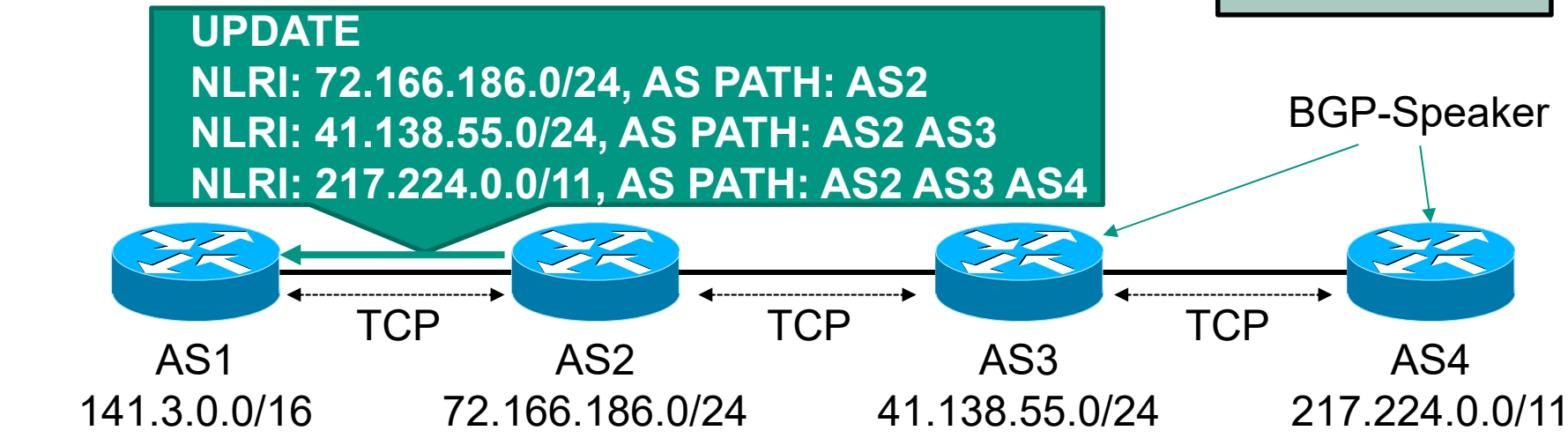


Zuteilung AS Nummer (ASN) und IP-Präfix durch Regional Internet Registry (RIR)

Border Gateway Protocol (BGP)

- Einzig eingesetztes Exterior Gateway Protocol (EGP)
- Etablierung einer BGP-Session über TCP
  - Darüber regelmäßiger Austausch von Routinginformationen
  - IP-Adressbereiche (Präfixe) und AS-Pfad
  - UPDATE-Nachrichten





[RFC4271]

NLRI: Network Layer Reachability Infomation

BGP-Angriffsziele

- Unautorisierte Bekanntgabe von Präfixen
  - Abhören, Manipulieren oder Unterdrücken von Datenverkehr
  - DoS-Angriff
- Fälschen von AS-PATH-Angaben
  - Künstliches Verbessern oder Verschlechtern von Routen (hat ggf. Auswirkung auf Kosten)
  - DoS-Angriff
- Angriffe auf BGP-/TCP-Session
  - Manipulation der Routen
  - DoS-Angriff

Mehr Details in: [RFC7132]

YouTube-Ausfall

- Am 24. Februar 2008 beschließt die pakistanische Regierung die landesweite Sperrung von YouTube
  - Pakistan Telecom (AS 17557) gibt über BGP das Präfix 208.65.153.0/24 bekannt, welches eigentlich YouTube gehört
  - Dies verbreitet sich innerhalb weniger Minuten weltweit
    - Die Folge: YouTube-Aufrufe werden direkt nach Pakistan geleitet
      → YouTube ist nicht mehr erreichbar
  - YouTube gibt nach ca. 90 Minuten die zwei Präfixe 208.65.153.0/25 und 208.65.153.128/25 bekannt
    - Aufgrund des Longest Matching Prefix werden wieder die korrekten Routen benutzt
  - Die fehlerhaften Routen werden außerdem künstlich verschlechtert bis sie nach ca.140 Minuten komplett zurückgezogen werden

http://www.ripe.net/news/study-youtube-hijacking.html

MitM Hijacking

- Angreifer leitet Verkehr zu seinem „Opfer“ über sich um
  - Einfach durch Bekanntgabe der Präfixe des Opfers
  - Ziel: Abhören, Manipulieren oder Unterdrücken von Datenverkehr
  - Erstmalig beschrieben von Kapela
    - „Stealing The Internet“ im Jahr 2008
- Renesys beobachte 2013 über 1.500 MitM-Angriffe auf unterschiedliche Präfixe
- Problem
  - Solche Angriffe sind schwer zu erkennen
  - Wie soll man entscheiden, ob Hops auf dem Übertragungspfad legitime Knoten sind oder zu einem MitM-Angriff gehören?

… umgeleiteter Verkehr

- Datenverkehr von einem AS in Denver zu einem AS in Denver wird über ein isländisches AS umgeleitet

MitM Hijacking

- Präfixe von ASen lassen sich durch Bekanntgabe hijacken
  - Es existieren keine überprüfbaren Abbildungen zwischen ASN und IP-Präfixen
  - Fehlende Vertrauenskette bei der Vergabe von Präfixen
- Bisherige Gegenmaßnahmen
  - Alarmsysteme, welche die globalen Routing-Informationen überwachen und fehlerhafte Bekanntgaben von eigenen Präfixen melden
  - Filtern der eingehenden Routen von anderen ASen (aufwändige manuelle Konfiguration)
- Solange nicht *alle* ASe die Routen ihrer Kunden filtern, besteht das Problem weiter!
  - Schwächstes Glied genügt einem Angreifer

BGP-Schutzziele

- Schutz in der Kontrollebene
  - AS-Autorisierung für Bekanntgabe eines Präfixes (Route Origination Authorization)
    - Auch im Auftrag eines anderen ASes
    - z.B. bei Transit-Datenverkehr
  - Authentizität der Routinginformationen (Path Security)
    - ASN, Präfix und Pfadinformationen in BGP-UPDATE-Nachrichten
- Schutz auf dem Transportweg einer BGP-Session
  - Vertraulichkeit und Integrität der übertragenen Nachrichten
  - Schutz der TCP-Session (z.B. durch TCP-AO oder IPsec)

