FZI Forschungszentrum Informatik
Forschungsbereich EID

Sicherheit für die Top-Level Domain *.de* durch Secure DNS

Projektzeitraum:
1. Oktober 2002 bis 31. März 2003

Vorgelegt von:
Dipl. Phys. Stefan Dieterle
Dr.-Ing. Peer Wichmann

Unter Mitarbeit von:
Dipl. Inform. Erik-Oliver Blass
Cand. Inform. Jochen Breuer
Cand. Inform. Rolf Kampffmeyer
Cand. Inform. Axel Rengstorf

Auftraggeber:
BSI Bundesamt für Sicherheit in der Informationstechnik
Ansprechpartner:
Dr. Stefan Wolf

Karlsruhe, den 14. Mai 2003

Version 1.0

FZI

1 Einführung

1.1 Problemstellung

In der vorgelegten Studie wird der gegenwärtige Betrieb des Domain Name System (DNS) unterhalb der Top-Level Domain *.de* analysiert. Sowohl die Prozesse, die bei der Vergabe und Pflege der Domaindaten notwendig sind, als auch die Bereitstellung des Dienstes DNS werden vorgestellt. Über diese Analyse hinaus wird aufgezeigt, welche zukünftigen Maßnahmen notwendig sind, um Sicherheit für den DNS-Service (die Namens- und IP-Adressumwandlung) zu bieten.

Unterstützt werden die organisatorischen Prozesse durch eine Public Key-Infrastruktur, welche eine Authentifizierung der am Betrieb beteiligten Partner (DENIC, ISP) ermöglicht.

Weitergehende Sicherheitsmaßnahmen, insbesondere das Sicherheitsprotokoll DNSSEC, werden beschrieben. Es wird dargestellt gegen welche Art von Angriffsszenarien eine Schutzwirkung erreicht werden kann. Fragen hinsichtlich der Eignung sowie der Möglichkeit einer zukünftigen Einführung werden beurteilt.

Sicheres DNS („Secure DNS“[1]) ist nicht einfach nur eine kryptografische Absicherung des DNS-Protokolls, sondern eine umfassende Erweiterung des gegenwärtigen DNS-Dienstes, welche sich vor allem auf die organisatorischen und infrastrukturellen Prozesse auswirkt und deren Änderung bzw. Erweiterung erfordert. Dies macht die Einführung kompliziert und aufwändig.

Ist die Absicherung des DNS-Dienstes überhaupt notwendig?

Der Domain Name Service darf als einer der grundlegenden Dienste der Internetkommunikation angesehen werden, quasi als deren Rückgrat. Die Umwandlung der Web- und Emailadresse oder des Hostnamens auf die numerische IP-Adresse steht bei den meisten Diensten am Anfang. Kann dieser Dienst nicht zweifelsfrei gewährleistet werden, dann ist bei der aufgebauten Verbindung sogenanntes DNS-spoofing[2] nicht ausgeschlossen. Missbrauch wie z.B. Denial of Service, Darstellung betrügerischer Informationen auf falschen Webseiten, oder die Manipulation übermittelter Daten sind nur ein paar der möglichen Schadensszenarien.

Das Internet wird für die private, kommerzielle und behördliche Kommunikation immer wichtiger. Dies bedeutet aber auch, dass E-Commerce Angebote wahrgenommen werden und auch E-Government- Dienstleistungen für den Bürger zu den selbstverständlichen Abläufen gehören. Durch die E-Government-Aktivitäten ist der Staat mit seinen Dienstleistungen auch im Internet präsent. Neben dem Schaden, den die öffentlichkeitswirksame Darstellung durch Sicherheitsmängel nehmen würde, gibt es auch zahl-

[1] Unter Secure DNS verstehen wir im Folgenden die Sicherheitsprotokolle DNSSEC, TSIG und SIG(0) zusammen mit den begleitenden infrastrukturellen und organisatorischen Maßnahmen, die notwendig sind, um eine kryptografisch gesicherte verlässliche Bereitstellung des Domain Name Service zu gewährleisten. In der Literatur wird dies oft auch als DNSSEC bezeichnet und synonym verwendet. Ebenfalls ist die Bezeichnung Domain Name System Security Extensions aus [RFC 2535] gebräuchlich.

[2] Spoofing kann in diesem Zusammenhang durch Manipulation übersetzt werden.
Anglizismen werden im Text dann verwendet, wenn es in der Fachsprache üblich ist, diese zu gebrauchen bzw. wenn eine Übersetzung die Bedeutung ändern würde. Die Anglizismen werden im Anhang aufgeführt.

reiche Angebote, deren Ausfall oder Verwundbarkeit fatale Folgen für die Gesellschaft haben könnten.

Im Hinblick auf die zukünftige Entwicklung des Internets ist es notwendig, für eine stabile Bereitstellung dieser Infrastruktur zu sorgen, damit sich sowohl der Bürger als auch die Wirtschaft auf das Funktionieren dieser Prozesse verlassen können.

Die Unterstützung des Sicherheitsprotokolls DNSSEC kann zusammen mit ergänzenden Maßnahmen die Sicherheit bei der Umwandlung der Internetnamen in IP-Adressen und umgekehrt gewährleisten.

1.2 Ziel der Studie

Auf welche Fragen gibt die Studie Antworten?

- Wie sicher ist der derzeitige DNS-Betrieb, gibt es Gefahren und Schwachpunkte?
- Sind Sicherheitsprotokolle wie DNSSEC notwendig?
- Welche infrastrukturellen Maßnahmen sind hierfür erforderlich?
- Ist eine PKI-Unterstützung vorteilhaft?
- Wie sehen die internationalen Schnittstellen aus?
- Welches sind die empfohlenen nächsten und übernächsten Schritte?

Welche Thesen werden durch die Studie gestützt?

- DNS ist auch bei maximaler Sicherheitsunterstützung durch Administration und Systemschutz immer noch ein unsicheres Protokoll.
- Das Protokoll DNSSEC lässt sich vorteilhaft mit einer PKI verknüpfen.
- Nimmt der Kontakt zwischen Registrar, Registry und Zonenbetreibern durch häufigeren Schlüsselaustausch zu, dann müssen in größerem Rahmen automatisierte Verfahren zum Einsatz kommen. Dies begünstigt eine PKI-Unterstützung.
- Der Sicherheitsbetrieb DNS erzwingt Betriebsrichtlinien auf unterschiedlichen Ebenen.
- Eine Vielzahl an technischen und organisatorischen Schwierigkeiten sind zu bewältigen.

1.3 Inhalt

Nachfolgend wird der Inhalt der einzelnen Kapitel der Studie vorgestellt.

Kapitel 2

stellt den herkömmlichen DNS-Betrieb für die Top-Level Domain *.de* und die hierfür Verantwortlichen vor. Herkömmliche Sicherheitsempfehlungen werden angesprochen.

Kapitel 3

Die DENIC eG wird im Kontext der internationalen Organisation betrachtet.

Kapitel 4

Die möglichen Angriffszenarien werden genannt und Bedrohungsszenarien vorgestellt. Als Ausweg wird Secure DNS vorgeschlagen.

Kapitel 5

Das Sicherheitsprotokoll DNSSEC wird erklärt. Das Umfeld der Problemstellung (Standardisierung, Serversoftware, Client-Applikationen) wird erörtert.

Kapitel 6

Für die Umsetzung ist es notwendig, DNSSEC in eine Public Key-Infrastruktur einzubinden. Grundlegende PKI-Aufgaben und Sicherheitsanforderungen werden vorgestellt und auf die DENIC eG angewendet.

Kapitel 7

Die Ausgestaltung organisatorischer Prozesse, die den bisherigen DNS-Betrieb auf Seiten der ISP und der DENIC eG erweitern, werden angedacht.

Kapitel 8

Die Standardisierungsbemühungen sind schon weit gediehen, aber noch nicht abgeschlossen. Kapitel 8 versucht eine Antwort auf die Frage - „Wann ist das Protokoll fertig zum Einsatz?“ - zu geben.

Kapitel 9

Secure DNS ist kein Allheilmittel. Es bleiben weitere Problemstellungen, für die Lösungen gefunden werden müssen.

Kapitel 10

Die Ergebnisse werden in einer Empfehlung zusammengefasst.

2 Ausgangslage DNS-Betrieb

Zuständig für die Registrierung von Domainname unterhalb der Top-Level Domain *.de* und den Betreib des Primary Nameservers für *.de* ist die DENIC eG (www.denic.de). Eine Chronologie der DENIC-Entwicklung ist im Tätigkeitsbericht 2002 abgedruckt [DENIC-TB]. DENIC ist eine eingetragene Genossenschaft. Die Mitglieder[3] sind die sogenannten Internet Service Provider (ISP). Derzeit (Februar 2003) sind dies 183 (siehe Abbildung 1). Aus der Entwicklung der Mitgliederzahlen ist - neben den ebenfalls immer noch anwachsenden Zahlen für registrierte Domainnamen (Abbildung 2) - auf eine weiter zunehmende Verbreitung des Internets in Deutschland zu schließen.

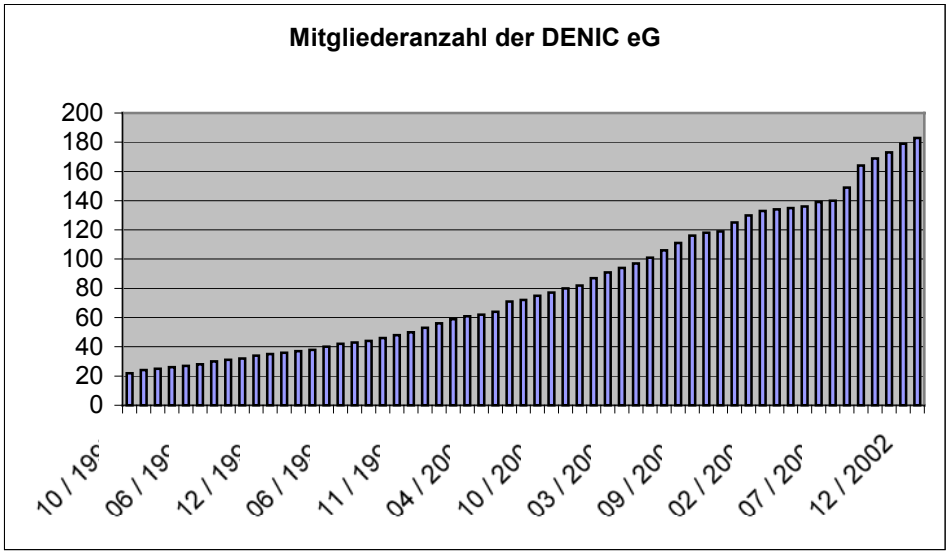


Abbildung 1: Entwicklung der DENIC Mitgliederzahlen, 1997-2003

Zu den Aufgaben der DENIC eG gehören:

- Betrieb des Primary-Nameservers für die Top-Level Domain *.de*
- Bundesweit zentrale Registrierung von Domains unterhalb der Top-Level Domain *.de* [4]
- Administration des Internet in Zusammenarbeit mit internationalen Gremien (CENTR, ICANN, CORE). Diese werden in Kapitel 3 vorgestellt.
- Bereitstellung verschiedener Datenbankdienste (für die Domainregistrierung und „whois[5]“ Abfage.
- Bereitstellung verschiedener Informationen, insbesondere zu rechtlichen Fragen bei der Domainregistrierung und -verwaltung

[3] Eine Liste aller DENIC Mitglieder ist unter http://www.denic.de/doc/DENIC/mitglieder.shtml erhältlich.

[4] Domaindaten sind: Domainnamen, 2 Nameservereinträge in unterschiedlichen Subnetzen, admin-c, tech-c, zone-c, DENIC-handle bzw. RIPE-handle).

[5] whois - Internet user name directory service. Mittels des Dienstes “whois” können bei DENIC Informationen zu Domainnamen abgefragt werden.

Abbildung 2: Anzahl der registrierten Domainnamen unterhalb .de

Die dargestellten und weitere Statistiken finden sich unter [DENIC-Stat].

