OpenDNSSEC

Folien basieren auf Material des OpenDNSSEC Projekt Team

MEN&MICE

OpenDNSSEC - Wer

- Roy Arends
- Rickard Bellgrim
- Alex Dalitz
- John A Dickinson
- Jelte Jansen
- Sion Lloyd
- Matthijs Mekking
- Stephen Morris
- Jakob Schlyter
- Patrik Wallström

OpenDNSSEC - Was

- OpenDNSSEC ist ein “DNSSEC Zone-signing” System welches den Prozess der Schlüsselverwaltung und der Zonen-Signierung automatisiert.

- DNSSEC auf Knopfdruck!

OpenDNSSEC - Ziele

- DNSSEC sollte einfach einzurichten sein
- die Anzahl der DNSSEC Benutzer erhöhen
- Erfahrungen von DNSSEC Installationen einbringen
- Automatisierte Schlüssel-Verwaltung
- Hardware Beschleunigung

OpenDNSSEC - Ziele - 2

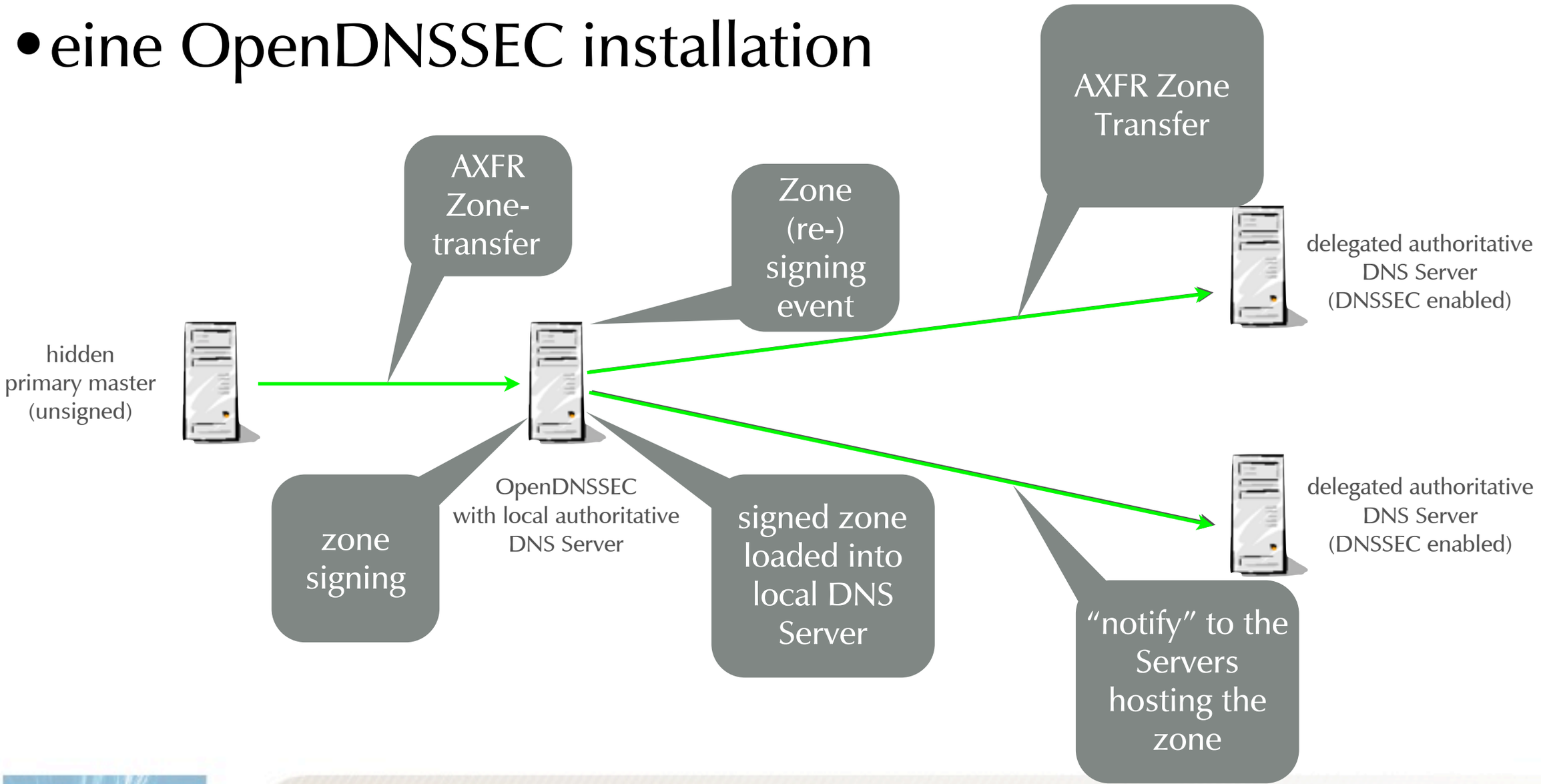
- OpenSource Software unter einer BSD Lizenz