Mechanismen zum Schutz für BGP

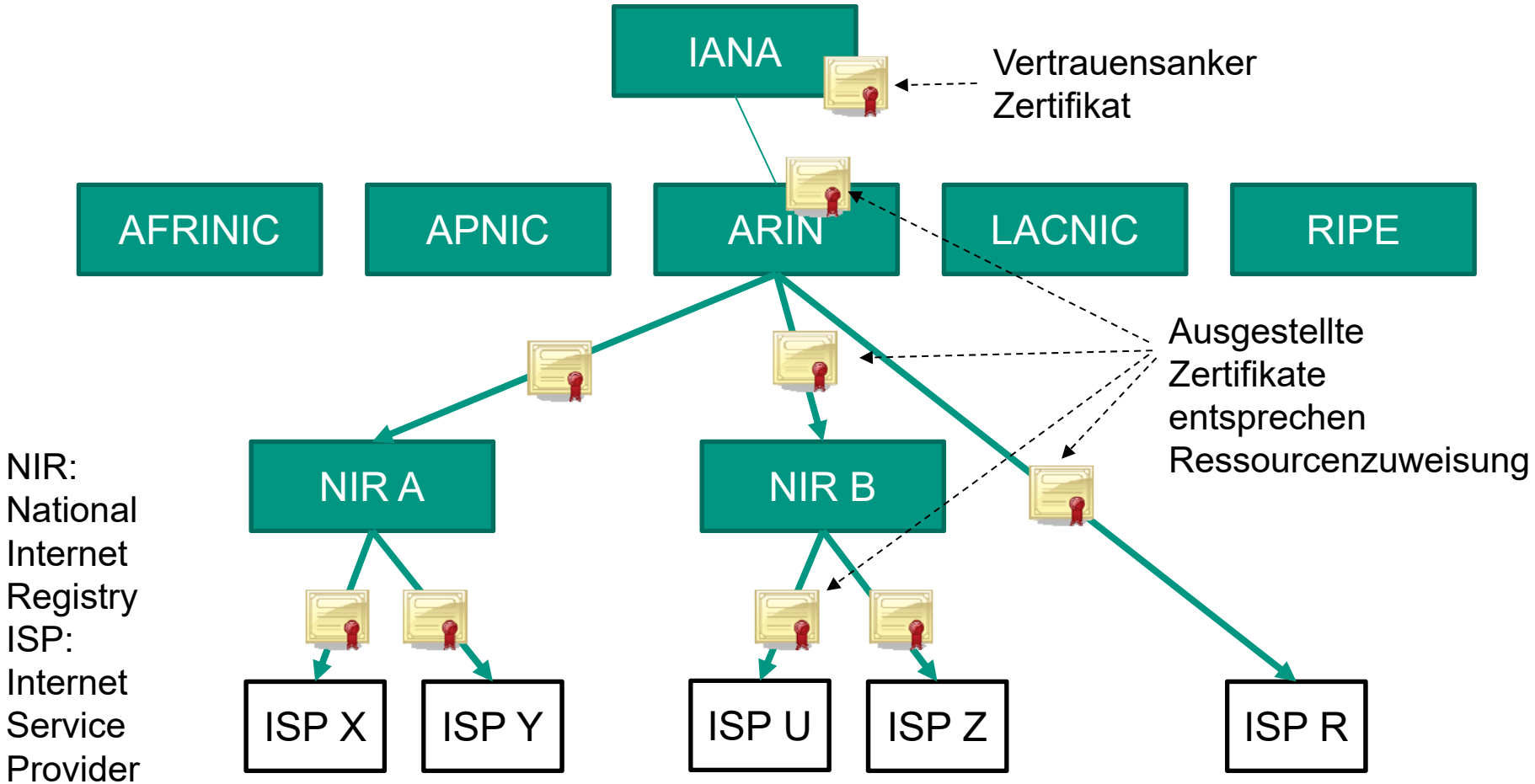
- Vielzahl an Entwicklungen für sichere Routing-Protokolle
- Aber
  - Umsetzung in der Praxis sehr aufwändig
  - Abwärtskompatibilität nicht immer gegeben
  - Hohe zusätzliche Last auf den Routern
- Beispiel BGPSec
  - Resource Public Key Infrastructure (RPKI) mit Zertifikaten zur Autorisierung (nicht Authentifizierung!)
  - Digitale Signatur von Routing-Objekten (Route Origination Authorization und Sicherheit AS-Pfad)
    - Von IP-Adressen, AS-Nummer, AS-Identität, BGP-Router-Identität, Abbildung zwischen AS und Router, Pfadinformationen
    - Vertrauensanker bis zur IANA
  - Zusätzliches BGP-Attribut zum Transport von Signaturen

[RFC6480]

Resource Public Key Infrastructure (RPKI)

- Ressourcen: IP-Adressraum + AS-Nummern

[RFC6480]



NIR: National Internet Registry
ISP: Internet Service Provider

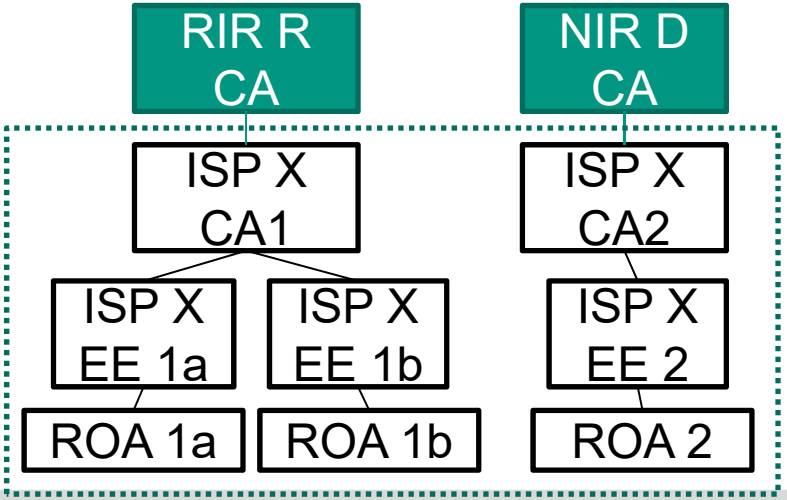
RPKI Organisation

- Verteiltes System zur Ablage und Verteilung der RPKI-Information (u.a. Zertifikate, signierte Objekte)
- Repository Publication Points
  - Verzeichnis mit Dateien (Manifest, Zertifikate, CRL, signierte Objekte)
  - per URL auffindbar (X.509 Subject Information Access Erweiterung)
  - Manifest enthält für alle Objekte im Repository: Liste der Objekt-Namen und Hashwerte der Objektinhalte, sowie Signatur
- erfordert Zugriffskontrolle
  - sonst unautorisiertes Löschen etc. möglich
- lose synchronisiert, kein Push-Mechanismus vorhanden
  - Unproblematisch, denn Zeitanforderungen sind gering


[RFC6481]

RPKI Bestandteile

- Ressourcen-Zertifikate
  - X.509-Zertifikate, die Berechtigungen für Ressourcen (=IP-Adressraum und ASNs) attestieren
  - CA-Zertifikate: ermöglichen das Ausstellen von EE-Zertifikaten und CA-Zertifikaten für weitere Unterzuordnungen (Sub-Delegation)
  - EE-Zertifikate (End-Entity)
    - dient zur Signatur der Ressourcen-Objekte, z.B. ROAs
    - eigener privater Schlüssel je EE-Zertifikat
    - ermöglicht Widerruf von Ressourcen-Objekten durch CRL für EE-Zertifikate
- Beispiel:
  ISP X hat zugeordnete Ressourcen von RIR R und NIR D

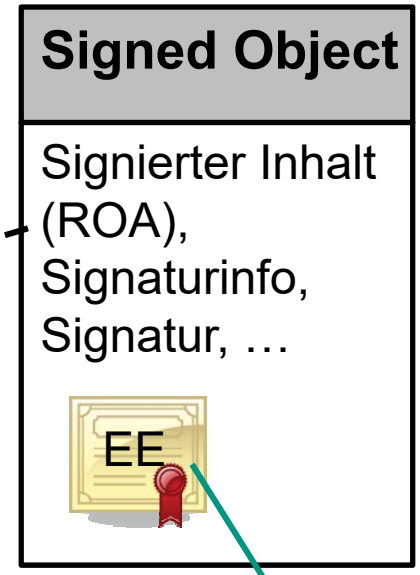


[RFC6480]

RPKI – Signiertes Objekt

- Mittels Cryptographic Message Syntax kodiert [RFC3369]
- Enthält zu signierende Daten, z.B. ROA, Signatur, sowie EE-Zertifikat
- Beispiel für Route Origination Authorization (ROA) Inhalt:

```
Origin ASN:       AS28001
Not valid Before: 2017-04-28 07:52:21
Not valid After:  2022-04-28 07:52:21
Trust Anchor:     repository.lacnic.net
Prefixes:    200.3.12.0/22 (max length /24)
             200.10.60.0/23 (max length /24)
             2001:13c7:7002::/48 (max length /48)
             2001:13c7:7010::/46 (max length /47)
             200.7.86.0/24 (max length /24)
             2001:13c7:7012::/47 (max length /47)
```



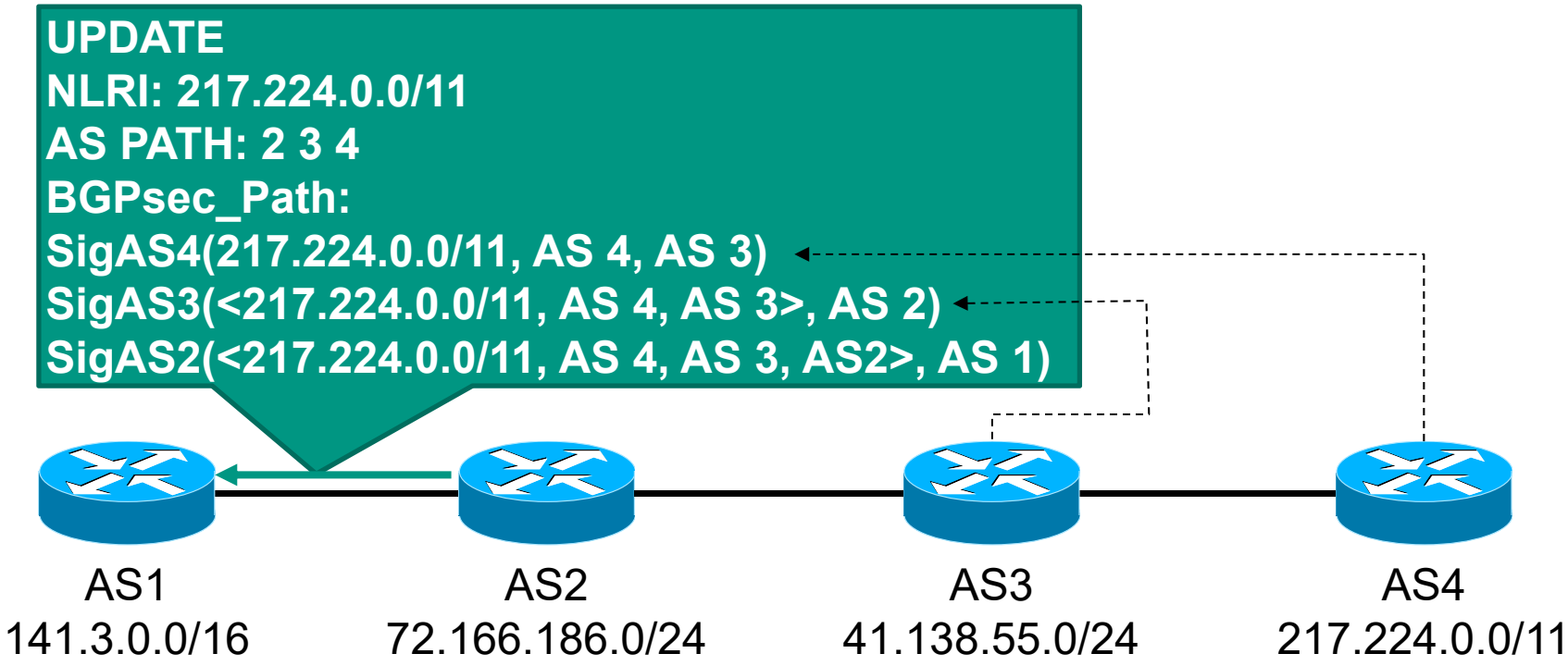
[RFC6488]

