Nameserver Predelegation Check

Dokumentation

Dok.-Version:	1.4.1	**Dok.-Status:**	Final
Dok.-Stand:	01.12.2015	**Dok.-Name:**	Nameserver Predelegation Check-Dokumentation-DNS Services-V1.4.1-2015-12-01

Impressum

Autor(en)	Abteilung	Telefon	E-Mail
DNS Services	DNS Services	+49-69-27 235 272	info@denic.de

Dokument-Freigabe

Dokument-Version	Freigegeben von	Freigegeben am
1.4.1	DNS Services	01.12.2015

Verteiler

Name
Mitglieder
Öffentlichkeit

Inhalt

1. Allgemeines

1.1 Über dieses Dokument

Die vorliegende Dokumentation beschreibt die geltenden Anforderungen an Nameserver und Zonendaten, die erfüllt sein müssen, damit eine Domain von der 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 andere Internetinfrastrukturelemente. 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 RFC 1591 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 RFC 4697[1]. 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.

[1] RFC 4697 Observed DNS Resolution Misbehavior (http://www.ietf.org/rfc/rfc4697.txt)

2. Nameserver Predelegation Check

2.1 Warnungen und Fehlermeldungen des Nameserver Predelegation Checks (Nameserver-Policy)

Obligatorisch zu erfüllende Anforderungen werden mit "muss" oder "darf nicht" beschrieben, ein Verstoß führt zur Ausgabe von ERROR.

Empfehlungen werden mit "soll" beschrieben, ein Verstoß führt zur Ausgabe von WARNING.

2.1.1 Generelle Anforderung

Alle im Auftrag angegebenen Nameserver müssen erreichbar und für die beantragte Zone autoritativ sein [sonst Ausgabe von ERROR].

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 der DENIC ist, eine Delegation aber zu seinen Lasten geht, wird auf diesem Wege das Einverständnis mit dieser Delegation unterstellt, wenn die Zone autoritativ bedient wird. Im übrigen entspricht die Vorabprüfung dem Geist und Text der RFCs 1034[2] und 1035[3].

2.1.2 Redundante Anbindung

1. Es sind mindestens zwei Nameserver erforderlich, 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 [sonst Ausgabe von ERROR].

   Erläuterung: RFC 1035 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 (siehe RFC 4697) bei der Nichterreichbarkeit der Nameserver einer delegierten Zone wird besonderer Wert auf die Diversität in der Netztopologie gelegt.

   Beispiel:

   erlaubt:

   a. *Nameserver1 mit der IP-Adresse: 192.0.2.1 und Nameserver2 mit der IP-Adresse: 198.51.100.1*
   b. *Nameserver1 mit der IP-Adresse: 192.0.2.1 und Nameserver2 mit der IP-Adresse:* 2001:db8:85a3::8a2e:370:7334

   nicht erlaubt:

   c. *Nameserver1 mit der IP-Adresse: 192.0.2.1 und Nameserver2 mit der IP-Adresse: 192.0.2.1*
   d. *Nameserver1 mit IP-Adresse:* 2001:db8:85a3::8a2e:370:7334 und Nameserver2 mit der IP-Adresse: 2001:db8:85a3::8a2e:370:7336

