# Möglichkeiten zur Provisionierung von DNSSEC-Schlüsselmaterial

---

## Entwurf

| | | | |
|---|---|---|---|
| Dok.-Version: | 0.1 | Dok.-Status: | Draft |
| Dok.-Stand: | 23.11.2009 | Dok.-Name: | Provisionierung_DNSSEC-Schlüsselmaterial-Entwurf-V0.1-2009-11-23 |

# Impressum


| Autor(en) | Adresse | Telefon | E-Mail |
|---|---|---|---|
| Peter Koch | DENIC eG<br>Kaiserstrasse 75-77<br>60329 Frankfurt<br>Deutschland | +49 69 27 235 0 | pk@denic.de |
| Marcos Sanz | dito | +49 69 27 235 0 | sanz@denic.de |


# Copyright



# Dokument-Freigabe

| Dokument-Version | Freigegeben von | Freigegeben am |
|---|---|---|
| <Versions-Nr.> | <Name> | <Datum> |

# Verteiler

| Name | Funktion |
|---|---|
| | |
| | |

# Änderungshistorie

| Version | Stand | Bearbeiter | Änderungen |
|---|---|---|---|
| 0.1 | 23.11.2009 | Peter Koch, Marcos Sanz | Erster Entwurf |
| | | | |
| | | | |

# Inhalt

# 1 Übersicht

## 1.1 Abstract

Dieser Entwurf stellt zwei Möglichkeiten zur Provisionierung von DNSSEC-Schlüsselmaterial an die Registry gegenüber und spricht eine Empfehlung aus.

## 1.2 Einleitung

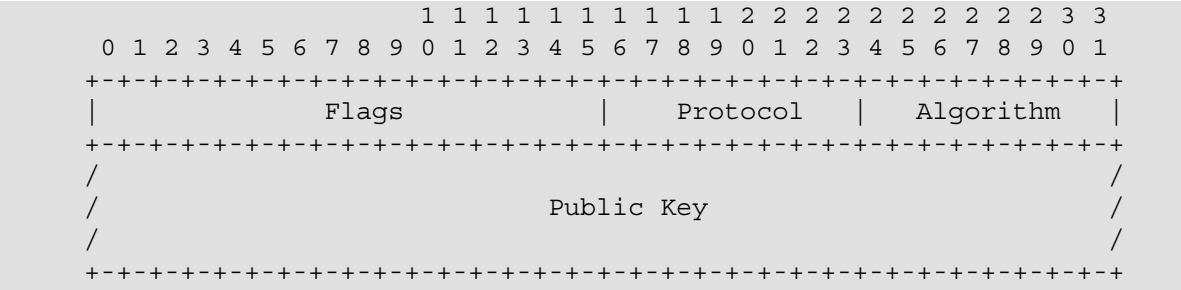
Bei der Registrierung (oder Änderung bestehender Registrierungen) von Domains für .de übertragen Provider mittels MRIv2 (DENIC-24) oder RRI (DENIC-11) Daten an die Registry (hier: die DENIC). Um im Rahmen des DNSSEC-Testbeds die DNS-Erweiterung DNSSEC (RFC4033 [2], RFC4034 [3], RFC4035 [4]) auch für die delegierten Zonen unterstützen zu können, muss dieser zu übertragende (zu provisionierende) Datensatz erweitert werden. Im Folgenden wird beschrieben, warum eine solche Erweiterung des Datenmodells ausreicht und wie sie im Detail gestaltet werden kann.