BGPsec

- Integritätsschutz der Pfadinformation entlang des gesamten Wegs notwendig
  - „Partial Path Signing“ nicht sinnvoll → erlaubt weitreichende Angriffe
  - Erfordert striktes Modell bei Umsetzung
  - BGPsec-Einsatz wird bei Etablierung der BGP-Session ausgehandelt (je Richtung und Protokoll-Familie IPv4/IPv6)
- Jeder BGP Speaker erhält BGP Router Certificate
  - Verbindet ASN mit Public Key
  - Mehrere BGP Speaker nutzen den gleichen privaten Schlüssel
  - BGP Speaker signiert UPDATE-Nachrichten für sein AS

BGPsec

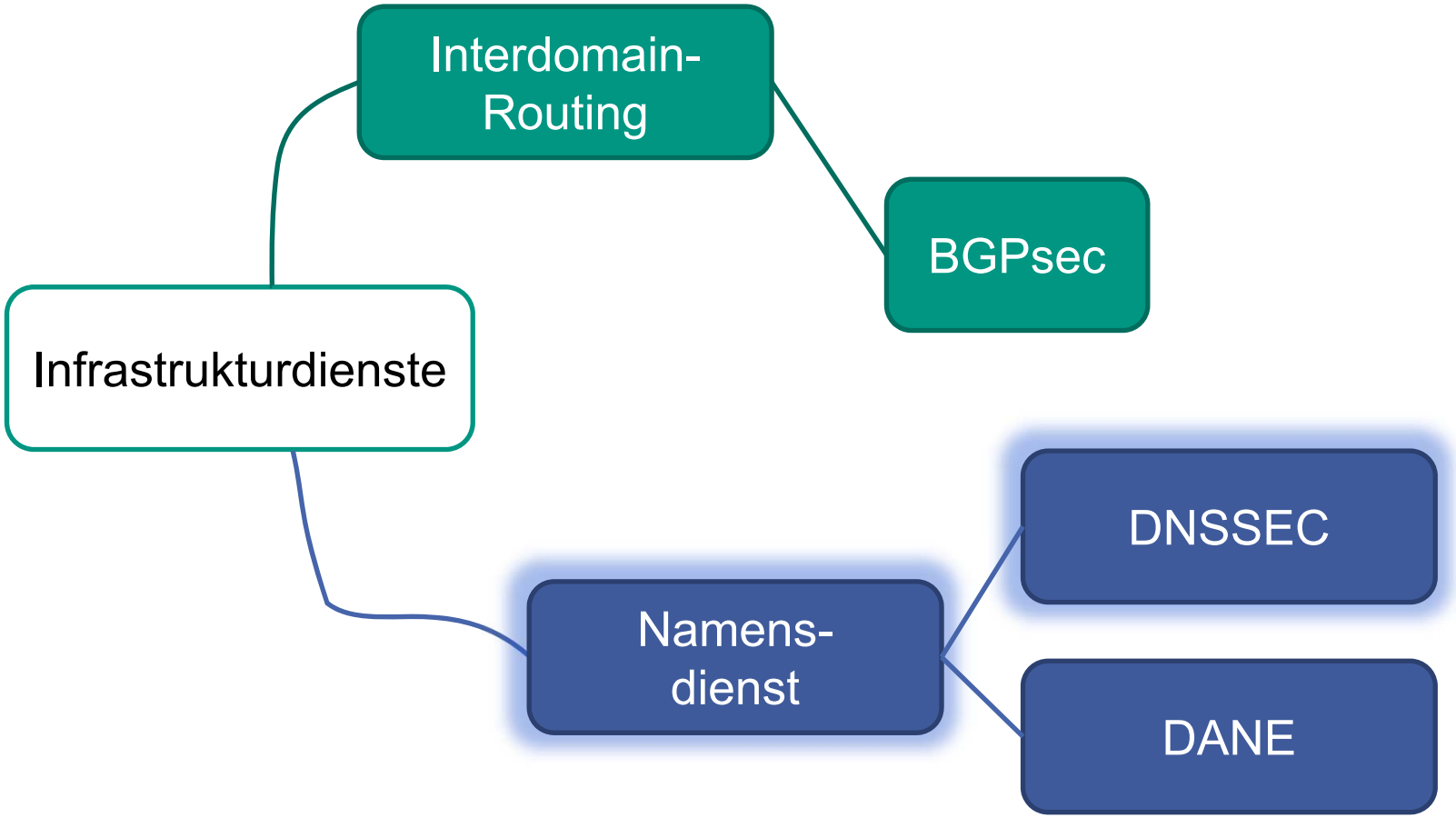
- Jedes AS signiert erhaltene Pfadinformation und die Weitergabe an das nächste AS („forward signing“)
- Zusätzlich: ROA-Überprüfung



Zusammenfassung BGPsec

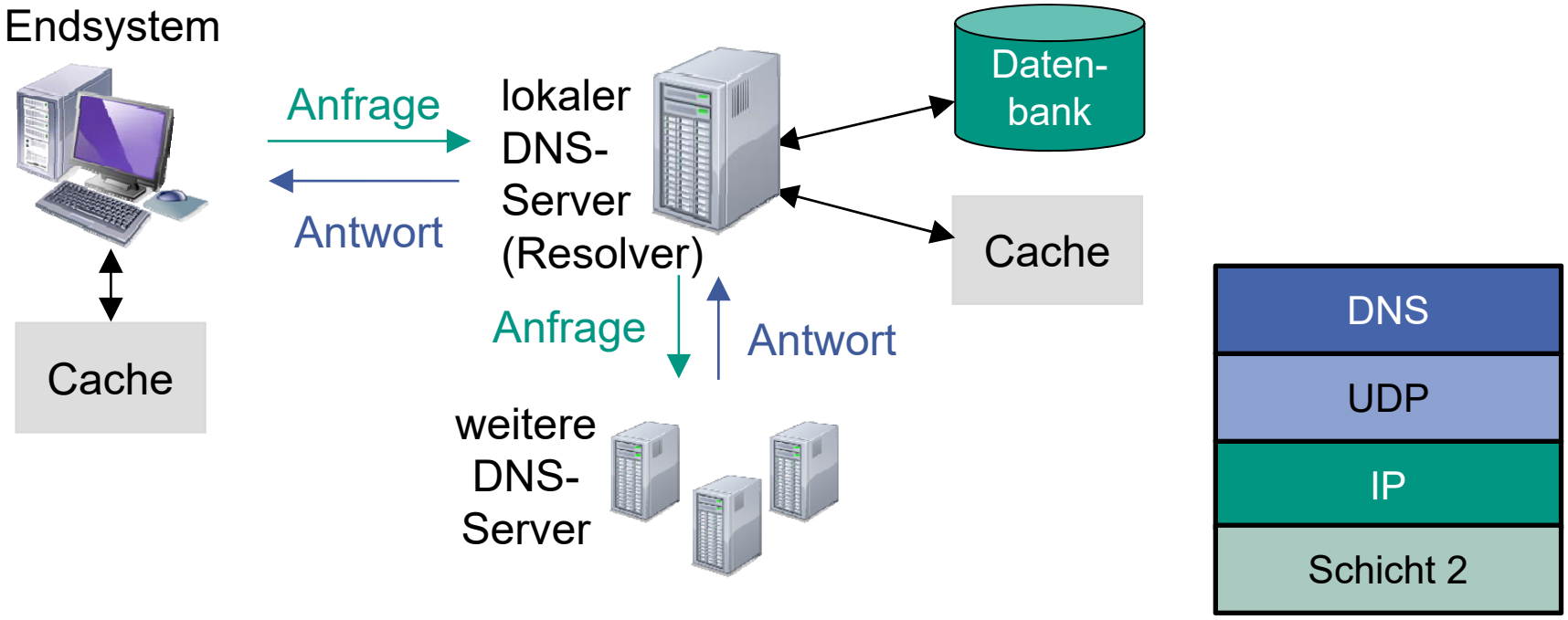
- Internetprotokolle sind auf Vertrauensbasis entwickelt
  - Protokollteilnehmer haben inhärentes Vertrauen untereinander
  - Annahme: Angreifer haben kein Zugriff auf Netzwerk
- Umsetzung von sicheren Routing-Protokollen notwendig
  - Aus AS-Sicht einen Angriff zu erkennen, ist schwierig
  - BGP hält das Internet zusammen
  - Angriffe auf BGP können gravierende globale Auswirkungen haben
- BGPsec ermöglicht Überprüfung
  - der Zuteilung von Ressourcen (IP-Präfixe und ASNs)
  - der Integrität der Routinginformation (AS-Pfad)