2.1 Daten zur Betriebstechnik DNS für *.de*

Mittlerweile betreibt DENIC ein Netz aus einem Primary-Nameserver und zehn Secondary-Top-Level Domainservern für *.de*. Diese sind an verschiedenen internationalen Standorten platziert, wie in Abbildung 3 zu sehen ist. Dies führt zu einer Reduzierung der Antwortzeiten. Beispielsweise konnten die Antworten des DENIC Nameservers auf Anfragen aus Japan von 270 auf unter fünf Millisekunden verringert werden [DENIC-P]. Anfragen aus Großbritannien können durch den Server in London in der halben Zeit (25 Millisekunden) beantwortet werden.

DNS-Name	IP-Adresse	Ort
dns.denic.de	194.246.96.79	Frankfurt/Main

Tabelle 1: Primary-Nameserver

DNS-Name	IP-Adresse	Ort
dns2.de.net	194.246.96.49	Frankfurt/Main
sss-de1.de.net	193.159.170.187	Stuttgart
auth03.ns.de.uu.net	192.76.144.16	Dortmund
sss-at.denic.de	193.171.255.34	Wien
sss-jp.denic.de	210.81.13.179	Tokio
sss-nl.denic.de	193.0.0.237	Amsterdam
sss-uk.de.net	62.53.3.68	London
sunic.sunet.se	192.36.125.2	Stockholm
sss-us1.de.net	206.65.170.100	Elmsford, USA

DNS-Name	IP-Adresse	Ort
sss-us2.denic.de	167.216.196.131	San Jose, USA

Tabelle 2: Secondary-Nameserver

Die Gründe für diese weltweite Verteilung des DENIC Nameservernetzes liegen darin, dass in Spitzenzeiten jeder einzelne Server über 20.000 Anfragen pro Minute beantworten muss. Insgesamt zählt DENIC täglich mehr als 100 Millionen Anfragen an seine DNS-Server[6,7]. An diese Server werden bzgl. Der Performance und Verfügbarkeit sehr hohe Anforderungen gestellt. Konzepte zur Ausfallsicherheit und Redundanz sind umgesetzt. Als Nameserversoftware wird ISC-Bind in der Version Bind 9.2.1 und 8.3.4 mit jeweils den aktuellen Patches eingesetzt[8]. Die Nameserver werden einmal am Tag neu gestartet. Ein dynamischer Update findet nicht statt. Konzepte zur Unterstützung dieses Verfahrens werden aber evaluiert. Das Zonenfile wird nach der Erstellung vom Primary an die Secondary-Server mittels scp[9] verteilt.

Abbildung 3: .de-Nameserver[10]

2.2 Statistische Daten zur *.de* Zone

Derzeit (Januar 2003) sind **4.516.135** delegierte[11] Domains und **1.583.831** Domains mit direkten MX/A Einträge[12] (NSentry-Domains) in der .de Zone eingetragen. Insgesamt sind das **6.099.966** Domains**.** Dies entspricht einer Zonenfilegröße von über 550 MByte. Zuständig für diese Informationen sind insgesamt 9.227.594 Nameserver Einträge. Da-

[6] Pressemitteilung DENIC, 12. November 2002: Neue DeNIC-Nameserver zeigen Wirkung. http://www.denic.de/doc/DENIC/presse/nameserver2.html
[7] Die Namen der *.de*-Rootserver sind auch mit dem Unix Kommando `dig @a.root-servers.net de. any` abrufbar.
[8] Heterogenität: Durch den Einsatz verschiedener Bind-Versionen für den Nameservice-Betrieb soll erreicht werden, dass nicht das gesamte Primary-Secondary-System durch denselben Angriff verwundbar ist.
[9] http://www.openssh.org
[10] DENIC Abbildung http://www.denic.de/images/nameservermap.gif
[11] Domains mit vollem IP-Zugang und Nameserverunterstützung (NS).
[12] MX/A Domains haben keine externe Nameserverunterstützung und werden daher direkt in die *.de*-Zone eingetragen. Sie werden für Electronic Mail oder Adresseeinträge verwendet (http://www.denic.de/hilfe/domainauftrag.html).

bei handelt es sich nicht um verschiedene Server. Es wird meistens auf einem Server der Nameservice für mehrere Domains bereitgestellt. Insgesamt sind für die **6.099.966** Domains 34.168 unterschiedliche Nameserver zuständig.

Der Abbildung 4 ist zu entnehmen, dass auf 22 Servern 45,8% der Domains delegiert werden. Dies sind vorwiegend die Nameserver der großen ISPs mit teilweise über 200.000 Domains auf einem Nameserver. Am anderen Ende befinden sich 50.811 Domainnamen, die auf halb so vielen Rechnern betrieben werden. Dies sind meist Kunden, die ihren Nameservice selbst betreuen. Der Provider stellt dann nur den Secondary-Service zur Verfügung.

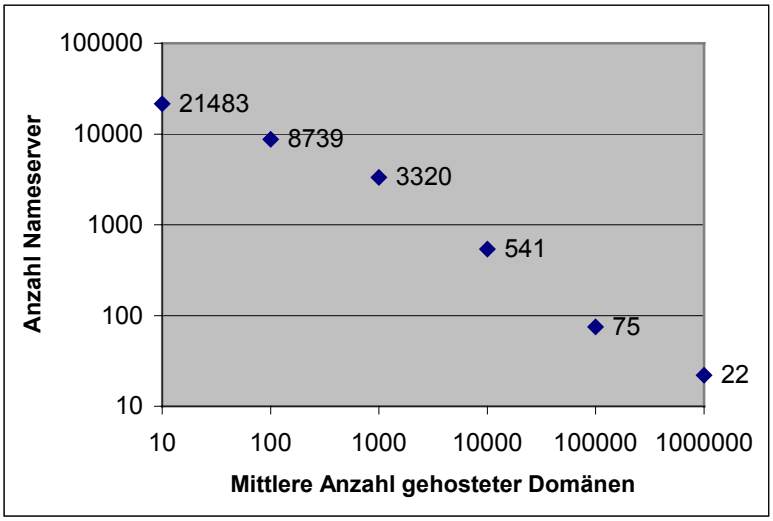


Abbildung 4: Verteilung der Domainnamenszuständigkeit auf die Internet Nameserver

Bereich	Anzahl an Domains im Bereich	Anzahl an NS im Bereich
1 – 9	50811	21483
10 -- 99	304006	8739
100 -- 999	1286097	3320
1000 -- 9999	1476056	541
10000 -- 99999	2091692	75
über 100000	4402362	22

Tabelle 3: Datengrundlage für Abbildung 4

2.3 Sicherheitsbetrieb DENIC

DENIC nimmt seine Verantwortung bezüglich des sicheren DNS-Betriebes sehr ernst. Dies ist dem jährlichen Jahresbericht zu entnehmen. Verschieden Maßnahmen machen dies deutlich [DENIC-TB]:

1999:

a) Evaluierung und Implementierung eines DNSSEC-Protokolls, um sicheres IP in der *.de*-Zone zu ermöglichen. (siehe Abschnitt 4.7.2 DENIC-Studie).

b) Aufbau eines eigenen Secondary-Systems (3 bis 4 Standorte) in Kooperation mit anderen nationalen Domainregistrierungsstellen.

c) Verbesserung der Performance und Verfügbarkeit

2000:

a) Fortsetzung der Untersuchung zur DNSSEC-Evaluierung

b) Fortführung des Aufbaus eines eigenen Secondary-Systems

c) Einrichtung einer Backup-Lokation für die Technik

d) Redundanz der Stromversorgung

2001:

a) Schwerpunktthema Internetsicherheit

b) Redundante Verfügbarkeit aller Dienste

c) Schwachstellenanalyse

d) Zugangskontrolle

e) Test von Notfall- und Ausfallszenarien

f) Erstellung eines Risikohandbuchs

g) Verbesserte Betriebsüberwachung

2002:

a) Einführung PGP-Signaturen für das Registrierungssystem

b) Ausbau Backup Rechenzentrum

c) Datenspeicherung in DBS

d) Inhaltliche Unterstützung der vom BSI an das FZI in Auftrag gegebenen Studie zu Secure DNS.

2.4 Internet Service Provider

Die Internet Service Provider stellen ihren Kunden lokale Zugänge zum Internet zur Verfügung[13] und vertreten gegenüber der DENIC die Kundenwünsche für die Domainregistrierung. Möchte ein Internetbenutzer eine Domain registrieren, dann wendet er sich an einen Internet Service Provider. Dieser ISP kann, sofern er Mitglied[14] bei der DENIC eG ist, den Domainauftrag an DENIC weitergeben. Ist der beantragte Name noch nicht registriert, kann er für den Kunden beantragt werden. Die ISPs bieten weitere unterschiedliche Dienstleistungen bezüglich des Hostings, der Internetpräsenz, des Mailzugangs und des DNS-Dienstes an.

2.4.1 Sicherheitsbetrieb ISP

Bei einigen ISPs wurde im Rahmen der Studie eine Befragung zu den organisatorischen Abläufen und den Sicherheitsanforderungen an den Betrieb durchgeführt. Diese wurde jedoch nur bei wenigen Mitgliedern vorgenommen und ist somit statistisch nicht repräsentativ. Bei den Befragten handelt es sich meist um größere Betreiber, die eine langjährige Erfahrung im DNS-Betrieb besitzen.

[13] Nicht alle ISP's sind Access Provider.
[14] Nichtmitglieder (Reseller) haben über einen registrierten ISP die Möglichkeit, die Domainanträge an das DENIC weiter zu leiten.

Die Befragung ergab folgende Ergebnisse:

- Der Computer auf dem der Nameserver läuft, wird vorwiegend nur für den Nameservice eingesetzt.
- Trennung von Nameservice für delegierte Domains und dem Dienst „Kundennameservice[15]“. Es werden getrennte Server eingesetzt.
- Sicherheitsproblem mit ISC-BIND sind bekannt, aktuelle Patches werden regelmäßig eingespielt.
- Logfile Auswertung zur Erkennung von Angriffen. Spezielle Spoofing-Angriffe wurden nicht festgestellt.
- Transaktions- Signaturen werden beim Zonentransfer nicht eingesetzt.
- Der dynamische Update-Mechanismus wird eingesetzt, Secure Dynamic Update ist bisher noch nicht bekannt.
- Die Methoden der Kundenauthentifizierung sind unterschiedlich.

Während der Gespräche konnte auch ein großes Interesse an der Technik DNSSEC festgestellt werden. Es wurde vorgeschlagen, die Ergebnisse der Studie an die Internet Service Provider u.U. in modifizierter Form zu verteilen.

2.5 Sicherheitsbetrieb Domainregistrierung

Die ISP müssen sich authentifizieren, um ihre Anträge über Email an DENIC zu stellen (eine Webschnittstelle bzw. das EPP-Verfahren[16] sind in Vorbereitung). Seit dem 1. Oktober 2002 ist die Verwendung des Public Key-Verfahrens PGP zwingend vorgeschrieben[17]. DENIC tritt an dieser Stelle als Zertifizierungsinstanz (CA) auf. Ein Provider, der an diesem Verfahren teilnehmen möchte, um seine Anträge stellen zu können, muss persönlich bei DENIC vorstellig werden, um seinen Registrierungsantrag abzugeben. Alternativ wird eine telephonische Überprüfung durchgeführt. Die Schlüsselgenerierung wird vom Provider selbst vorgenommen. Der öffentliche Schlüssel wird von DENIC zertifiziert. Die weitere Emailkommunikation findet unter Verwendung der Provider- und der DENIC-Schlüssel statt.

Der Ablauf eines Auftrages zur Domainverwaltung ist in Abbildung 5 skizziert.

