



OpenDNSSEC

Folien basieren auf Material des OpenDNSSEC Projekt Team



MEN&MICE

© Men & Mice <http://menandmice.com>

OpenDNSSEC - Wer

nominet

kirei

NLnet
Labs

.se

sinodun

SURF
NET

SIDN

- 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

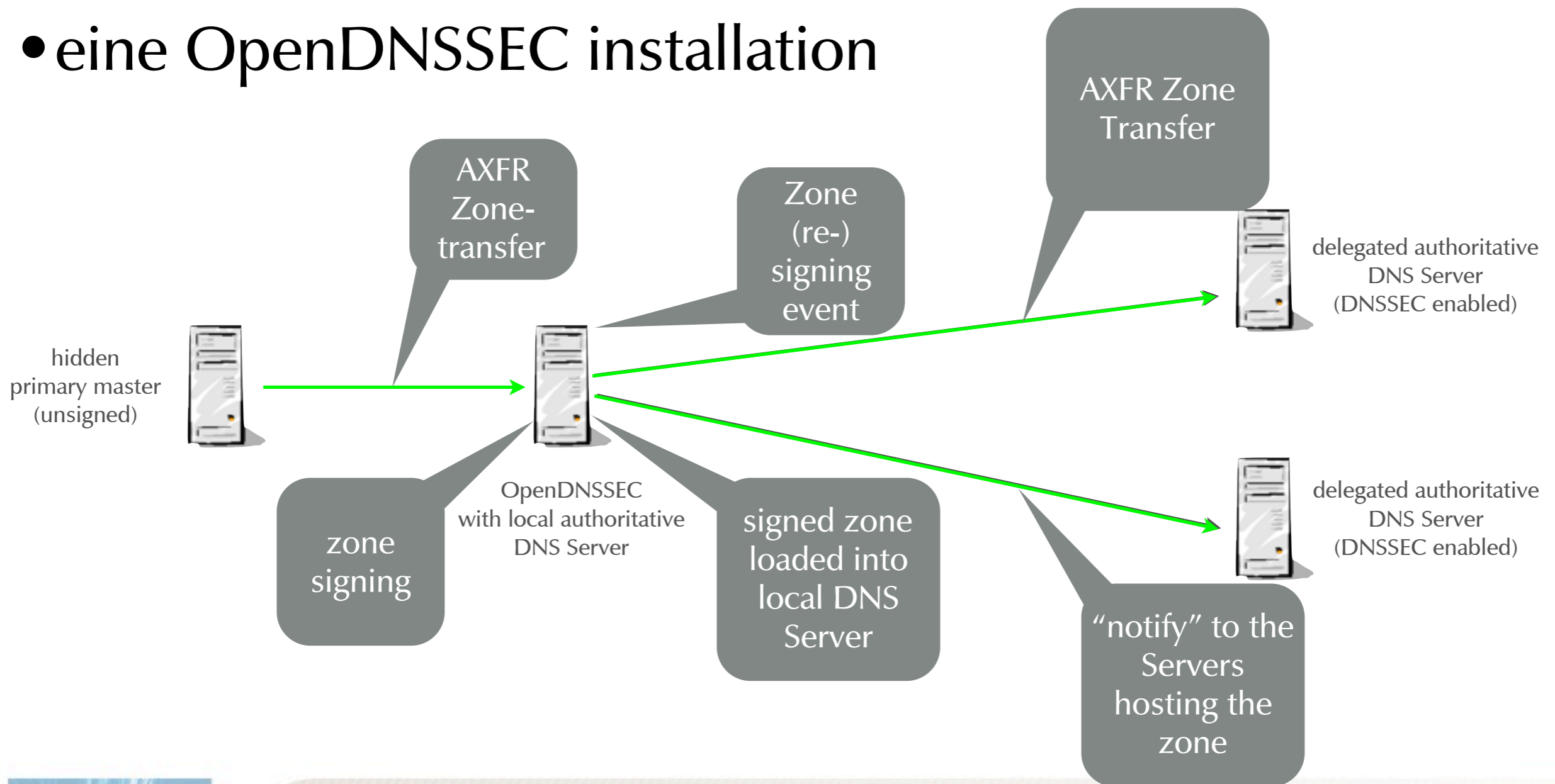
- DNSSEC sollte einfach einzurichten sein
- die Anzahl der DNSSEC Benutzer erhöhen
- Erfahrungen von DNSSEC Installationen einbringen
- Automatisierte Schlüssel-Verwaltung
- Hardware Beschleunigung