Überblick


Interdomain-
Routing
BGPsec
Infrastrukturdienste
DNSSEC
Namens-
dienst
DANE

Domain Name System (DNS)

- Ziel
  - Verwendung logischer Namen statt IP-Adressen zur Adressierung von Rechnern (insbesondere Servern)
  - Struktur von Namensservern die zu Abfrage genutzt werden



Resource Records (RR)

- Varianten von Resource Records

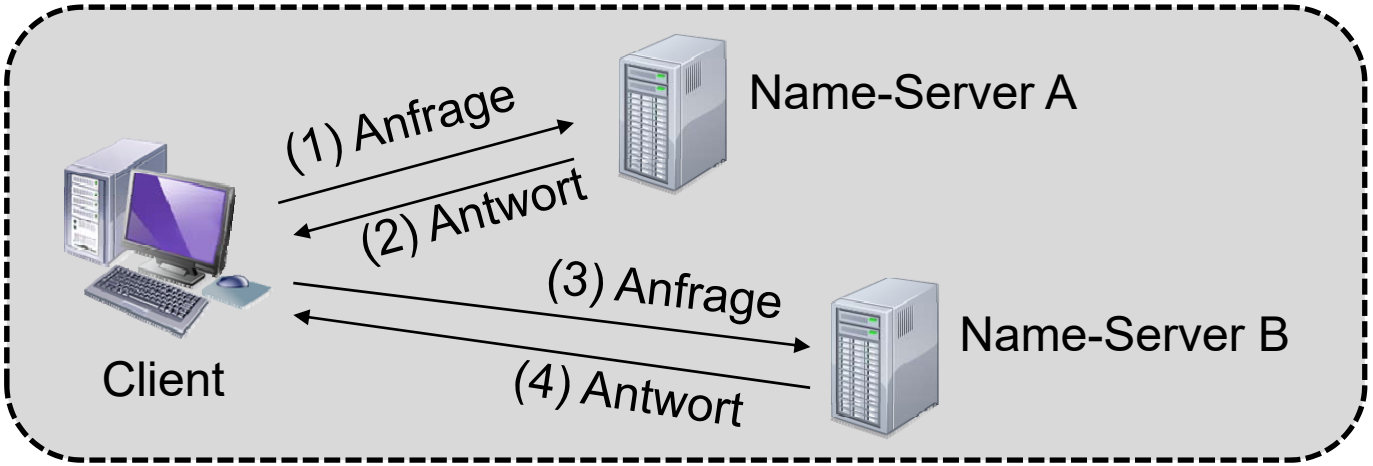
Typ	Beschreibung
A bzw. AAAA (Address)	Abbildung Name auf IPv4/IPv6-Adresse
MX (Mail Exchange)	E-Mail-Server einer Domäne
NS (Nameserver)	Nameserver einer Domäne
CNAME (Canonical Name)	„Alias“-Namen für Rechner/Domänen
PTR (Pointer)	Abbildung IP-Adresse auf Name
HINFO (Host Info)	Zusätzliche Informationen (CPU, …)

- Weitere Resource Records-Typen definiert in RFC 1035
  - http://www.iana.org/assignments/dns-parameters

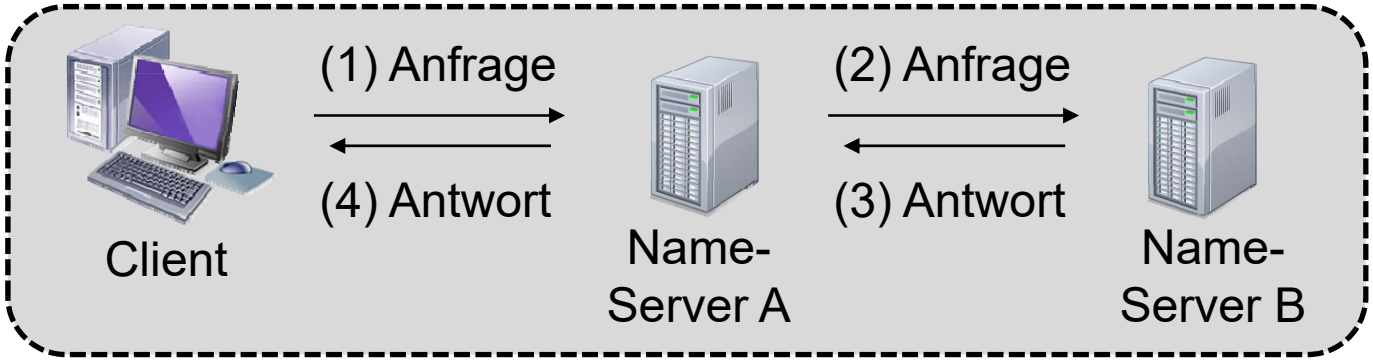
[RFC1035]

