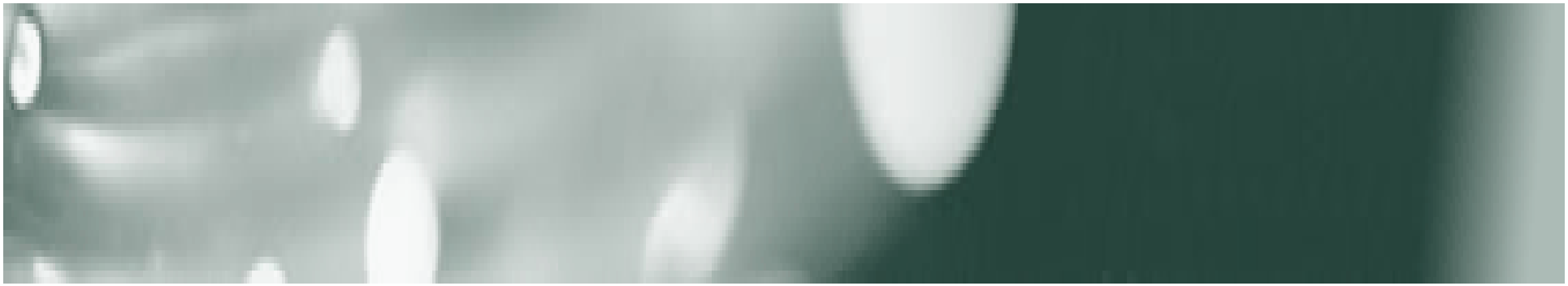


DNSSEC

-Gewöhnen‘s sich schon mal dran -

Peter Koch <koch@denic.de>

Berlin, 9. Februar 2006

SEC sells

DNSSEC - das war doch gleich?

