Nameserver Predelegation Check - Kommentiert

Inhaltsverzeichniss

EN

1. Einführung

1.1. Über dieses Dokument

Die vorliegende Dokumentation beschreibt die geltenden Anforderungen an Nameserver und Zonendaten, die erfüllt sein müssen, damit eine Domain von DENIC an diese Nameserver delegiert werden kann. Die Policy und die damit verbundenen Checks werden hier dargestellt.

1.2. Motivation

Das Domain Name System (DNS) ist ein hierarchisch aufgebauter, verteilter und replizierter Datenbestand zur Abbildung von Namen in Adressen und anderen Internetinfrastrukturelementen. Hierarchie und Verteilung werden durch Delegationen implementiert. Direkt unterhalb der Wurzel des Namensraumes liegen die Top Level Domains (TLDs), deren Verwaltung u.a. durch das Dokument RFC1591 geregelt ist. Dem TLD-Verwalter obliegt die stabile, dem Stand der Technik entsprechende Pflege der Zonendaten und der Best Practices folgende Betrieb der entsprechenden Nameserver.

Das DNS ist wegen seiner Verteilung und Redundanz hochgradig fehlertolerant. Es können jedoch

durch Netzstörungen und Konfigurationsfehler Situationen entstehen, in denen Domains nicht oder falsch aufgelöst werden, siehe auch RFC4697. Der Internetnutzer bemerkt zwar die Fehlfunktion, kann die Ursache aber nicht immer im DNS lokalisieren. In besonders ungünstigen Konstellationen können DNS-Fehlfunktionen zu Störungen in Netzbereichen führen, die von der Ursache weder betroffen, noch für sie verantwortlich sind, geschweige denn in der Lage wären, sie zu beseitigen. Im Interesse eines funktionierenden Gesamtsystems und eines nach außen wie innen stabil versorgten Namensraumes prüft die TLD-Verwaltung daher gewisse Voraussetzungen vor der Delegation, ohne deren Erfüllung eine Delegation nicht erfolgt. Darüber hinaus gibt es eine Reihe von Kriterien, die nicht absolut kritisch sind, deren Erfüllung aber die Dienstqualität verbessern kann.

2. Allgemeine Anforderungen

2.1. Nameserver Policy

Der Predelagation Check verwendet verschiedene Issue-Typen (d.h. WARNING, ERROR), um Verstöße innerhalb der Überprüfung zu erfassen. Somit stellt jede Anforderung auch ein Kriterium dar, das entweder erfüllt sein **MUSS** oder **SOLL**. Die Zuordnung zwischen Anforderung und deren Einhaltung ist wie folgt definiert:

ERROR: Obligatorisch zu erfüllende Anforderungen werden mit **MUSS** beschrieben, ein Verstoß führt zur Ausgabe eines **ERROR**, welcher das Check-Gesamtergebnis letztlich negativ beeinflusst.

WARNING: Empfehlungen werden mit **SOLL** beschrieben, ein Verstoß führt zur Ausgabe einer **WARNING**, welche das Check-Gesamtergebnis letztlich nicht beeinflusst.

2.1.1. Autoritative Nameserver

Jeder der im Auftrag enthaltenen Nameserver **MUSS** erreichbar und für die beantragte Zone autoritativ sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
116	SOA record response must be authoritative
133	Answer must be authoritative

Erläuterung: Da der Betreiber des Nameservers sich sowohl vom Domaininhaber als auch vom verwaltenden Mitglied unterscheiden kann und darum im Rahmen der Domaindelegation kein Vertragspartner von DENIC ist, eine Delegation aber zu seinen Lasten geht, wird durch das autoritative Bedienen der Zone das Einverständnis zu dieser Delegation unterstellt. Im übrigen entspricht die Vorabprüfung dem Geist und Text der RFCs 1034 und 1035.

2.1.2. Redundante Anbindung

Die Anfrage **MUSS** mindestens zwei Nameserver beinhalten, von denen mindestens ein Nameserver über IPv4 angebunden sein **MUSS**. Für jeden Nameserver werden dessen sämtliche IPv4- und IPv6-Adressen für die weitere Prüfung ermittelt bzw. gegebenenfalls dem Auftrag

entnommen. Es **MUSS** mindestens einen Nameserver im Auftrag geben, dessen IP-Adresse sich von den IP-Adressen sämtlicher anderer Nameserver desselben Auftrags unterscheidet. Andernfals erfolgt entsprechend die Ausgabe folgender **ERROR**.

ERROR:

Code	Message
107	Insufficient diversity of nameserver' s IP addresses
125	Insufficient diversity of nameserver' s IPv4 addresses
127	Insufficient number of nameservers reachable
129	Invalid IPv4 or IPv6 address
132	Could not resolve any IP address for this nameserver

Erläuterung: RFC1035 sieht ausdrücklich vor, dass aus Redundanzgründen jede DNS-Zone von mindestens zwei unabhängigen Nameservern versorgt wird. Zur Vermeidung von negativen Effekten für die TLD-Server bei der Nichterreichbarkeit der Nameserver einer delegierten Zone wird besonderer Wert auf die Diversität in der Netztopologie gelegt.

