Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Einführung von DNSSEC und DANE im Bayerischen Hochschulnetz (BHN)

Sven Duscha, Bernhard Schmidt, Daniel Feuchtinger und Helmut Reiser

Überblick

Technik

- DNS = **D**omain **N**ame **S**ystem
- DNSSEC = **DNS Sec**urity Extensions
- DANE = **D**omain Name System based **A**uthenticated **N**amed **E**ntities

Organization

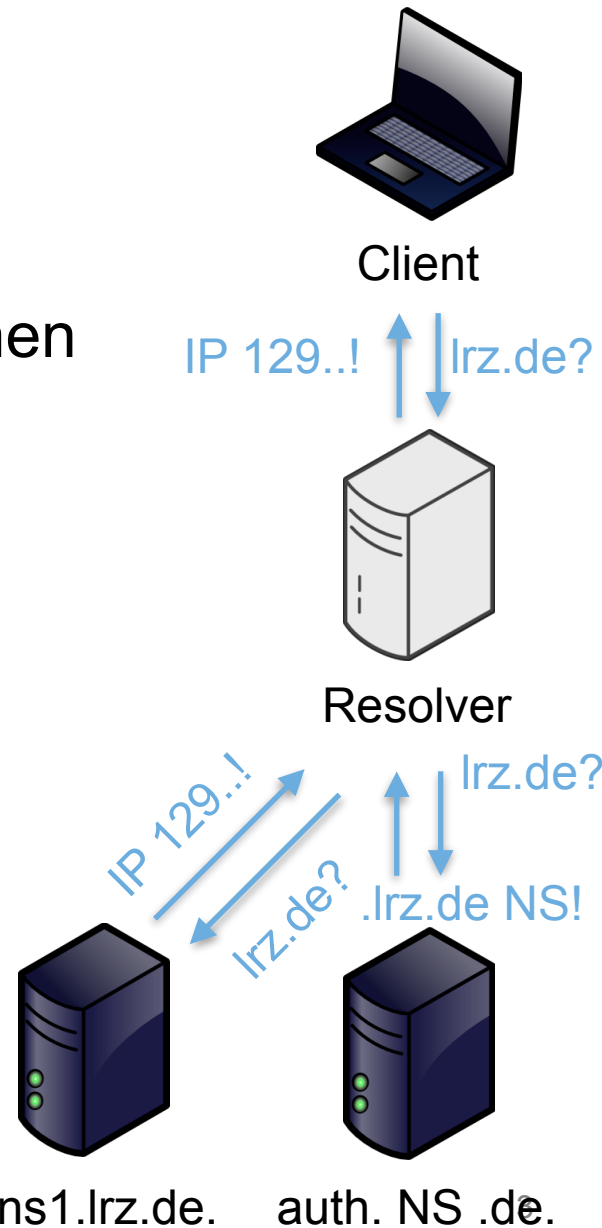
- Herausforderungen im BHN
- Förderung durch das Bayerische Forschungsministerium
- Unterstützung und Lösungen durch das Leibniz Rechenzentrum
- Umsetzung und Projektstatus