DNS-Abfragen

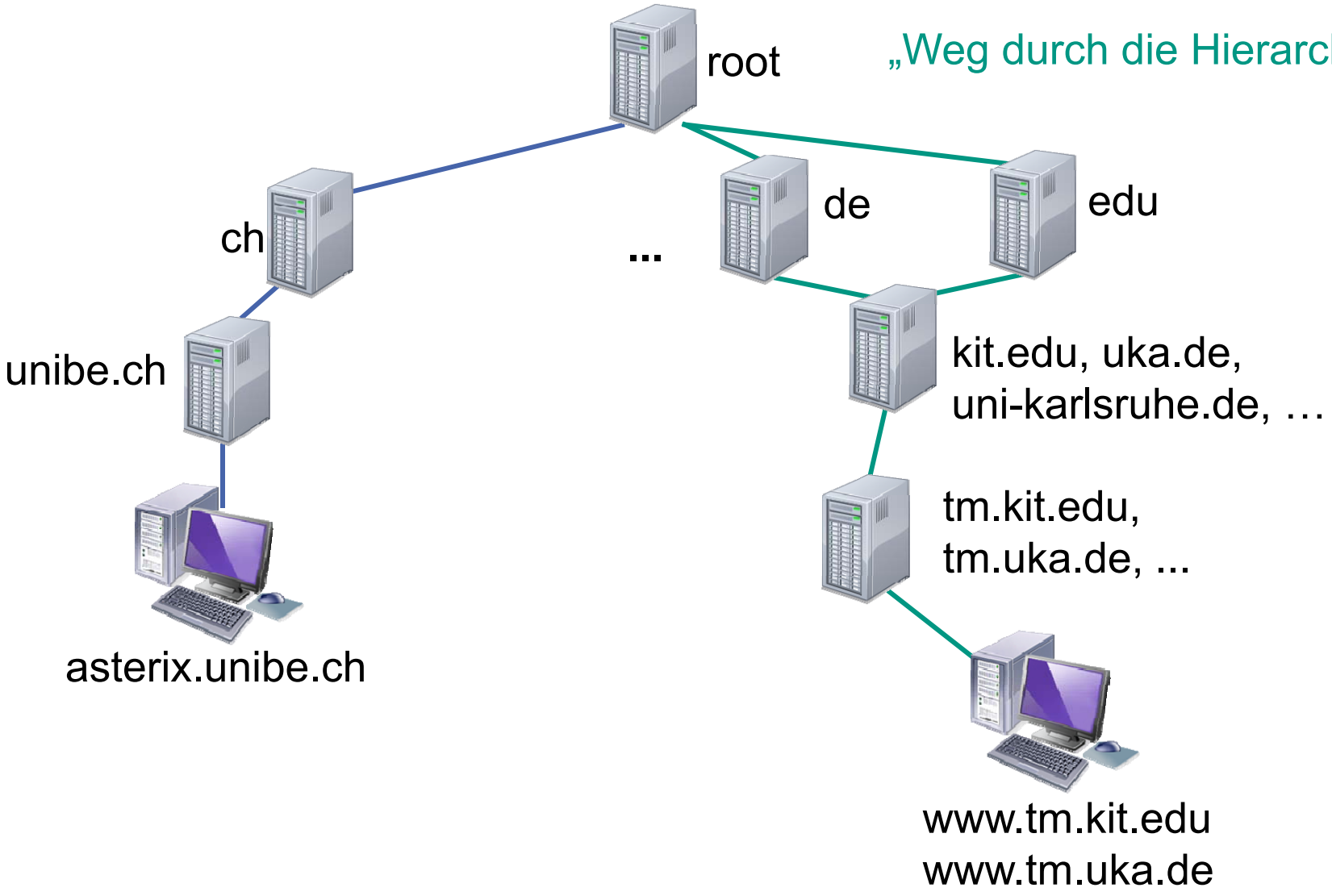
- Iterative Anfrage



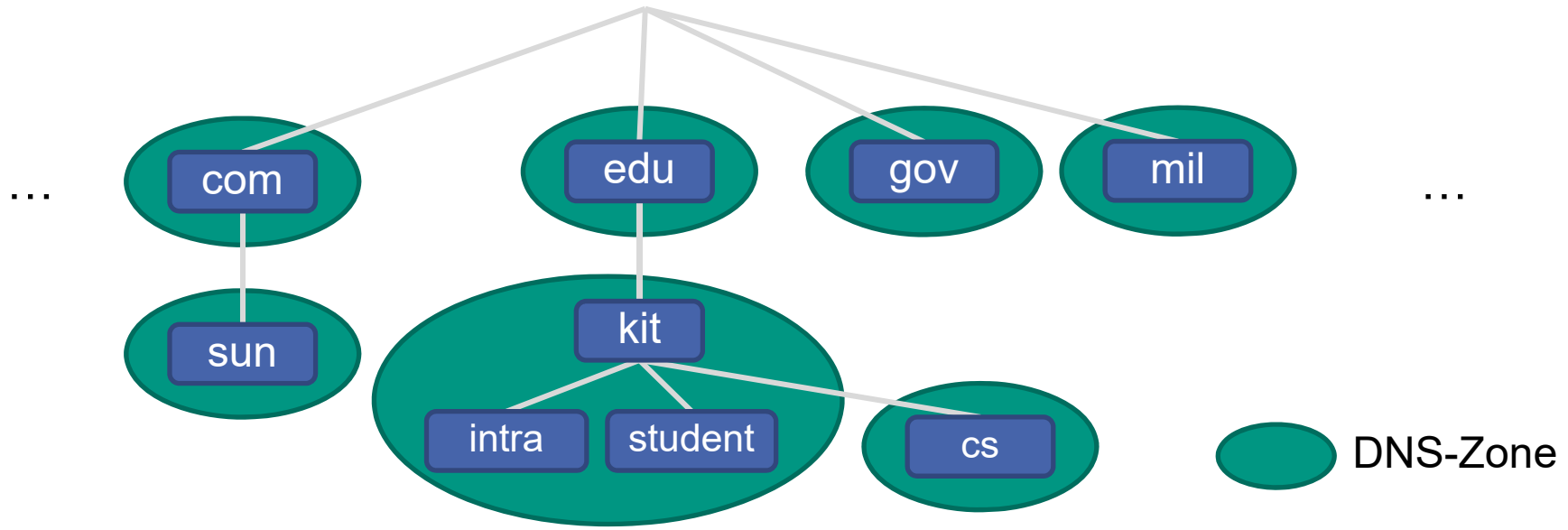
- Rekursive Anfrage



Nameserver-Hierarchie: Beispiel



Aufteilung in DNS-Zonen



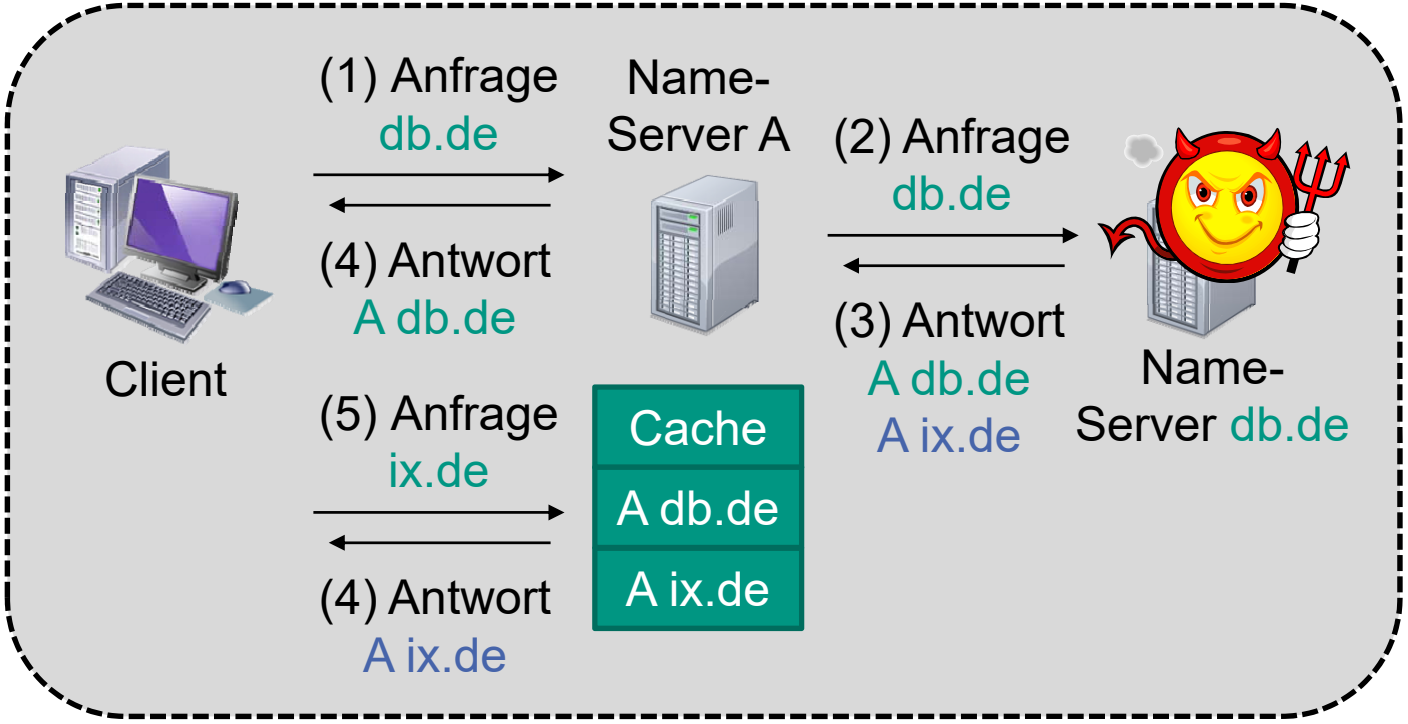
- Zonenkonzept
  - Repräsentiert den Teil des Domänenbaums für den ein Name-Server zuständig ist
  - Kann mehrere Subdomänen enthalten
- Zonendatei beschreibt eine Zone
  - Enthält die Resource Records (Namensinformationen) der Zone

DNS-Angriffsziele

- Unautorisierte Bekanntgabe von Records
  - Abhören, Verändern und Umleiten von Datenverkehr
  - DoS-Angriff
- Manipulation des Caches
  - Abhören, Verändern und Umleiten von Datenverkehr
  - DoS-Angriff
- Eindringen in UDP-Datenverkehr
  - Abhören oder Verändern
  - DoS-Angriff