# 2 Technischer Hintergrund

Um für die Validierung bei DNSSEC eine Vertrauenskette (*chain of trust*) aufbauen zu können, sieht das DNSSEC-Protokoll vor, in der delegierenden Zone einen Hinweis auf den oder die Schlüssel der delegierten Zone zu hinterlegen. (Wir gehen hier vereinfachend davon aus, dass es sich jeweils nur um einen Schlüssel handelt.) Die Vertrauenskette folgt damit dem Delegationspfad. Der entscheidende Schlüssel ist der *Key Signing Key* der delegierten Zone, der in der Regel als *Secure Entry Point* (SEP) markiert ist. Diese Information liegt in einem "DNSKEY"-RR in der delegierten Zone vor und ist dort (mindestens) von diesem "DNSKEY" selbst unterschrieben. In der delegierenden Zone wird diese Information aus Platzgründen nicht exakt wiederholt. Statt des eigentlichen Schlüssels wird dort ein entsprechender Fingerprint in einem "DS"-RR (*Delegation Signer*) abgelegt. Die Präsenz eines "DS" in der delegierenden Zone ist nur dann definiert, wenn diese Zone mit DNSSEC signiert ist. Der "DS"-RR ist, obwohl er Daten aus der delegierten Zone referenziert und am Delegationspunkt liegt -- im Gegensatz etwa zum "NS"-RRSet -- in der delegierenden Zone autoritativ und wird entsprechend dort und nur dort von einer DNSSEC-Signatur authentisiert.

## 2.1 Aufbau des DNSKEY-Records

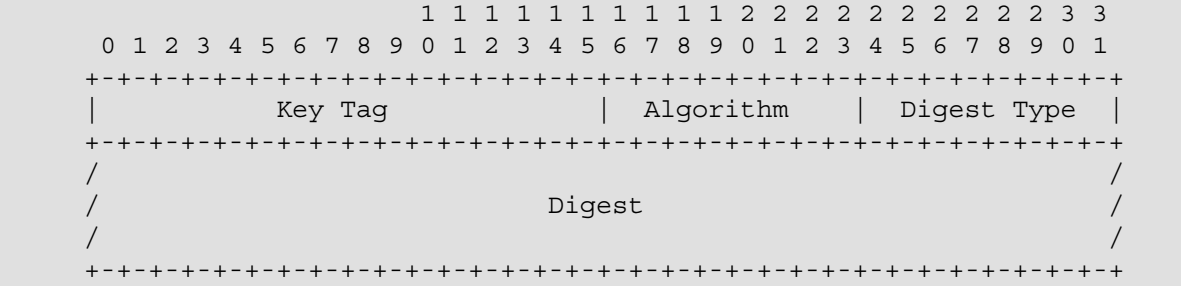
Das Format des "DNSKEY"-Records ist in Kapitel 2 von RFC4034 [3] beschrieben:




Unter den Flags findet sich je ein Eintrag für das Feld *Zone Key* und *Secure Entry Point*. In der Dezimaldarstellung kommen darum die Werte 256 und 257 vor. Zusätzliche Erweiterungen für den automatisierten Wechsel eines *Trust Anchors* sind in RFC5011 [7] beschrieben, hier aber nicht von Bedeutung. Das Feld *Protocol* beinhaltet immer den festen Wert für *DNSSEC*. Im Feld *Algorithm* schließlich wird der verwendete Public-Key-Algorithmus spezifiziert, der dann auch die innere Struktur und die Größe der eigentlichen Schlüsseldaten bestimmt. Zusätzlich wird dieses Feld genutzt, um mit Hilfe von Alias-Mechanismen die Verwendung von NSEC3 zu signalisieren.

## 2.2 Aufbau des DS-Records

Der "DS"-Record wird in Kapitel 5 des RFC4034 [3] spezifiziert:




Das Feld *Key Tag* erleichtert bei mehreren vorhandenen Schlüsseln ("DNSKEY"-RRs) dem validierenden Resolver das Auffinden des passenden Schlüssels. Der Wert ergibt sich einfacher aus den Schlüsseldaten als ein kryptographischer Hash und lässt sich -- um den Preis der möglichen Nicht-Eindeutigkeit -- schneller errechnen.

Das Feld *Algorithm* hat exakt dieselbe Bedeutung wie beim "DNSKEY"-RR. Mit dem *Digest Type* schließlich wird der verwendete Hashalgorithmus (SHA-1, SHA-256) angegeben.

Aus einem "DNSKEY"-RR bzw. den relevanten Daten kann der Inhalt eines "DS"-RR berechnet werden, nicht aber umgekehrt. Mit Hilfe eines "DS"-RR kann ein "DNSKEY"-RR eindeutig identifiziert werden, was der Bestimmung des "DS"-RR entspricht.

