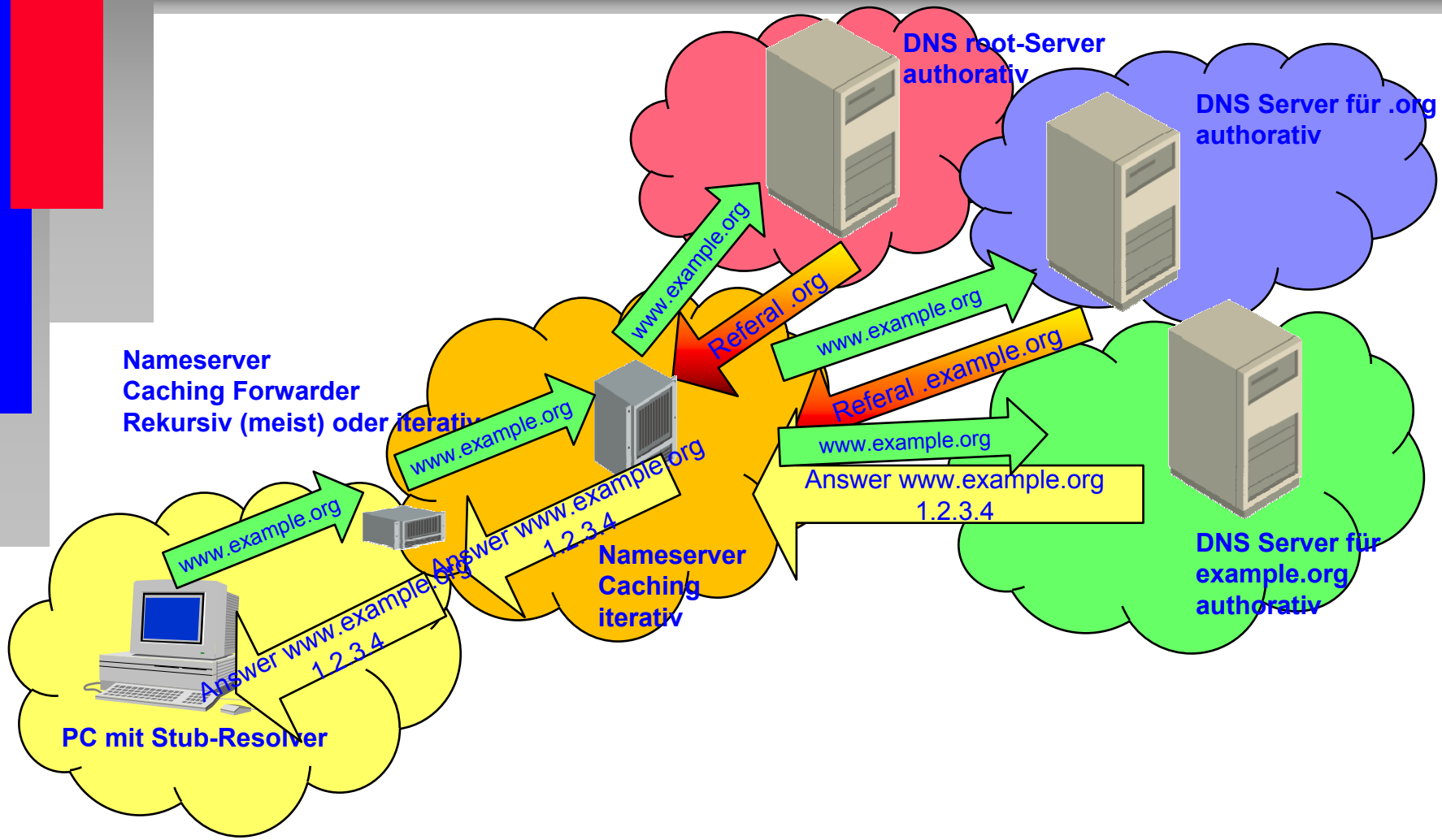
DNSSEC
Einführung

DNSSEC-Meeting
2. Juli 2009
Frankfurt

Inhalt

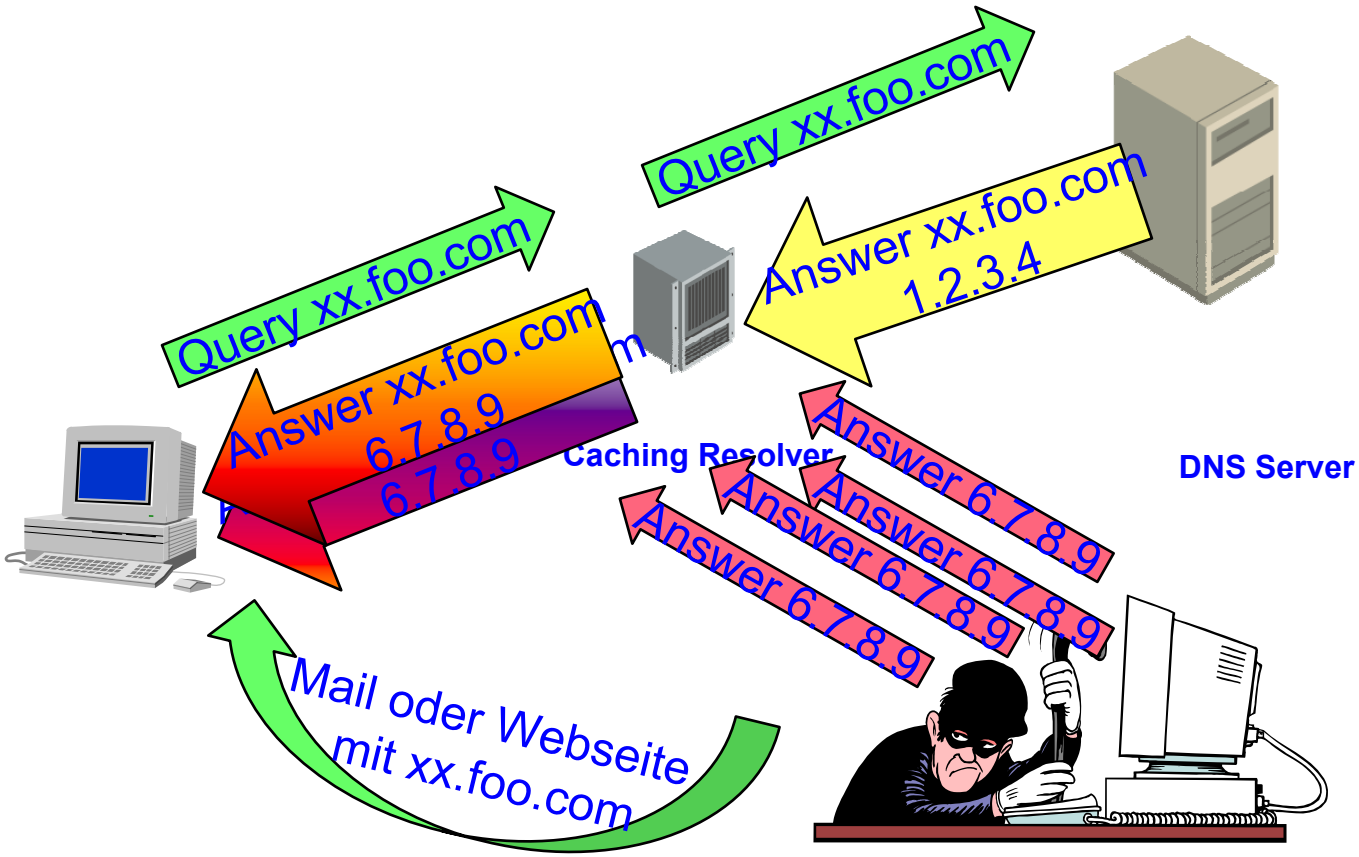
- Warum DNSSEC?
- Warum erst jetzt?
- Warum ein Testbed?
- Was ist DNSSEC?
- Wie funktioniert es?

Normaler Ablauf



Cache-Poisoning

- Funktionsweise



DNSSEC

- Verhindert die derzeit bekannten Arten von Cache-Poisoning
- Verhindert unbemerkte Manipulationen an den Daten durch dritte unterwegs

Alternativen?