- Einfach in eine bestehende DNS Infrastruktur einzubringen

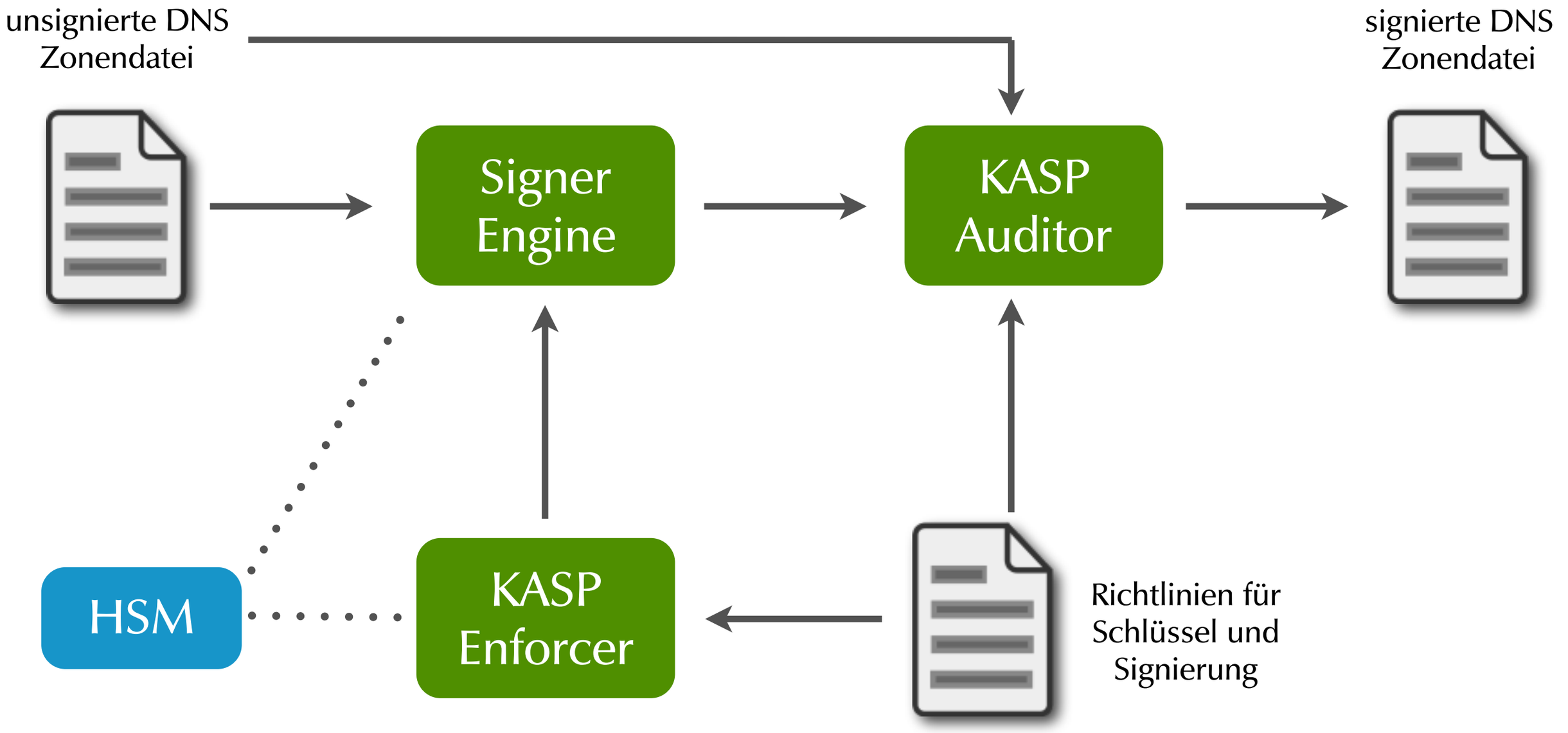
- Schlüssel-Speicherung und Hardware-Beschleunigung in Hardware mittels der PKCS#11 API