[15] Kundennameservice meint, dass ein Server zur Verfügung steht, den die Kunden für die Namensauflösung auf ihrem lokalen Computer eintragen können. Dieser Nameserver muss rekursiv betrieben werden. Dies stellt für die Sicherheit gegen Spoofing-Angriffe ein erhöhtes Risiko dar.
16 EPP: Extensible Provisioning Protocol. zur Standardisierung vorgeschlagenes Verfahren für die Domainregistrierung.
[17] DeNIC will sicherer werden. DeNIC-Sicherheitsloch: Alle *.de*-Domains manipulierbar
http://www.ix.de/newsticker/result.xhtml?url=/newsticker/data/pab-16.11.01-000/

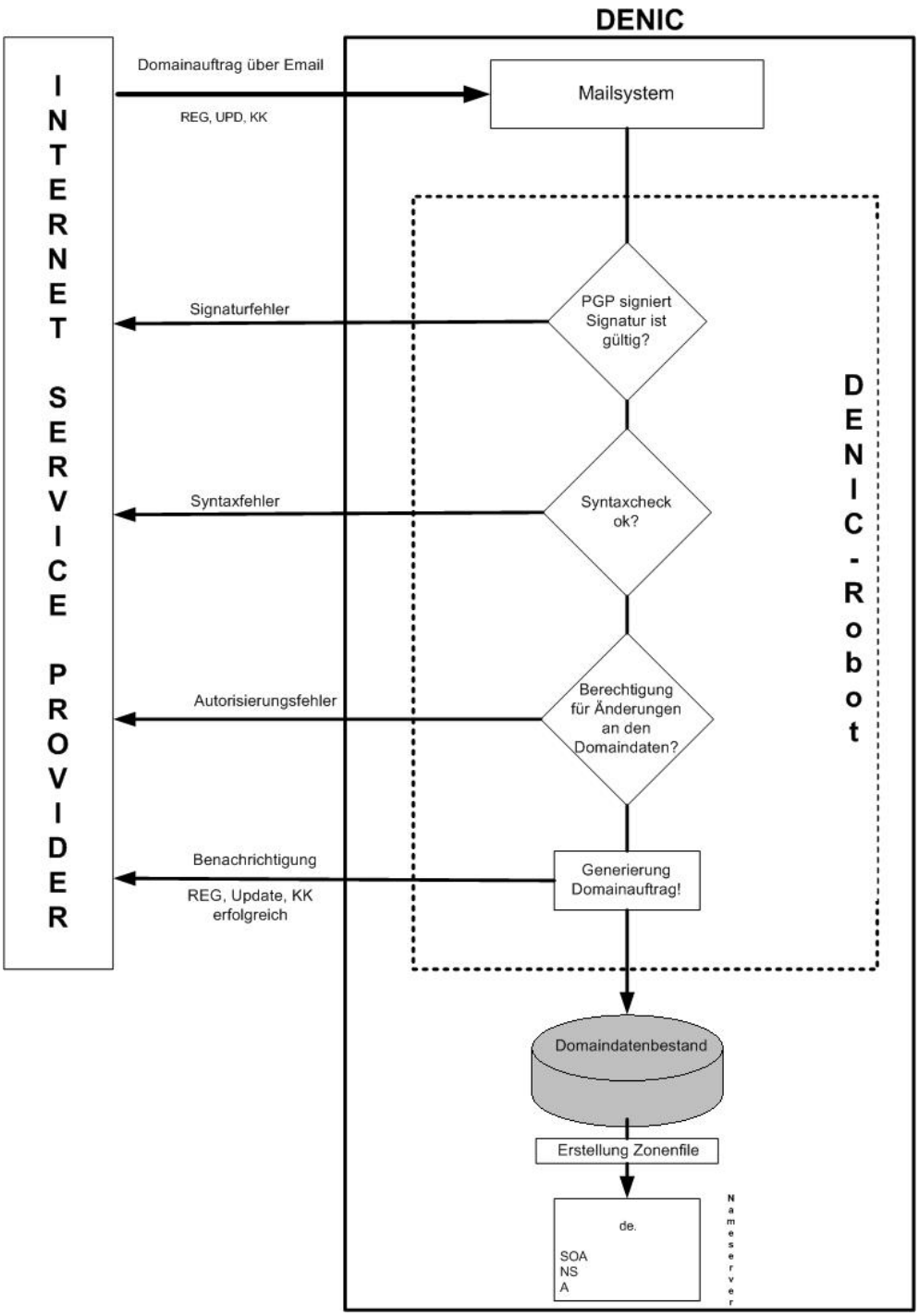


Abbildung 5: Domainantragsverwaltung bei DENIC

Die Registrierungsrichtlinien und Abläufe sind durch die DENIC eG vorgegeben. Das Registrierungsverfahren ist im Vergleich zu anderen (z.B. EPP siehe Abschnitt 6.2.2) proprietär und beruht nicht auf einem allgemeinen Standard. Es gibt aber Bestrebungen von DENIC, ein standardisiertes Verfahren anzubieten.

Das von DENIC eingesetzte Verfahren, die Authentizität der Teilnehmer und die Integrität der Daten mittels PGP-Signaturen zu verifizieren, kann als hinreichend sicher eingestuft werden. Wichtig ist hierbei, dass die zugrunde liegende PKI zuverlässig arbeitet.

In Kapitel 3 werden die Voraussetzungen für verlässliche PKI-Prozesse untersucht und eine Empfehlung ausgesprochen.

Nach erfolgreichem Eintrag der Daten in die Datenbank stehen die Daten für die Erzeugung der Zonendatei zur Verfügung. Dies geschieht einmal täglich. Nach einer Plausibilitätsprüfung der erzeugten Zone wird die Zone vom Primary-Nameserver einmal am Tag neu geladen. Außerdem wird die Zone an die Secondary-Nameserver verteilt.

2.6 Sicherheitsbetrieb Zonenverwaltung

Die Sicherheitsanforderungen an den Nameservice sind abhängig von der Stelle im Domainnamensbaum für die er betrieben wird. Je weiter oben ein erfolgreicher Angriff platziert werden kann, desto größer ist die Anzahl der betroffenen Nutzer, die letztendlich betroffen ist. Beispielsweise trägt DENIC mit *.de* eine größere Verantwortung als eine Domain, die unterhalb *.de* eingehängt ist. Darüber hinaus sind die Sicherheitsanforderungen auch abhängig vom „Zweck“ der Domain: Beispielsweise ist *bund.de* sicherlich sensitiver als „*lise-mueller-privat.de*“

Auf der Ebene der Domainnamen findet eine unterschiedliche Administration statt. Bei großen Zonen, wie sie von Unternehmen, öffentlichen Einrichtungen und Forschungsinstituten betrieben werden, ist meistens ein Administrator für die ordnungsgemäße DNS-Administration verantwortlich. Bei kleinen Zonen, wie sie privat oder für eine einfache Internetpräsenz (die sehr wohl auch wichtigen kommerziellen Zwecken dienen kann) vorkommen, wird die Administration des DNS vom Provider oder vom Kunden selbst durchgeführt. Die eigene DNS-Administration wird z.B. im Falle eines sogenannten „Root-Servers“[18]von einigen Webservice-Providern angeboten, bei denen die Kunden einen eigenen Internetserver mit Root-Zugriff gemietet haben. Es liegt nahe, dem professionellen Betrieb eine höhere Sicherheitsgarantie zuzusprechen. Dies liegt zum einen an der Erfahrung der Administratoren, vor allem aber daran, dass der DNS-Service auf Root-Servern als zusätzlicher Dienst läuft. Somit ist ein solcher Server über eine Vielzahl von Diensten, die er anbietet, angreifbar. Ein Nameserver sollte in der Regel immer nur Nameservice anbieten.

[18] Als Root-Server wird von verschiedenen Web-Hosting-Anbietern ein Computer bezeichnet, der vom Kunden selbst administriert wird (Root-Zugriff).

3 Internationale Schnittstellen

Der DNS-Betrieb für *.de* ist Teil des ganzen Domainnamensbaum. Auf derselben Hierarchieebene befinden sich weitere Länder Code Top-Level-Domains (ccTLDs) und die generischen Top-Level-Domains (gTLDs). Darüber ist die Root, die die Verantwortlichkeit für *.de* an DENIC delegiert. Daher ergeben sich einige Schnittstellen zu anderen Internetorganisationen, gerade auch überregional. In diesem Kontext muss die DENIC-Politik betrachtet werden.

3.1 Internethistorie

Der Geburtsort des Internets liegt in den USA. Dort wurden 1969 die ersten 4 Computerzentren miteinander verbunden. Auch die anfängliche Protokollentwicklung (RFC's) und der Ausbau des Netzes fanden dort statt. Deutschland bekam erst 1983 einen Anschluss an das Internet[19].

Daher ist es nicht überraschend, dass die wichtigsten Gremien mehrheitlich von US-Bürgern und US-Unternehmen besetzt sind. Mittlerweile jedoch ist das Internet nicht mehr nur ein rein amerikanisches Netzwerk, beinahe alle Länder sind an das Internet angeschlossen. Über die Anzahl der Domains unter der betreffenden Top-Level Domain, können auch erste Rückschlüsse über die Nutzung und wirtschaftliche Bedeutung des Internets in diesem Land gezogen werden. Beispielsweise ist die *.de*-Zone die größte ccTLD weltweit und kommt bei allen TLDs nach *.com* an der zweiten Stelle.

Rang	Domain	Registriert	Zugehörigkeit
1	.COM	21,336,063	Commercial
2	.DE	5,459,604	Germany / Deutschland
3	.NET	3,631,270	Network
4	.CO.UK	3,080,659	UK Commercial
5	.ORG	2,333,855	Organization
6	.INFO	828,223	Information
7	.IT	681,779	Italy
8	.BIZ	666,399	Business
9	.NL	617,045	The Netherlands
10	.CC	581,147	Cocos (Keeling) Islands
11	.TV	473,168	Tuvalu
12	.COM.AR	463,571	Argentina
…	...	…	...
358	.ZR	0	Not in use

Abbildung 6: Domain Zählung vom 2. März 2003

[19] http://de.dir.yahoo.com/computer_und_internet/internet_und_www/geschichte/
http://www.michaelkaul.de/Geschichte/geschichte.html
http://www.w3history.org/
Ross Wm. Rader, The Historie of DNS, June 2001. http://www.whmag.com/content/0601/dns/

Einen Überblick über den aktuellen Stand der Domainvergabe der betreffenden Top-Level Domains findet sich unter http://www.domainworldwide.com/. Allerdings gibt es auch ganz gravierende Ausnahmen wie etwa die global operierenden ccTLDs „*.tv*" oder „*.cc*". In Abbildung 6: Domain Zählung vom 2. März 2003 ist ein Ranking der zahlenstärksten Domains angegeben.

Aufgrund dieser weltweiten Internetnutzung werden immer wieder Forderungen laut, die US-Zentrierung aufzuheben und die Entscheidungsgremien mit einer stärkeren Beteiligung der anderen Länder zu besetzen. Aber nicht nur die Entscheidungsgremien auch große Teile der Internetinfrastruktur werden von den Amerikanern betrieben. Sie stehen zwar dem Rest der Welt zur Verfügung, allerdings mit gewissen Nachteilen[20,21].

So stehen beispielsweise nur 3 von 13 Rootservern an Standorten außerhalb der USA[22]. Dies ist aus netztopologischen Gesichtspunkten bezüglich der Erreichbarkeit und Lastverteilung ein erheblicher Nachteil. Dass eine gleichmäßige Verteilung der Root-Server sinnvoll wäre, zeigt sich auch daran, dass DENIC die Top-Level Domain Server für *.de* mittlerweile an verschiedenen internationalen Standorten platziert hat .

Im Folgenden werden die wichtigsten Internetorganisationen vorgestellt. Ein Überblick findet sich auch unter den DENIC Seiten[23] und bei der ISOC[24].

3.2 ISOC

Die **I**nternet **SOC**iety http://www.isoc.org ist eine internationale Organisation für die Zusammenarbeit und die Koordination des Internets, der Netzwerktechnologie und Anwendungen. Das Hauptziel ist die Förderung eines globalen Informationsaustausches. Sie ist eine Dachorganisation und umfasst die Internet Engineering Task Force (IETF), das Internet Architecture Board (IAB), die Internet Engineering Steering Group (IESG), und die Internet Research Task Force (Abbildung 7).

Diese Organisationen sind für die Festlegung der Internet Standards (RFC's) zuständig. Die Entwicklung dieser Standards geschieht auf einer breiten Basis (bottom up Ansatz) durch die Diskussion auf Mailinglisten und während IETF-Tagungen. An dieser Standardisierungsarbeit nehmen weltweit tausende von Entwicklern teil.

Die Mitglieder der ISOC drücken die ganze Breite der Internetgemeinschaft aus. Sie besteht aus Privatpersonen, Firmen, non-profit-Organisationen und Regierungsvertretungen. Das wichtigste Entscheidungsgremium der ISOC ist das Board of Trustees. Zur Erörterung technischer Fragen werden sogenannte Task Forces eingerichtet.