Beispiel: Gültiges Set von Nameservern

Nameserver	IP-Adresse
ns1.nic.nast	172.31.1.1', 'fd00:10:10::1:1
ns2.nic.nast	'fd00:10:10::2:2

Beispiel: Ungültiges Set von Nameservern

Nameserver	IP-Adresse
ns1.nic.nast	172.31.1.1', 'fd00:10:10::1:1
ns2.nic.nast	172.31.1.1', 'fd00:10:10::2:2

2.1.3. Glue Records

Grundsätzlich gilt die Narrow Glue Policy: Glue Records werden dann und nur dann in die .de- bzw. 9.4.164.arpa Zone eingetragen, wenn der Name eines Nameservers innerhalb der delegierten Domain liegt.

Hinsichtlich dessen können die folgenden Anforderungen abgeleitet werden.

2.1.3.1. Nameserver innerhalb der Zone

Liegt der Nameserver innerhalb der zu delegierenden Domain, **MUSS** mindestens eine IPv4- oder IPv6-Adresse (A-/AAAA-RRSet) angegeben werden. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
101	Missing glue record for the nameserver

Erläuterung: In der angegebenen Konstellation ist in jedem Fall mindestens ein Glue Record erforderlich.

2.1.3.2. Nameserver ausserhalb der Zone

Liegt der Nameserver nicht innerhalb der zu delegierenden Domain, **SOLL** keine IP-Adresse (A-/AAAA-RRSet) angegeben werden. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
102	Provided glue records not applicable

Erläuterung: DENIC wendet sowohl für .de als auch für 9.4.e164.arpa die *Narrow Glue Policy* an, erlaubt also Glue Records nur im eng begrenzten Fall, dass der Nameserver innerhalb der delegierten Zone liegt. Zusätzlich angegebene Adressen sind überflüssig und werden nicht übernommen. Die Warnung soll auf mögliche Eingabefehler hinweisen.

2.1.3.3. IP-Adressen und RRSet-Konsistenzen

Unter jeder im Auftrag angegebenen und berücksichtigten IP-Adresse (v4 bzw. v6) eines Nameservers **MUSS** dessen A- und AAAA-RRSet unmittelbar, vollständig, konsistent und autoritativ ermittelbar sein und mit den Daten im Auftrag übereinstimmen. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
106	Inconsistent set of nameserver IP addresses

Erläuterung: Da die Glue-Daten mit den autoritativen Daten koexistieren, muss sichergestellt werden, dass sie konsistent sind, die Adressangaben in den Glue Records also mit den auf „normalem Wege“ ermittelten autoritativen Daten übereinstimmen. Des Weiteren gebietet die Konsistenz, RRSets (Record Sets, also ein oder mehrere Records gleichen Typs) immer vollständig anzugeben, nicht etwa nur eine von zwei Adressen eines Nameservers für die Glue Records zu verwenden. Schließlich wird die „Narrow Glue Policy“ sowohl auf IPv4 als auch auf IPv6 angewandt, d.h. wenn entsprechende Records-Sets (A oder AAAA) in den autoritativen Daten existieren, müssen sie in Glue Records bereitgestellt werden.

2.1.4. SOA-Zonendaten

Bezüglich der Korrektheit der SOA-spezifischen RR-Daten können die nachfolgenden Anforderungen abgeleitet werden.

2.1.4.1. Refresh

Der Wert **SOLL** im Bereich von [3600,86400] Sekunden liegen. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
108	Refresh value ot of range

Erläuterung: Dieser Wert bestimmt die Häufigkeit des Datenabgleichs zwischen den Secondary Nameservern und dem Primary Master. Niedrige Werte erzeugen mehr DNS-Verkehr und mehr Last auf den beteiligten Systemen, hohe Werte verringern ggf. die Aktualität der Daten. Da diese Werte letztlich zwischen den Betreibern der beteiligten Nameservern abgestimmt sein müssen, wird lediglich gewarnt, wenn „übliche“ Werte unter- oder überschritten werden.

2.1.4.2. Retry

Der Wert **SOLL** im Bereich von [900,28800] Sekunden liegen und **SOLL** zwischen 1/8 und 1/3 von Refresh betragen. Andernfalls wird ein enstprechende **WARNING** ausgegeben.

WARNING:

Code	Message
109, 110	Retry value out of range

Erläuterung: Dieser Wert ersetzt nach dem ersten fehlgeschlagenen Versuch den unter Refresh angegebenen, bis entweder ein Abgleich erfolgreich war oder der Expire-Wert erreicht ist. Er ist darum kürzer zu wählen als Refresh, wobei ein zu kleiner Wert erneut zu Lastspitzen führen kann und ebenfalls eine Warnung auslöst. Des Weiteren wird sichergestellt, dass die Werte Refresh und Retry in einem solchen Verhältnis zueinander stehen, dass die Umschaltlogik überhaupt zu einem nennenswerten Vorteil führen kann.