Bump-in-the-Wire

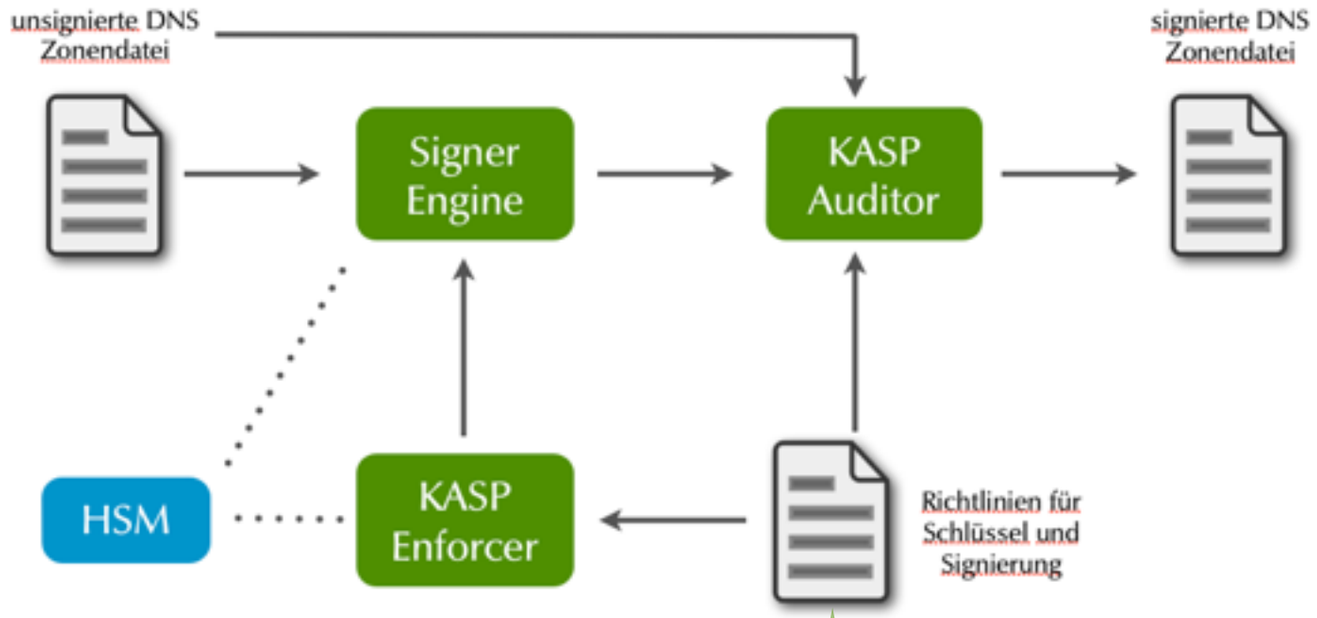
- eine OpenDNSSEC installation



Architektur

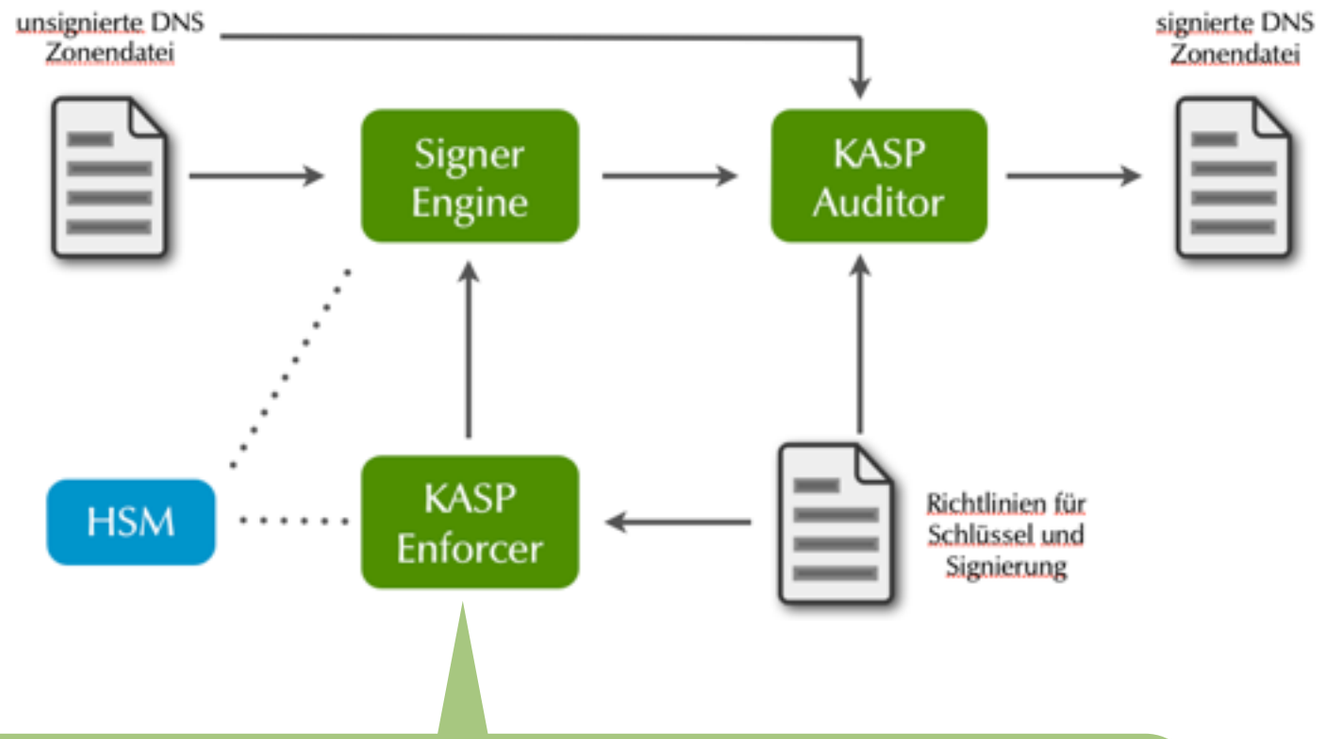


Richtlinien (Policy)



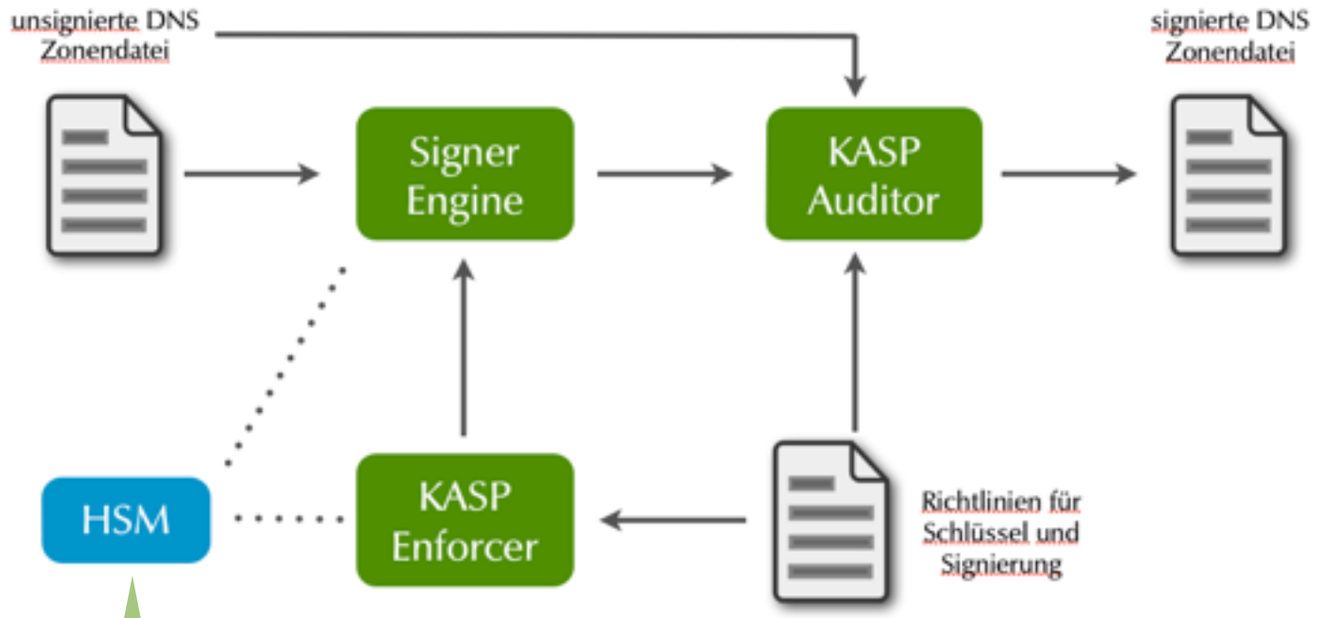
- Parameter des Zone-Signing
  - Schlüssellängen, Gültigkeit der Schlüssel und Signaturen
  - Algorithmus
  - NSEC/NSEC3

KASP Enforcer



- Erstellt Schlüssel im HSM
- Schlüssel-Wechsel (Key-Rolling)
- Wählt Schlüssel für Zone

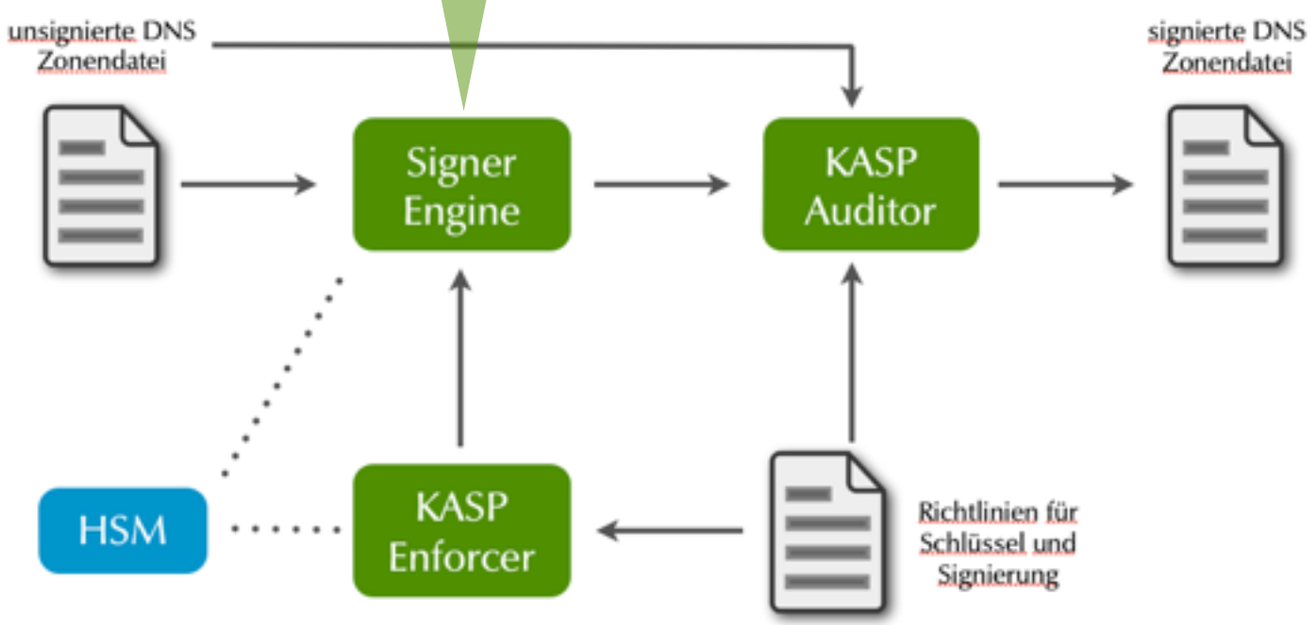
Hardware Security Module (HSM)