OpenDNSSEC - Ziele - 2

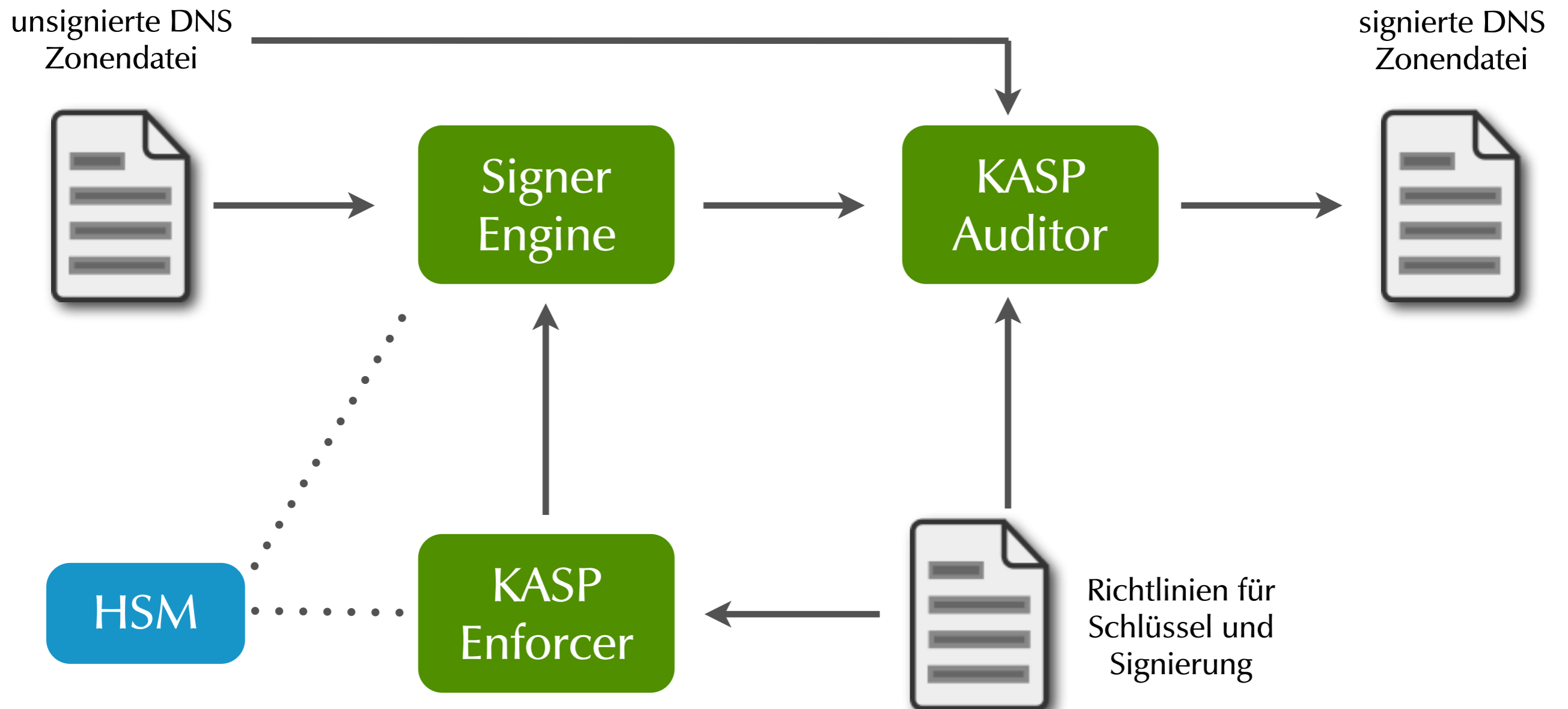
- OpenSource Software unter einer BSD Lizenz
- Einfach in eine bestehende DNS Infrastruktur einzubringen
- Schlüssel-Speicherung und Hardware-Beschleunigung in Hardware mittels der PKCS#11 API