Was nicht besser wird

Was besser wird

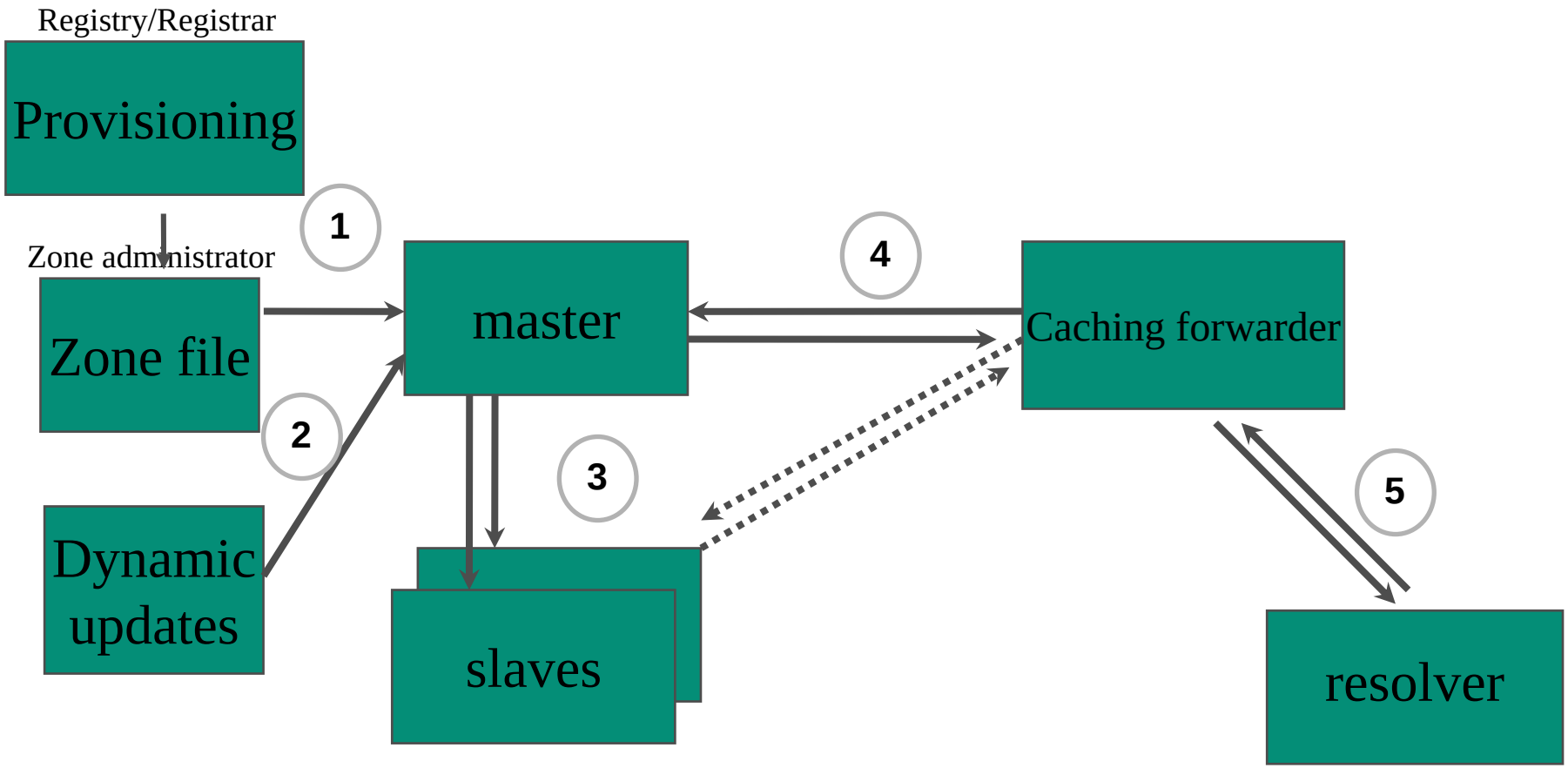
Bedenkenträger

DNSSEC und der Registrar

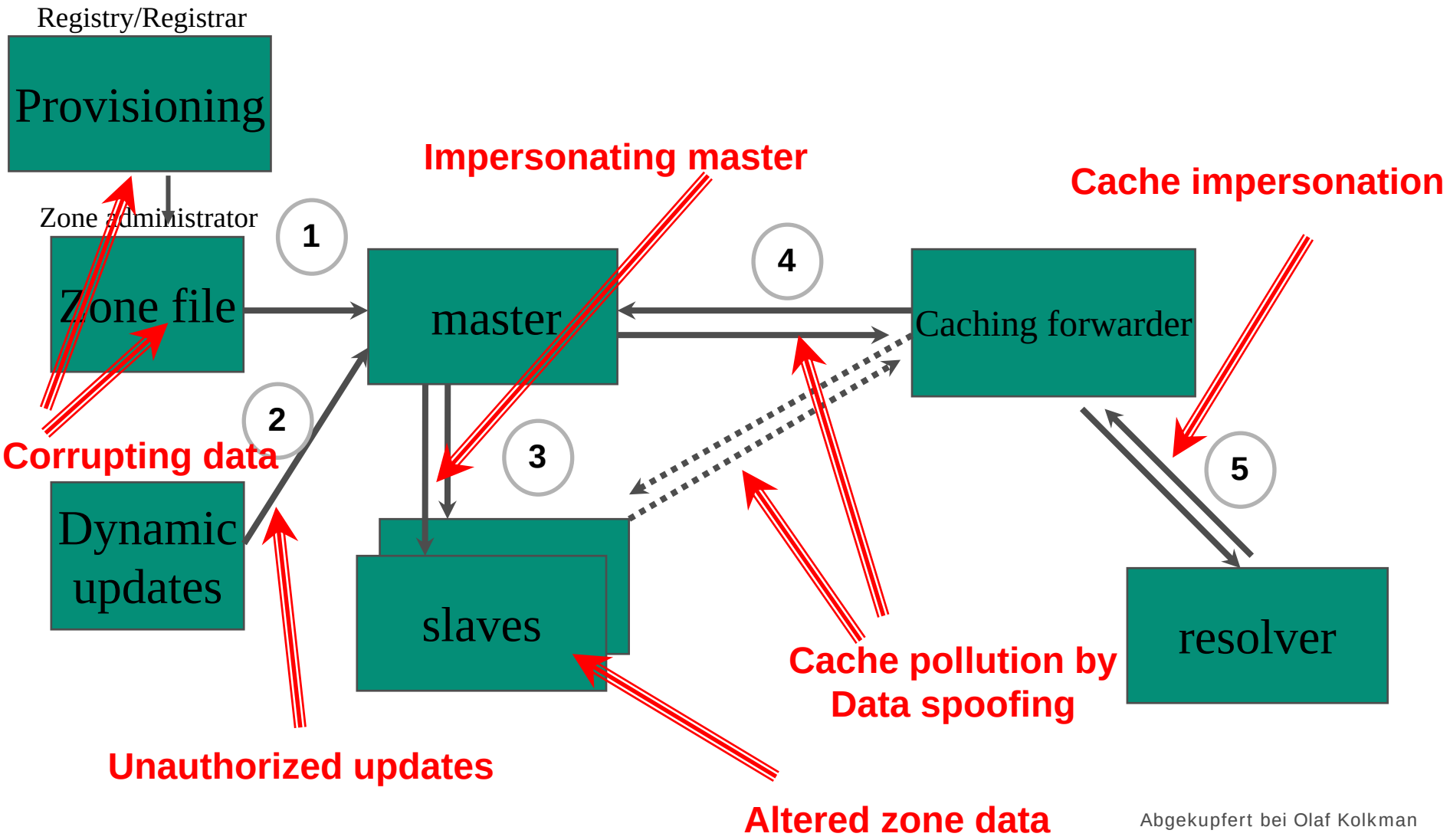
DNSSEC und der ISP

Chancen und Möglichkeiten

DNS-Datenfluß



Mögliche Angriffspunke



Abgekupfert bei Olaf Kolkman

Weiterhin dicke Bretter bleiben ...

- Bedienfehler (Authentizität vs. Korrektheit)
- Phishing
  - Leichtgläubige Anwender
  - Schlechte Benutzerkonditionierung
- Domain Hijacking
- Pharming, wenn es DNS-Nutzung ausschaltet
- Das Böse an sich

DNSSEC hilft gegen ...

- Cache Poisoning
  - Vulgo: Pharming
- Adress-Spoofing
- Zonenfile-Modifikation
  - Kompromittierung eines Nameservers
  - „Untreue“ Secondaries

Objection, your Honor!

Da waren doch noch …

- Zone Walking
- Die Root-Zone
- Die technische Komplexität

DNS tree/zone walking?

Die DNSSEC-Methode zum authentisierten Dementi ermöglicht eine Aufzählung des Zoneninhalts

- Privacy-Problem auf der Registry-Ebene
- … dadurch für Registrare/Registranten von Bedeutung
- Die IETF und Registries arbeiten an Abhilfe (Online Signing, NSEC3)
- Zone Walking ist für die allermeisten Kundenzonen kein Problem!
  - Sie enthalten ohnehin nur `www`
  - In anderen Fällen helfen die allgemeinen Lösungen
- Zone Walking ist kein Grund mehr, DNSSEC zu ignorieren
- Zone Walking ist kein Thema in der Root-Zone, in `IN-ADDR.ARPA` und ENUM!

DNSSEC und die Root-Zone