Historisch: Cache Poisoning

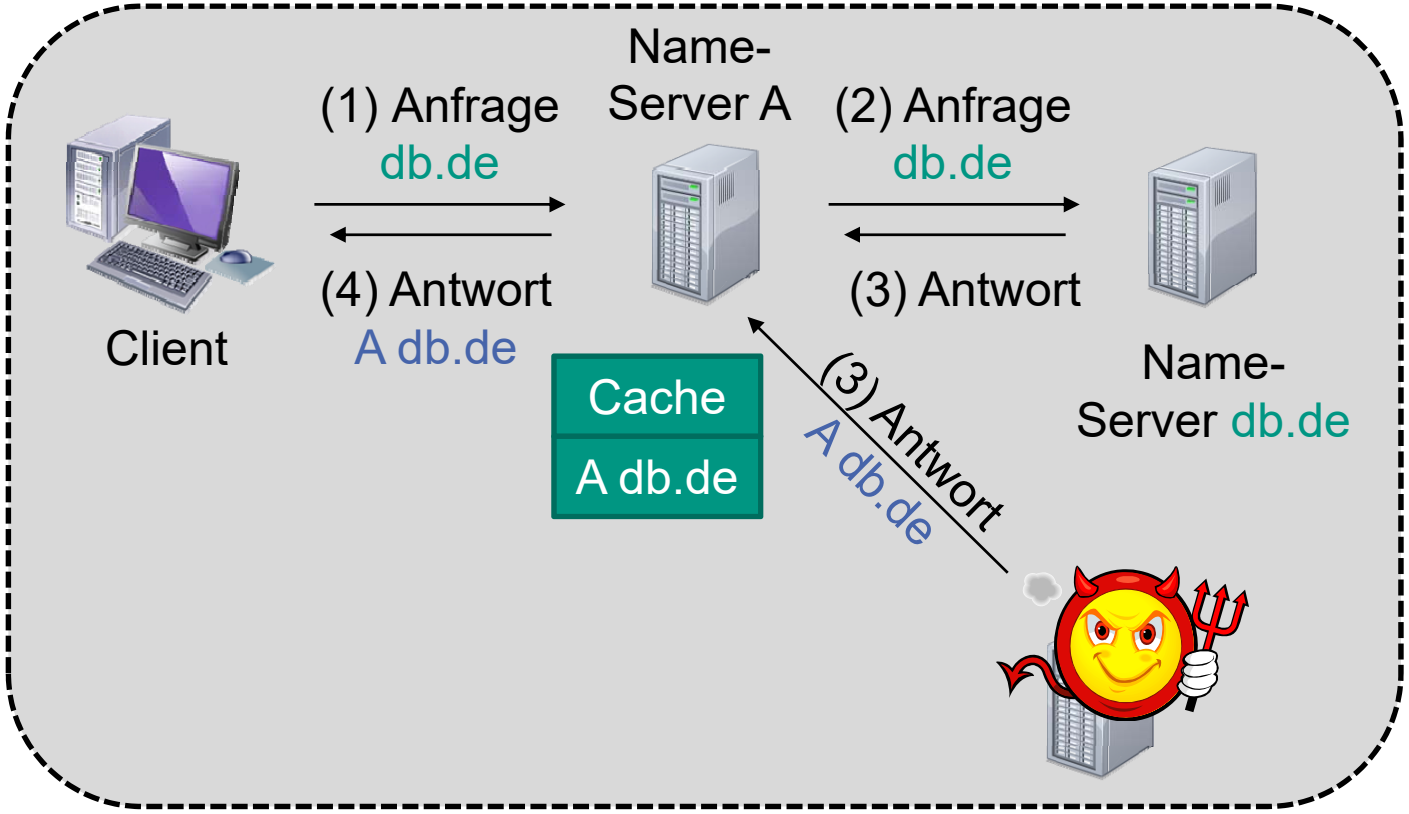
- Angreifer manipuliert Cache auf DNS-Server
  - Bei rekursiven Anfragen ungefragt gefälschte Einträge mitsenden



  - Opfer erhält so falsche IP zu Domainnamen

Historisch: Hijacking

- Angreifer fälscht Absender IP-Adresse des Nameservers um gefälschte Informationen zu verbreiten



- Erraten der passenden Query-ID (16 Bit) erforderlich

DNS-Umleitungen

- Einige Internet-Service-Provider leiten Anfragen zu nicht existierenden Domains auf eigene Dienste um
  - „Um bei der Suche zu helfen“
  - Um Werbung einzublenden
- Nichts anderes als gefälschte DNS-Antworten
  - Wie in den zwei vorherigen Beispielen
- Anstatt dessen sollten Anwender besser gesichert darüber informiert werden, dass Domainname nicht existiert!

DNS-Schutzziele

- Schutz in der Kontrollebene
  - Authentizität der RRs
    - z. B. Domainname, IP-Adresse, Mailserver, Alias
  - Welcher Nameserver berechtigt ist, Records bekannt zu geben
- Schutz auf dem Übertragungsweg einer DNS-Abfrage
  - Vertraulichkeit und Integrität der übertragenen Nachrichten
- Abhören von DNS-Abfragen kann die Privatsphäre verletzen

DNS Security Extensions (DNSSEC)

[RFC4033]

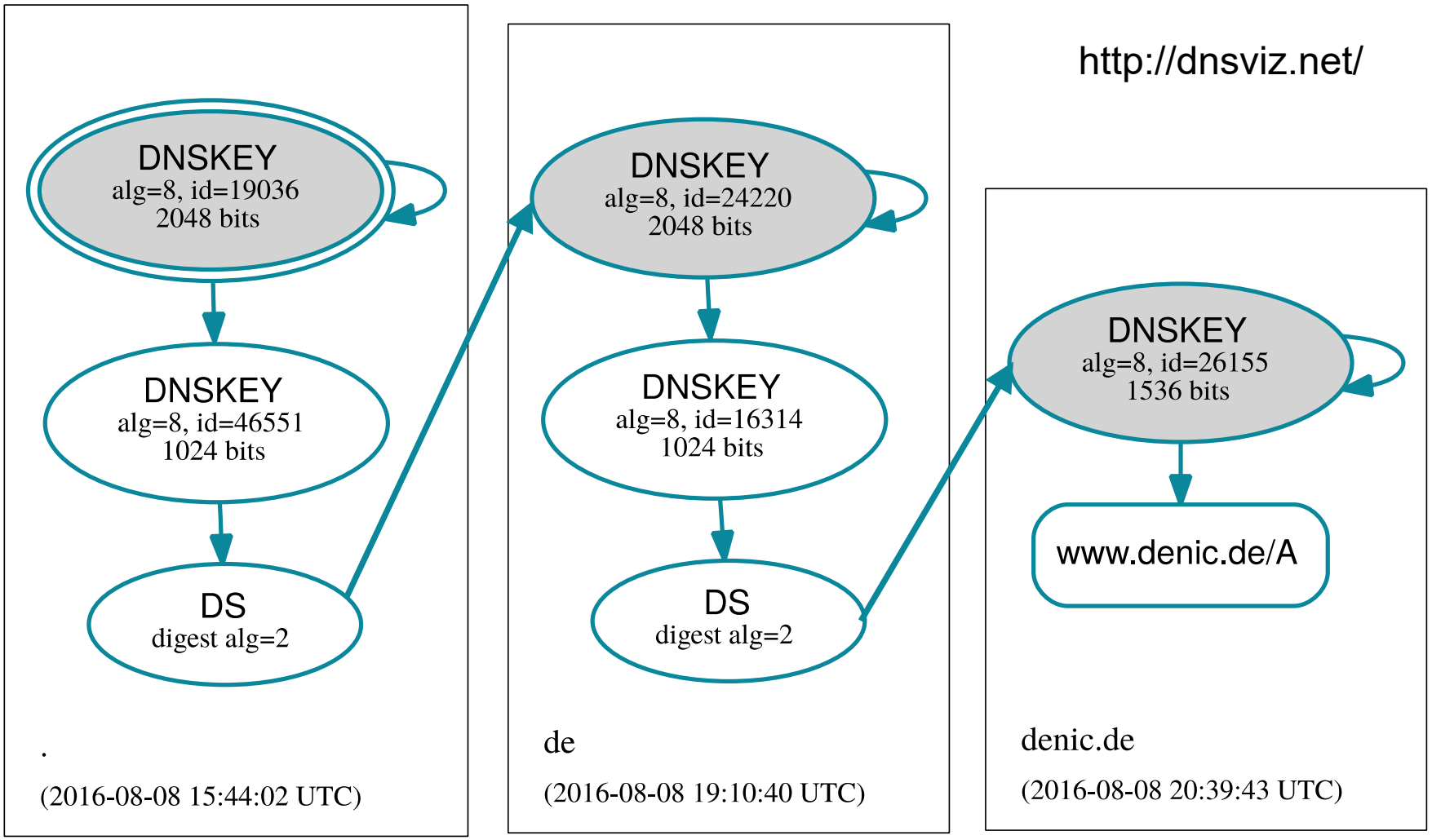
- Public Key Infrastructure (PKI) zur Authentifizierung der RRs
  - Verteilung der öffentlichen Schlüssel durch DNS selbst (keine Zertifikate!)
  - Unterscheidung Zone Signing Keys (ZSKs) und Key Signing Keys (KSKs)
  - Vertrauensanker bis zur ICANN
- Zusätzliche DNS-Records für öffentliche Schlüssel und Signaturen
  - Signaturen für RR Sets (Domainnamen, IP-Adressen, Mailserver, etc.) durch den Zonenadministrator
- Clients überprüfen Inhalt einer DNS-Antwort auf Integrität mittels öffentlichem Schlüssel
  - Antwort sollte Inhalt der autoritativen Zonendaten entsprechen