Bump-in-the-Wire

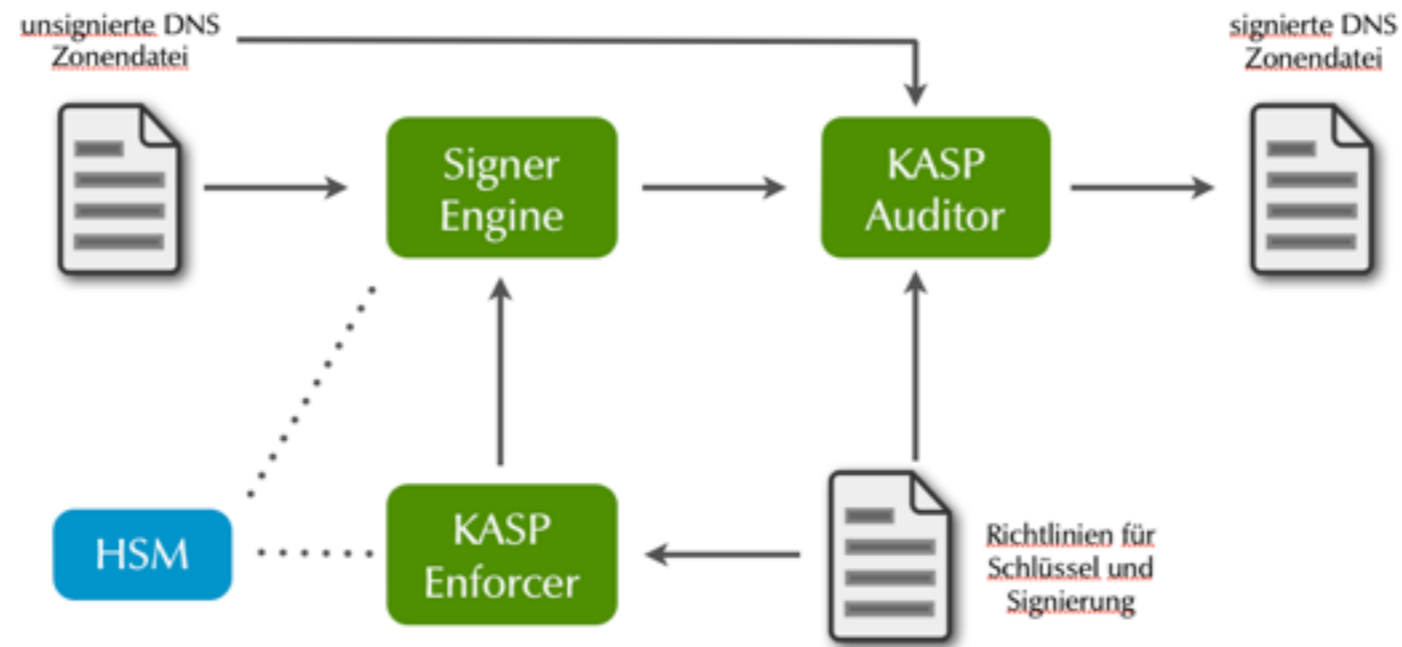
- eine OpenDNSSEC installation



Architektur

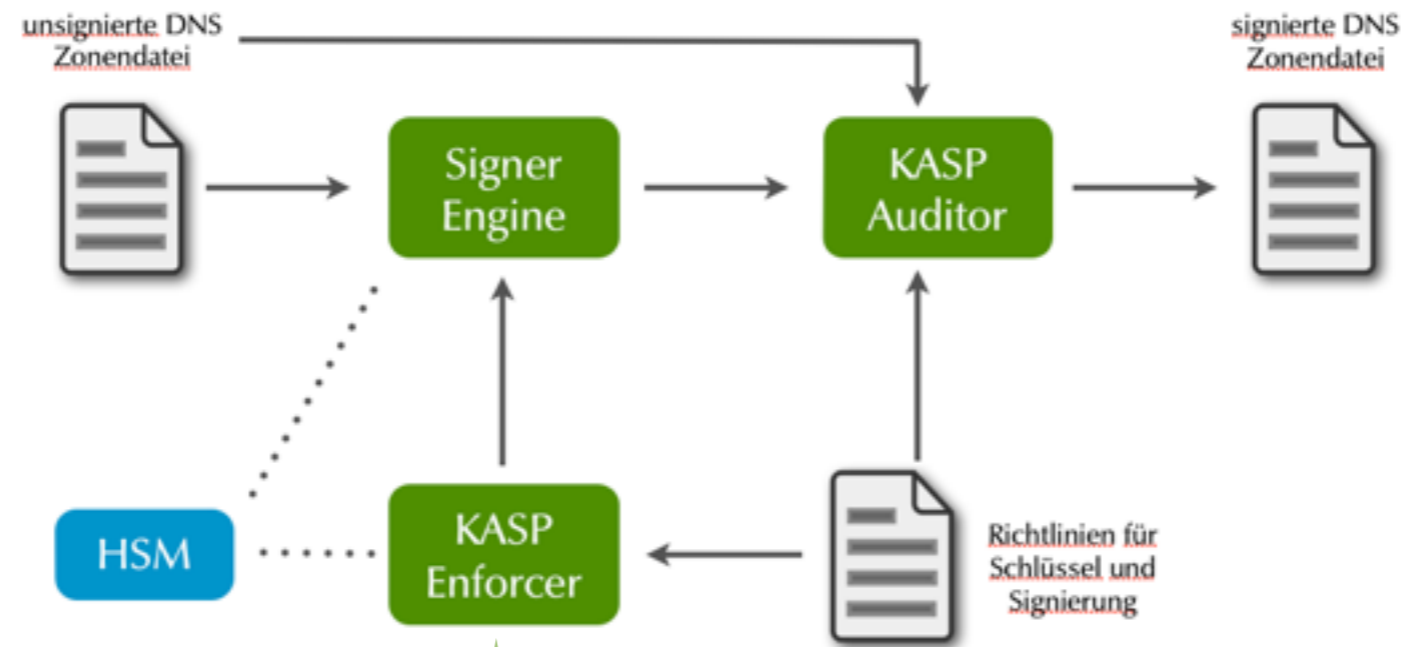


Richtlinien (Policy)