Fazit

DNS - Domain Name System

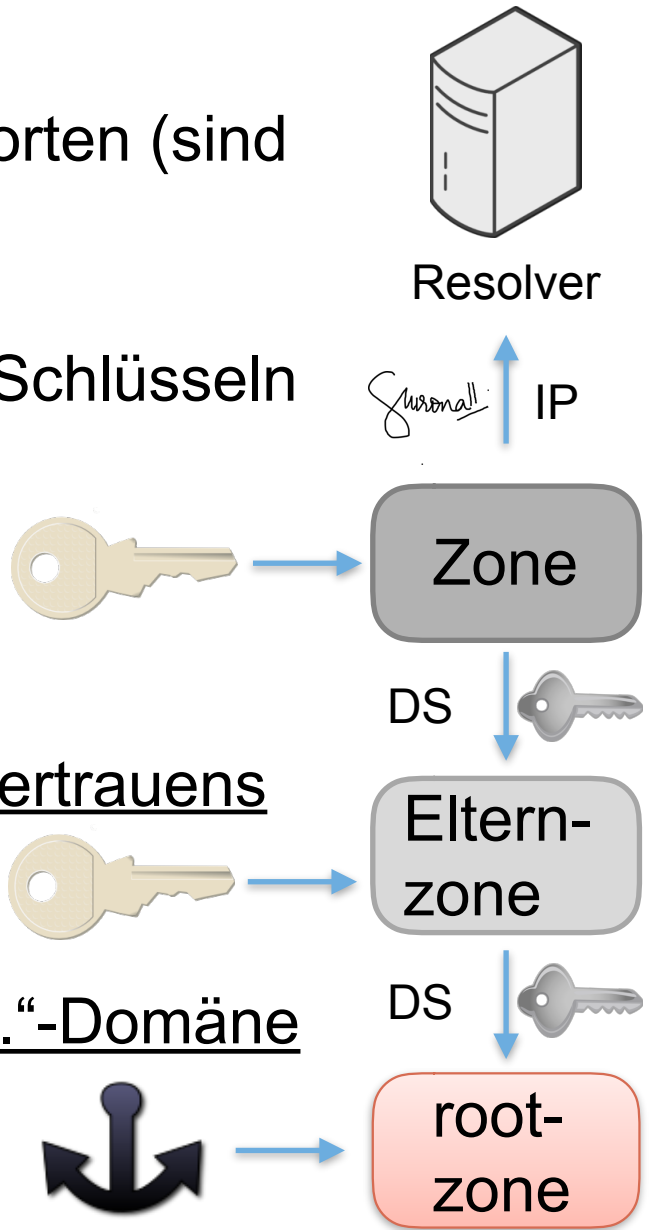
- DNS für Internetdienste benötigt
- verbindungslos (UDP) und unverschlüsselt
- dezentral und hierarchische Abfragen über Zonen
- basiert auf Vertrauen

- Angreifbar durch IP-Umleitungen, fremde Resolver, cache poisoning usw.
- Vorbereitung für „man-in-the-middle“-Attacken, Malwareangriffe u.ä.



DNSSEC - DNS Security Extensions

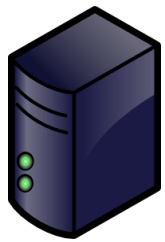
- DNSSEC (2004) erlaubt **authentische** Antworten (sind signiert, aber nicht verschlüsselt!)
- basiert auf PKI mit öffentlichen und privaten Schlüsseln
- jeder Zonenbetreiber ist für seine Verschlüsselung verantwortlich
- DNS-Hierarchie wird durch Delegation des Vertrauens („Delegated Signer“ DS) gewährleistet
- „Trust Anchor“ bilden die Schlüssel der root „.“-Domäne



DNSSEC

Parentzone de.

Delegated Signer



authoritative
nameserver

Zone lrz.de.

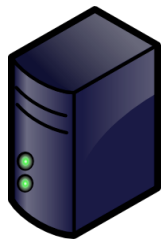
129.187.4.40

DNSSEC

Zone signieren

Parentzone de.

Delegated Signer



authoritative
nameserver

Zone lrz.de.

129.187.4.40

public key

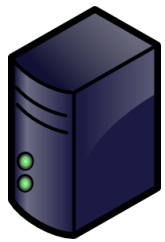
private key

DNSSEC

Zone signieren

Parentzone de.

Delegated Signer



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

private key

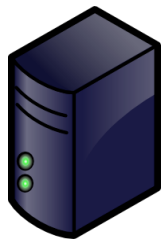
DNSSEC

Public key im DS

Parentzone de.

Delegated Signer

public key



authoritative nameserver

Zone lrz.de.

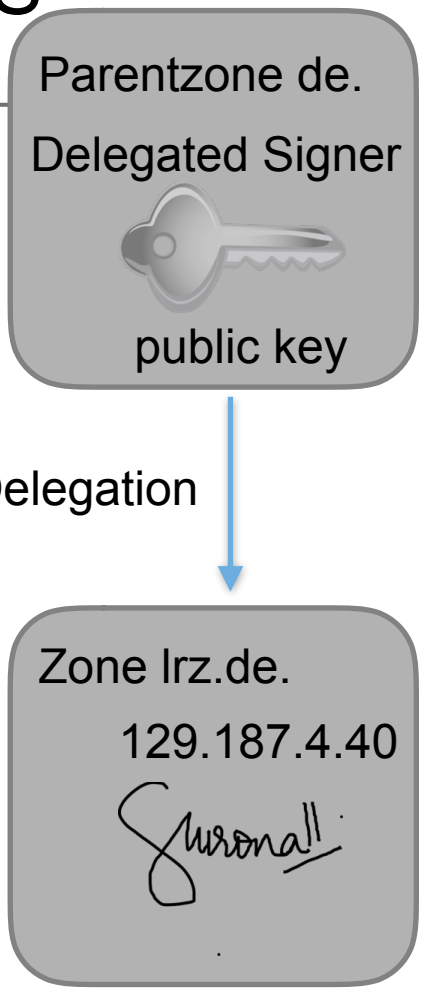
129.187.4.40

public key

private key

DNSSEC

Public key im DS



DNSSEC

DNS Anfrage

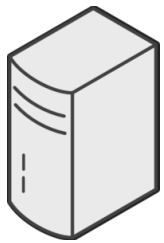
Client

Parentzone de.