2.1.4.3. Expire

Der Wert **SOLL** im Bereich von [604800,3600000] Sekunden liegen. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
111	Expire value out of range

Erläuterung: Dieser Wert bestimmt, wie lange erfolglose Abgleichversuche unternommen werden, bevor ein Slave die weitere Unterstützung der Zone einstellt. Werte unterhalb einer Woche sind sehr kritisch, weil sie dafür sorgen können, dass eine Zone binnen kurzer Zeit sämtliche autoritativen Nameserver verliert und dadurch zu 100% lahmgelegt wird. 1.000 Stunden, hier als Obergrenze angenommen, ist ein verbreiteter Wert, oberhalb dessen von einem ernsten Abgleichproblem ausgegangen werden kann, das nicht ignoriert werden sollte.

2.1.4.4. NegTTL

Der Wert **SOLL** im Bereich von [180,86400] Sekunden liegen. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
112	Minimum TTL out of range

Erläuterung: Dieser Wert bestimmt gemeinsam mit der TTL des SOA-Records die Lebensdauer negativer Antworten nach RFC2308. Zu große Werte (hier: länger als ein Tag) reduzieren den DNS-Verkehr nicht merklich bzw. werden von DNS-Caches ohnehin beschnitten. Sie wären darum wirkungslos. Zu geringe Werte (hier: kleiner als drei Minuten) führen letztlich zu einer kompletten Abschaltung des „negative Caching“, was es zu vermeiden gilt.

2.1.5. Anforderungen an weitere Daten in der Zone

2.1.5.1. NS-RRSet Konsistenz

Das NS-RRSet **MUSS** exakt mit der im Auftrag angegebenen Liste der Nameserver übereinstimmen. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
118	Inconsistent set of NS RRs

Erläuterung: RFC1034 sieht vor, dass die Angaben zu autoritativen Nameservern in der delegierenden und in der delegierten Zone übereinstimmen.

2.1.5.2. Kein CNAME-RR

Die beauftragte Zone (genauer: am Zonen-Apex) **MUSS** frei von einem CNAME-RR sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
115	SOA record response must be direct

Erläuterung: Zu einem CNAME-Record dürfen keine weiteren Record-Typen am selben Knoten im DNS-Baum existieren. Da für eine delegierte Zone aber mindestens der SOA-Record und die NS-Records vorhanden sein müssen, wäre das Vorhandensein eines CNAME-Records eine Protokollverletzung.

2.1.5.3. Referral Response

Die Referral Response **MUSS** (bei bis zu 191 Bytes langem QNAME und inkl. sämtlicher notwendiger Adressinformationen einschl. Glue Records) in ein DNS-UDP-Paket passen, darf also

512 Bytes nicht überschreiten. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
104	Calculated referral response larger than allowed

Erläuterung: Die Nameserver von DENIC antworten bei Anfragen nach Daten in delegierten Zonen mit einem Verweis (Referral) auf die tatsächlich zuständigen Nameserver der nächsten Hierarchiestufe. Standard-UDP-Pakete lassen maximal 512 Bytes Nutzlast zu. Um zu verhindern, dass die Antworten abgeschnitten werden und infolgedessen die Fragen über TCP erneut gestellt werden und die DENIC-Nameserver überproportional belasten, wird diese Längenbeschränkung eingeführt. Da der Platzverbrauch sowohl von der Länge der Nameservernamen und deren Komprimierbarkeit als auch von der Anzahl der Glue Records abhängt, ist eine solche Berechnung sicherer als die Vorgabe einer maximalen Anzahl von Nameservern.

2.1.5.4. Primary Nameserver

Die Angabe des Primary Nameservers im SOA-RR der beantragten Zone **SOLL** auf allen Nameservern übereinstimmen. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
113	Primary Master (MNAME) inconsistent across SOA records

Erläuterung: Auch dieses Requirement dient der Sicherstellung der unter SOA-Zonendaten angesprochenen Konsistenz.

2.1.6. Sonstige Vorgaben an die Nameserver

Weitere unkategorische Anforderungen sind nachfolgend aufgeführt.

2.1.6.1. IPv6

Jede IPv6-Adresse **MUSS** aus einem Adressraum stammen, der als Global Unicast gewidmet, als *allocated* markiert und *routbar* ist. Dies gilt für alle IPv6-Adressen der angegebenen Nameserver, unabhängig davon, ob es sich um einen Glue Record handelt. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
130	IPv6 address is not allocated
131	IPv6 address is not routable

Erläuterung: IPv6 kennt verschiedene Gültigkeitsbereiche für IP-Adressen („Scoping“). Um die Prüfergebnisse eindeutig und nachvollziehbar zu machen und global einheitliche Erreichbarkeit der Nameserver sicherzustellen, werden nur solche Adressen akzeptiert, die global eindeutig sind.