2 RFC 1034 Domain names - concepts and facilities (http://www.ietf.org/rfc/rfc1034.txt)

3 RFC 1035 Domain names - implementation and specification (http://www.ietf.org/rfc/rfc1035.txt)

2.1.3 Glue-Records

1. 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.
    a. Liegt der Nameserver innerhalb der zu delegierenden Domain, muss mindestens eine IPv4- oder IPv6-Adresse (A-/AAAA-RRSet) angegeben werden [sonst Ausgabe von ERROR].
    Erläuterung: In der angegebenen Konstellation ist in jedem Fall mindestens ein Glue-Record erforderlich.
    b. Liegt der Nameserver nicht innerhalb der zu delegierenden Domain, und es wird trotzdem mindestens eine IP-Adresse (v4 oder v6) dazu im Auftrag angegeben, werden diese IP-Adressen bei der Ausführung des Auftrags nicht berücksichtigt [sonst Ausgabe von WARNING].
    Erläuterung: Die 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. Unter jeder im Auftrag angegebenen und berücksichtigten (vergl. 2.1.3.1 a,b) IP-Adresse (v4 bzw. v6) eines Nameservers müssen dessen A- und AAAA-RRSet unmittelbar, vollständig, konsistent und autoritativ ermittelbar sein und mit den Daten im Auftrag übereinstimmen [sonst Ausgabe von ERROR].

    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[4]) 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.

[4] RFC 2181 Clarification to the DNS Specification (http://www.ietf.org/rfc/rfc2181.txt)

2.1.4 Anforderungen an die SOA-Daten in der Zone

1. *Entfällt: Die SOA-Seriennummern der Zonen auf allen Nameservern sollen übereinstimmen [sonst Ausgabe von WARNING].*
2. Für folgende SOA-Werte werden Richtwerte vorgegeben:
    a. "Refresh" soll in folgendem Bereich liegen: 3600 – 86400 (in Sekunden) [sonst Ausgabe von WARNING].
    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.
    b. "Retry" soll in folgendem Bereich liegen: 900 – 28800 (in Sekunden) [sonst Ausgabe von WARNING].
    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.
    c. "Retry" soll zwischen 1/8 und 1/3 von "Refresh" betragen [sonst Ausgabe von WARNING].
    Erläuterung: Hiermit wird sichergestellt, dass die Werte „Refresh“ und „Retry“ in einem solchen Verhältnis zueinander stehen, dass die Umschaltlogik überhaupt zu einem nennenswerten Vorteil führen kann.
    d. "Expire" soll in folgendem Bereich liegen: 604800 – 3600000 (in Sekunden) [sonst Ausgabe von WARNING].
    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% lahm delegiert wird. 1000 Stunden, hier als Obergrenze angenommen, ist ein verbreiteter Wert, oberhalb dessen von einem ernsten Abgleichproblem ausgegangen werden kann, dass nicht ignoriert werden sollte.
    e. "negTTL" soll in folgendem Bereich liegen: 180 – 86400 (in Sekunden). [sonst Ausgabe von WARNING].
    Erläuterung: Dieser Wert bestimmt gemeinsam mit der TTL des SOA-Records die Lebensdauer negativer Antworten nach RFC 2308. 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

1. Das NS-RRSet muss exakt mit der im Auftrag angegebenen Liste der Nameserver übereinstimmen [sonst Ausgabe von ERROR].

   Erläuterung: RFC 1034 sieht vor, dass die Angaben zu autoritativen Nameservern in der delegierenden und in der delegierten Zone übereinstimmen.

2. Für die beantragte Zone (genauer: am Zonen-Apex) darf kein CNAME-RR existieren [sonst Ausgabe von ERROR].

   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.

3. 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].

   Erläuterung: Die Nameserver der 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.

4. Die Angabe des Primary Nameservers im SOA -RR der beantragten Zone soll auf allen Nameservern übereinstimmen [sonst Ausgabe von WARNING].

   Erläuterung: Auch dieser Test dient der Sicherstellung der unter 2.1.4 (1) angesprochenen Konsistenz.

2.1.6 Sonstige Vorgaben an die Nameserver

1. IPv6-Adressen müssen aus einem Adressraum stammen, der als Global Unicast gewidmet, als ALLOCATED[5] markiert und routbar[6] ist. Dies gilt für alle IPv6-Adressen der angegebenen Nameserver, unabhängig davon, ob es sich um einen Glue-Record handelt [sonst Ausgabe von ERROR].

   Erläuterung: IPv6 kennt verschiedene Gültigkeitsbereiche für 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. Rekursive Abfragen sollen nicht zugelassen sein [sonst Ausgabe von WARNING].