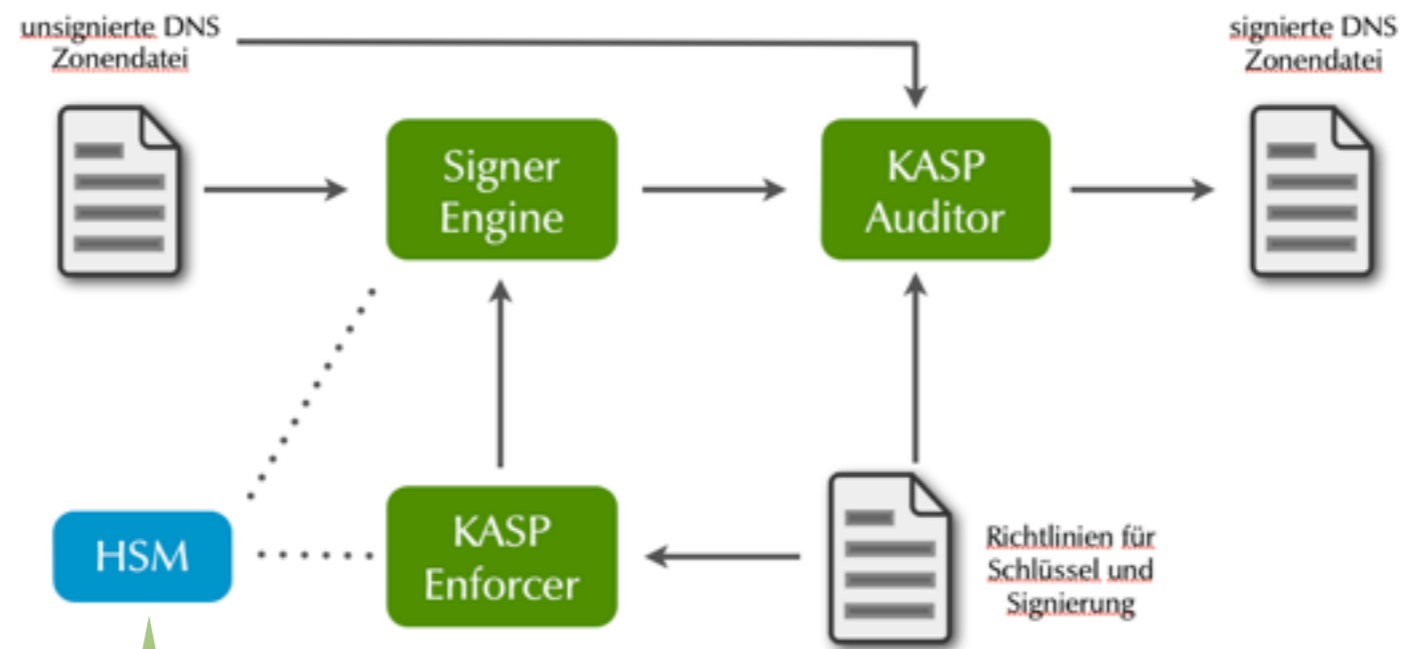
- Parameter des Zone-Signing
 - Schlüssellängen, Gültigkeit der Schlüssel und Signaturen
 - Algorithmus
 - NSEC/NSEC3