# 3 Diskussion

Bei der (initialen) Provisionierung des Schlüsselmaterials an die Registry (delegierende Zone) kann entweder der "DS"-RR vorgefertigt übergeben werden oder der "DNSKEY" übergeben und von der Registry der "DS"-RR berechnet werden.

## 3.1 Argumente für DS

Für die Verwendung des "DS"-Records bei der Provisionierung sprechen einige Argumente:

- Die delegierende Zone (bzw. deren Registry) muss die von der delegierten Zone verwendeten Hashes bzw. Signaturalgorithmen nicht kennen oder "verstehen", es wäre auch die Unterstützung unbekannter Hashfunktionen möglich.
- Wo keine Berechnung stattfindet (weil der "DS"-RR bereits vorliegt), können auch keine Berechnungsfehler gemacht werden. Die Registry könnte den "DS"-RR "blind", so wie er übergeben wird, in die Zone eintragen.
- Der "DS"-RR ist kürzer und damit leichter zu handhaben als der "DNSKEY" selbst.
- Der "DNSKEY" ist bereits im DNS (in der delegierten Zone) zu finden, wäre also online nachzuprüfen. Für den "DS"-RR gibt es keine Online-Quelle, solange er nicht in der delegierenden Zone publiziert ist (Redundanzargument).

## 3.2 Argumente für DNSKEY

- Der Schlüssel ist das eigentlich wesentliche Datum, dessen Authentizität in der delegierenden Zone sichergestellt werden soll.
- Der "DNSKEY"-RR liegt dem Domaininhaber/Operator unmittelbar vor.
- Der "DS"-RR ist im DNS-Protokoll in der delegierenden Zone autoritativ und sollte darum von dort stammen.
- Bei Übergabe des Schlüssels kann man direkt das Vorhandensein in (bzw. die Übereinstimmung mit) den Live-Daten prüfen.
- Aus dem "DNSKEY" lässt sich immer der "DS"-RR berechnen, nicht aber umgekehrt. Um beide Werte in der Hand zu haben, muss vom "DNSKEY" ausgegangen werden.
- Die Erzeugung des "DS"-RR aus einem registrierten "DNSKEY" gibt der delegierenden Zone die Freiheit, die Stärke der Hashfunktion selbst zu bestimmen.
- Der übergebene "DNSKEY" enthält die Information, ob es sich um einen SEP handelt.

## 3.3 Konzept der Proof of Possession

Im Betrieb von *Certification Authorities* (CAs) ist das Konzept der *Proof of Possession* von Bedeutung. Man versteht darunter die Bedingung, dass eine Zertifikatsanforderung von einem Nachweis begleitet ist, dass der Anfordernde Zugriff auf das private Pendant des öffentlichen Schlüssels besitzt, für den das Zertifikat angefordert wird. Daraus folgt an dieser Stelle keine klare Präferenz für "DNSKEY" oder "DS", es lassen sich aber Anforderungen and die Prüfung und Weiterverarbeitung ableiten.

# 4 Vergleich mit EPP

RFC4310 [5] erweitert EPP, um Schlüsselmaterial an die Registry übergeben zu können. Dies geschieht durch eine Erweiterung (*Extension Mapping*) des im RFC3731 [1] definierten *Domain Name Mappings*. (Dies war die zum Zeitpunkt der Veröffentlichung von RFC4310 [5] aktuelle Spezifikation, die mittlerweile durch RFC5731 [8] ersetzt wurde.) In diesem Mapping werden "DS"-RRs als Pflichtübergabeparameter vorgesehen und "DNSKEY"-RRs nur als zusätzliche, optionale Eingaben. Dabei handelt es sich um eine seinerzeit durchaus kontroverse Designentscheidung, die auf Teilen des damals noch nicht veröffentlichten, aber schon in Bearbeitung befindlichen RFC4641 [6] basierte und der (anno 2005) keine operationelle Erfahrung zu Grunde lag. Man war zunächst davon ausgegangen, RFC4641 [6] werde aufgrund einer naheliegenden Hoheit der delegierten Zone über ihre kryptographischen Parameter den "DS"-RR als Kommunikationsgegenstand zwischen delegierter und delegierender Zone vorsehen. Dabei empfahl RFC4641 [6] am Ende aber nur, "DS"-RRs in der Registry zu speichern (4.4.2) und erzwang den "DS"-RR nicht als Gegenstand eines Registrierungsinterfaces. Ebenfalls sah RFC4641 [6] am Ende auch Kommunikationswege vor, die rein auf "DNSKEY"-Austausch basieren.