Für die technologische Weiterentwicklung des Internets, wurden 1983 zwei Organisationen gegründet. Die Internet Engineering Task Force (IETF) und die Internet Research Task Force (IRTF). Beide bestehen aus mehreren Arbeitsgruppen (WG) mit bestimmten Aufgabengebieten.

[20] Heise Online 21.12.2001. DNS-Root-System soll unter US-Aufsicht bleiben. http://www.heise.de/newsticker/data/jk-21.12.01-001/

[21] Der A-Root-Server, der Oberste aller Root-Rechner, steht nach wie vor unter der Kontrolle des US-Handelsministeriums. Diesem ist die ICANN darüber hinaus weisungsgebunden.

[22] Eine Übersicht über alle Rootserver findet sich unter http://root-servers.org/.

[23] http://www.denic.de/doc/kontextintro.html

[24] http://www.isoc.org/standards/orgs.shtml

Die Vorsitzenden dieser WG bilden zusammen mit weiteren Wissenschaftern die Internet Engineering Steering Group (IESG) bzw. die Internet Research Steering Group.

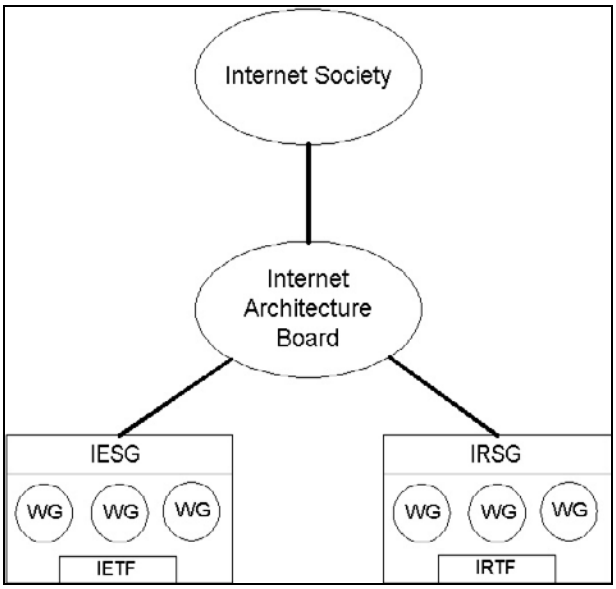


Abbildung 7: Dachorganisation ISOC

3.2.1 IETF

Die **I**nternet **E**ngineering **T**ask **F**orce ist eine große offene internationale Gemeinschaft von Netzwerkdesignern, Internetbetreibern, Firmenvertretern und Forschern, die alle mit der Entwicklung der Internet Architektur und dem reibungslosen Betrieb des Internets betraut sind. Die aktuelle technische Arbeit der IETF wird in Arbeitsgruppen von unterschiedlicher thematischer Ausrichtung[25] (z.B. Routing, Transport, Sicherheit) vorgenommen. Dabei findet die meiste Kommunikation über Mailinglisten statt. Dreimal jährlich wird ein großes Meeting veranstaltet, um operationale und technische Probleme zu lösen [RFC 3160]. Vom 16-21. März 2003 fand das 56th IETF Meeting in San Francisco, CA, USA statt.

Die Mitarbeit bzgl. des Domain Name Systems geschieht über zwei Arbeitsgruppen.

1. dnsop: Domain Name Server Operations

   Hierin werden Richtlinien für den DNS-Betrieb und die Administration entwickelt. Protokollspezifische Fragestellungen gehören ebenso dazu, wie die Leistungsanalyse des Betriebs. Auch aktuelle DNSSEC-Themen werden verfolgt.

2. dnsext: DNS Extensions

   Hier werden ausschließlich Themen diskutiert, die mit der Protokollentwicklung von DNSSEC in Zusammenhang stehen.

Die Diskussion auf den Mailinglisten sind technisch sehr anspruchsvoll und zeichnen sich durch ein hohes Emailaufkommen aus. Neben allgemeinen protokollspezifischen Fragen, werden sehr häufig sogenannte Drafts vorgestellt. Drafts sind Dokumente mit einer 6 monatigen Lebensdauer. Während dieser Zeit werden sie durch die Mitglieder der Mailinglisten verbessert, überarbeitet und anschließend verlängert oder verworfen. Wird ein Draft akzeptiert, dann wird er in den Status eines RFC's erhoben [RFC 2026].

[25] http://www.ietf.org/html.charters/wg-dir.html

3.2.2 IRTF

Ähnlich wie die IETF ist auch die **I**nternet **R**esearch **T**ask **F**orce organisiert. Die IRTF bildet das wissenschaftliche Gerüst, in dem zukünftige Entwicklungen und Vorschläge für neuartige Techniken entwickelt werden sollen.

3.2.3 IAB

Das **I**nternet **A**rchitecture **B**oard http://www.isi.edu/iab/ ist verantwortlich für die Definition einer umfassenden Internetarchitektur. Das IAB unterstützt die IETF durch Beratung. Weiter fungiert das IAB als Gutachter für die ISOC und beaufsichtigt eine Reihe von kritischen Internet Aktivitäten.

3.3 ICANN

Die **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers - 1998 gegründet - ist eine non-profit-Organisation, welche zuständig ist für die Vergabe von IP-Adressen und Top-Level Domainnamen. Außerdem fällt der Betrieb des Root-Server-Systems und die Koordination der Internettechnologien (Protokolle, Parameter und Dienste) in ihren Aufgabenbereich. Diese Aufgaben oblagen früher der IANA[26].

„In den Arbeitsgruppen der ICANN ist DENIC seit Anbeginn mit dem Ziel einer kritischen, aber konstruktiven Mitarbeit präsent." [Jahresbericht 2002]. Dass dies notwendig ist, zeigt ein Vorfall im Juni 2002. Seit diesem Zeitpunkt weigerte sich ICANN die Eintragung neuer *.de*-Nameserver im A-Root-Server vorzunehmen und die Löschung des alten KPNQwest Nameservers durchzuführen. Der Grund lag darin, dass sich einige ccTLDs - darunter auch DENIC - geweigert hatten, die eigenen Zoneninformationen über `axfr`[27] der ICANN zur Verfügung zustellen. Dies könnte ernsthafte Probleme für die Namensauflösung mit sich bringen, für den Fall, dass der KPNQWest Server geändert würde. Dadurch würden die DNS-Queries, die an diesen Server gehen, falsch beantwortet werden[28].

ICANN beruft sich hierbei auf die neuformulierten Regeln für die Delegation von Länderdomains (ICP-1)[29]. Diese wurden aber nicht mit den ccTLDs abgestimmt, sondern diesen nur vorgeschrieben.

3.3.1 ICANN-Studienkreis

Um Einfluss auf die Internetpolitik zu nehmen, wurde 1999 der ICANN Studienkreis http://www.icann-studienkreis.net/ gegründet. Dieser ist ein offenes Netzwerk von Personen aus Politik, Wirtschaft und Wissenschaft zur Information und Diskussion der Entwicklung der "Internet Corporation for Assigned Names and Numbers". Es findet einmal im Jahr eine grosse Tagung statt. Die letzte war im Januar in Berlin. Getragen wird der Studienkreis er von den drei deutschsprachigen Registries DENIC eG in Frankfurt, nic.at GmbH in Salzburg, SWITCH in Zürich.

[26] Die Internet Assigned Numbers Authority (www.iana.org) war ein Projekt des Information Science Institute of Southern California. Die IANA wurde von dem Internet Pionier Jon Postel mit gegründet und aufgebaut.
[27] Für Berechtige ist der Zonentransfer z.B. mit `dig @nameserver domainname.tld axfr` abrufbar.
[28] http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/anw-16.09.02-000/
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-14.02.03-004/
[29] ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation. http://www.icann.org/icp/icp-1.htm

Dass es einen großen Klärungsbedarf gibt an der Rolle und der Struktur der ICANN, zeigt sich auch an ihren undurchsichtigen Umstrukturierungsprozessen. Für viele Internetinteressierte sind diese Vorgänge aufgrund ihrer Komplexität und fortlaufenden Weiterentwicklung nur noch schwer nachvollziehbar[30].

3.3.2 ICANN-watch

David Post, David J. Farber und Michael Froomkin betreiben die amerikanische ICANN Watch (http://www.icannwatch.org/). ICANN Watch will der Organisation ICANN auf die Finger schauen, um zu verhindern, dass sie zu einer übermächtigen Netzregierung wird.

3.4 CENTR

Das **C**ouncil of **E**uropean **N**ational **T**op **L**evel **D**omain **R**egistries) www.centr.org ist die Vereinigung der Internet Länder Code Top-Level Domain (ccTLD) Registrierungsstellen wie etwa DENIC für *.de (Deutschland).* Die volle Mitgliedschaft steht allen ISO 3166-1 ccTLD Registrierungsstellen offen. Daher sind sowohl europäische als auch nichteuropäische Mitglieder vertreten. Die Absicht von CENTR ist die Unterstützung und Teilnahme in der Entwicklung von Standards für die ccTLDs. Die Organisation hat eine europäische Ausrichtung.

In regelmäßigen Abständen finden Meetings statt, in denen die Belange der ccTLDs diskutiert werden. Registrierungsregeln und Prozeduren werden hier ausgetauscht und diskutiert. Insbesondere aber politische Themen wie z.B. die Neugestaltung von ICANN und die Rechte der Europäer. CENTR fungiert hier quasi als politisches Sprachrohr, um die Interessen der Europäer wahrzunehmen.

Innerhalb von CENTR wurde von DENIC ein Projekt initiiert, bei dem verschieden Registries einen Secondary-Server gemeinsam betreiben. Dadurch soll sich der Aufwand für den Betrieb des weltweiten Secondary-Netzes verringern.

3.5 CORE

Das Council of Registrars CORE ist eine internationale gemeinnützige Gesellschaft von Registraren unter Schweizer Recht http://www.corenic.org . Die Mitglieder von CORE bieten in der Regel Registrierungsdienstleistungen für die neuen gTLD's an.

3.6 RIR

Die **R**egional **I**nternet **R**egistries (RIR) sind die Vertreter der Registries für IPv4- und IPv6-Adressen [RIR]. Der IP-Adressraum wird in einer hierarchischen Art verteilt. ICANN bzw. die frühere IANA kontingentiert i.Allg. /8 Blöcke[31] im IP-Adressraum und vergibt diese weiter an die regionalen Internet Registries wie das Ripe NCC, ARIN, APNIC und LACNIC. Diese teilen den Netzbereich weiter auf in /16 Bereiche und teilen diese den lokalen Internet Service Providern zu. Von den ISPs werden IP-Nummern und Bereiche an die Endkunden vergeben.

[30] Auf dem Weg zu ICANN II, 31.10.2002
http://www.heise.de/newsticker/data/jk-31.10.02-008/
Neuer Präsident für Internet-Verwaltung ICANN, 20.03.2003
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-20.03.03-006/

[31] Die /X Notation wird auf der DENIC-Seite http://www.denic.de/doc/faq/allgemeines.html#a0004 erklärt. Beispielsweise bedeutet /8 ein zusammenhängender Bereich von 16.777.216 IP-Adressen

3.6.1 RIPE NCC

Das **R**éseaux **IP** **E**uropéens **N**etwork **C**oordination **C**entre ist geographisch für den europäischen Raum, den nahen Osten, Zentralasien und Afrika nördlich des Äquators zuständig. Als Dienstleistungen werden neben der Vergabe von IP-Bereichen, die Vergabe von Nummern für autonome Systeme und das Management eines Teils des Reverse Adressraumes angeboten. Dreimal jährlich findet das sogenannte Ripe Meeting statt. An diesem treffen sich die Mitglieder der lokalen Registries, Firmenvertreter und Internetbetreiber. Während des Meetings liegt der Schwerpunkt der Arbeit auf Sitzungen in Arbeitsgruppen[32]. Hier findet die Weiterführung der Emaildiskussionsforen statt. Zur technischen und operativen Unterstützung werden vom Ripe NCC auch Schulungen zu speziellen Themen angeboten. Insbesondere zu Secure DNS findet mittlerweile mehrmals jährlich eine Veranstaltung an unterschiedlichen Orten statt[33].