2.1.6.2. Keine Rekursiv-Abfragen

Die Durchführung einer rekursiven Abfrage **SOLL** nicht zugelassen sein. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
120	Recursive queries should not be allowed

Erläuterung: Aus Gründen der Sicherheit und der korrekten Sicht auf den Namensraum entspricht eine strikte Trennung von autoritativen und rekursiven Nameservern der operationellen Praxis.

2.1.6.3. TCP-Erreichbarkeit

Erreichbarkeit über TCP **SOLL** gegeben sein. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
902	Timeout
908	Connection refused

Erläuterung: RFC1034 und RFC1035 spezifizieren für DNS sowohl die Nutzung von UDP- als auch TCP-Transport, wobei UDP Vorrang genießt und den überwiegenden Anteil des Verkehrs auch bedient. Unter gewissen Umständen (z.B. Antwortgröße) kann es für einen Resolver notwendig werden, auf TCP auszuweichen, was von RFC123 ausdrücklich unterstützt wird.

3. DNSSEC-Anforderungen

3.1. 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. Die Vertrauenskette folgt damit dem Delegationspfad.

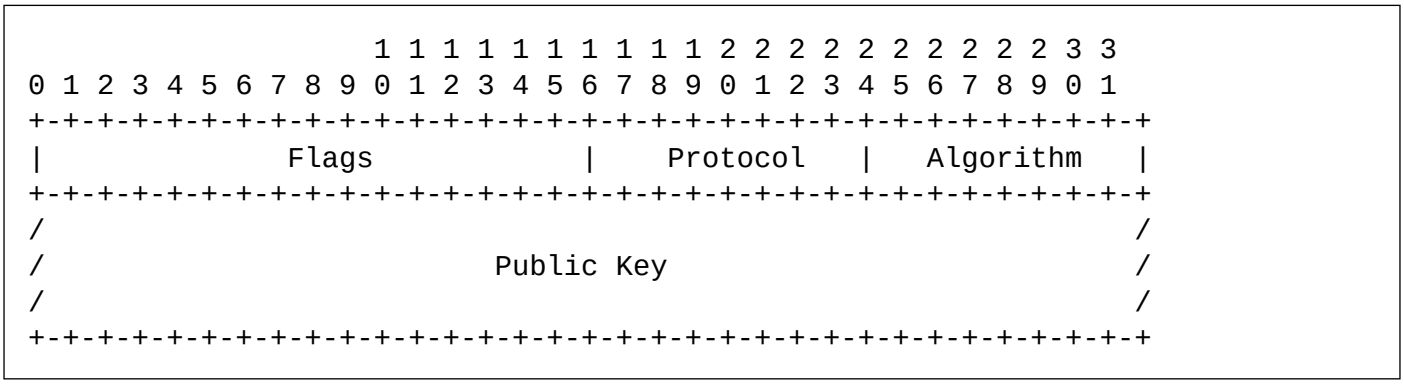
Der entscheidende Schlüssel ist der Key Signing Key der delegierten Zone, der in der Regel als Secure Entry Point (SEP) markiert ist. Diese Information liegt in einem DNSKEY-RR in der delegierten Zone vor und ist dort (mindestens) von diesem DNSKEY selbst unterschrieben. In der delegierenden Zone wird diese Information aus Platzgründen nicht exakt wiederholt. Statt des eigentlichen Schlüssels wird dort ein entsprechender Fingerprint in einem DS-RR (Delegation Signer) abgelegt.

Für die Provisionierung des Schlüsselmaterials wird der DNSKEY-RR verwendet. Bis zu fünf DNSKEY-RRs können pro Domain registriert werden. Im Rahmen der Zonengenerierung werden die entsprechenden DS-Records erzeugt (derzeit genau ein DS-RR pro mitgeteiltem Trust

Anchor), signiert und mit der Zone verteilt.

3.2. Aufbau des DNSKEY-RR

Jeder Dnskey-RR wird als Wire-Text-Format im Auftrag übergeben (siehe RFC4034). Der Aufbau ist wie folgt:



Unter den Flags findet sich je ein Eintrag für das Feld Zone Key und Secure Entry Point. Im Feld Algorithm 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.

3.3. DNSKEY-Typen & Signierung

Mit der erstmaligen Einführung des DS-RR in RFC3658 wurde auch die Unterscheidung des Zone Signing Keys (ZSK) und des Key Signing Keys (KSK) begonnen. Während der erste die eigentlichen Daten (RRSets) in der Zone signiert, dient der zweite, als der KSK, ausschließlich zur Authentisierung des ZSK. Mit dieser Trennung wurde den unterschiedlichen Anforderungen an die Schlüssel Rechnung getragen. Eine Änderung des KSK erfordert eine Interaktion mit der delegierenden Zone, sollte darum moderat häufig vorkommen und erfordert somit einen längerlebigen (daraus folgt meist: längeren) Schlüssel. Der ZSK kann einfacher gewechselt werden und wird darum in der Regel kürzer gewählt, was zumindest für das RSA-Verfahren zu kürzeren Signaturen und damit zu kleineren Zonendateien und zu kleineren Antwortpaketen führt. Hinweise zu Schlüssellängen und -wechseln finden sich in unter anderem in RFC4641. Während die Trennung eine Erleichterung hinsichtlich der Parameterwahl darstellt, erhöht sie andererseits die Komplexität ds Protokolls. Allerdings ist sie nicht zwingend. Die Verwendung nur eines Schlüssels anstelle eines KSK/ZSK-Paares unter Inkaufnahme der oben beschriebenen Nachteile ist protokollkonform und kommt in der Praxis gelegentlich vor. Theoretisch wäre es auch möglich, weitere Indirektionen in die Schlüsselbeziehungen einzuführen. Da allerdings eine Signatur ein RRSet immer vollständig erfasst, muss jede Signatur über dem DNSKEY-RRSet zwangsläufig alle dort enthaltenen Schlüssel authentisieren. Es reicht also, die Fälle ZSK+KSK und ZSK=KSK zu berücksichtigen.