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

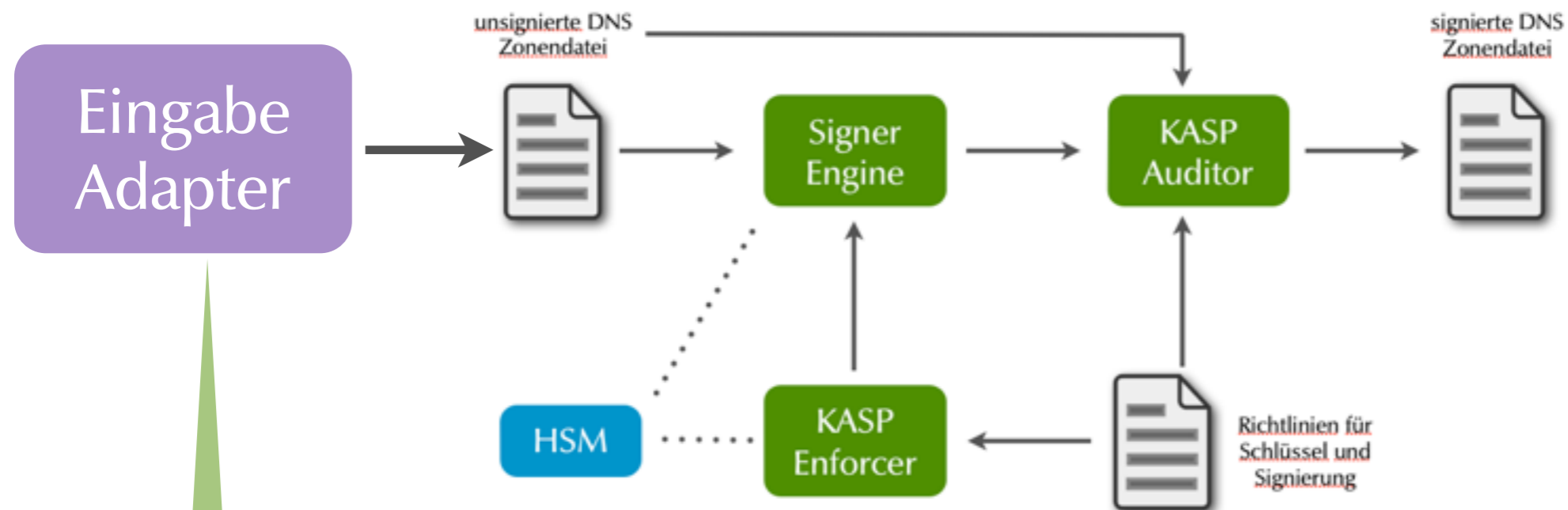


KASP Auditor

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

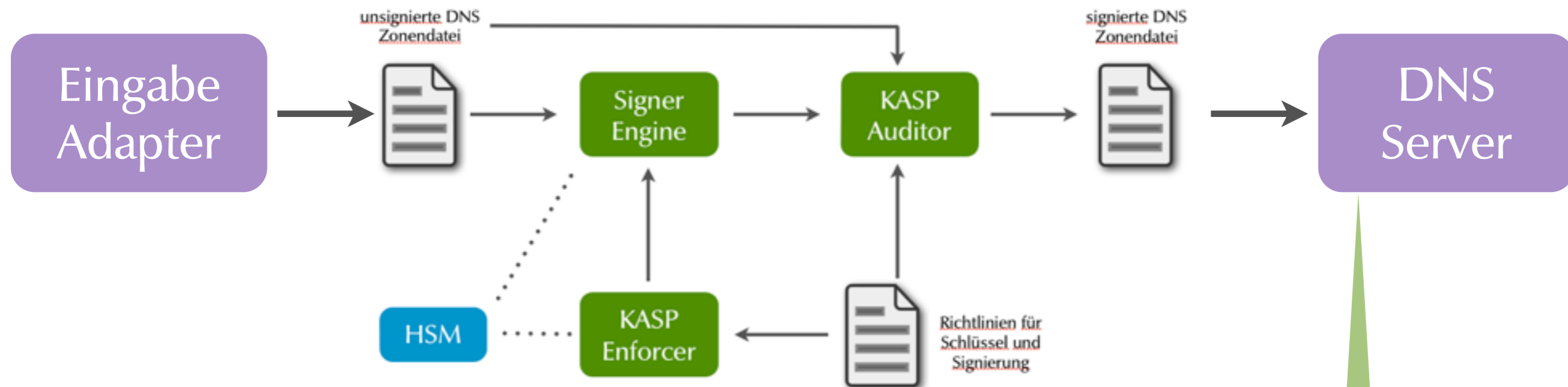


Eingabe



- holt Zonendaten per Zonentransfer
- reagiert auf DNS Notify

Ausgabe



- beliebiger authoritativer 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