- Speichert die Schlüssel
- Hardware-Unterstützung des Signierens
- benutzt PKCS#11 API
- OpenDNSSEC kommt mit einer Software HSM Emulation - SoftHSM

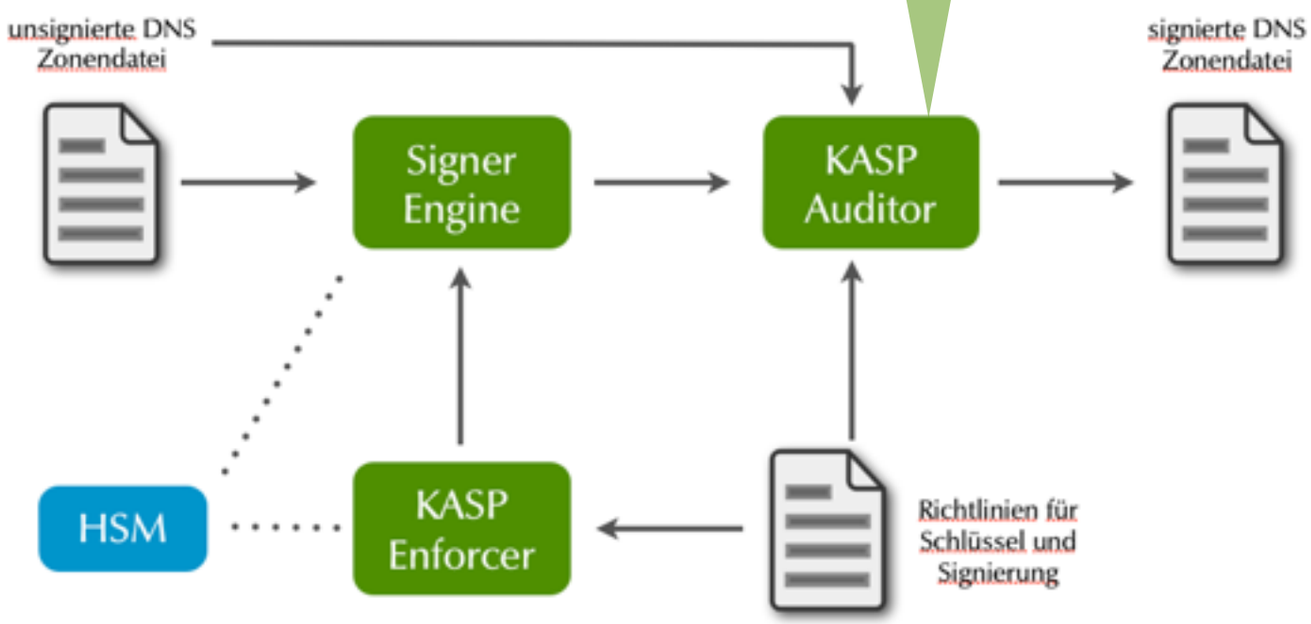
Signer Engine

- Automatisches signieren der Zonen
  - kann Signaturen wiederverwenden (wenn nicht zu alt)
  - kann die Gültigkeit der Signaturen über einen Zeitraum strecken (Jitter)
- Verwaltet NSEC/NSEC3 Einträge
- Aktualisiert SOA Serien-Nummer