- Diskussionen seit einem Jahr
- Viele Ideen, Beispiele sind:
  - Use TCP
  - 0x20 – zusätzliche Bits für Entropie
  - Add random text
  - Ask twice (or n times)
  - Don‘t accept new data if already in cache
  - EDNS Ping before accepting answers
  - Accept only if roundtrip time is similar
  - DNSCurve
  - TSIG, VPN-channel, IPSEC
  - . . .
- Bisher wurde keine der Lösungen allgemein akzeptiert

Zeitpunkt

- Über DNSSEC wird schon lange diskutiert
- Die erste Definition (RFC2065 von 1997) war noch nicht praxistauglich, enthielt jedoch bereits viele der Elemente von DNSSEC
- Erst die im Jahr 2005 veröffentlichten RFC4033, RFC4034 und RFC 4035 beschreiben eine im Internet einsetzbare Version von DNSSEC
- DNSSEC Standards erfüllen mehr Anforderungen (NSEC3 definiert in RFC5155 Anfang 2008)
- Implementierungen werden verfügbar und stabiler im Betrieb
- Hardware (Crypto-HW) wird für DNSSEC verfügbar
- Entwicklung, Test und Erprobung laufen parallel weiter
- Druck und Notwendigkeit werden größer

Testbed

- Es fehlt noch ausreichende Betriebserfahrung
- Viele Elemente in der Prozesskette müssen angepasst und optimiert werden
- Im Testbed können empfohlene Betriebsparameter (Schlüssellängen, Schlüsselgültigkeit usw.) auf ihre Tauglichkeit geprüft werden
- Software- und Hardwareperformance können geprüft werden
- Zuverlässigkeit von Komponenten (Software, Hardware und embedded Systemen) kann erprobt werden
- Vermutungen über das Anwachsen der Datenmengen und Paketgrößen können verifiziert oder korrigiert werden
- Abschätzungen der notwendigen Aufwände für Einrichtung und Betrieb können in einer begrenzten aber realistischen Umgebung verifiziert werden

DNSSEC

- Was kann DNSSEC
  - data integrity authentication
  - data origin authentication
  - key distribution
- Was kann DNSSEC nicht
  - confidentiality for queries or responses
  - any form of access control