3.6.2 Weitere RiR's

ARIN
American Registry for Internet Numbers
http://www.arin.net

APNIC
Asia Pacific Network Information Centre
http://www.apnic.net

LACNIC
Latin American and Caribbean IP address Regional Registry
http://lacnic.net

Die Gründung eines weiteren RIR's wurde vorgeschlagen.[34]

AfriNIC
African Network Information Center
http://www.afrinic.org/

3.7 Deutsche Internetverbände und -organisationen

3.7.1 ISOC.de

In einer zunehmend von Markt und Wettbewerb geprägten Umgebung schafft die ISOC die Voraussetzung für den Fortbestand und Zusammenhalt des Internet. Seit 1995 bildet die ebenfalls 1992 gegründete Deutsche Interessengemeinschaft Internet (DIGI e.V.) eine deutsche Sektion der ISOC (http://www.isoc.de).

Ihre Ziele sind:

- Förderung des Informationsaustausches zwischen Netzwerkbenutzern
- Sicherstellung der erforderlichen Administration des deutschen Internets
- Unterstützung der Koordination zwischen den Dienstanbietern
- Unterstützung der Weiterentwicklung von Dienst und Technik

[32] http://www.ripe.net/ripe/wg/index.html
[33] http://www.ripe.net/cgi-bin/courselist.pl.cgi
[34] Derzeit warden die Aufgaben

- Erweiterung der Reichweite des Internets und Verbesserung der Interkonnektion mit Netzwerken und -diensten anderer Technik
- Förderung des fairen Wettbewerbs und der konstruktiven Zusammenarbeit der Dienstanbieter zur Optimierung von Preisen und Leistungen im Sinne der Nutzer
- Forum zur Formulierung der Nutzerinteressen

3.7.2 FSM e.V.

Die Freiwillige Selbstkontrolle Multimedia (FSM) ist ein eingetragener Verein, der 1997 von vielen Medienverbänden und einigen Unternehmen gegründet wurde. Die neue Selbstkontrollorganisation bietet jedermann die Möglichkeit, sich über strafbare oder jugendgefährdende Inhalte im Netz zu beschweren oder Fragen zum Thema Jugendschutz im Internet zu stellen. Eingehende Beschwerden behandelt die FSM in einem geordneten Verfahren. Berechtigten Beschwerden versucht sie abzuhelfen. Sie leistet dadurch einen wichtigen Beitrag im Kampf gegen den Missbrauch des weltweiten Datennetzes.

Gemeinsam mit ausländischen sogenannten Internet-"Hotlines" hat die FSM 1999 den europäischen Dachverband INHOPE gegründet (http://www.inhope.org). Dies dient dem Ziel, ein internationales Netz von freiwilligen Selbstkontrollen im Internet aufzubauen (http://www.fsm.de).

3.7.3 BITKOM

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vertritt 1.300 Unternehmen, davon gut 700 als Direktmitglieder mit ca. 120 Mrd. Euro Umsatz und mehr als 700.000 Beschäftigten. Hierzu zählen Produzenten von Endgeräten und Infrastruktursystemen sowie Anbieter von Software, Dienstleistungen, neuen Medien und Content. Mehr als 600 Direktmitglieder gehören dem Mittelstand an. BITKOM setzt sich insbesondere für eine Verbesserung der rechtlichen und politischen Rahmenbedingungen in Deutschland, für eine Modernisierung des Bildungssystems und für die Entwicklung der Informationsgesellschaft ein (http://www.bitkom.org).

4 Bedrohungsanalyse

Bevor Bedrohungsszenarien gegen das Domain Name System (DNS) beschrieben werden, wird die Struktur des DNS und die Namensauflösung erklärt.

4.1 Einführung in das Domain Name System

Das Domain Name System ist eine weltweit verteilte Datenbank. Der Hauptzweck ist, Domainnamen auf Internetadressen abzubilden. Z.B. wird dem Namen `www.fzi.de` die Adresse `141.21.4.3` zugeordnet. Eine weitere wichtige Anwendung ist, einen Host zu finden, der Emails weiterleitet. Wenn man z.B. eine Email an `jemand@fzi.de` schicken möchte, sucht der eigene Mailserver aus dem DNS die Information heraus "E-mails an `fzi.de` werden von `mailhost.fzi.de` angenommen und der hat die Adresse `141.21.6.1`". Alles weitere wird dann über das SMTP Protokoll abgewickelt.

Domainname

Ein Domainname besteht aus einer Reihe Marken, die durch Punkte getrennt sind. Z.B. "`www.fzi.de.`" . Jeder Domainname endet in einem "." (Fully Qualified Domain Name FQDN), doch dieser wird beim Benutzerinterface gerne weggelassen.

Baumstruktur

Das DNS hat eine Baumstruktur. Die Wurzel (Root) hat den Namen "`.`". Von dort verzweigen die 15 generischen Top-Level Domains (gTLD): „*aero.*“, „*arpa.*“, „`biz.`“, „`com.`“, „`coop.`“, „`edu.`“, „`gov.`“, „`info.`“, „`int.`“, „`mil.`“, „`museum.`“, „`name.`“, „`net.`“, „`org.`“, , „`pro.`“ und die 241 Länderdomains (ccTLD) „`ac.`“, ..., „`de.`“, ... , „`zw.`“ Je weiter rechts im Namen eine Marke ist, desto höher liegt sie im Baum.

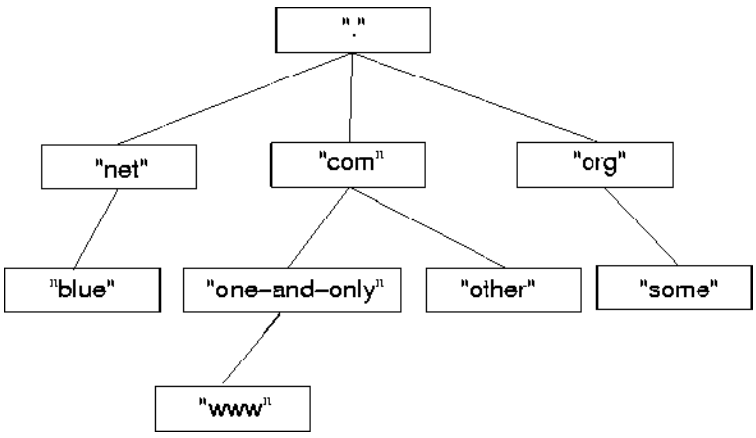


Abbildung 8: DNS-Baumstruktruktur

Resource Records

Ein Resource Record (RR) besteht aus Domainnamen, Typ, Daten, Time To Live-Wert (TTL) und Klasse. Die Daten können z.B. eine Internetadresse sein, Information über Emailserver, ein beliebiger Text, oder etwas anderes. RFC 1035 legt zunächst 16 Datentypen fest und weitere können jederzeit hinzukommen. Der TTL gibt an, wie lange der Resource Record in anderen Nameservern zwischengespeichert werden darf (siehe Caching). Die Klasse kann einen von drei Werten annehmen: IN (Internet), HS (Hesiod) und CH (Chaos). Gewöhnlich ist sie auf IN gesetzt, denn dafür wurde das DNS schliesslich entworfen.

Beispiele für Resource Records:

```
fzi.de.      100      IN SOA  drake.eid.fzi.de. dieterle.fzi.de. (
                                      2      ; serial
                                  10800      ; refresh (3 hours)
                                   3600      ; retry (1 hour)
                                 604800      ; expire (1 week)
                                   3600      ; minimum (1 hour)
                                           )

dnssec.fzi.de.                  IN   NS    drake.eid.fzi.de

drake.eid.fzi.de.               IN   A     192.249.249.7

                                IN   MX    10 mailhost

mailhost.fzi.de.                IN   A     192.249.249.3

7.249.249.192.in-addr.arpa. IN   PTR   drake.eid.fzi.de.
```

Zone

Eine Zone ist ein gestutzter Unterbaum des DNS-Namensraumes (Abbildung 9). Eine Zone beginnt bei einem Domainnamen, z.B. `fzi.de`. Dieser Domainname hat einen RR vom Typ "Start of Authority", SOA, der den Beginn einer neuen Zone markiert. Jeder Name "darunter" gehört zu der Zone, es sei denn, er liegt in einer Unterzone. Beispiel: `fzi.de`, `www.fzi.de` und `mailhost.fzi.de` liegen in der Zone von `fzi.de`. `more.than.one.label.fzi.de` liegt auch in der Zone, da weder bei `one.label.fzi.de` keine Subzone anfängt, noch bei `than.one.label.fzi.de`, usw. ... (bei keinem der Domainnamen ist ein SOA RR gespeichert). `more.than.one.label.fzi.de` liegt zwar in der Zone von `fzi.de`, aber es sind keine Daten damit verknüpft.

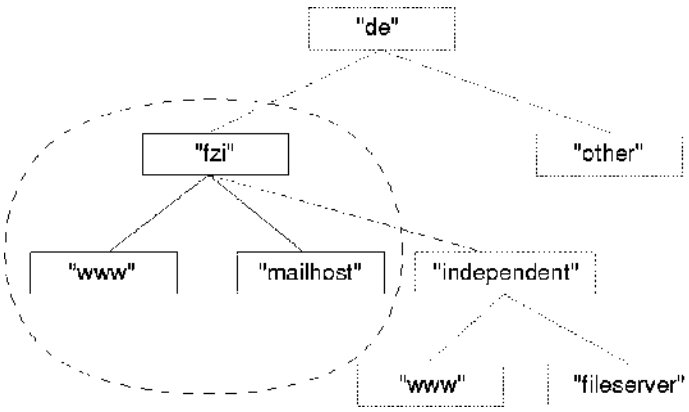


Abbildung 9: Zone im DNS-Baum

Hätte `fzi.de` eine Subzone "`independent.fzi.de`", so würden alle DNS-Anfragen nach Namen unterhalb von `independent.fzi.de` an Nameserver jener Zone delegiert (Abbildung 10).

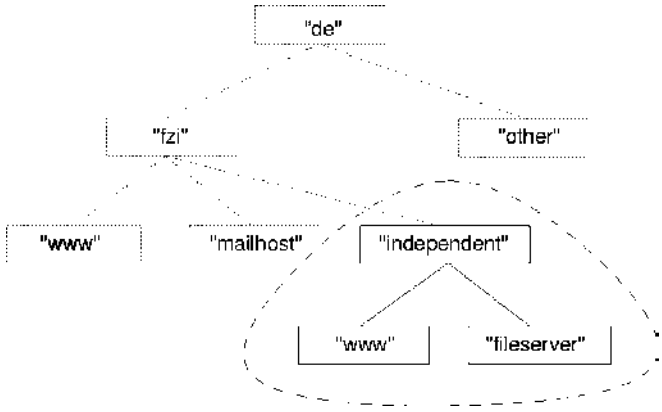


Abbildung 10: Sub-Zone

Nameserver

Ein Nameserver ist für eine Zone zuständig. Er hat alle RRs dieser Zone. Auf diese Art ist das DNS eine verteilte Datenbank. Nameserver beantworten DNS-Anfragen.

Resolver

Ein Resolver ist Software auf dem Client-Computer, die Nameserver kontaktiert, um im DNS Resource Records (RR) zu finden. Gewöhnlich ist an einen Nameserver auch ein Resolver gekoppelt, damit er selbst Informationen im DNS nachschlagen kann.

DNS-Nachricht

Eine DNS-Nachricht ist ein Paket aus einer eindeutigen Identifikationsnummer (Message-ID), verschiedenen Flags und einigen RRs. Mit solchen Paketen tauschen Nameserver und Resolver RRs aus.