3.4. DNSKEY-RR Sichtbarkeit

Ein im Auftrag übergebener DNSKEY-RR ist sichtbar, wenn er im DNSKEY-RRSet der delegierten Zone enthalten ist.

3.5. Validierungskette und Konzept

Im Betrieb von DNSSEC ist die Validierung der *Proof of Possession* und der *Chain of Trust* von maßgebender Bedeutung. Diese sind wie folgt definiert:

Proof of Possession: Beinhaltet die Gültigkeitsprüfung der Signatur des DNSKEY-RRSet der delegierten Zone. Der im Auftrag übergebene KSK wird dazu gewöhnlich verwendet. Diese Überprüfung garantiert die Integrität und Authentizität des DNSKEY-RRSet der Zone.

Chain of Trust: Beinhaltet die Gültigkeitsprüfung der Signatur des SOA-RR der delegierten Zone. Der im Auftrag übergebene oder im DNSKEY-RRSet enthaltene ZSK wird dazu gewöhnlich verwendet. Diese Überprüfung dient zur Sicherstellung und Aufbau einer "Vertrauenskette" innerhalb der Zonen-Delegation. Damit auch nicht registrierte Domains überprüft werden können, erfolgt diese Validierung nur in der delegierten Zone. Eine fortlaufende Validierung der Vertrauenskette auf höheren Zonen-Ebenen erfolgt nicht.

Basierend auf diesem Konzept ergeben sich die nachfolgenden Anforderungen.

3.6. Anforderungen

Zu Beginn wird das im Auftrag übergebene Schlüsselmaterial einer mehrstufigen Prüfung unterzogen (z.B. Flags, Algorithmen, Public-Key-Feld etc.), im Folgenden werden dann weitere Tests unter Einbeziehung der im DNS abrufbaren Information ausgeführt.

3.6.1. DNSKEY: Parameter

Ein im Auftrag übergebener Schlüssel **MUSS** eindeutig sein, **MUSS** sich also in mindestens einem Feld von den restlichen unterscheiden. Die maximale Anzahl an Schlüsseln im Auftrag **MUSS** ¬ 5 sein. Andernfalls erfolgt die Ausgabe eines entsprechenden **ERROR**.

ERROR:

Code	Message
208	Duplicate DNSKEY RR
210	Max 5 DNSKEY RR allowed

3.6.2. DNSKEY: Flags

Im Feld Flags dürfen ausschließlich Bits gesetzt sein, die in der IANA-Registry als zugewiesen markiert sind. Das Feld wird ausschließlich als numerischer Wert (0 - 65535) übergeben.

3.6.2.1. ZONE Bit

Bit 7 (ZONE) **MUSS** gesetzt sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
200	DNSKEY RR ZONE flag (bit 7) must be set

Erläuterung: Vorgeschrieben in RFC4034.

3.6.2.2. REVOKE Bit

Bit 8 (REVOKE) **MUSS** gecleared sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
201	DNSKEY RR REVOKE flag (bit 8) must not be set

Erläuterung: Folgt aus RFC5011. Ein zurückgerufener Schlüssel kann nicht als Trust Anchor fungieren.

3.6.2.3. SEP Bit

Bit 15 (SEP) **SOLL** gesetzt sein. Sonst Ausgabe von **WARNING**.

WARNING:

Code	Message
202	DNSKEY RR SEP flag (bit 15) should be set

Erläuterung: Dieses Feld soll den KSK im DNSKEY-RRSet identifizieren. Es entspricht Best Practice, es für KSKs bzw. Trust Anchor zu setzen, auch wenn Validatoren es nicht auswerten sollen.

3.6.2.4. Erlaubte Werte

Gemäß ZONE Bit, REVOKE Bit und SEP Bit **MUSS** also entweder 256 (ZONE) und 257 (ZONE, SEP) als möglicher Wert gewählt werden. Alle anderen Werte implizieren einen **ERROR**.

ERROR:

Code	Message
221	Unknown flags in DNSKEY RR are set

3.6.3. DNSKEY: Protocol

Das Feld Protocol **MUSS** den Wert "3" haben. Dieser Wert ist in RFC4034 zwingend vorgeschrieben und wird somit statisch erwartet. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
209	DNSKEY RR has invalid protocol

3.6.4. DNSKEY: Algorithm

Im Feld Algorithm **MUSS** ein Wert vorkommen, der in der folgenden Untermenge aus der IANA-Registry enthalten ist.