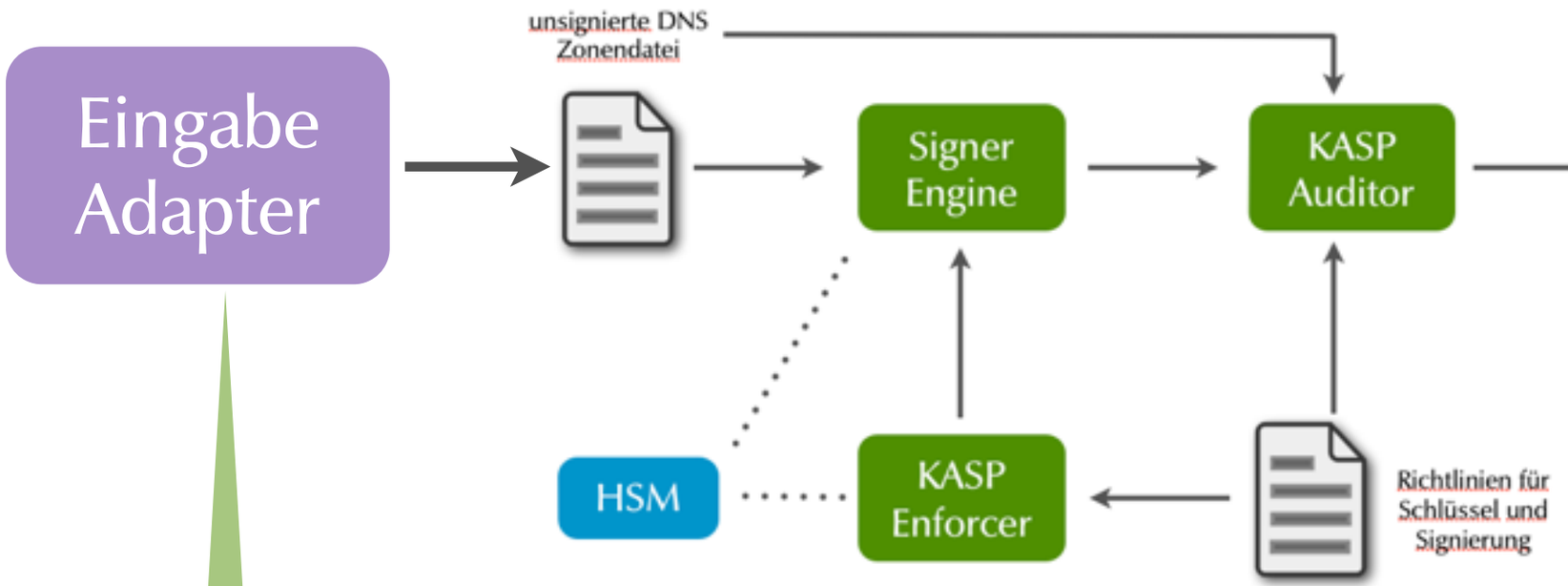


KASP Auditor

- prüft die signierte Zone anhand der Ursprungsdatei und der Richtline
- Kann die Auslieferung der Zone stoppen, wenn Unregelmäßigkeiten erkannt werden
- Wir von anderen Programmierern in einer anderen Programmiersprache entwickelt

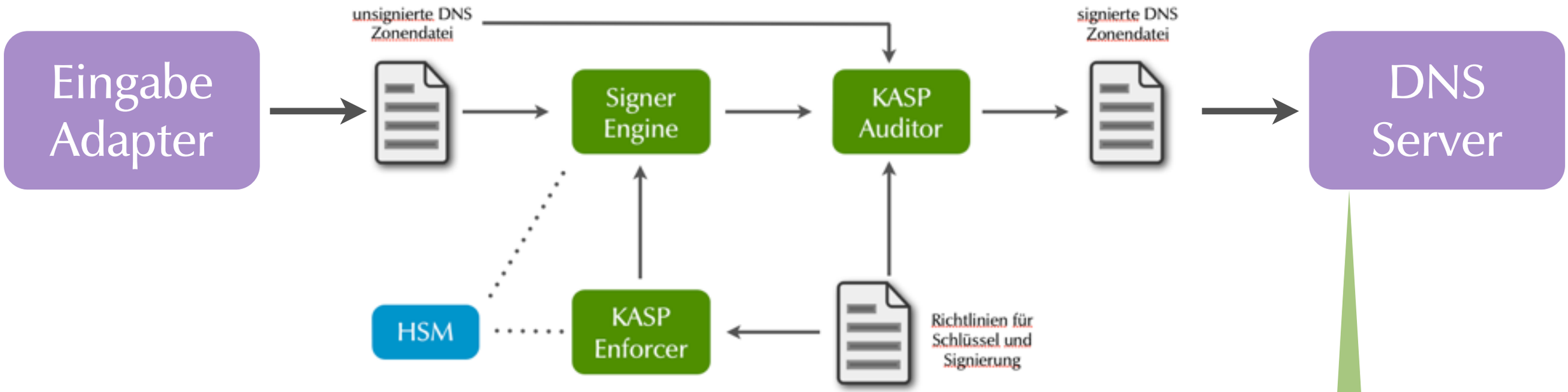


Eingabe



- holt Zonendaten per Zonentransfer
- reagiert auf DNS Notify

Ausgabe



- beliebiger authorativer DNS Server kann benutzt werden
  - BIND, NSD, Windows DNS
- alternativ kann ein Script ausgeführt werden

wer benutzt OpenDNSSEC

- .se
- .uk
- .dk
- Compricer AB
- ICANN
- YASK AB
- SurfNET
- 75% der ccTLDs in Europa planen den Einsatz von OpenDNSSEC (laut Umfrage unter den ccTLD Betreibern)

Status

- 1.0 alpha - Juli 2009
- 1.0 beta - Oktober 2009
- 1.0 - Februar 2010
- 1.1- Mai 2010
- 1.2 - Dezember 2010 (Release Candidate verfügbar)
- Release plan
  - Version 2.0 - 2011

Version 1.2

- Signer Engine nun in C implementiert (vorher Python)
  - schneller, keine Abhängigkeiten zu Python mehr
- Signer Statistiken
- gemeinsame Benutzung von Schlüsseln in verschiedenen Zonen verbessert
- verbesserte MySQL Unterstützung

Plan für Version 2.0

- Zone transfers mit IXFR und dynamischen Updates
- “Continuous signing”
- Powerfail/crash recovery
- Web interface