DNS Erweiterungen

- DNSKEY
  - Öffentlicher Schlüssel für die Zone
- RRSIG
  - Signiertes RRset
- NSEC3
  - Zeigt nicht existente Namen oder RRs an
  - Nutzt Hash-Werte auf nächsten existierenden Eintrag, damit Zonen nicht einfach abgelaufen werden können
- DS
  - Delegation Signer
  - Enthält Hash des Public Keys der Child-Zone
  - Wird signiert durch RRSIG mit DNSKEY der Parent Zone
  - Verfolgung der Vertrauenskette

Beispiel www.denic.de

http://dnsviz.net/



Beispiel RRSIG

```
www.denic.de. 3600 IN A 81.91.170.12
www.denic.de. 3600 IN RRSIG A 8 3 3600 (
              20170719110000 20170705110000 26155 denic.de.
              jHZmoNSgTgFfza5r0yBrQ88r+Co2Fi7cSht1KZgm+u6w
              yeyjaVQg8AnkWwnFl9HNgPZfHYNOl7oO9PpQAKyIea/y
              VVLMBg6ShAH46/HfdLOJR2tP4khBf1FgXJvICdzsIH/p
              di2UIRaTRJBYMJsNcSIx6TcHuUSIB4iiLPs8yjLoGGwC
              yB3Lzgaa6ThpBVCztXXNmb3/epacgb5+X6C8cefcCrwz
              QKmy2B812Np3hP4b1p0tC8We1NAD/UXObUs0 )
denic.de.     3600 IN NS ns3.denic.de.
denic.de.     3600 IN NS ns2.denic.de.
denic.de.     3600 IN NS ns1.denic.de.
denic.de.     3600 IN RRSIG NS 8 2 3600 (
              20170719110000 20170705110000 26155 denic.de.
              D+zmppaaFBB+0dRfnmthQGMyPRS4ITjMQYSJlFkzaxxJ
              XUPTn9fEhTNiWjunfqjolZv1h92+/QG5DAg3WyMK3fUs
              Gvw9nyu98KX7Lokio/PL52KAVop1ZKGVgWuZWMMNAv75
              45VKkNVZy68dXg03Nlyj42H67u72iTkz1vO+UkBsUaL5
              3syHF81G/ZvXxMGxKC9NHCY+/l2sWieiS5tSajES8YnG
              GWh68lc8KNiV6S2JZIjmBToSzGDGU2xShyEv )
```

Beispiel DNSKEY

```
denic.de.    3600 IN DNSKEY 257 3 8 (
             AwEAAb/xrM2MD+xm84YNYby6TxkMaC6PtzF2bB9WBB7u
             x7iqzhViob4GKvQ6L7CkXjyAxfKbTzrdvXoAPpsAPW4p
             kThReDAVp3QxvUKrkBM8/uWRF3wpaUoPsAHm1dbcL9ai
             W3lqlLMZjDEwDfU6lxLcPg9d14fq4dc44FvPx6aYcymk
             gJoYvR6P1wECpxqlEAR2K1cvMtqCqvVESBQV/EUtWiAL
             NuwR2PbhwtBWJd+e8BdFI7OLkit4uYYux6Yu35uyGQ==
             ) ; KSK; alg = RSASHA256; key id = 26155
denic.de.    3600 IN RRSIG DNSKEY 8 2 3600 (
             20170719110000 20170705110000 26155 denic.de.
             iVDUXaxZoUHbOmHU13C9Muq+mlbooCJvtbhHUUAkbKMr
             VcOTr5cv4GMG6/YuiUnOuhoQgqkhEqpvj0xtQHlKq6Vc
             fgGj+0BfrX2EuPmx8Byk+OFPDGKPjUNUVw6Pj/CQ2XTZ
             A4WJRmYvu2g9umItlM3LYfjzZcsuoBgnbeK527LcpVtc
             juYColoDTeVB/NMgjewvWK9GBezL6R0qTC5i+O3R1JO9
             AWLfuVoTyI878KFrOGqCVcFI5+fjiowjg/5U )
```

Aktuell: DNSSEC KSK Rollover

- 27.10.2016: Neuer KSK (ID: 20326) der Root-Zone erstellt
  - https://www.iana.org/reports/2017/root-ksk-2017.pdf
- **11.07.2017**: Neuer KSK wird publiziert
- 19.09.2017: Wechsel ZSK der Root-Zone
- 11.10.2017: Neuer KSK signiert Root-Zone
- 11.01.2018: Alter KSK (ID: 19036) wird ungültig

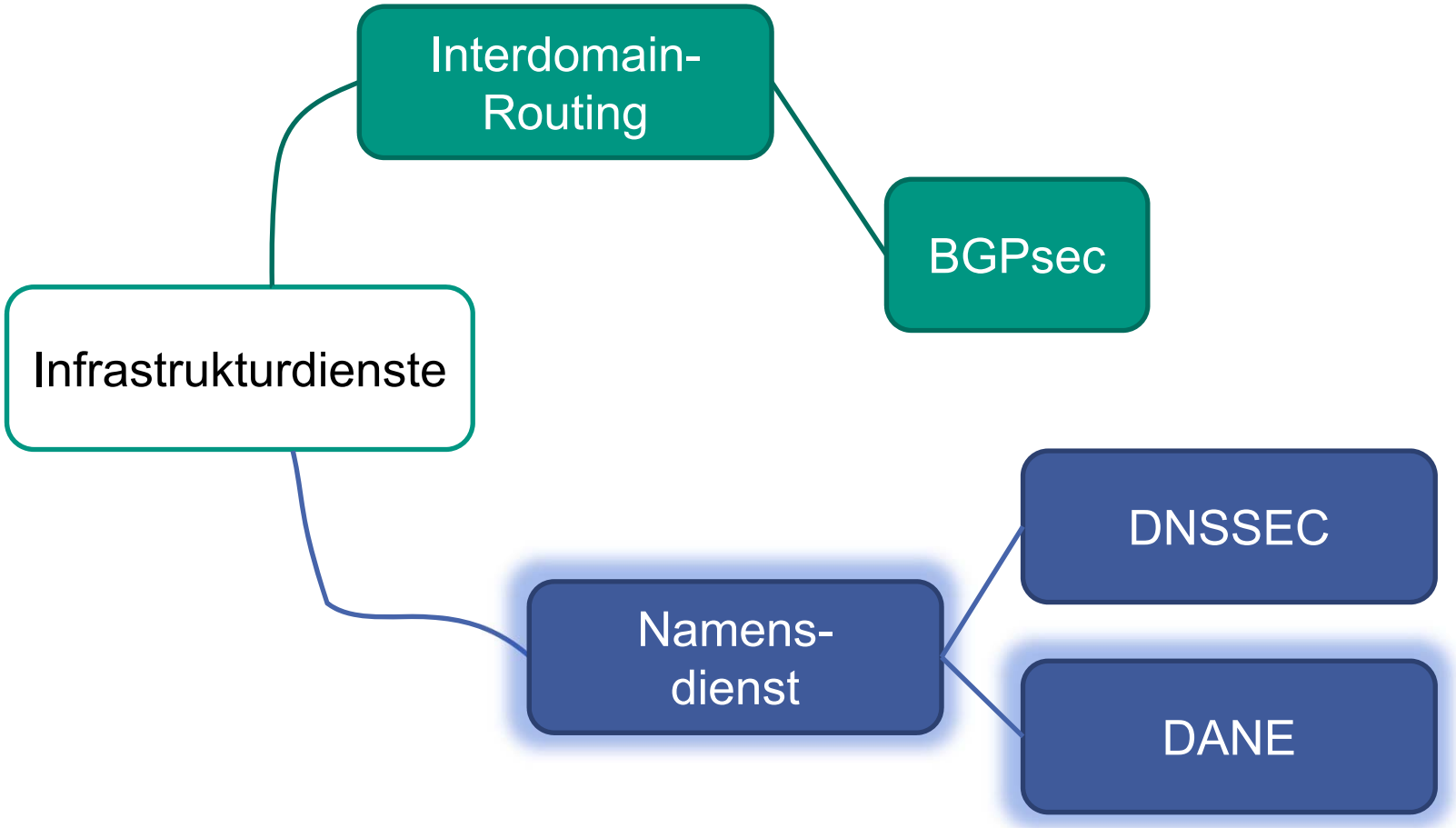
- Automatismus in RFC 5011 „Automated Updates of DNS Security (DNSSEC) Trust Anchors” sollte KSK/ZSK für Clients automatisch aktualisieren


[RFC5011]

Was DNSSEC nicht schützen kann

- Selbst wenn DNS-Auskunft authentisch ist, können Pakete in Richtung der abgefragten Zieladresse umgeleitet werden
  - MitM-Angreifer auf dem Pfad zwischen Quelle und Ziel
  - Angriffe auf das Routing (siehe BGP)
- Authentizität eines Server normalerweise über X.509-Zertifikat
  - Vgl. Vorlesungsteil über Vertrauensmodelle
- Allerdings kann Angreifer ein gültiges Zertifikat erlangen
  - Über fahrlässige CA oder andere Schwachstellen
- DNSSEC garantiert nicht, dass Server authentisch ist!