Unterstützte Algorithmen: 3, 5, 6, 7, 8, 10, 12, 13 ,14

Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
220	DNSKEY RR has invalid algorithm

HINWEIS: Die Algorithmen 3, 5, 7 und 12 sind als *Deprecated* eigestuft. Der Support wird daher in zukünftigen Releases eingestellt werden.

3.6.5. DNSKEY: Public Key

Das Feld Public Key **MUSS** den öffentlichen Schlüssel in Base64-Codierung enthalten. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
207	DNSKEY RR public key must be base64 encoded

Die interne Struktur hängt vom verwendeten Algorithmus ab, so entsprechend auch deren nachfolgende Anforderungen:

3.6.5.1. RSA

Für die RSA-basierten Algorithmen 5, 7, 8 und 10 gilt Folgendes.

3.6.5.1.1. Modulos

Der Modulos **MUSS** zwischen [512,4096] Bit lang sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
203	DNSKEY RR RSA key modulus length in bits out of range

3.6.5.1.2. Exponent

Der Exponent **MUSS** 128 Bit lang sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
204	DNSKEY RR RSA public key exponent length in bits must not exceed 128 bits

Erläuterung: Die Grenzen folgen aus RFC3110.

3.6.5.2. DSA

Für die DSA basierten Algorithmen 3 und 6 gilt Folgendes.

3.6.5.2.1. T Parameter

Der Parameter T **MUSS** einen Werte zwischen [0,8] annehmen. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
205	DNSKEY RR DSA public key parameter T out of range

3.6.5.2.2. Bytelänge

Die Bytelänge **MUSS** 213 + T * 24 entsprechen. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
206	DNSKEY RR DSA public key has invalid size

3.6.5.3. ECDSA

Die ECDSA Algorithmen 13 und 14 unterscheiden sich wiefolgt:

- In ECDSAP256SHA256 (13) **MUSS** der Schlüssel 512 Bit lang sein. Sonst Ausgabe von **ERROR**.
- In ECDSAP384SHA384 (14) **MUSS** der Schlüssel 768 Bit lang sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
226	DNSKEY RR ECDSA public key has invalid size

Erläuterung: Diese Werte ergeben sich aus RFC6605.

3.6.5.4. GOST

Der Schlüssel **MUSS** die Länge 512 Bit haben. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
227	DNSKEY RR GOST public key has invalid size

Erläuterung: Dieser Wert ergibt sich aus RFC5933.

3.6.6. DNSKEY-RRSet

3.6.6.1. Status

Das DNSKEY-RRSet **MUSS** an allen autoritativen Servern identisch sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
211	Inconsistent DNSKEY RR in nameserver response

3.6.6.2. Sichtbarkeit

Mindestens ein im Auftrag übergebener Schlüssel **MUSS** im DNSKEY-RRSet der delegierten Zone SICHTBAR sein. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
213	Did not find any DNSKEY RR from request in all nameserver responses

Für jeden nicht sichtbaren Schlüssel wird eine **WARNING** erzeugt.

WARNING:

Code	Message
212	Did not find DNSKEY RR from request in all nameserver responses

Erläuterung: Eventuell im DNSKEY-RRSet zusätzlich vorhandene Schlüssel werden nicht betrachtet. Eine Übereinstimmung der von unterschiedlichen Servern bezogenen Signaturen ist die Regelannahme, wird aber nicht ausdrücklich geprüft oder gefordert. Insbesondere dem DSA- und ECDSA-Verfahren wird so ermöglicht, online zu signieren.

3.6.7. Validierung Proof of Possession

Mindestens ein sichtbarer im Auftrag übergebener Schlüssel **MUSS** die Signatur DNSKEY-RRSet

gültig validieren. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
216	No visible DNSKEY found signing the DNSKEY RR obtained in response

Erläuterung: Diese Anforderung dient der Umsetzung der Proof of Possession.

3.6.8. Validierung Chain of Trust

Zum SOA-RR der delegierten Zone **MUSS** eine aktuell gültige Validierungskette mit mindestens einem sichtbaren im Auftrag übergebenen Schlüssel existieren. Das bedeutet, dass mindestens ein Schlüssel aus dem Auftrag oder aus dem DNSKEY-RRSet die Signatur des SOA-RR gültig validiert. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
217	No visible DNSKEY found in signing directly or indirectly the SOA RR obtained in response

Erläuterung: Diese Anforderung enstpricht der Chain of Trust und verhindert Security Lameness. Die Validierung ist auf die delegierte Zone beschränkt, damit auch unregistrierte Domains beauftragt werden können.

3.6.9. Übergreifende Regeln

Neben den auf die Zonendaten abgestellten Anforderungen ergeben sich durch DNSSEC-Anforderungen an die autoritativen Server bzw. die sie umgebende Infrastruktur weitere Regeln.