© Men & Mice <http://menandmice.com>

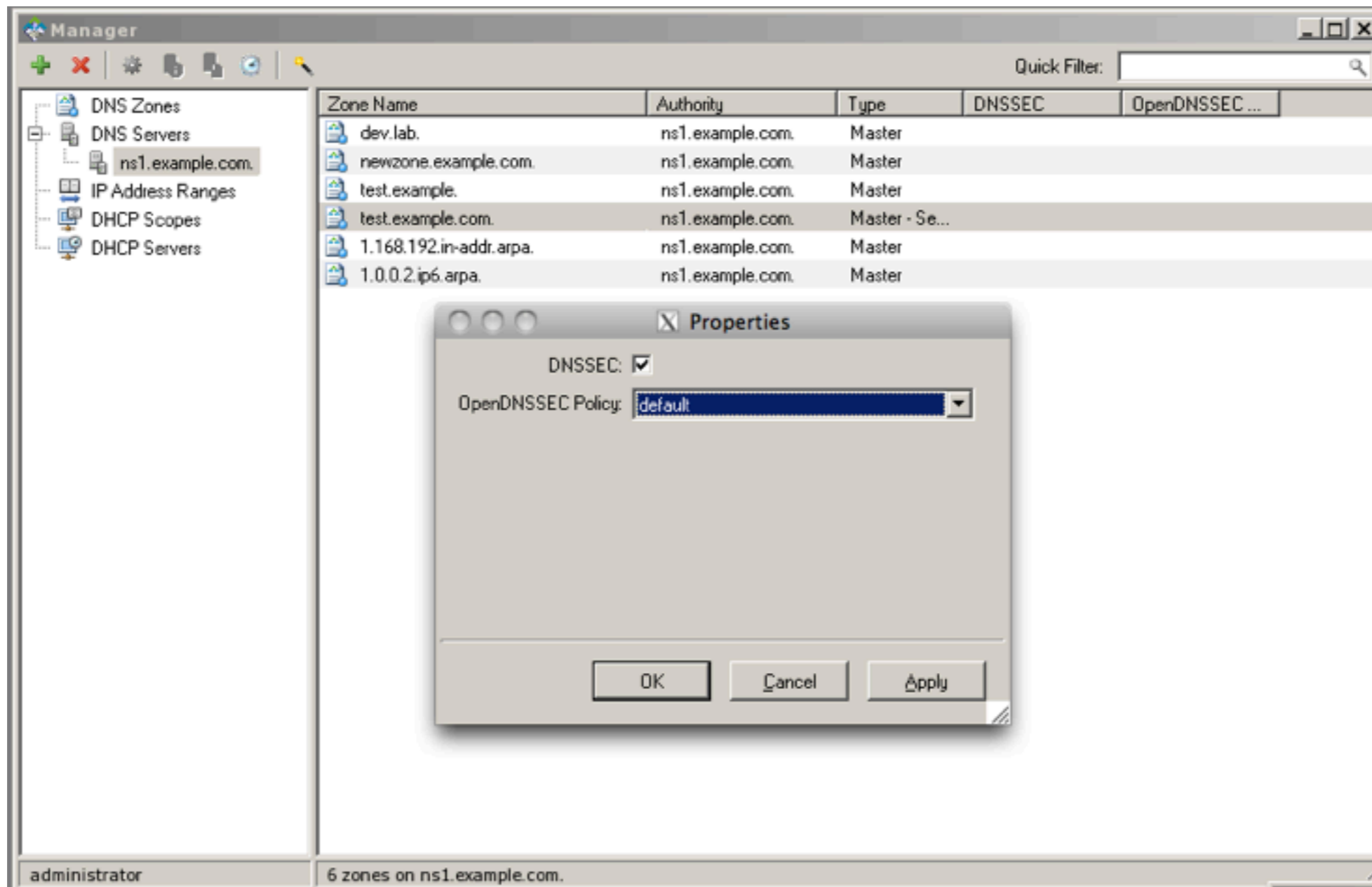
Men & Mice Suite

- 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

test.example.com. on ns1.example.com.