- Root-Zone stellt den zentralen *Trust Anchor*
- Technische Probleme nachrangig
- Geringe Vorwarnzeit

Technische Komplexität?

Gebt dem Kaiser, was …

- Wesentlicher Teil des Schlüsselmanagements kann vor dem Endkunden „versteckt“ werden
  - Der Zonenverwalter bekommt eine eigene Rolle
- Der *ohnehin* abgesicherte Verkehr zwischen Registrar und Registry wird um wenige Attribute erweitert
- Der Anwender muß die Bits und Bytes nicht verstehen
  - DNS selbst galt „damals“ auch als kompliziert

Was ändert sich für Registrare?

- Kundeninteraktion (nur bei kundengepflegten Zonen)
- Provisionierung der Schlüssel/Fingerprint-Daten
- Regelmäßige Neusignierung der Zonendaten
- DNSSEC-fähige Nameserver
  - Hardware, Software und entsprechende Ressourcen
  - Berechnung notwendig, Kapazität wird im Allgemeinen reichen
- Aufklärung, Werbung für Registranten

Was ändert sich für ISPs?

- DNSSEC-fähige (autoritative) Nameserver
  - Hardware, Software und entsprechende Ressourcen
  - Berechnung notwendig, Kapazität wird im Allgemeinen reichen
- Regelmäßige Neusignierung der Zonendaten
- Secure Resolving als Dienstleistung
  - Trust Anchor Management
  - Ressourcenbereitstellung

Chancen

- Erschließung neuer DNS-basierter Dienste mit mehr Indirektionsebenen
  - Service Location
  - ENUM
  - Mail-Sender-Authentisierung
  - Schlüsselverteilung (SSH, IPSec, ...)
- Secure Resolving
- Identity Management

Fragen?

Vielen Dank!

<koch@denic.de>