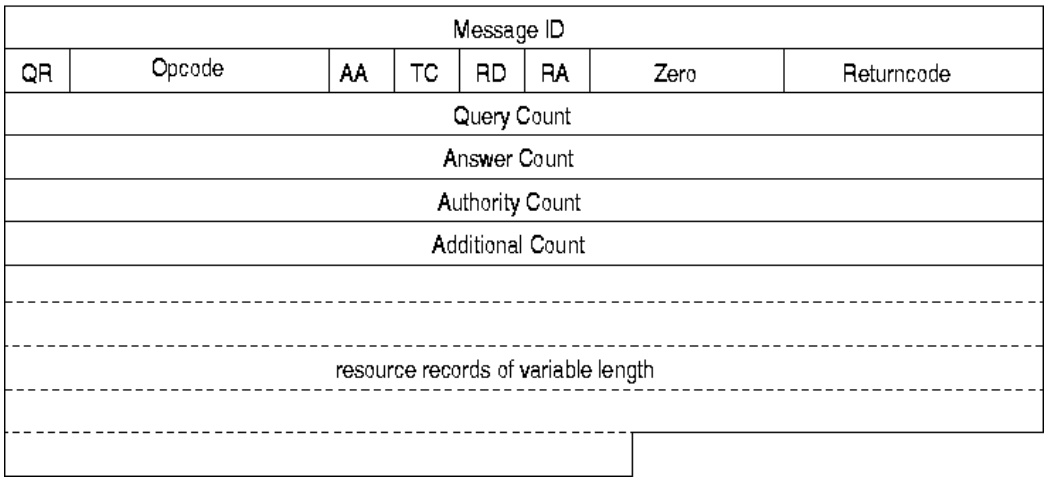


Abbildung 11: Format einer DNS-Nachricht

FLAG	Bedeutung wenn die Bits gesetzt sind.
QR	Legt den Typ der Nachricht fest: Frage oder Antwort.
Opcode	Art der Anfrage: Bsp. Standard Anfrage oder Status-Anfrage.
AA	Die Antwort ist autoritative.
TC	Tuncation. Zeigt an, dass die Nachricht abgeschnitten wurde.
RD	Recursion Desired. Rekursive Namensauflösung ist erwünscht.
RA	Recursion available. Rekursive Namensauflösung war verfügbar.
Zero	Reserviert für zukünftige Nutzung.
Returncode	Antwortcode.

Tabelle 4: Header-Flags

Der Header einer DNS-Nachricht enthält die 16 Bit große Identifikationsnummer, 16 Bit Flags (und vier 16 Bit Zähler (Query Count, Answer Count, Authority Count, Additional Count), für die Anzahl der RRs in den hierfür definierten Abschnitten "Query", "Answer", "Authority" und "Additional". Die Identifikationsnummer war ursprünglich nur dafür gedacht, dass die Anfragen eindeutig sind, und nicht um böswillig falsche Nachrichten auszuschließen. Ein Client setzt die IDs von seinen Anfragen auf verschiedene Werte. Die Antwort auf eine Frage enthält dieselbe ID. Wenn der Client eine Antwort bekommt, kann er sie anhand der ID sofort einer bisher unbeantworteten Anfrage zuordnen. In frühen Implementierungen von ISC-BIND wurde die ID bei jeder ausgehenden Anfrage um eins erhöht. Die IDs waren zwar eindeutig, aber leicht zu erraten.

Rekursive Anfragen, Resolver

Der Header einer DNS-Nachricht enthält ein Bit mit der Bezeichnung "recursion desired" oder RD. Wenn bei einer Anfrage dieses Bit gesetzt ist, bedeutet das, dass der bearbeitende Nameserver "rekursiv" arbeiten soll. In diesem Modus schaut er zunächst in den lokalen Daten, ob die Antwort da zu finden ist. Wenn ja, schickt er ein Antwortpaket an den Client zurück. Wenn nicht, wird er weitere Nameserver kontaktieren, bis er die Antwort bekommt, oder eine Nachricht, die besagt, dass die Antwort nicht existiert. Er

schickt entweder die Antwort an den Client, oder eine Nachricht, dass diese nicht existiert.

Iterative Anfrage

Im nicht-rekursiven Modus kontaktiert der Nameserver keine anderen Server.
Wenn der Domainname der Anfrage in einer Zone liegt, für die der Nameserver zuständig ist, sucht er die Antwort bei den lokalen Daten. Wenn sie dort zu finden war, schickt er sie an den Client. Wenn nicht, schickt er eine DNS-Nachricht ohne RRs im "Answer" Abschnitt. Entweder existiert zum angefragten Domainnamen auch kein RR eines anderen Typs, dann wird der Fehlercode auf NXDOMAIN gesetzt "no such domain", oder es gibt zwar einen RR, aber sein Typ stimmt nicht mit dem der Anfrage überein. Im zweiten Fall wird der Fehlercode auf NOERROR gesetzt.

Wenn der Client nach Information von einer Zone fragt, z.B. nach "`www.target.org.`", für die der Nameserver nicht zuständig ist, hat der Nameserver die Antwort nicht (es sei denn, sie liegt im Cache, siehe Caching), und er weiss nicht, ob die Antwort existiert oder ob RRs mit dem selben Namen aber anderem Typ existieren. Der Nameserver schickt eine DNS-Nachricht zurück, die keine RRs im "Answer" Abschnitt enthält, dafür aber eine Liste von Nameservern, die "näher" an der Zone liegen, die "`www.target.org.`" enthält. Ein Nameserver ist näher an "`www.target.org.`" als ein anderer, wenn er für eine Zone zuständig ist, die tiefer liegt als die Zone des anderen Nameservers.

Wenn der Client eine nicht-rekursive Anfrage stellt, muss er normalerweise mehrere Nameserver kontaktieren, bis er die Antwort bekommt. Dieser Prozess wird Namesauflösung genannt. Software, die das leistet wird Resolver genannt (s.o.).

Caching

Ein Nameserver, der den rekursiven Modus unterstützt, speichert üblicherweise die nachgeschlagenen Resource Records in seinem Cache. Das reduziert die Anzahl der verschickten DNS-Nachrichten und es beschleunigt das Nachschlagen. Eine Anfrage nach der Adresse von "`www.ottawa.ca`" dauert ohne Caching z.B. 540ms und mit Caching nur 70ms. Eine Verzögerung von einer halben Sekunde ist für den menschlichen Benutzer deutlich spürbar.

Stub Resolver

Ein Stub Resolver kann nur rekursive Anfragen schicken. Er verlässt sich darauf, dass der Nameserver rekursive Anfragen unterstützt. Einen Cache gibt es beim Nameserver und in der Regel nicht beim Client. Das ist vorteilhaft, da so mehrere kleine Caches zu einem großen kombiniert werden, d.h. der Cache wird besser genutzt. Bei Suse-Linux-Systemen wird mittlerweile auch mit einem lokalen Cache gearbeitet. (z.B. nscd - name service cache daemon).

Beispiel

Ein Anwender tippt "`www.ottawa.ca`" in seinen Browser. Der Browser lässt das Betriebssystem (Stub Resolver) die Internetadresse von `www.ottawa.ca` nachschlagen. Das Betriebssystem kennt nur die Adresse von zwei lokalen Nameservern (in diesem Beispiel), also schickt es eine DNS-Anfrage an einen davon (z.B. `141.21.4.3`) mit der

Frage nach dem Domainnamen "www.ottawa.ca." und dem Typ "A", der für Internetadresse steht. Das RD Bit (recursion desired) wird gesetzt.

Der Nameserver auf Host 141.21.4.3 ist nicht für "www.ottawa.ca." zuständig und kennt keine Nameserver, die für "www.ottawa.ca.", für "ottawa.ca." oder für "ca." zuständig wären. Aber er kennt die Nameserver für ".", die Root-Nameserver. Das sind die "nächsten" Nameserver zu "www.ottawa.ca.", die unser Nameserver kennt, deswegen fragt er einen von ihnen (z.B. a.root-servers.net mit der IP 198.41.0.4). Das RD Bit setzt er dabei nicht.

a.root-servers.net ist für "." zuständig, nicht für "www.ottawa.ca.",und kennt daher die Antwort nicht. Aber er kennt Nameserver, die für "ca." zuständig sind, weil "ca." eine Subzone von "." ist. a.root-servers.net schickt ein Antwortpaket an unseren Nameserver(141.21.4.3), das folgende Information enthält:

"Diese Nameserver sind für 'ca.' zuständig: clouso.risq.qc.ca, relay.cdnnet.ca, rs0.netsol.com, merle.cira.ca, ns1cira.ca, und sie haben folgende IP Adressen: 192.26.210.1, 192.73.5.1, 216.168.224.206, 64.26.149.98, 129.33.164.84".

141.21.4.3 wählt einen davon (z.B. clouso.risq.qc.ca) und fragt wieder nach "www.ottawa.ca.". clouso.risq.qc.ca ist auch nicht für "www.ottawa.ca." zuständig, aber zufällig hat er die gesuchte Information in seinem Cache: Die Adresse von "www.ottawa.ca." ist 192.234.223.142. Das schickt er an unseren Nameserver, der es wiederum an den Client weiterleitet, und eine Kopie in seinen Cache schreibt. Der Client war der Rechner, von dem aus jemand die Webseite von Ottawa sehen wollte. Der Browser kennt die Adresse jetzt, holt die Webseite und zeigt sie an.

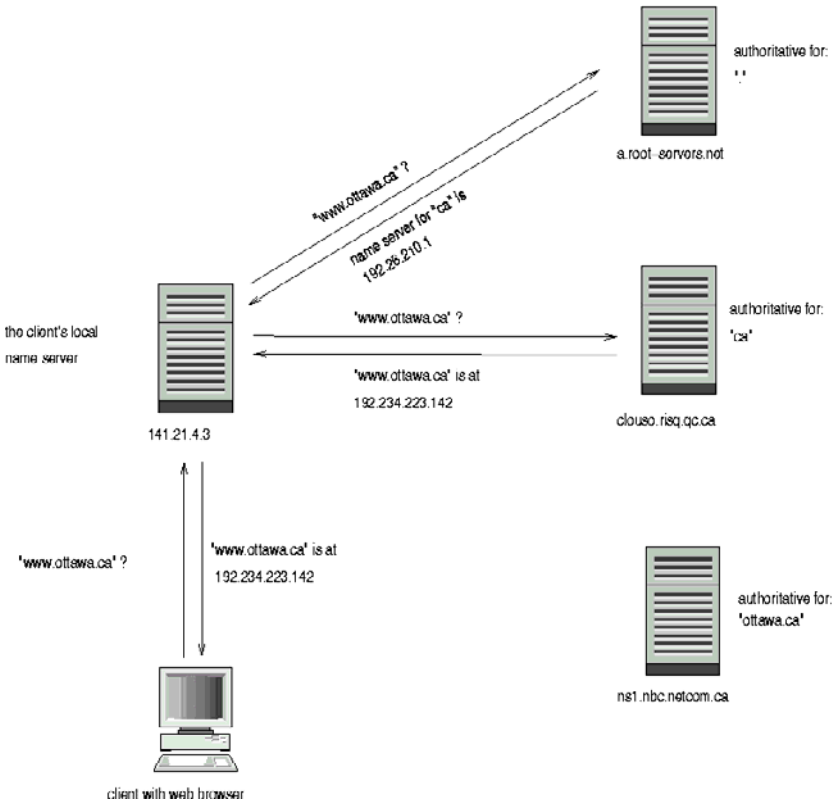


Abbildung 12: Namensauflösung

Das nächste Mal, wenn jemand die Adresse von www.ottawa.ca braucht bevor der zugehörige TTL Wert abgelaufen ist, wird das Nachschlagen im DNS einfacher sein. Der Browser (bzw. das Betriebssystem) schickt eine Anfrage für "`www.ottawa.ca.`" an an den NS `141.21.4.3`. Dieser NS hat die Antwort in seinem Cache und braucht daher keine weiteren Nameserver zu kontaktieren. Er liefert einfach die Antwort.

Eine vollständige Beschreibung des DNS findet man in [Albitz] oder in [RFC 1034] und [RFC 1035].

4.2 Potenzielle Angriffsszenarien

Es gibt unterschiedlichste Angriffsszenarien[35] [Bellovin 95, Threats] gegen das DNS-System. Zu vielen Angriffsszenarien sind Tools im Internet verfügbar. Die wichtigsten werden zusammen mit Schutzmaßnahmen vorgestellt.

Netzwerk

Abhören des lokalen Datenverkehrs.

Ein Angreifer kann DNS-Anfragen abhören und falsche Antworten generieren, wenn der Client-Rechner z.B. am selben Netzwerk angeschlossen ist wie der Rechner des Angreifers. Der Angreifer wartet, bis er eine DNS-Anfrage des Clients mitliest, die er fälschen möchte. Dann konstruiert er ein Antwortpaket mit der selben Message ID und beliebigen Resource Records in der Answer Section.