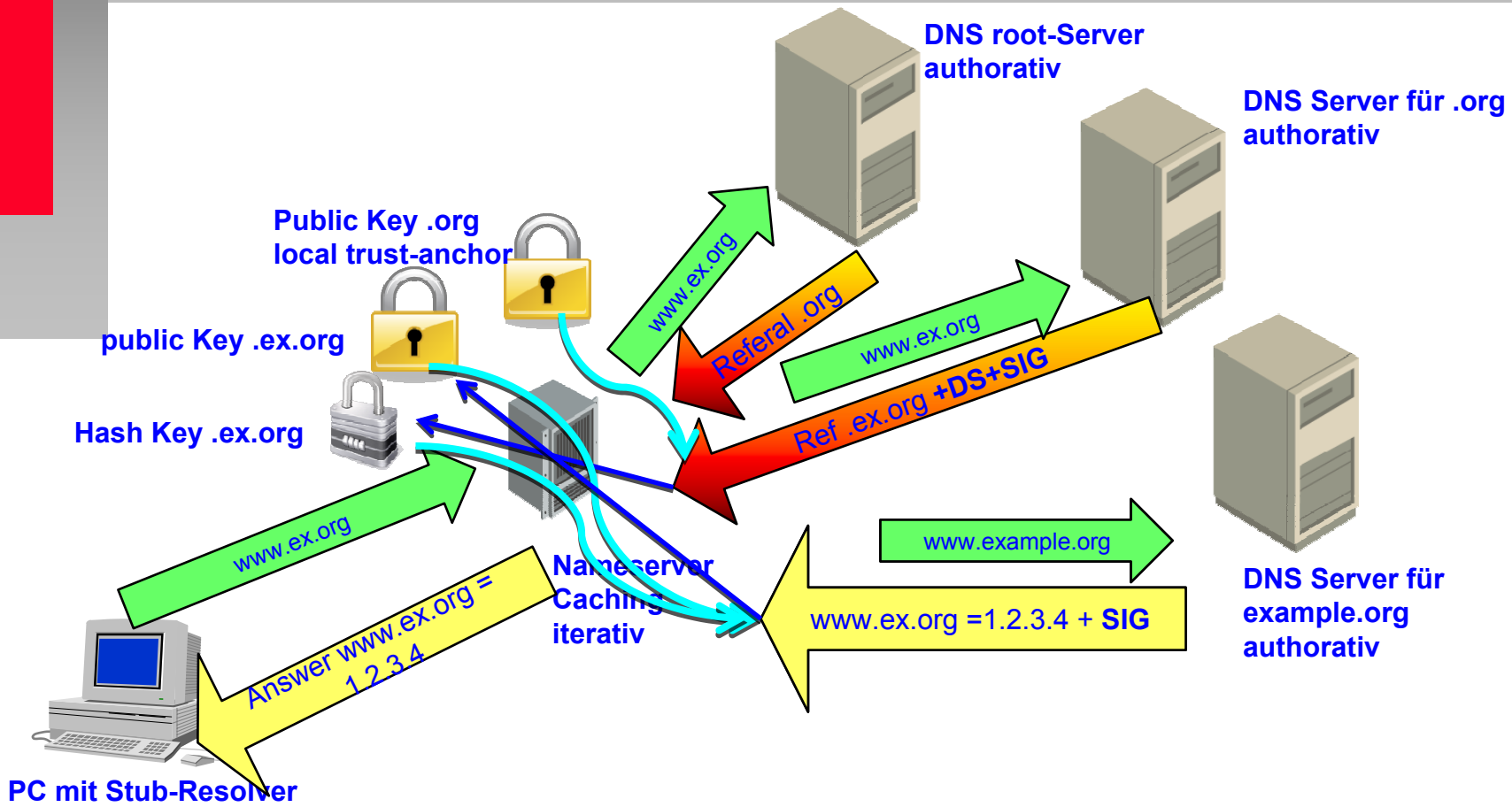
DNSSEC relevante Records

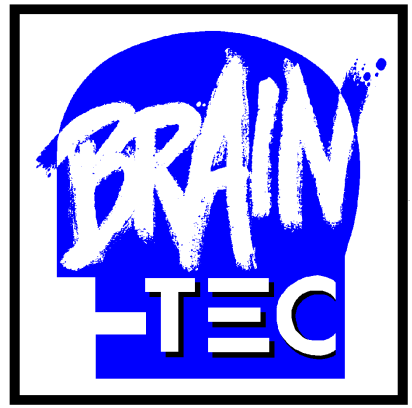
- DS
  - zeigt an, dass delegierte Zone signiert ist
  - enthält Key-Tag und HASH des Keys
- DNSKEY
  - öffentlicher Schlüssel
  - enthält Schlüsseltyp und Schlüsseldaten
- RRSIG
  - Signatur für eine gruppe von Records
  - enthält Liste der abgedeckten Record-Typen, Signaturtyp, Anzahl der gesicherten Records, ursprüngliche TTL, früheste Gültigkeit, späteste Gültigkeit, Key-Tag, Name (DNS-Zone) des Signierenden, Signatur
- NSEC3
  - Platzhalter um das Nichtvorhandensein von Records mit DNSSEC sichern zu können
  - enthält HASH-Typ, HASH-Länge. HASH-Anzahl, Initialwert, HASH des Namens des nachfolgenden Records, OPT-Out flag

DNSSEC-Einführung

- Zone sichern
  - Schlüssel erzeugen
  - öffentliche Schlüssel in Zone eintragen
  - Zone mit privaten Schlüsseln signieren
  - DNSSEC einschalten und signierte Zonendaten laden
  - DS-records mit den Hashes der öffentlichen Schlüssel in die übergeordnete Zone eintragen
  - Alternativ öffentliche Schlüssel über DLV oder anderes Verfahren verteilen
- Zone validieren
  - Trust-Anchor konfigurieren
  - DNSSEC einschalten (Anfragen werden mit DO-Bit gesendet)

DNSSEC Ablauf





BRAINTEC Netzwerk-Consulting GmbH

Hans Peter Dittler

www.braintec-consult.de

hpdittler@braintec-consult.de

dittler@isoc.de

Herstellerunabhängige Beratung für
Vernetzung und Kommunikation
Karlsruhe