OpenDNSSEC Unterstützung in der Men & Mice Suite

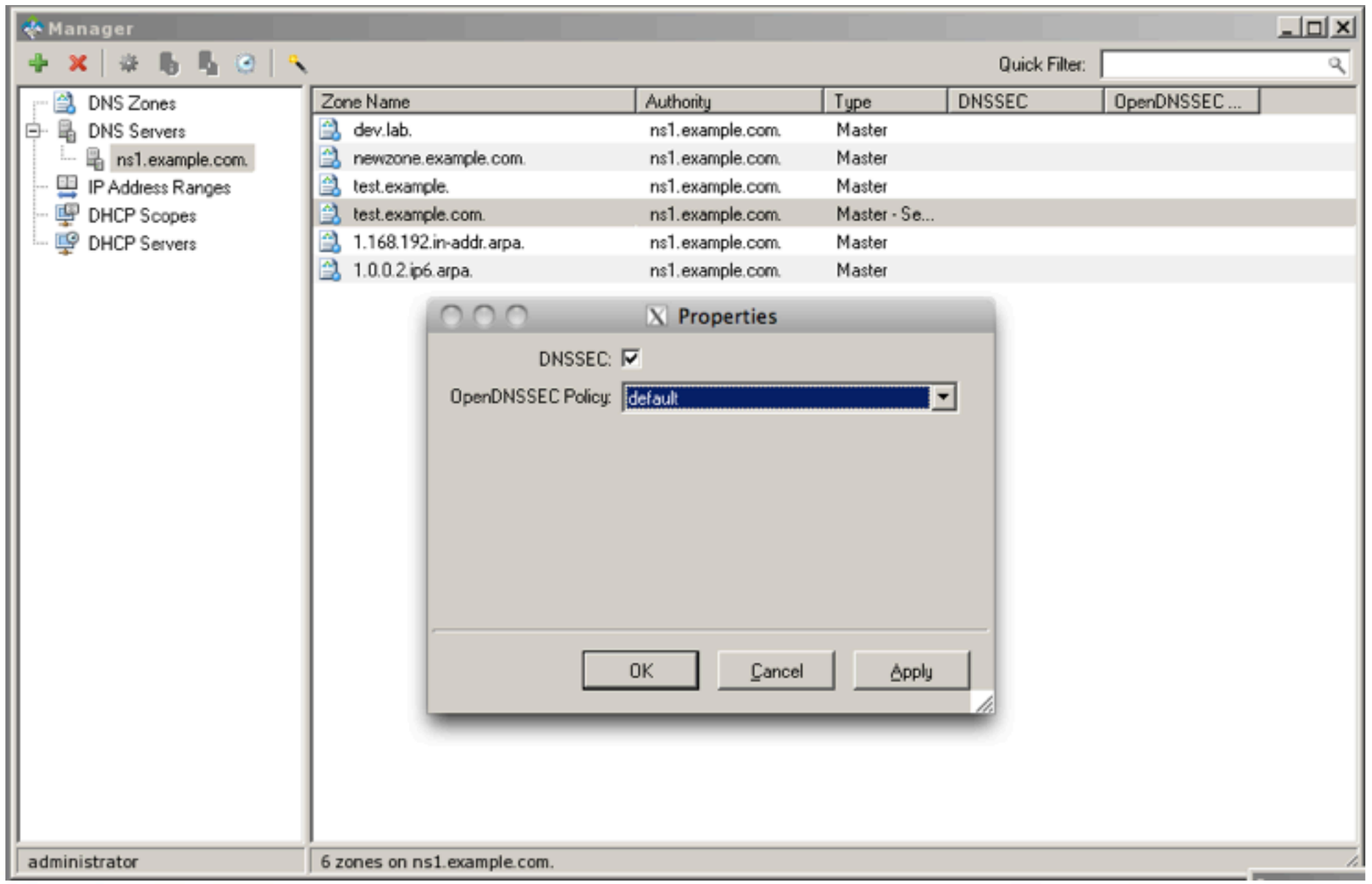
Men & Mice Suite

- Die Men & Mice Suite ist eine Overlay DNS Verwaltungssoftware
  - BIND und Microsoft DNS
  - Linux, Solaris, MacOS X, Windows Server, FreeBSD
- Windows GUI, Web-Interface (AJAX), Kommandozeilen API und SOAP API

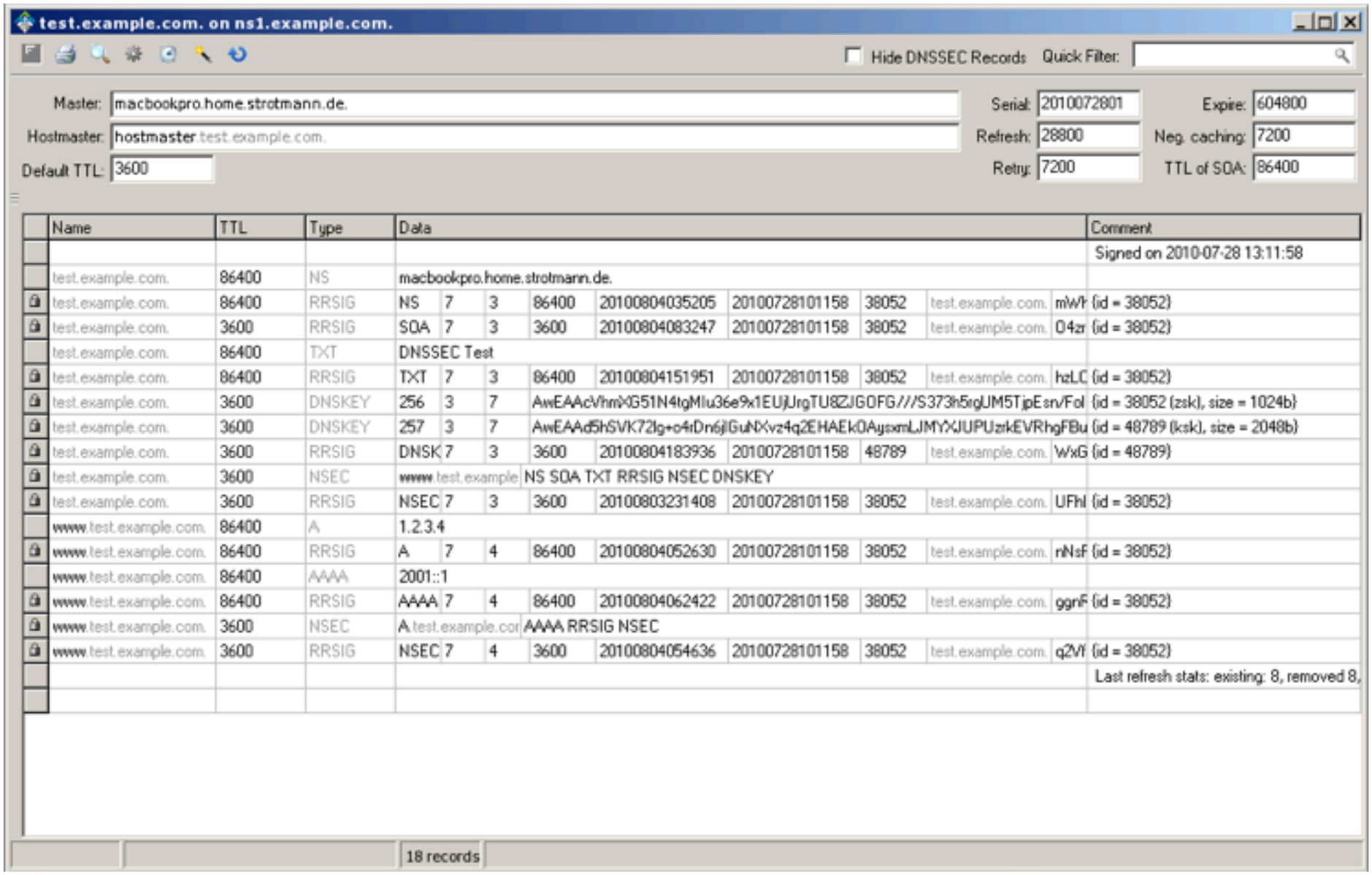
Men & Mice Suite und DNSSEC

- flexibler Plug-In Mechanismus für DNSSEC Tools
  - **OpenDNSSEC**
  - Secure64 DNS Signer
  - BIND 9.7.x+
  - Windows DNS in 2008R2