Master: macbookpro.home.strotmann.de. Serial: 2010072801 Expire: 604800
 Hostmaster: hostmaster.test.example.com. Refresh: 28800 Neg. caching: 7200
 Default TTL: 3600 Retry: 7200 TTL of SOA: 86400

Name	TTL	Type	Data	Comment
				Signed on 2010-07-28 13:11:58
test.example.com.	86400	NS	macbookpro.home.strotmann.de.	
test.example.com.	86400	RRSIG	NS 7 3 86400 20100804035205 20100728101158 38052 test.example.com.	mWf (id = 38052)
test.example.com.	3600	RRSIG	SOA 7 3 3600 20100804083247 20100728101158 38052 test.example.com.	04zr (id = 38052)
test.example.com.	86400	TXT	DNSSEC Test	
test.example.com.	86400	RRSIG	TXT 7 3 86400 20100804151951 20100728101158 38052 test.example.com.	hzLC (id = 38052)
test.example.com.	3600	DNSKEY	256 3 7 AwEAAcVhmXG51N4tgMlu36e9x1EUJlrgTU8ZJG0FG///S373h5rgJM5TjpEsrV/Fol	(id = 38052 (zsk), size = 1024b)
test.example.com.	3600	DNSKEY	257 3 7 AwEAAAd5hSVK72lg+o4fDn6jGuhNkvz4q2EHAek0AysxmLJMYXJUPUzrkEVRhgFBu	(id = 48789 (ksk), size = 2048b)
test.example.com.	3600	RRSIG	DNSK 7 3 3600 20100804183936 20100728101158 48789 test.example.com.	WxG (id = 48789)
test.example.com.	3600	NSEC	www.test.example.com NS SOA TXT RRSIG NSEC DNSKEY	
test.example.com.	3600	RRSIG	NSEC 7 3 3600 20100803231408 20100728101158 38052 test.example.com.	UFHl (id = 38052)
www.test.example.com.	86400	A	1.2.3.4	
www.test.example.com.	86400	RRSIG	A 7 4 86400 20100804052630 20100728101158 38052 test.example.com.	rNsf (id = 38052)
www.test.example.com.	86400	AAAA	2001::1	
www.test.example.com.	86400	RRSIG	AAAA 7 4 86400 20100804062422 20100728101158 38052 test.example.com.	ggnF (id = 38052)
www.test.example.com.	3600	NSEC	A.test.example.com AAAA RRSIG NSEC	
www.test.example.com.	3600	RRSIG	NSEC 7 4 3600 20100804054636 20100728101158 38052 test.example.com.	q2Vf (id = 38052)
				Last refresh stats: existing: 8, removed 8,

18 records

Men & Mice Suite und DNSSEC

The screenshot shows the Men & Mice Suite interface for managing DNS records. The window title is "test.example.com. on ns1.example.com.". The interface includes a toolbar with icons for file operations and a "Hide DNSSEC Records" checkbox. Below the toolbar, there are input fields for "Master" (macbookpro.home.strotmann.de), "Hostmaster" (hostmaster.test.example.com), and "Default TTL" (3600). To the right, there are fields for "Serial" (2010072801), "Expire" (604800), "Refresh" (28800), "Neg. caching" (7200), "Retry" (7200), and "TTL of SOA" (86400). A table displays the following records:

Name	TTL	Type	Data	Comment
				Signed on 2010-07-28 13:11:58
test.example.com.	86400	NS	macbookpro.home.strotmann.de.	
test.example.com.	86400	TXT	DNSSEC Test	
www.test.example.com.	86400	A	1.2.3.4	
www.test.example.com.	86400	AAAA	2001::1	
				Last refresh stats: existing: 8, removed 8,

At the bottom of the window, it indicates "6 of 18 records".