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

3. Erreichbarkeit über TCP soll gegeben sein [sonst Ausgabe von WARNING].

   Erläuterung: RFC 1034 und 1035 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 RFC 1123 ausdrücklich unterstützt wird.

---

[5] "IANA IPv6 Global Unicast Address Assignments"

http://www.iana.org/assignments/ipv6-unicast-address-assignments/ipv6-unicast-address-assignments.xml

6 "IANA IANA IPv6 Special Purpose Address Registry"

http://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xml

3. Nameserver Predelegation Check für DNSSEC

3.1 Technischer Hintergrund

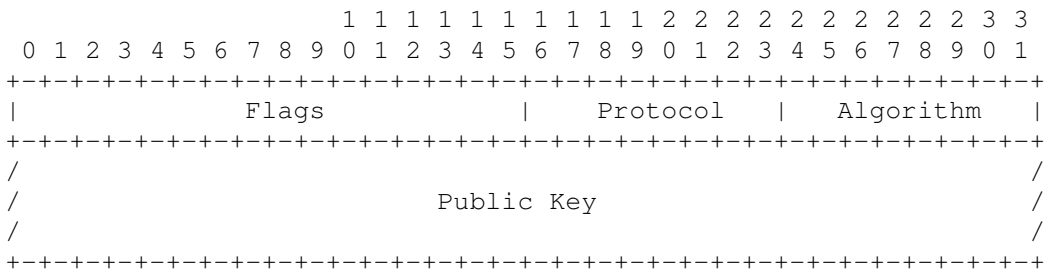
Um für die Validierung bei DNSSEC eine Vertrauenskette (chain of trust) aufbauen zu können, sieht das DNSSEC-Protokoll vor, in der delegierenden Zone einen Hinweis auf den oder die Schlüssel der delegierten Zone zu hinterlegen. Die Vertrauenskette folgt damit dem Delegationspfad.

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[7] erzeugt (derzeit genau ein DS-RR pro mitgeteiltem Trust Anchor), signiert und mit der Zone verteilt.

3.2 Aufbau des Dnskey-Records

Das Format des Dnskey-Records ist in Kapitel 2 von RFC 4034 beschrieben:



Unter den Flags findet sich je ein Eintrag für das Feld Zone Key und Secure Entry Point. Zusätzliche Erweiterungen für den automatisierten Wechsel eines Trust Anchors sind in RFC 5011[8] beschrieben. 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 Trennung von KSK und ZSK

Mit der erstmaligen Einführung des DS-RR in RFC 3658[9] 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,

[7] Siehe RFC 4034 Resource Records for the DNS Security Extensions (http://www.ietf.org/rfc/rfc4034.txt)

[8] RFC 5011 Automated Updates of DNS Security (DNSSEC) Trust Anchors (http://www.ietf.org/rfc/rfc5011.txt)

[9] RFC 3658 Delegation Signer (DS) Resource Record (RR) (http://www.ietf.org/rfc/rfc3658.txt)

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 RFC 4641[10].

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 Nutzung und Veröffentlichung von Schlüsseln

Ein zur Registrierung übergebener DNSKEY-RR ist sichtbar, wenn er im DNSKEY-RRSet einer Zone enthalten ist.

3.5 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. Aus Sicherheitsgründen ist eine Übernahme dieser Praxis in den DNSSEC-Betrieb empfehlenswert (siehe auch Kapitel 3.6.3).

3.6 Technische Voraussetzungen und Prüfungen

Zur Übernahme in die Datenbank und zur korrekten Weiterverarbeitung sowie zur Sicherstellung eines ordentlichen Betriebs wird das Schlüsselmaterial einer mehrstufigen Prüfung unterzogen. Zunächst werden die übergebenen Daten an sich untersucht, im folgenden dann Tests unter Einbeziehung der im DNS abrufbaren Information angestellt.