3.6.9.1. EDNS0 Support

Jeder autoritative Server **MUSS** die DNSSEC-Protokollerweiterung EDNS0 unterstützen, somit auf Anfragen mit dem DO-Bit signierte, DNSSEC-konforme Antworten liefern. Sonst Ausgabe von **ERROR**.

ERROR:

Code	Message
218	Received invalid answer to a DO-Bit query

3.6.9.2. UDP-basiertes EDNS0

Jeder autoritative Server **SOLL** UDP hinsichtlich der Erweiterung EDNS0 mit ausreichender Paketgröße und Verfügbarkeit unterstützen. Andernfalls erfolgt die Ausgabe einer entsprechenden **WARNING**.

WARNING:

Code	Message
214	Querying some authoritative nameservers via EDNS0 UDP failed

3.6.9.3. Wiederverwendung der bestehenden TCP-Verbindung

Jeder autoritative Server **SOLL** gemäß RFC7766 bereits bestehende TCP-Verbindungen wiederverwenden können um unnötigen Overhead durch zusätzlichen Verbindungsausfbau zu vermeiden. Andernfalls erfolgt die Ausgabe einer entsprechenden **WARNING**.

WARNING:

Code	Message
229	TCP connection reuse should be allowed

3.6.9.4. Verfügbarkeit des DNSKEY-RRSet

Das DNSKEY-RRSet **MUSS** entweder via TCP oder UDP signiert abrufbar sein. Andernfalls erfolgt die Ausgabe eines entsprechenden **ERROR**.

ERROR:

Code	Message
219	Unable to retrieve DNSKEY RR with TCP or EDNS0
902	Timeout
908	Connection refused

4. Glossar

4.1. Issues

Code	Severity	Message	Section ref.
101	ERROR	Missing glue record for the nameserver	Nameserver innerhalb der Zone
102	WARNING	Provided glue records not applicable	Nameserver ausserhalb der Zone
104	ERROR	Calculated referral response larger than allowed	Referral Response
106	ERROR	Inconsistent set of nameserver IP addresses	IP-Adressen und RRSet-Konsistenzen

Code	Severity	Message	Section ref.
107	ERROR	Insufficient diversity of nameserver’s IP addresses	Redundante Anbindung
108	WARNING	Refresh value out of range	Refresh
109	WARNING	Retry value out of range	Retry
110	WARNING	Retry value out of range	Retry
111	WARNING	Expire value out of range	Expire
112	WARNING	Minimum TTL out of range	NegTTL
113	WARNING	Primary Master (MNAME) inconsistent across SOA records	Primary Nameserver
115	ERROR	SOA record response must be direct	Kein CNAME-RR
116	ERROR	SOA record response must be authoritative	Autoritative Nameserver
118	ERROR	Inconsistent set of NS RRs	NS-RRSet Konsistenz
120	WARNING	Recursive queries should not be allowed	Keine Rekursiv-Abfragen
125	ERROR	Insufficient diversity of nameserver' s IPv4 addresses	Redundante Anbindung
127	ERROR	Insufficient number of nameservers reachable	Redundante Anbindung
129	ERROR	Invalid IPv4 or IPv6 address	Redundante Anbindung
130	ERROR	IPv6 address is not allocated	IPv6
131	ERROR	IPv6 address is not routable	IPv6
132	ERROR	Could not resolve any IP address for this nameserver	Redundante Anbindung
133	ERROR	Answer must be authoritative	Autoritative Nameserver
200	ERROR	DNSKEY RR ZONE flag (bit 7) must be set	ZONE Bit
201	ERROR	DNSKEY RR REVOKE flag (bit 8) must not be set	REVOKE Bit
202	WARNING	DNSKEY RR SEP flag (bit 15) should be set	SEP Bit
203	ERROR	DNSKEY RR RSA key modulus length in bits out of range	Modulos
204	ERROR	DNSKEY RR RSA public key exponent length in bits must not exceed 128 bits	Exponent

Code	Severity	Message	Section ref.
205	ERROR	DNSKEY RR DSA public key parameter T out of range	T Parameter
206	ERROR	DNSKEY RR DSA public key has invalid size	Bytelänge
207	ERROR	DNSKEY RR public key must be base64 encoded	DNSKEY: Public Key
208	ERROR	Duplicate DNSKEY RR	DNSKEY: Parameter
209	ERROR	DNSKEY RR has invalid protocol	DNSKEY: Protocol
210	ERROR	Max 5 DNSKEY RR allowed	DNSKEY: Parameter
211	ERROR	Inconsistent DNSKEY RR in nameserver response	Status
212	WARNING	Did not find DNSKEY RR from request in all nameserver responses	Sichtbarkeit
213	ERROR	Did not find any DNSKEY RR from request in all nameserver responses	Sichtbarkeit
214	WARNING	Querying some authoritative nameservers via EDNS0 UDP failed	UDP-basiertes EDNS0
216	ERROR	No visible DNSKEY found signing the DNSKEY RR obtained in response	Validierung Proof of Possession
217	ERROR	No visible DNSKEY found in signing directly or indirectly the SOA RR obtained in response	Validierung Chain of Trust
218	ERROR	Received invalid answer to a DO-Bit query	EDNS0 Support
219	ERROR	Unable to retrieve DNSKEY RR with TCP or EDNS0	Verfügbarkeit des DNSKEY-RRSet
220	ERROR	DNSKEY RR has invalid algorithm	DNSKEY: Algorithm
221	ERROR	Unknown flags in DNSKEY RR are set	Erlaubte Werte
227	ERROR	DNSKEY RR GOST public key has invalid size	GOST
228	ERROR	DNSKEY RR ED public key has invalid size	[req:dnskey-alg-eddsa]