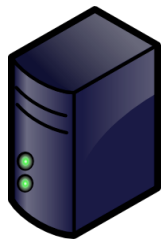
Delegated Signer

public key

Delegation



resolving nameserver



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

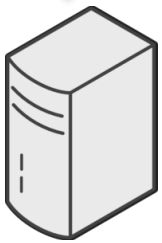
private key

DNSSEC

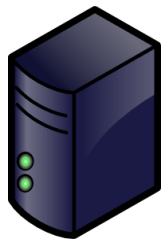
DNS Anfrage

Client

servicedesk.lrz.de?



resolving nameserver



authoritative nameserver

Parentzone de.

Delegated Signer

public key

Delegation

Zone lrz.de.

129.187.4.40

public key

private key

DNSSEC

DNS Anfrage

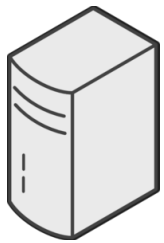
Client

Parentzone de.

Delegated Signer

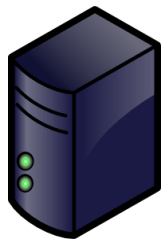
public key

Delegation



resolving nameserver

public key?



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

private key

DNSSEC

DNS Anfrage

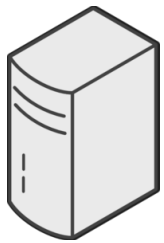
Client

Parentzone de.

Delegated Signer

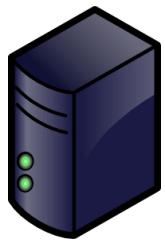
public key

Delegation



resolving nameserver

public key!



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

public key

private key

DNSSEC

DNS Anfrage

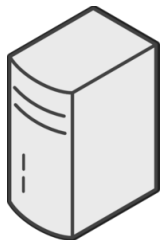
Client

Parentzone de.

Delegated Signer

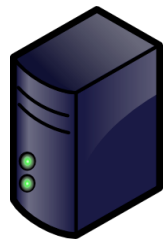
public key

Delegation



resolving nameserver

servicedesk.lrz.de?



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

public key

private key

DNSSEC

DNS Anfrage

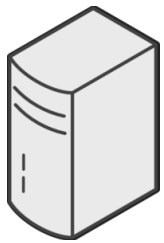
Client

Parentzone de.

Delegated Signer

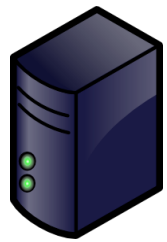
public key

Delegation



resolving nameserver

129.187.4.40



authoritative nameserver

Zone lrz.de.

129.187.4.40

public key

public key

private key

DNSSEC

DNS Anfrage

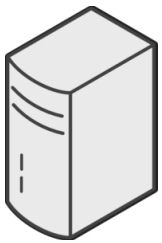
Client

Parentzone de.

Delegated Signer

public key

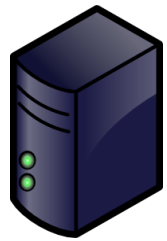
Delegation



resolving nameserver

129.187.4.40

public key



authoritative nameserver

public key

Zone lrz.de.

129.187.4.40

private key

DNSSEC

DNS Anfrage

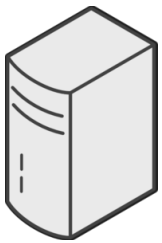
Client

Parentzone de.

Delegated Signer

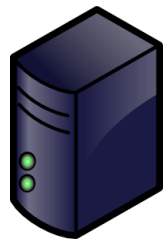
public key

Delegation



resolving nameserver

129.187.4.40



authoritative nameserver

Zone lrz.de.

129.187.4.40

Hash

public key

public key

private key

DNSSEC

DNS Anfrage

Client

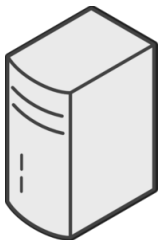
Parentzone de.