3.6.1 Parameter der übergebenen DNSKEY-Records

Die zur Registrierung übergebenen Schlüssel müssen eindeutig sein, müssen sich also in mindestens einem Feld unterscheiden [sonst Ausgabe von ERROR]. Es kann vorkommen, dass Schlüssel (Public Key) mit unterschiedlichen Flags mehrfach übergeben wird. Key-Tags werden nicht auf Eindeutigkeit geprüft [sonst Ausgabe von ERROR].

3.6.1.1 *DNSKEY: Flags*

Im Feld *Flags* dürfen ausschließlich Bits gesetzt sein, die in der IANA-Registry als zugewiesen markiert sind. [sonst Ausgabe von ERROR]

[10] Siehe RFC 4641 DNSSEC Operational Practices (http://www.ietf.org/rfc/rfc4641.txt)

Das Feld wird ausschließlich als numerischer Wert (0 - 65535) übergeben.

1. Bit 7 (ZONE) muss gesetzt sein [sonst Ausgabe von ERROR].

   Vorgeschrieben in RFC 4034, Kapitel 2.1.1.

2. Bit 8 (REVOKE) darf nicht gesetzt sein [sonst Ausgabe von ERROR].

   Folgt aus Kapitel 2.1 von RFC 5011. Ein Zurückgerufener Schlüssel kann nicht als Trust Anchor fungieren.

3. Bit 15 (SEP) sollte gesetzt sein [sonst Ausgabe von WARNING].

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

Derzeit mögliche Werte sind also 256 (ZONE) und 257 (ZONE, SEP), wobei nur letzterer ohne Warnung akzeptiert wird.

3.6.1.2 *DNSKEY: Protocol*

Das Feld *Protocol* muss den Wert "3" haben. Dieser Wert ist in Abschnitt 2.1.2 von RFC 4034 zwingend vorgeschrieben.

3.6.1.3 *DNSKEY: Algorithm*

Im Feld *Algorithm* dürfen die Werte vorkommen, die in der IANA-Registry[11] enthalten, dort als nutzbar markiert und nicht für private Zwecke reserviert sind.

Derzeit trifft das auf die Werte 3, 5, 6, 7, 8, 10, 12, 13, 14 zu. Als kryptographische Algorithmen sind dabei RSA, DSA, ECDSA und GOST mit verschiedenen Hashverfahren definiert.

3.6.1.4 *DNSKEY: Public Key*

Das Feld Public Key enthält den öffentlichen Schlüssel in Base64-Codierung[12]. Die interne Struktur hängt vom verwendeten Algorithmus ab, so entsprechend auch deren Prüfung:

RSA (Relevant für die Werte 5, 7, 8, 10)

1. Der Modulus muss zwischen 512 und 4096 Bit (jeweils einschließlich) lang sein [sonst Ausgabe von ERROR].

2. Der Exponent darf maximal 128 Bit lang sein [sonst Ausgabe von ERROR].

   Die Grenzen folgen aus RFC 3110[13] und für den Exponenten zusätzlich aus der Begrenzung der Zeilenlänge bei der Provisionierung.

   Eine Bewertung der Schlüsselstärke erfolgt nicht.

DSA (Relevant für die Werte 3, 6)

3. Der Parameter T darf Werte zwischen 0 und 8 (jeweils einschließlich) annehmen [sonst Ausgabe von ERROR].

4. Die Länge muss 213 + T * 24 entsprechen [sonst Ausgabe von ERROR].

---

[11] Domain Name System Security (DNSSEC) Algorithm Numbers (https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml)

[12] Siehe RFC 4648 The Base16, Base32, and Base64 Data Encodings (http://www.ietf.org/rfc/rfc4648.txt)

[13] Siehe RFC 3110 The RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS) (http://www.ietf.org/rfc/rfc3110.txt)

Diese Grenzen sind in RFC 2536[14] festgelegt.