Men & Mice Suite und DNSSEC

Men & Mice • Web Interface

http://localhost/MenAndMice/main.htm

MEN&MICE Version 6.2 • © 2010 Men & Mice

Server: localhost administrator Log Out

Zone View

Filter

1 to 4 out of 4 previous next

Zone Name	Authority	DNSSEC	OpenDNSSEC Policy
dev.lab.	ns1.example.com.		
newzone.example.com.	ns1.example.com.		
test.example.	ns1.example.com.		
test.example.com.	ns1.example.com.	Yes	default

Men & Mice Suite und DNSSEC

Men & Mice • Web Interface

http://localhost/MenAndMice/main.htm

MEN&MICE Version 6.2 • © 2010 Men & Mice Server: localhost administrator Log Out

Advanced Zone View << test.example.com. Filter

+ Add Record 1 to 17 out of 17 previous next

Name	Type	Data	Comment
	SOA	macbookpro.home.strotmann.de. hostm...	
	NS	macbookpro.home.strotmann.de.	
	RRSIG	NS 7 3 86400 20100804035205 20100...	{id = 38052}
	RRSIG	SOA 7 3 3600 20100804083247 20100...	{id = 38052}
	TXT	DNSSEC Test	
	RRSIG	TXT 7 3 86400 20100804151951 2010...	{id = 38052}
	DNSKEY	256 3 7 AwEAAcVhmXG51N4tgMIu36e9...	{id = 38052 (zsk), size = 1024b}
	DNSKEY	257 3 7 AwEAAAd5hSVK72lg+o4rDn6jIG...	{id = 48789 (ksk), size = 2048b}
	RRSIG	DNSKEY 7 3 3600 20100804183936 20...	{id = 48789}
	NSEC	www NS SOA TXT RRSIG NSEC DNSKEY	
	RRSIG	NSEC 7 3 3600 20100803231408 2010...	{id = 38052}
www	A	1.2.3.4	
www	RRSIG	A 7 4 86400 20100804052630 201007...	{id = 38052}
www	AAAA	2001::1	
www	RRSIG	AAAA 7 4 86400 20100804062422 201...	{id = 38052}
www	NSEC	A AAAA RRSIG NSEC	
www	RRSIG	NSEC 7 4 3600 20100804054636 2010...	{id = 38052}

Fragen?



MEN&MICE

© Men & Mice <http://menandmice.com>

Kontakt:

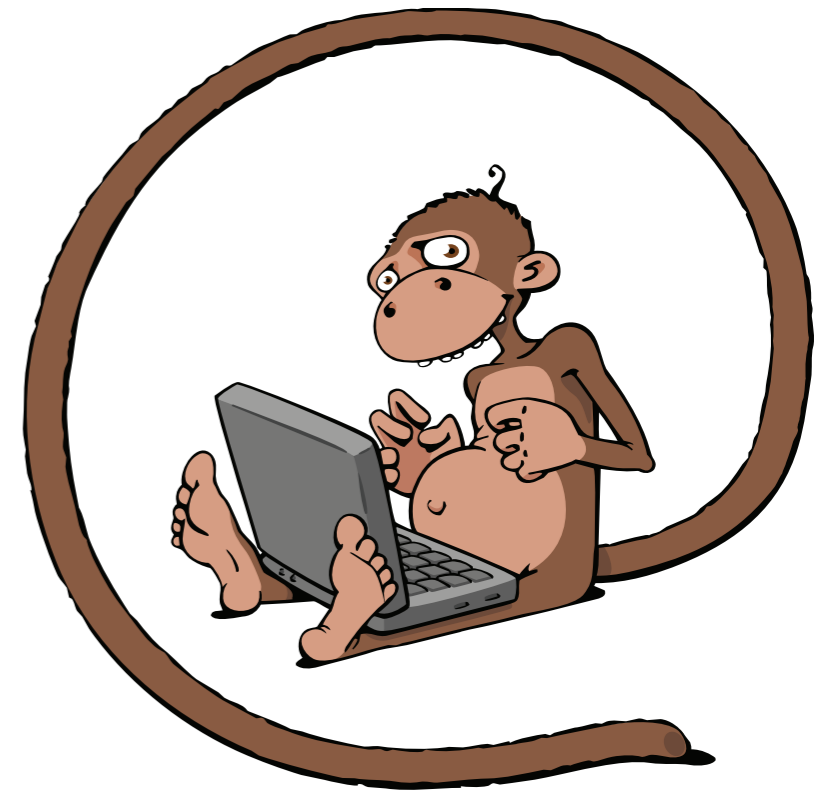
OpenDNSSEC: www.opendnssec.org

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



MEN&MICE

© Men & Mice <http://menandmice.com>



Vielen Dank!

E-Mail:
carsten@menandmice.com

MEN&MICE

© Men & Mice <http://menandmice.com>