Voraussetzungen: Eine Netzwerktechnologie, bei der lokaler Datenverkehr abgehört und auch eingeschleust werden kann. In einer geswitchten Umgebung müssen die Switches angreifbar sein, sodass die Daten an den Rechner des Angreifers gesendet werden, die eigentlich nicht für ihn bestimmt sind.

Auswirkung: Der Angreifer kann einem einzelnen Benutzer falsche DNS-Daten unterschieben.

Abhilfe: Eine Netzwerktechnologie, die kein Abhören erlaubt, oder Detektion des Abhörens. Kommt das gefälschte Paket vor dem richtigen an, so wird der UDP Port möglicherweise schnell genug geschlossen, so dass das richtige Paket eine ICMP Nachricht "Port-Unreachable" hervorruft.

Erraten der Message-ID

Kann der Angreifer die DNS-Anfrage von `ns.target.org` nicht abhören, so hat er noch die Möglichkeit, sie zu erraten. Zu den benötigten Informationen gehört die Message-ID, der Zeitpunkt der Anfrage, der angefragte Domainname und sein Typ, die Zieladresse der Anfrage und der Port, von dem aus die Anfrage geschickt wurde. Die meisten Parameter kann der Angreifer selbst bestimmen, indem er eine Anfrage an `ns.target.org` schickt, deren Antwort `ns.target.org` noch nicht kennt, sodass es selbst eine entsprechende Anfrage losschickt. Der Angreifer konstruiert ein Antwortpaket, das auf die Anfrage passt, und schickt es ebenfalls an `ns.target.org`. Wenn die Message-ID des Antwortpakets mit der Message-ID von ns.target.org geschickten Anfrage übereinstimmt, wird `ns.target.org` das Antwortpaket akzeptieren. Da die Message-ID nur 16 Bit groß ist, ist dieser Angriff realistisch. Bei 65.000 Versuchen hat der Angreifer eine Chance von 63%, eine gültige Antwort zu generieren. Voraussetzung

[35] SANS-Institut Security Reading Room DNS Issues http://rr.sans.org/DNS/

dafür ist, dass seine Antwortpakete vor der richtigen Antwort bei dem betreffenden Nameserver ankommen[36]. Die Chance des Angreifers hängt daher davon ab, wie viele falsche Antworten er schicken kann, bevor die richtige Antwort ankommt.

Geburtstagsangriff[37]

Wenn ein Nameserver mehrere Anfragen für die gleiche Information ausschickt, wird die Chance, eine passende Message-ID zu erraten, für den Angreifer deutlich erhöht [BirthAtt]. Ein Nameserver verhält sich so, wenn er eine Anfrage ausschickt, ohne zu überprüfen, ob er schon eine entsprechende Anfrage ausgeschickt hat, und die Antwort nur noch nicht eingetroffen ist. Ein falsches Antwortpaket wird dann akzeptiert, wenn seine Message-ID mit einer noch unbeantworteten Anfrage übereinstimmt.

Abhilfe: Ein Nameserver muss eine Antwort eindeutig einer offenen Anfrage zuordnen, und darf nicht mehrere offene Anfragen haben, auf die die gleiche Antwort passt. Ein wirksamer Schutz ist auch die Verhinderung der Auflösung von rekursiven Anfragen von Unberechtigten.

Betriebssystem

Übernahme eines Gateways

Ein Angreifer kann versuchen, einen Gateway Rechner unter seine Kontrolle zu bringen, und DNS-Pakete zu fälschen, die über diesen Rechner geleitet werden.

Voraussetzungen: Der Gateway muss erstens kompromittierbar sein und zweitens den DNS-Verkehr weiterleiten, den der Angreifer verfälschen will.

Auswirkung: Der Angreifer kann je nach Wichtigkeit des Gateways vielen Benutzern falsche DNS-Daten unterschieben.

Übernahme eines Nameservers

Ein Angreifer kann versuchen, den primären DNS-Server der Zone, in der er Resource Records fälschen will, unter seine Kontrolle zu bringen.

Voraussetzungen: Der Server muss kompromittierbar sein.

Auswirkung: Alle Anfragen können gefälschte Resource Record erhalten. Auch die sekundären DNS-Server für diese Zone verbreiten den gefälschten Resource Record, sobald sie ihre Zoneninformation erneuert haben. Der Angreifer kann aber keine Resource Records anderer Zonen fälschen.

Protokoll

Zonenfremde Resource Records mitschicken

Ein Nameserver kann in Antworten auf normale Anfragen (falsche) Informationen über fremde Zonen mitschicken. Normalerweise sollten zonenfremde Informationen ignoriert werden. Ausnahmen sind Adressen von Nameservern in Subzonen, und Adressen von Nameservern, deren Auflösung ohne zonenfremde Resource Records zu einem unlösbaren Zyklus führt.

Voraussetzungen: Der Angreifer hat Zugriff auf einen Nameserver, der durch Delegation in den DNS-Baum eingebunden ist. Der angegriffene Resolver vertraut zonenfremden Resource Records in Antworten.

[36] Ein gleichzeitiger Denial of Service Angriff, auf den für die Beantwortung der Anfrage zuständigen Nameserver, erhöht daher die Chance auf einen erfolgreichen Angriff.
[37] http://www.kb.cert.org/vuls/id/457875

Auswirkungen: Der falsche Resource Records gelangt in den Cache des Resolvers und wird von dort an Clients weitergegeben, die ihn anfordern.

Abhilfe: Ein Resolver darf einem zonenfremden Resource Record nur dann trauen, wenn er ihn nicht von den Nameservern bekommen kann, die für ihn zuständig sind. Ein Resource Record, dem ein Resolver trauen muss ist z.B. ein notwendiger Glue Record, d.h. die Adresse eines Nameservers, der in einer Subzone des befragten Nameservers liegt, und für diese zuständig ist.

In einer FZI-internen Studie wurde dieser Angriff im Detail untersucht. Die Ausgangsfragestellung war, inwieweit das DNS-Protokoll von seinem Design her Angriffe unterstützt. Zusammenfassen lässt sich feststellen:

Durch einen Designfehler des DNS-Protokolls werden von Nameservern Informationen von anderen Nameservern angenommen, für die jene nicht zuständig sind (zonenfremde Daten). In einem Fall ist dieses Verhalten durch den Internet Standard RFC1034 festgelegt. Als Voraussetzung für diesen Angriff benötigt ein Angreifer nur Zugriff auf einen Nameserver für eine registrierte Zone; es kann auch sein eigener Nameserver sein.

Der Angriff erhält seine Wirksamkeit dadurch, dass falsche Informationen in den Cache gelangen, und wird daher auch "Cache Poisoning" genannt.

Verwundbarkeit:

Nur die ersten Implementierungen von ISC-Bind (Version 4) halten sich genau an den Standard und implementieren den Designfehler. Falls die zonenfremden Daten jedoch von einem Forwarder kommen, werden sie auch von aktuellen Bind-Versionen akzeptiert (Version 8.2.3 – 9.2.2).

Abhilfe: Forwarding, insbesondere für Teilbereiche des DNS, darf nur für Nameserver weiter eingerichtet werden, denen volles Vertrauen entgegen gebracht wird.

Nameserver Software

BIND-Exploits

Bei den zwanzig häufigsten Software-Fehlern wird unter Unix, die ISC-BIND Software an neunter Stelle aufgeführt[38]**.** Es ist daher absolut empfohlen, wenn ISC-BIND zum Einsatz kommt, eine aktuelle Version einzusetzen und die regelmäßigen Patches einzuspielen [BIND-Vul].

Resolver Bibliothek

Angriffe gegen die Clients über Verwundbarkeiten in der Resolver Bibliothek [Res-Vul].

Zugriff auf Zonendaten

Zonentransfer

Daten eines Zonetransfers können unterwegs verfälscht werden. Voraussetzungen: Der Angreifer hat einen Rechner zwischen Primärem und Sekundärem Server unter Kontrolle.

Auswirkungen: Sekundäre Nameserver antworten mit gefälschten Resource Records.

Abhilfe: Verschlüsselung des Zonentransfers mit Transaktionssignatur TSIG.

Dynamic Update Schnittstelle

Die Sicherung der Dynamic Update Schnittstelle wird über Transaktions-Signaturen vorgenommen [DynUpd].

[38] The Twenty Most Critical Internet Security Vulnerabilities. http://www.sans.org/top20/#U9

Organisatorische Prozesse

Die Absicherung der organisatorischen Prozesse kann durch Verfahren, die die Authentizität der Beteiligten sicher stellt und die Datenintegrität gewährleistet, erreicht werden. Dies leisten Signaturverfahren. Angriffe auf die organisatorische Schnittstelle werden dadurch stark erschwert. Eine Kompromittierung kann weiterhin erreicht werden, durch die Brechung der verwendeten Schlüssel, durch interne Täter, die die Schlüssel kennen oder durch die Ausnutzung von schwachen CA-Mechanismen.

4.3 Mögliche Schadensfälle

Zur Verdeutlichung der Gefahren, die von DNS-spoofing ausgehen können, werden verschiedene Möglichkeiten von Angriffen aufgeführt denen der Spoofing-Angriff zugrunde liegt. Eine Angriffsmöglichkeit wird im Detail beschrieben[39].

4.3.1 Denial of Service

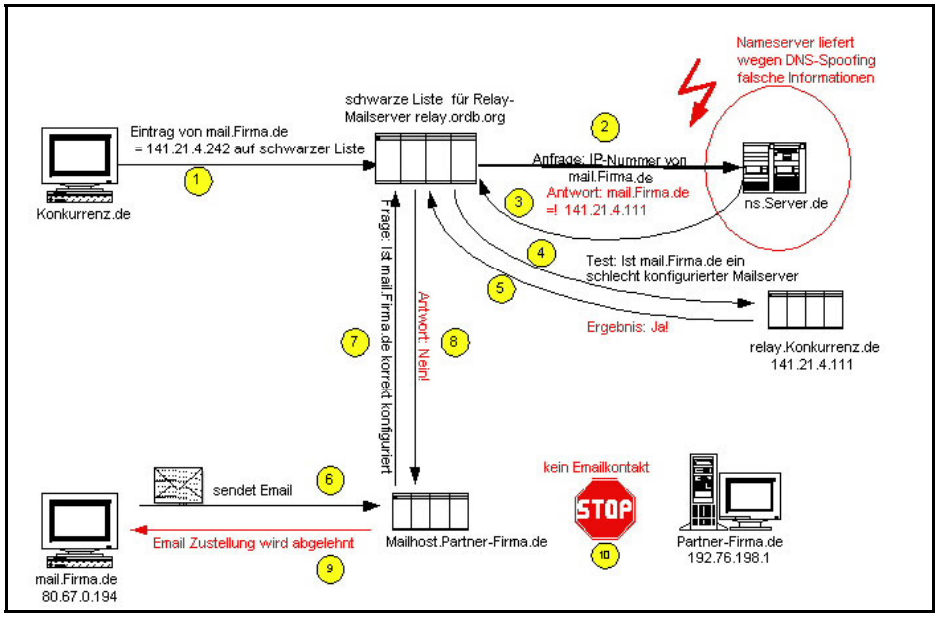


Abbildung 13: Denial of Service Angriff

1. Eintrag von mail.Firma.de auf einer schwarzen Liste durch die Konkurrenz.
2. Nameserveranfrage um `mail.Firma.de` aufzulösen.
3. Gefälschte Antwort des Nameservers
4. Test des Black-List-Servers ob `mail.Firma.de` ein offener Relay-Server ist.
5. Ergebnis: Ja (der falsche Server wird von der Konkurrenz betrieben).
6. `mail.Firma.de` sendet Email an `Partner-Firma.de`.
7. Mailhost prüft gegen schwarze Liste, ob er die Mail annehmen darf.
8. Ergebnis: Nein! (da `mail.Firma.de` auf der schwarzen Liste steht).

[39] Sämtliche angeführten Internetnamen und Adressen sind frei erfunden.

9. Email Zustellung wird abgelehnt.
10. `Firma.de` und `Partner-Firma.de` haben keinen Emailkontakt mehr.

Als Konsequenz ist ein großer Teil der ausgehenden Email von `Firma.de` blockiert.