Delegated Signer

public key

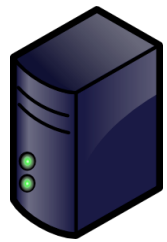
Delegation

= ?



resolving nameserver

129.187.4.40



authoritative nameserver

Zone lrz.de.

129.187.4.40

Hash

public key

public key

private key

DNSSEC Authenticated Data

Client

AD Flag

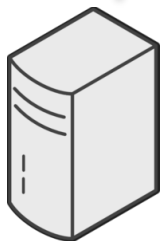
129.187.4.40

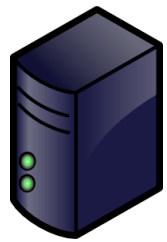
Parentzone de.

Delegated Signer

public key

Delegation





Zone lrz.de.

129.187.4.40

= !

resolving nameserver

authoritative nameserver

129.187.4.40

Hash

public key

public key

private key

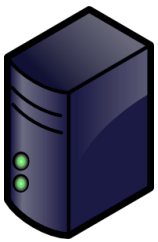
DANE - Was ist das?

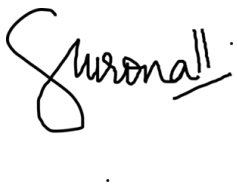
- “**D**omain name system based **A**uthenticated **N**amed **E**ntity”
- Einer Entität kann ein Zertifikat authentisch zugeordnet werden
- DNSSEC garantiert Authentizität für einen Eintrag auf DNS
- TLSA = „TLS certificate association“: Zertifikatshash im DNS
- Public Key erlaubt Verifizierung dieses Hashes über den DNS

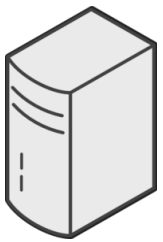
DANE - Probleme der CA-Zertifizierung

- TLS: Authentifikation über Zertifikatskette
- Root-CA-Zertifkate müssen vorgehalten werden
- Root-CAs stellten oftmals falsche Zertifikate aus (Diginotar, Wosign, Startcom …)

- DANE liegt in der Hand des Zonenbetreibers eines Nameservers
- DNS muss sowieso vertraut werden
- DNSSEC authentifiziert dieses Vertrauen







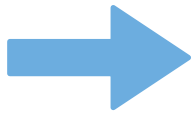
DNS → TLSA + RRSIG → Zertifikat → Server

DANE - Vorteile für den SMTP-Mailversand

- TLS-Zertifikate oft nicht verifizierbar oder abgelaufen
- DANE/TLSA-Eintrag im DNS einfacher zu verwalten
- Downgrade-Attacken können verhindert werden
  TLS über DANE verbindlich vorzuschreiben
- Zertifikate können schnell zurück gezogen werden

Herausforderungen bei der Einführung im BHN

- Trotz Ihrer Vorteile für DNS, sind DNSSEC und DANE noch nicht weit verbreitet…
- Administratoren fürchten Ausfälle bei der Umstellung wichtiger Services wie DNS und Email
- Universitäten und Hochschulen sind eigenständig, nutzen verschiedenste Systeme für DNS und Mailverkehr
- keine Lösung „ein System für alle“
- bisher noch kein so großes Projekt auf Landesebene