RFC4310 [5] wurde im Rahmen der Entstehung von RFC5011 [7] kritisiert und es ist nicht ausgeschlossen, dass eine Überarbeitung im Standardisierungsprozess stattfindet, so wie das bei allen anderen EPP-Dokumenten auf den Weg zum *Full Standard* geschehen ist.

# 5 Vergleich mit anderen Registries?

Von anderen Registries, die DNSSEC in Produktion einsetzen oder dies angekündigt haben, wird das Schlüsselmaterial der delegierten Zonen auf unterschiedliche Arten entgegengenommen. Die folgende Tabelle gibt eine ausschnittsweise Übersicht der größten/relevantesten TLDs.

Ausgewählte TLDs (zzgl. Rootzone und RIPE NCC) zeigen kein völlig einheitliches Bild:

| TLD | live | RR-Typ fuer TA/SEP |
|---|---|---|
| BG. | ja | nutzt DS |
| BR. | ja | nutzt DS |
| CH., LI. | ja | DNSKEY/DS |
| CZ. | ja | nutzt DNSKEY |
| EU. | nein | wird DNSKEY nutzen |
| SE. | ja | DNSKEY/DS |
| COM. | nein | wird DS nutzen |
| GOV. | ja | nutzt DNSKEY |
| MUSEUM. | ja | entfällt |
| ORG. | ja | nutzt DS |
| . | nein | wird DS nutzen |
| RIPE NCC | ja | DS in der RIPE-DB |

In den Fällen, in denen sowohl "DS" als auch "DNSKEY" erwähnt sind, hängt die Verfügbarkeit der Methode u.U. von der Wahl der Provisionierungsschnittstelle ab. Manche TLD-Registries fragen nach der Übermittlung des "DS"-RR grundsätzlich online zusätzlich den "DNSKEY"-RR ab.

In vielen Fällen ist die Wahl auf "DS" statt "DNSKEY" gefallen, weil die Registry EPP einsetzt und RFC4310 [5] die Übergabe des "DS"-RR als obligatorisch voraussetzt.

# 6 Ergebnis

Keine relevante DNSSEC-Spezifikation schreibt eindeutig die Verwendung von "DS" oder "DNSKEY" bei der Provisionierung vor. Eine Reihe von aktuellen Vorschlägen, die eine Signalisierung des Schlüsselwechsels *in band* vorsehen (vgl. auch RFC5011 [7]) sind mangels Alternative darauf angewiesen, dass die delegierende Zone die "DS"-Records selbst erzeugt.

Aufgrund der vorstehenden Überlegungen **empfiehlt DENIC, im Testbed die Provisionierung mittels "DNSKEY" zu implementieren**. Sollte sich im Laufe des Betriebes herausstellen, dass diese Variante zu unhandlich ist oder sonstige Probleme bereitet, könnte noch im Testbed ohne Auswirkung auf alle existierenden sicheren Delegationen auf die Registrierung von "DS"-RRs umgestellt werden, inklusive automatisierter Umstellung der Bestandsdaten.

# 7 Literaturverzeichnis

[1] [RFC3731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", RFC 3731, March 2004.

[2] [RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[3] [RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.

[4] [RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[5] [RFC4310] Hollenbeck, S., "Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)", RFC 4310, December 2005.

[6] [RFC4641] Kolkman, O. and R. Gieben, "DNSSEC Operational Practices", RFC 4641, September 2006.

[7] [RFC5011] StJohns, M., "Automated Updates of DNS Security (DNSSEC) Trust Anchors", RFC 5011, September 2007.

[8] [RFC5731] Hollenbeck, S., "Extensible Provisioning Protocol (EPP) Domain Name Mapping", STD 69, RFC 5731, August 2009.