Überblick


Interdomain-
Routing
BGPsec
Infrastrukturdienste
DNSSEC
Namens-
dienst
DANE

Problem mit TLS-Zertifikaten

- Unklar, welche CAs für welche Domänen X.509-Zertifikate ausstellen dürfen
  - Public Key Infrastructure (PKIX) ist Oligarchie mit >200 Vertrauensankern
  - Immer wieder Vorfälle unberechtigt ausgestellter Zertifikate
- Nutzung unpassender Zertifikattypen
- Selbstsignierte Zertifikate haben keinen richtigen Vertrauensanker

DANE: Überprüfung von Server-Zertifikaten

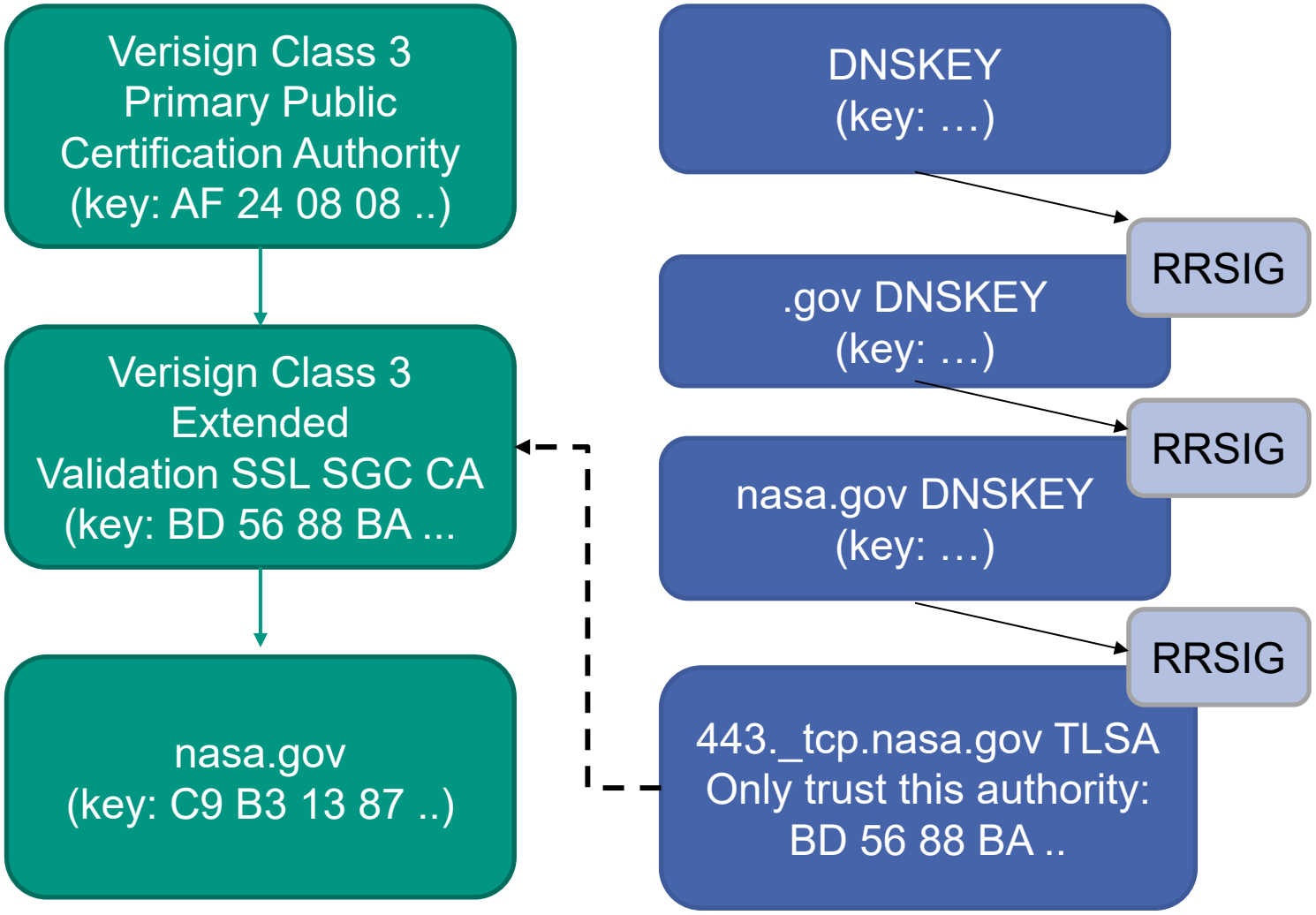
- Ziel
  - Überprüfbarkeit ob Server-Zertifikat tatsächlich zur Domain gehört
    - z.B. für Mail- und Web-Server
  - Schutz vor „unbeabsichtigter“ Ausstellung gültiger Zertifikate

- DNS-based Authentication of Named Entities (DANE)
  - Zertifikate für Server werden per DNSSEC gesichert in Zone hinterlegt
    - Fingerprint (Hashwert) des authentischen Zertifikates
    - Zusätzlicher DNS-Record: TLSA
  - Client kann per DNSSEC überprüfen ob angebotenes Server-Zertifikat mit hinterlegtem übereinstimmt

- Zusätzliche Hürde für Angreifer


[RFC6698]

Verknüpfung mit DNSSEC



DANE Beispiel

```
_443._tcp.www.example.com. IN TLSA (
  0 0 1 d2abde240d7cd3ee6b4b28c54df034b9
        7983a1d16e8a410e4561cb106618e971 )
```

SHA-256 über
PKIX CA Zertifikat

Zusammenfassung DNS / DNSSEC / DANE

- Auch DNS wurde auf Vertrauensbasis entwickelt
  - Kein Schutz auf Kontrollebene
  - Kein Schutz von DNS-Abfragen
- Daher dringend sichere DNS-Protokolle notwendig
  - DNSSEC bietet gute Möglichkeiten DNS-Angaben zu authentifizieren
  - Vertrauensanker ausgehend von Root-Servern
  - DANE bietet zusätzlich Überprüfbarkeit von Server-Zertifikaten
- Vertrauen ist gut, Kontrolle ist besser!

Literatur

[IANA] Internet Assigned Numbers Authority (IANA); https://www.iana.org/

[ICANN] Internet Corporation for Assigned Names and Numbers (ICANN); https://www.icann.org/

[RFC1035] P. Mockapetris; DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION; Nov. 1987

[RFC3369] R. Housley; Cryptographic Message Syntax (CMS), Aug. 2002

[RFC4033] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose; DNS Security Introduction and Requirements; Mar. 2005

[RFC5011] M. StJohns, Automated Updates of DNS Security (DNSSEC) Trust Anchors, Sep. 2007

[RFC4271] Y. Rekhter, T. Li, S. Hares; A Border Gateway Protocol 4 (BGP-4); Jan. 2006

[RFC6480] M. Lepinski, S. Kent; An Infrastructure to Support Secure Internet Routing; Feb. 2012

Literatur

[RFC6480] M. Lepinski, S. Kent; An Infrastructure to Support Secure Internet Routing; Feb. 2012

[RFC6481] G. Huston, R. Loomans, G. Michaelson; A Profile for Resource Certificate Repository Structure; Feb. 2012

[RFC6488] M. Lepinski, A. Chi, S. Kent; Signed Object Template for the Resource Public Key Infrastructure (RPKI); Feb. 2012

[RFC6698] P. Hoffman, J. Schlyter; The DNS-Based Authentication of Named Entities (DANE) - Transport Layer Security (TLS) Protocol: TLSA; Aug. 2012

[RFC7132] S. Kent , A. Chi; Threat Model for BGP Path Security; Feb. 2014