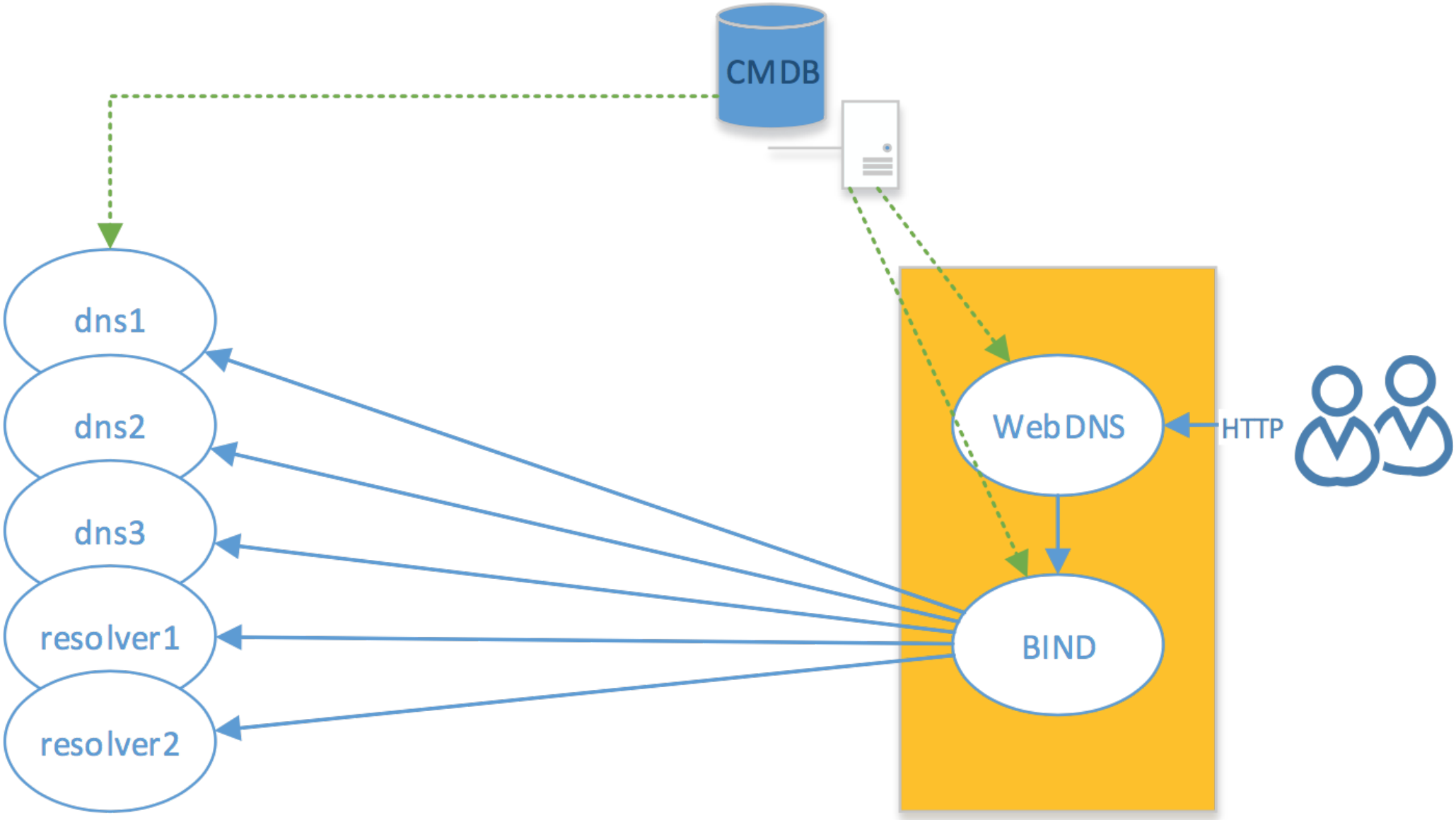


Förderung durch das Bayerische Forschungsministerium

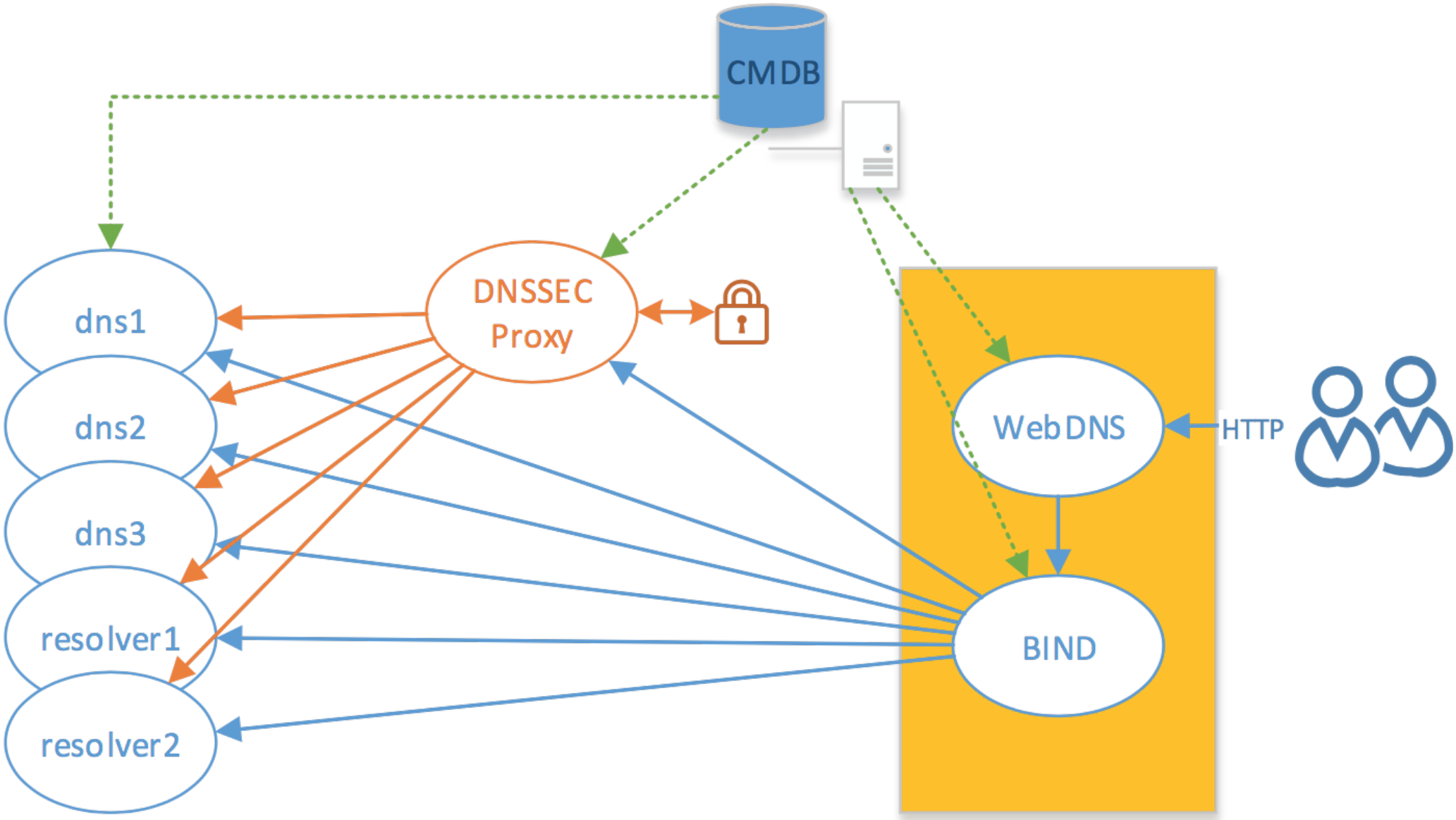
Unterstützung und Lösungen durch das LRZ

- Wiki mit Grundlagen und anwendungsbezogene Anleitungen
- Kurse für Administratoren mit Übungen
- Erarbeitung eines Konzepts zur nahtlosen Integration in bestehende DNS-Verwaltung
- Direkte Ansprechpartner am LRZ
- Unterstützung bei der Konfiguration vor Ort
- Monitoring der DNSSEC/DANE-Verifizierung