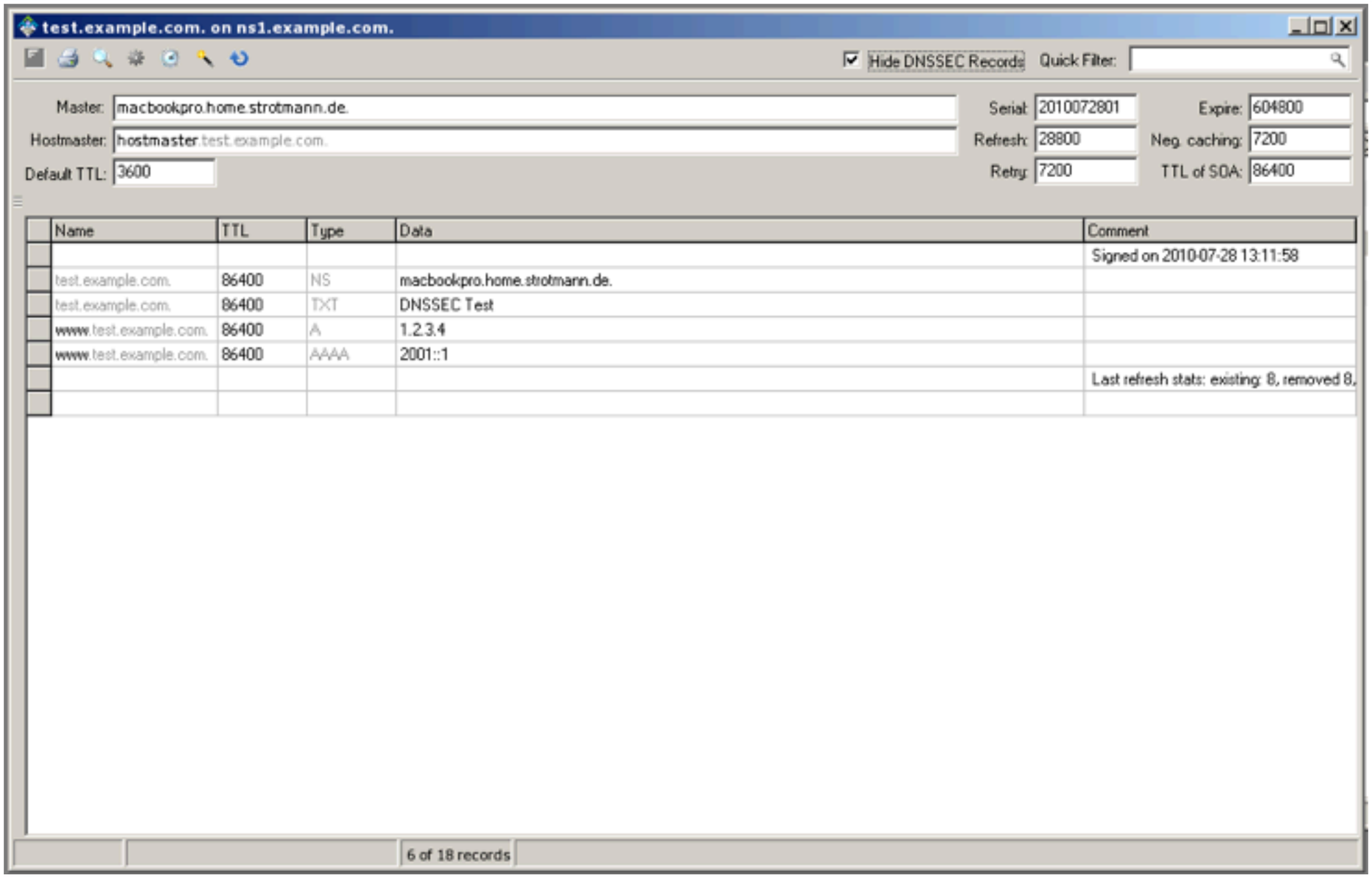
Men & Mice Suite und DNSSEC



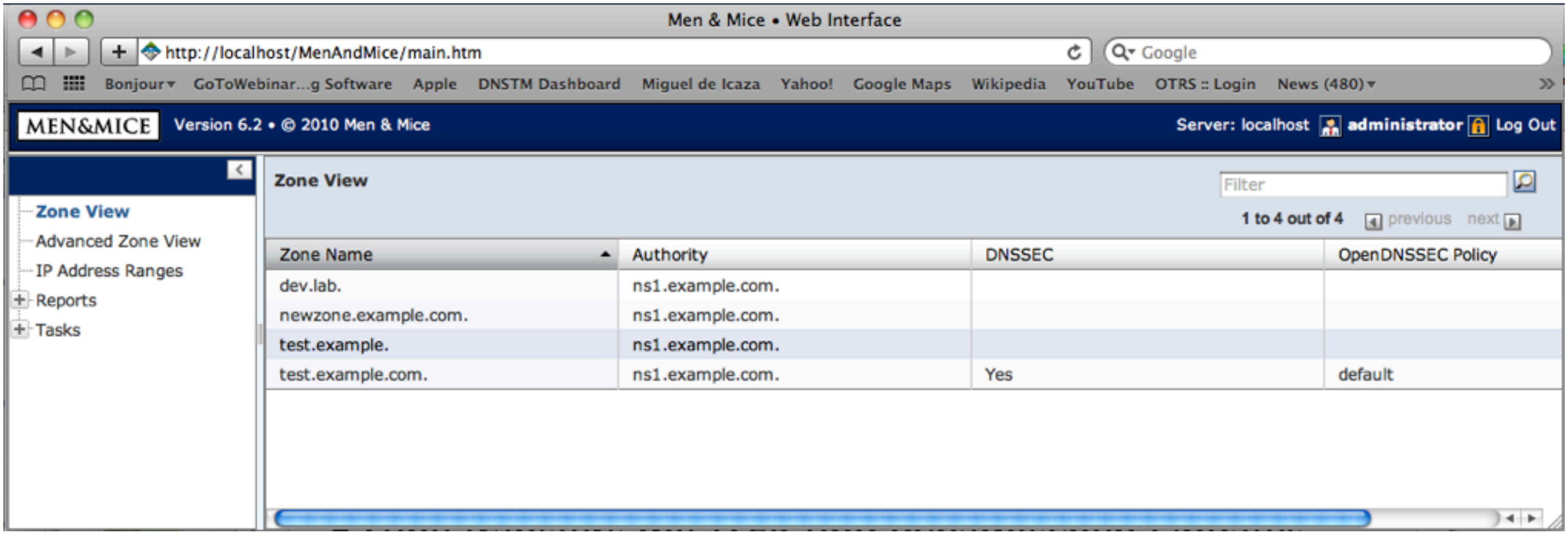
Men & Mice Suite und DNSSEC



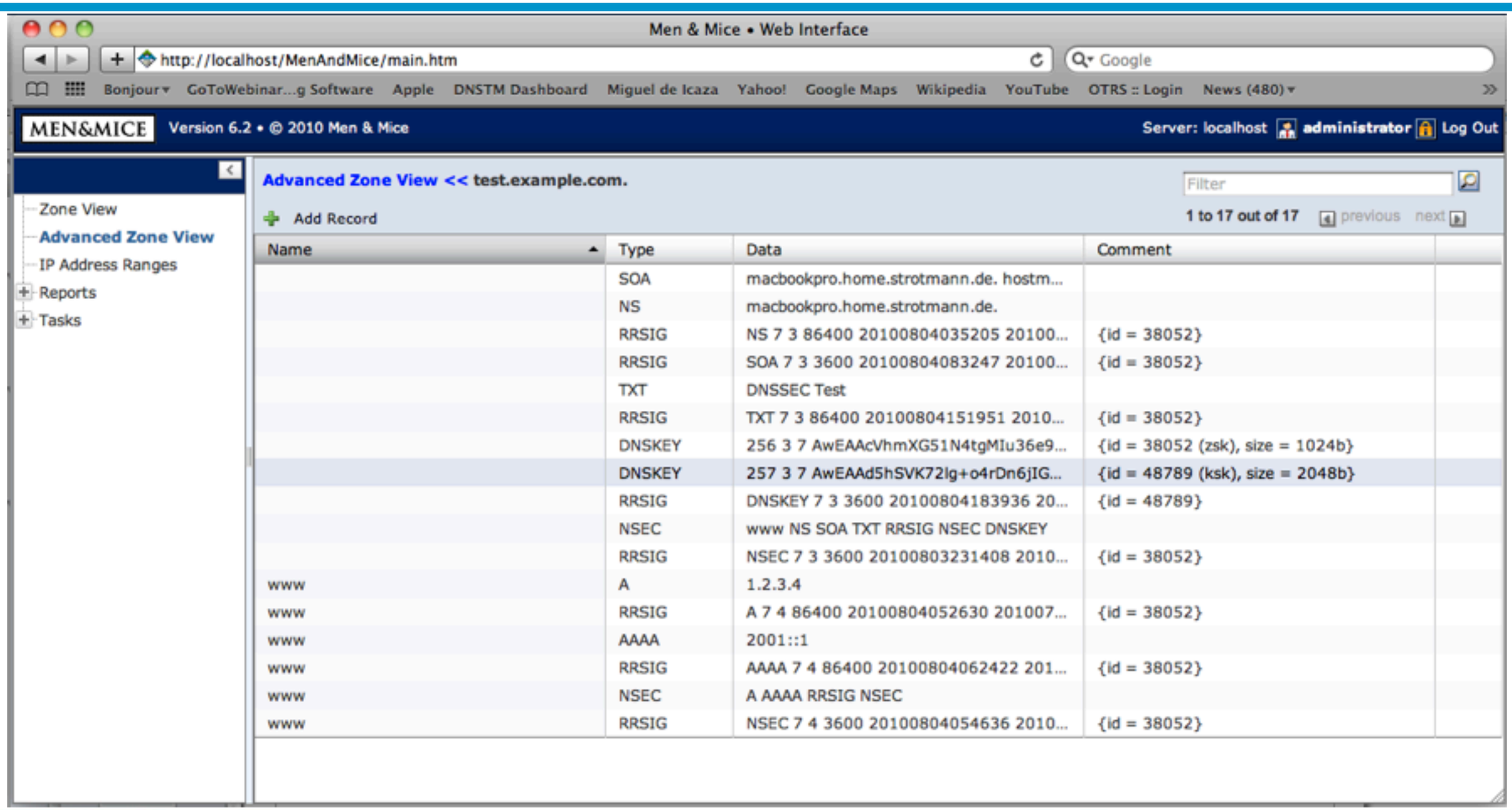
Men & Mice Suite und DNSSEC



Men & Mice Suite und DNSSEC



