

# DNSSEC - DNSSEC Schlüsselparameter

Patrick Koetter und Carsten Strotmann, sys4 AG

# Agenda

---

1. DNSSEC Algorithmen
2. DNSSEC Schlüssel-Größen
3. DNSSEC Signer 'best-practice'

# DNSSEC Algorithmen

---

- RSAMD5 - ist im RFC genannt, wurde aber nie implementiert
- RSASHA1 - jede DNSSEC Software muss diesen Algorithmus unterstützen, er gilt aber als "schwach" und sollte nicht mehr benutzt werden
- *RSASHA256*
- *RSASHA512*
- *ECDSA* - RFC 6605, April 2012
- *ECCGOST* - wird in Russland benutzt
- DSA (nur 1024bit Schlüssel, Validierung langsamer als RSA ohne Sicherheits-Gewinn, wird in der Praxis nicht eingesetzt, wird aus DNSSEC-Software entfernt)
- Ed25519 / Ed448 für DNSSEC - RFC 8080 - noch nicht weit verbreitet

# DNSSEC RSA-Schlüsselgrößen

---

- Mit jedem Bit verdoppelt sich die Arbeit, per 'Brute-Force' den privaten Schlüssel zu finden
- Verdopplung der RSA-Schlüssel-Größe bewirkt
  - Erstellen von Signaturen dauert bis zu 8 mal länger
  - Validieren von Signaturen auf einem DNS-Resolver dauert bis zu 4 mal länger
  - Schlüssel-Records und Signaturen in DNS-Antworten werden größer

# Das Problem mit zu großen DNS-Antwort-Paketen

---

- Fragmentierung von IPv4 und IPv6 UDP Paketen
  - Performance
  - IPv6 Pakete mit Extension Header (Fragment Header) können beim Internet-Transit geblockt werden
  - UDP Fragmentierungs-Angriffe gegen nicht DNSSEC-Validierende Resolver
  - DNS Amplification Angriffe

Ziel: DNSKEY RRSet beim KSK-Rollover + Notfall KSK < 1232 Byte DNS Antwort

# KSK/ZSK Signatur über den DNSKEY RRSSet bei BIND 9

---

- BIND 9 erstelle zwei Signaturen über den DNSKEY RRsSet einer Zone
  - Signatur vom KSK (notwendig)
  - Signatur vom ZSK (optional)
- Um die Antwort-Größe klein zu halten, kann die optionale ZSK-Signatur abgeschaltet werden

```
options {  
    [...]  
    dnssec-dnskey-kskonly yes;  
};
```

# Lebensdauer von DNSSEC-Schlüsseln

---

- DNSSEC Schlüssel haben keine technische Lebensdauer, nur eine organisatorische
- Die Administratoren einer DNSSEC-Zone entscheiden, wann ein DNSSEC-Schlüssel ausgetauscht wird
- Das Austauschen eines DNSSEC-Schlüssels nennt man "Key-Rollover"
- Schlüssel mit schwachen Algorithmen oder kurzen Schlüssel-Längen sollten in kurzen Intervallen ausgetauscht werden
  - 1024bit RSASHA256 -> 30 Tage (ZSK)
  - 1536bit RSASHA256 -> 120 Tage (ZSK)
  - 2048bit RSASHA256 -> 360 Tage (KSK)
  - 2560bit RSASHA256 -> 720 Tage+ / 2 Jahre+ (KSK)

## KSK und ZSK

---

- Aus organisatorischen Gründen wird die Sicherheit einer DNSSEC auf zwei getrennte Schlüssel aufgeteilt: den Key-Signing-Key (KSK) und den Zone-Signing-Key (ZSK)



## KSK:

- Der Key-Signing-Key erstellt nur eine Signatur - über den DNSKEY Record Set
- Der Hash des KSK wird in der Eltern-Zone gespeichert um die Vertrauenskette aufzubauen (DS-Record).  
Daher hat der KSK eine Abhängigkeit zur Eltern-Zone, immer wenn der KSK gewechselt wird muss auch der DS-Record in der Eltern-Zone aktualisiert werden
- Da die Änderung des DS-Records oft manuell durchgeführt wird (und fehleranfällig ist) wird versucht, den KSK seltener zu wechseln. Der KSK wird als starker Schlüssel erzeugt.

## ZSK:

- Der Zone-Signing-Key hat keine Abhängigkeiten zu externen Ressourcen, er kann jederzeit ausgetauscht werden.
- Der ZSK wird daher häufiger getauscht, der Schlüssel muss daher nicht so stark ausgelegt sein

## DNSSEC Signer "Best-Practice" (1)

---

- Bei Zonen mit hohen Sicherheitsanforderungen sollte den die privaten DNSSEC-Schlüssel offline gehalten werden
  - Dies erzwingt manuelles Signieren der Zone
- Schlüssel können in Hardware-Security-Modulen (HSM) sicher gespeichert werden

# HSM

- Auswahl-Kriterien HSM für den Gebrauch mit DNSSEC
  - Anzahl der Schlüssel-Speicherstellen (Slots)
  - Zeitnahe Unterstützung von neuen Betriebssystem-Versionen (Linux Distributionen)
  - Zeitnahe Unterstützung neuer OpenSSL Versionen
  - Stabilität der HSM-Treiber

## DNSSEC Signer "Best-Practice" (2)

- Für Zonen mit mittleren bis geringen Sicherheitsanforderungen wird ein "hidden-primary" Signer empfohlen
- Die Schlüssel-Dateien sollten über die Betriebssystem-Rechte gesichert werden
- Bei voller Automation der Schlüssel-Wechsel brauchen DNS-Server-Administratoren keine Lese-Berechtigung auf die Inhalte der Schlüssel
- Logins und Zugriffe auf Schlüsseldateien per Audit mitprotokollieren (Protokolle online auf einen Protokoll-Server senden)

## DNSSEC Signer "Best-Practice" (3)

- Zonen-Inhalte können durch DNS-Delegation auf verschiedene Zonen oder verschiedene DNS-Server verteilt werden
- Jede Zone, jeder Server kann ein unterschiedliches Sicherheits-Niveau unterstützen
- Beispiel: Haupt-Zone "example.com" signiert per "hidden-signer" (Schlüssel nicht aus dem Internet erreichbar), Sub-Zone mit E-Mail-Adressen- Hashes (OPENPGPKEY und SMIMEA in \_securemail.example.com) gesichert per "NSEC3-NARROW" und Online-Schlüssel auf jedem autoritativen Server

Fragen?

---