DNSSEC Signing Proxy und DNS-Verwaltung



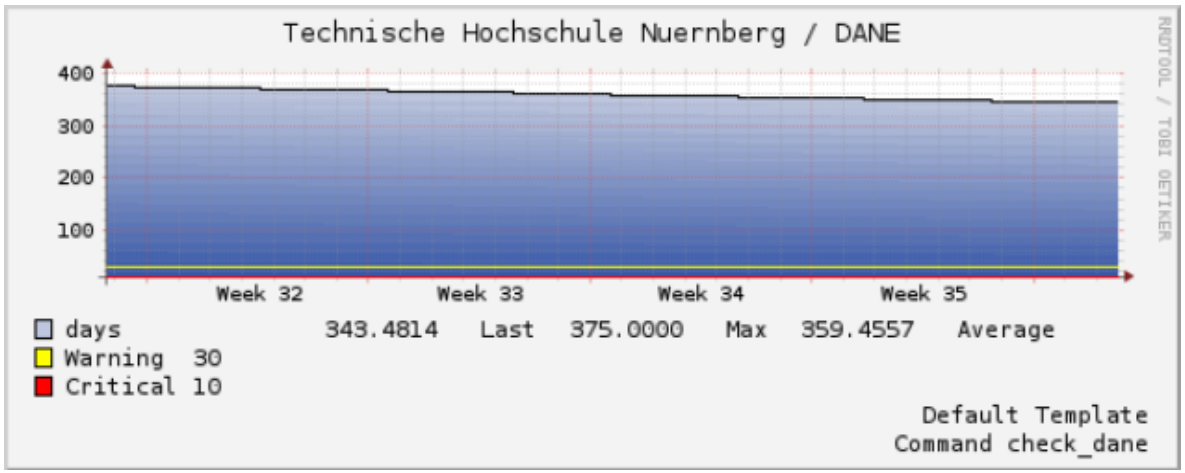
DNSSEC Signing Proxy und DNS-Verwaltung



Monitoring der Haupt- / Emaildomänen

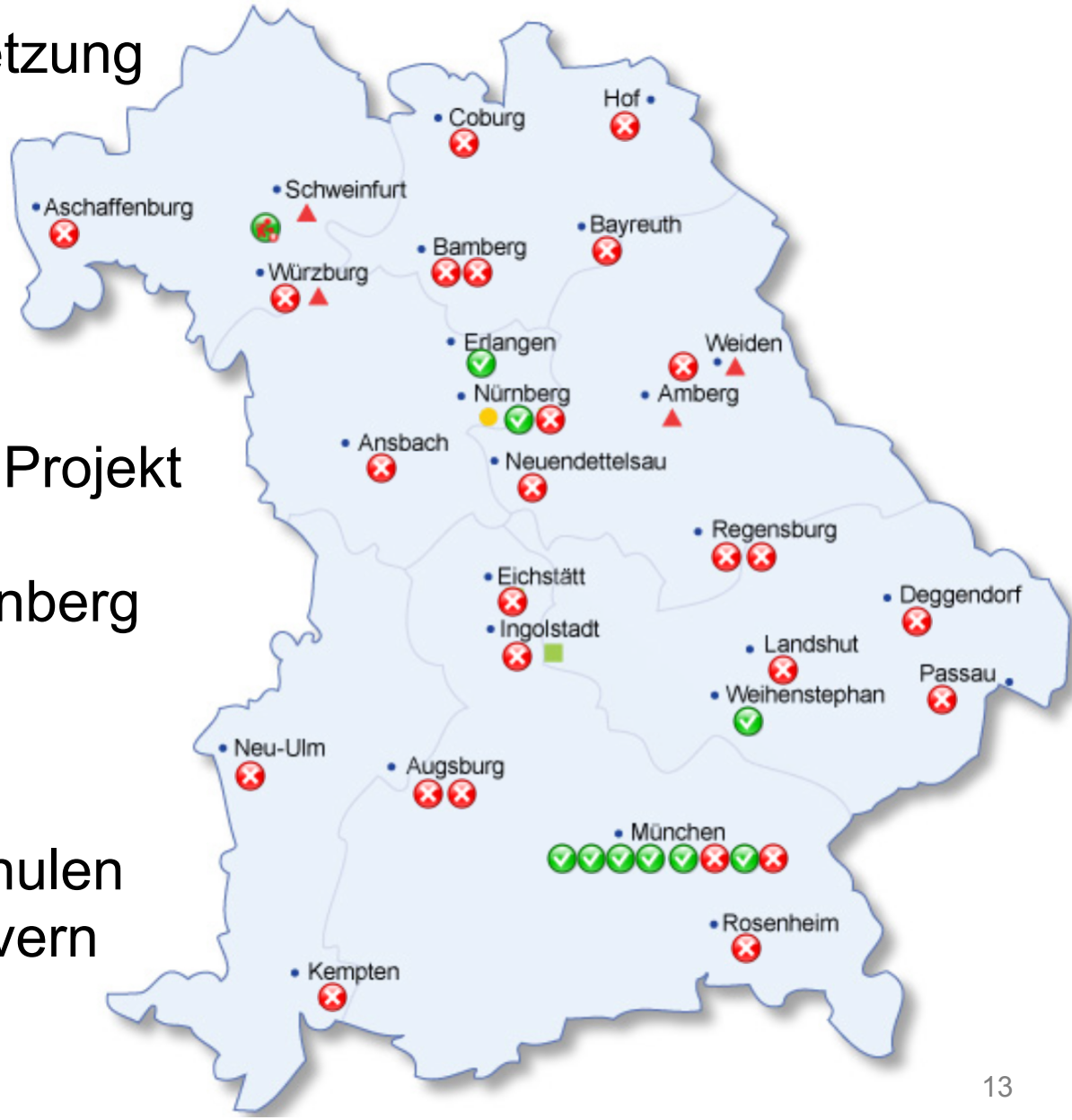
DNSSEC DS 2	OK	03-20-2017 12:38:46	11d 2h 22m 11s	1/5	KSK 56155 found in DS RRsets of parent.	
DNSSEC Keys	OK	03-20-2017 12:38:48	11d 5h 5m 52s	1/5	KSK: 56155 ZSK: 36246	
DNSSEC-ldns	WARNING	03-20-2017 12:38:46	11d 2h 25m 11s	1/5 (#538)	Error: DNSSEC signature will expire too soon for ws07.ws.dnssec.bayern. NS	