Men & Mice Suite und DNSSEC

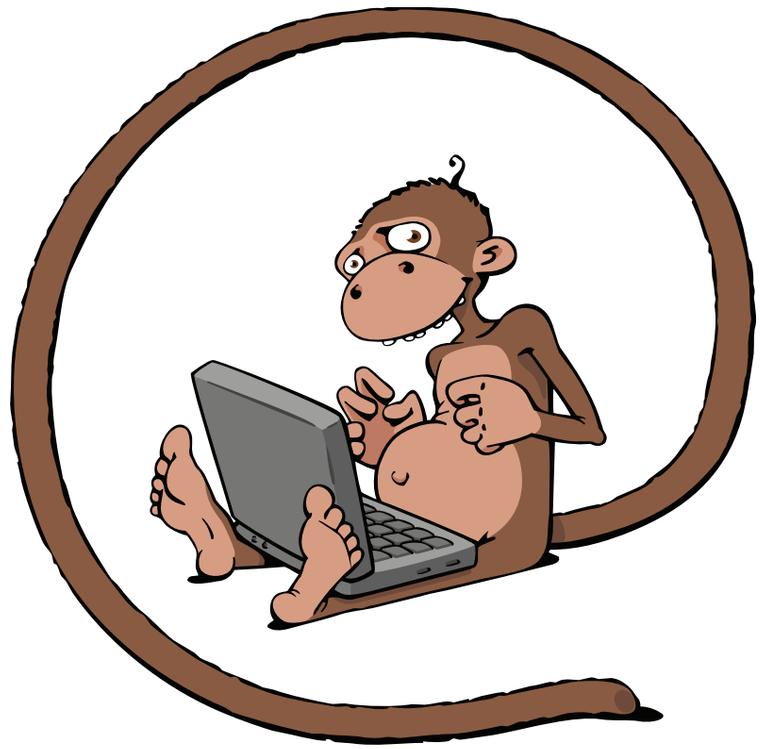


Fragen?

Kontakt:

OpenDNSSEC: www.opendnssec.org

Men & Mice: www.menandmice.com
sales@menandmice.com



Vielen Dank!

E-Mail:
carsten@menandmice.com

MEN&MICE