Code	Severity	Message	Section ref.
229	WARNING	TCP connection reuse should be allowed	Wiederverwendung der bestehenden TCP-Verbindung
901	ERROR	Unexpected RCODE	
902	ERROR	Timeout	TCP-Erreichbarkeit
903	ERROR	Timeout with recursive resolver	
904	ERROR	Port unreachable	
908	ERROR	Connection refused	TCP-Erreichbarkeit
909	ERROR	Host unreachable	
910	ERROR	Broken pipe	
911	ERROR	Connection aborted	
999	WARNING	Unexpected exception	

4.1.1. Issue-Anpassungen

4.1.1.1. Abgelöste Issues

Code	Severity	Message	Section ref.	Remarks
103	WARNING	Nameservers having IPv6 glue records should have IPv4 glue records too (NS, # of IPv4 glues, # of IPv6 glues)" RECURSION_AVAILABLE ¬ "Recursive queries should not be allowed (resolver)	IP-Adressen und RRSet-Konsistenzen	Obsolet
114	ERROR	Inconsistent serial number across SOA records	IP-Adressen und RRSet-Konsistenzen	Obsolet

Code	Severity	Message	Section ref.	Remarks
118	ERROR	NS query response is empty	NS-RRSet Konsistenz	Obsolet
215	ERROR	Timeout after switching from UDP to TCP - switch to TCP due to truncation	Verfügbarkeit des DNSKEY-RRSet	Obsolet
222	WARNING	Querying some authoritative nameservers via EDNS0 UDP causes timeout	UDP-basiertes EDNS0	Obsolet
223	ERROR	Timeout after switching from UDP to TCP - switch to TCP due to timeout	Verfügbarkeit des DNSKEY-RRSet	Obsolet
224	WARNING	Querying some authoritative nameservers via EDNS0 UDP causes unreachable	UDP-basiertes EDNS0	Obsolet
225	ERROR	Timeout after switching from UDP to TCP	Verfügbarkeit des DNSKEY-RRSet	Obsolet
905	ERROR	Invalid DNSKEY RR public key - conversion problem		Obsolet
906	ERROR	Invalid DNSKEY RR DSA public key - conversion problem		Obsolet
907	ERROR	DNSKEY RR from nameserver response cannot be compared with DNSKEY RR from request - conversion problem		Obsolet

4.1.1.2. Angepasste Issues

Code	Severity	Message	Section ref.	Change
105	ERROR	All IPv6 Addresses must be Global Unicast dedicated, allocated and routable	IPv6	Aufgeteilt in Issues: 130, 131
107	ERROR	Insufficient diversity of nameserver's IPv4 addresses	Redundante Anbindung	Überführt in Issue: 125
107	ERROR	Insufficient number of nameservers reachable via IPv4	Redundante Anbindung	Überführt in Issue: 127
107	ERROR	Insufficient number of nameservers reachable	Redundante Anbindung	Überführt in Issue: 127
119	WARNING	Some Nameservers not reachable via TCP	TCP-Erreichbarkeit	Aufgeteilt in Issues: 902, 908
121	WARNING	Received a truncated response	UDP-basiertes EDNS0	Überführt in Issue: 214
209	ERROR	At least one DNSKEY RR must be specified in request	DNSKEY: Protocol	Message: DNSKEY RR has invalid protocol
212	WARNING	Did not find DNSKEY RR from request in nameserver response	Sichtbarkeit	Message: Did not find DNSKEY RR from request in all nameserver responses
213	ERROR	No DNSKEY RR from request found in nameserver response	Sichtbarkeit	Message: Did not find any DNSKEY RR from request in all nameserver responses
214	WARNING	Some nameservers not reachable via EDNS0 with sufficient packet size	UDP-basiertes EDNS0	Message: Querying some authoritative nameservers via EDNS0 UDP failed
908	ERROR	TCP Connection refused	TCP-Erreichbarkeit	Message: Connection refused
909	ERROR	Socket error		Message: Host unreachable

4.1.1.3. Neue Issues

Code	Severity	Message	Section ref.
133	ERROR	Answer must be authoritative	Autoritative Nameserver
228	ERROR	DNSKEY RR ED public key has invalid size	[req:dnskey-alg-eddsa]
910	ERROR	Broken pipe	
911	ERROR	Connection aborted	