- Icinga2-basiert, mit open source oder selbst geschriebenen Checkskripten
- Zeitnahe Benachrichtigung der Administratoren
- Historie von DNSSEC/DANE-Ausfällen



DANE-Unterstützung (Stand 06.09.2017)

Bis jetzt nur zögerliche Umsetzung durch Administratoren:



- FAU eigenhändig schon vor Projekt
- Technische Hochschule Nürnberg
- HAW Würzburg-Schweinfurt
- 7 Universitäten und Hochschulen auf LRZ Name- und Mailservern

Probleme und Lösungen

Probleme…

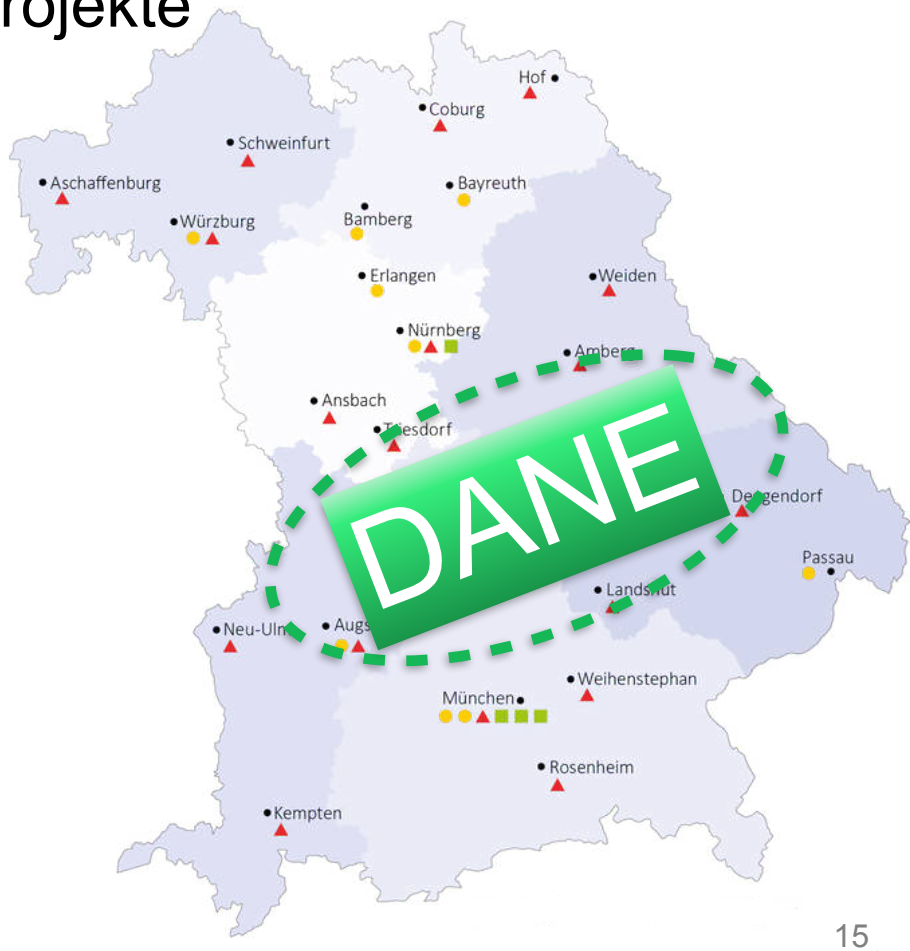
- andere Projekte derzeit wichtiger
- keine „manpower“ / Mitarbeiterwechsel
- geplante Umstellung / Hardwareersetzung der Nameserver / Mailserver
- Umstellung der Software nötig
- Mail-Appliances unterstützen kein ausgehendes DANE

Lösungen

- genannte Zeitpläne Ende 2017 / Anfang 2018…
- 2 Hochschulen wünschen Unterstützung vor Ort
- Postfix-basierter Mailrelayserver nach Mail-Appliances
- LRZ-Nameserver als Slave, DNSSEC-Signierung und kein eigener öffentlicher Master mehr

Fazit

- Unterstützung durch LRZ wird gern gesehen
- Fehlende Ressourcen und andere Projekte sind das größte Problem, das einer zügigen Einführung im Wege steht
- Probleme sind nicht technischer, sondern vor allem organisatorischer Art



Vielen Dank für Ihre Aufmerksamkeit! Fragen?