Eine Bewertung der Schlüsselstärke erfolgt nicht.

ECDSA (Relevant für die Werte 13, 14)

5. Für den Algorithmus ECDSAP256SHA256 (13) muss der Schlüssel die Länge 512 Bit haben [sonst Ausgabe von ERROR].
6. Für den Algorithmus ECDSAP384SHA384 (14) muss der Schlüssel die Länge 768 Bit haben [sonst Ausgabe von ERROR].

   Diese Werte ergeben sich aus RFC 6605[15], Abschnitt 4.

GOST (Relevant für den Werte 12)

7. Der Schlüssel muss die Länge 512 Bit haben [sonst Ausgabe von ERROR].

   Dieser Wert ergibt sich aus RFC 5933[16], Abschnitt 2.

[14] Siehe RFC2536 DSA KEYs and SIGs in the Domain Name System (DNS) (http://www.ietf.org/rfc/rfc2536.txt)

[15] Siehe RFC 6605 Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC (https://tools.ietf.org/rfc/rfc6605.txt)

[16] Siehe RFC 6605 Use of GOST Signature Algorithms in DNSKEY and RRSIG Resource Records for DNSSEC (https://tools.ietf.org/rfc/rfc5933.txt)

3.6.2 Sichtbarkeit und Status der DNSKEY-Records

Das DNSKEY-RRSet muss an allen autoritativen Servern identisch sein [sonst Ausgabe von ERROR].

Mindestens einer der zur Registrierung übergebenen Schlüssel muss sichtbar sein [sonst Ausgabe von ERROR]. Für jeden nicht sichtbaren Schlüssel wird eine WARNING erzeugt. 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.

3.6.3 Einsatz der DNSKEY-Records

Mindestens ein sichtbarer zur Registrierung übergebener Schlüssel muss das DNSKEY-RRSet gültig signieren [sonst Ausgabe von ERROR].

Diese Anforderung dient der Umsetzung des *Proof of Possession*.

3.6.4 Validierung mit DNSKEY-Records

Zum SOA-RR der delegierten Zone muss eine aktuell gültige Validierungskette mit mindestens einem sichtbaren zur Registrierung übergebenen Schlüssel existieren [sonst Ausgabe von ERROR].

Ein SOA-RR ist in jeder Zone vorhanden und wird im Rahmen der Predelegationchecks ohnehin abgefragt. Durch die Prüfung der Validierung wird Security Lameness vorgebeugt.

3.6.5 Übergreifende Regeln

Neben den auf die Zonendaten abgestellten Prüfungen ergeben sich durch DNSSEC Anforderungen an die autoritativen Server bzw. die sie umgebende Infrastruktur:

1. Alle autoritativen Server müssen DNSSEC unterstützen, somit auf Anfragen mit dem DO-Bit signierte, DNSSEC-konforme Antworten liefern [sonst Ausgabe von ERROR].
2. Alle autoritativen Server sollen TCP und EDNS0 mit ausreichender Paketgröße unterstützen [sonst Ausgabe von WARNING].
3. Das DNSKEY-RRSet muss auf mindestens einem dieser Wege (also via TCP oder EDNS0) signiert abrufbar sein [sonst Ausgabe von ERROR].

In den Predelegation-Checks wird bereits geprüft, ob DNS über TCP unterstützt wird. Für DNSSEC kommt hier die Variante EDNS0 hinzu, wobei wie in Kapitel 2 beschrieben zunächst eine der beiden Methoden unterstützt werden muß, beim Fehlen der zweiten aber wegen der möglichen operativen Konsequenzen und der Verletzung von Kapitel 3 aus RFC 4035 (ehemals RFC 3226) gewarnt wird. Punkt 3 schließlich formuliert explizit, was als Vorbedingung für die davor genannten Prüfungen ohnehin erfüllt sein muss, nämlich ein Zugriff auf das signierte DNSKEY-RRSet.