4.4 Statistik: Gegenwärtiger DNS-Server-Betrieb für *.de*

In einer FZI-internen Studie wird gegenwärtig untersucht, wie der von den ISP angebotene Dienst „Nameservice“, betrieben wird. Ausgehend von einer Stichprobe an Nameserver werden an diese die unten aufgeführten Fragen gestellt und ausgewertet. Die Untersuchung ist noch nicht abgeschlossen. Erste Ergebnisse mit einer Stichprobe von 450 zufällig ausgewählten Nameservern (aus einer Gesamtheit von 34.168) liegen aber bereits vor.

Folgende Fragestellungen sind von Interesse:

- Wie viele Nameserver sind erreichbar?
- Welches Software Produkt wird für den Nameservice eingesetzt? In welcher Version?
- Arbeitet der Server rekursiv? Wird gecached?
- Wird ein Zonentransfer für eine autoritative Zone erlaubt?
- Werden andere Dienste auf dem Nameserver angeboten (www, mail, ftp, telnet, ...)?
- Welches Betriebssystem in welcher Version kommt zum Einsatz?
- In welcher Zone liegen die Nameserver?
- Fehler im Zonenfile? „Lame delegation[40]“?
- Für wie viele Zonen ist der Nameserver zuständig?
- Wie viele Nameserver werden von ISPs betrieben, wie viele von lokalen Zonenadministratoren. Gibt es da auffällige Unterschiede?
- Wie lange dauern die Antwortzeiten?

4.4.1 BIND Version

Die Ermittlung der BIND Version kann durch einfaches Auslesen der BIND Variable „version.bind“ erfolgen. Dazu kann das unter Unix verfügbare Programm „`dig`“ aus der ISC-BIND Distribution verwendet werden.

```
dig @<nameserver> version.bind ch txt
```

Nameserver, die den Inhalt von „version.bind“ zurück lieferten	306

[40] Unter einer „lame delegation“ (engl.) - Lahme Delegation (deutsch) versteht man eine Delegation einer Zone an einen Nameserver, der von dieser Zuständigkeit nichts weiß oder falsch konfiguriert ist, sodass er nicht autoritativ für die Zone ist.

Nameserver, die den Inhalt von „version.bind“ nicht zurück lieferten	71
Nameserver, die auf „dig“ nicht antworten (timeout)	38
Nameserver, die nicht erreichbar sind	35

Tabelle 5: Ergebnis der Versionsermittlung

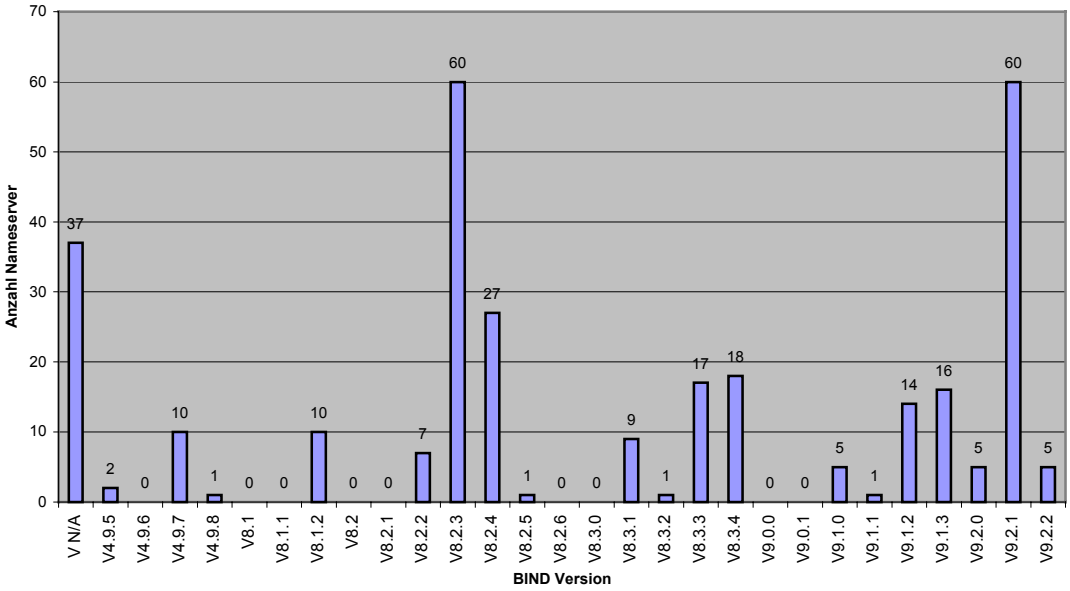


Abbildung 14: Auswertung BIND Versionen

Als erstes Ergebnis der Werte in Tabelle 5 und Abbildung 14 halten wir fest, das 71 % der 450 Nameserver, die auf „`dig`“ antworteten, ihre Version unmittelbar durch die BIND Variablen „version.bind“ offenbarten. Zur Auswertung kommen hier `450 – 38 – 35 = 377` Nameserver. Von den 306 Nameserver aus Tabelle 5 lieferten 37 einen eine gefälschte Versionskennung zurück. Daraus ergeben sich (`100/377*269=71`) 71%.

Der Abbildung kann weiter entnommen werden, dass viele Nameserver ältere BIND Versionen installiert haben, welche Sicherheitslücken aufweisen.

4.4.2 Portscan ausgewählter Dienste

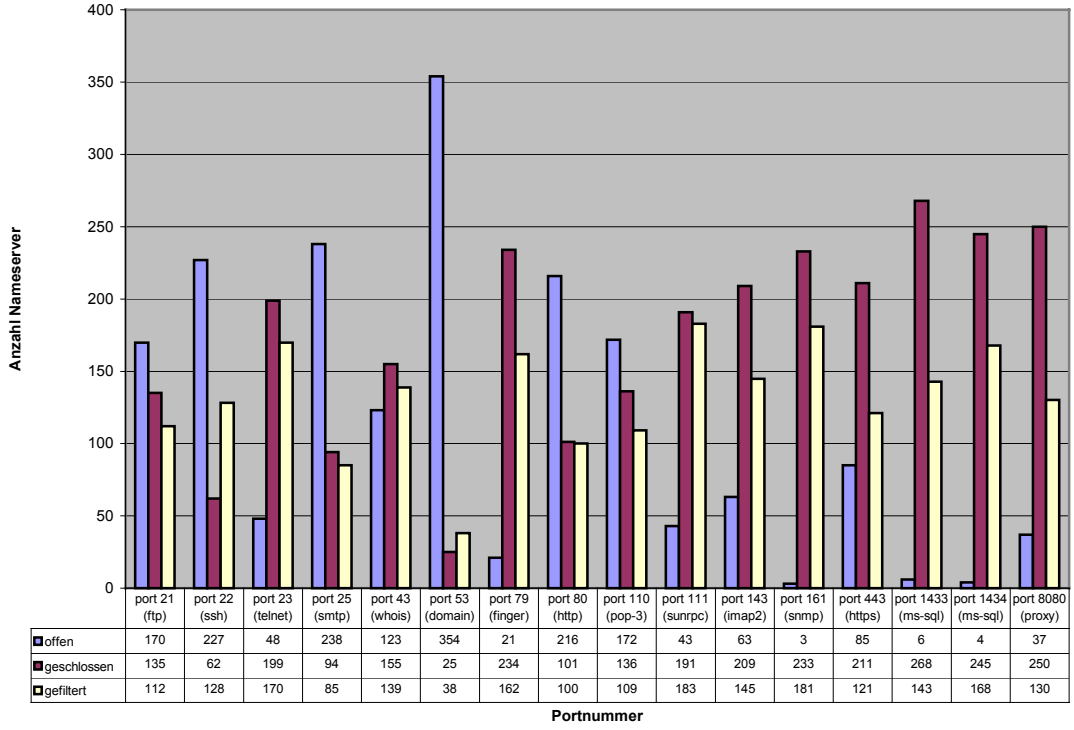
Zur Feststellung welche Dienste auf den zu analysierenden Nameservern angeboten werden haben wir in unserem Test einen Portscan durchgeführt. Hierbei werden die Ports wichtiger Dienste mit dem Unix-Programm „`nmap`[41]“ analysiert.

```
nmap -p <portlist> <nameserver>
```

Aus Abbildung 15 ist ersichtlich, das viele Dienste, die auf Nameservern eigentlich nicht benötigt werden, doch angeboten werden. Bemerkenswert ist hier der Port 1433 des

[41] Network exploration tool and security scanner. http://www.insecure.org/nmap/

Microsoft-SQL-Servers, der bei 6 Nameservern offen war. Dieser wird zum einen nicht gebraucht und er war Aufgrund des Internet-Wurms SQLSlammer erst im Januar 2003 in den Medien. Auffällig ist darüber hinaus, das bei 25 Nameservern der Port 53 geschlossen war, dies deutet auf eine lahme Delegation[40] hin.



	port 21 (ftp)	port 22 (ssh)	port 23 (telnet)	port 25 (smtp)	port 43 (whois)	port 53 (domain)	port 79 (finger)	port 80 (http)	port 110 (pop-3)	port 111 (sunrpc)	port 143 (imap2)	port 161 (snmp)	port 443 (https)	port 1433 (ms-sql)	port 1434 (ms-sql)	port 8080 (proxy)
offen	170	227	48	238	123	354	21	216	172	43	63	3	85	6	4	37
geschlossen	135	62	199	94	155	25	234	101	136	191	209	233	211	268	245	250
gefiltert	112	128	170	85	139	38	162	100	109	183	145	181	121	143	168	130

Abbildung 15: Auswertung Portscan

4.4.3 Zonentransfer

Ein weitere wichtige Fragestellung im Bereich Nameserver ist, ob ein Nameserver einen Zonentransfer, der von einem beliebigen Rechner initiiert wird, durchführt. Der Einfachheit halber wurde versucht den Zonentransfer mit der zugehörigen Domäne des Nameservers ausführen zu lassen.

```
dig @<nameserver> <domain> axfr
```

Nameserver, die erreichbar waren	417
Nameserver, die nicht erreichbar waren	33
Nameserver, die für „ihre“ Domäne verantwortlich (autoritativ) sind	341
Nameserver, die für „ihre“ Domäne nicht verantwortlich (autoritativ) sind	38
Nameserver, die keine Antwort gaben	34
Nameserver, die einen Zonentransfer erlaubten	175

Nameserver, die einen Zonentransfer nicht erlaubten	166

Tabelle 6: Ergebnis des Zonentransfers

Das wichtigste Ergebnis, welches sich aus Tabelle 5 entnehmen lässt ist, das 51 % der erreichbaren Nameserver, die für „ihre“ Domäne verantwortlich sind, einen Zonentransfer zulassen. Dieser Zonentransfer kann einem potenziellen Angreifer weitere Anhaltspunkte über Rechner- und Netzinfrastruktur geben.

4.4.4 Antwortverhalten

Nameserver können iterativ oder rekursiv arbeiten. Bei rekursiver Arbeitsweise des abgefragten Nameservers versucht dieser die Antwort einer bestimmten Anfrage zu ermitteln, auch wenn er die Antwort selbst nicht weiß. Bei iterativer Arbeitsweise würde der abgefragte Nameserver nicht die Antwort, sondern einen weiteren Nameserver nennen, der für die Anfrage zuständig ist.

Ob ein Nameserver rekursiv arbeitet kann durch eine Anfrage (zum Beispiel: Adressauflösung) mit “dig” in Erfahrung gebracht werden. Durch gesetzte “Flags” in der Antwort ist die Art, wie der Nameserver arbeitet, zu ermitteln.

```
dig @<nameserver> www.abcdef.com A
```

Nameserver, die erreichbar waren	338
Nameserver, die auf „dig“ nicht antworten (timeout)	78
Nameserver, die nicht erreichbar waren	34
Nameserver, die rekursiv antworteten	290

Tabelle 7: Ergebnis der Auswertung der Flags

Aus Tabelle 6 lässt sich leicht entnehmen, das (`100/338*290 = 85,8`) 86 % der erreichbaren Nameserver auf die Anfrage rekursiv antworteten. Sie werden dadurch zusätzlich belastet und sind verwundbar.

4.5 Sicherheitsempfehlung für den DNS-Betrieb

Der Nameservice Betrieb - mit und ohne die Sicherheitsunterstützung durch Secure DNS - ist eng verbunden mit der Betriebssystemsicherheit des Hosts, Zugangsschutz Firewallkonzepten und der korrekten Administration bzw. Konfiguration des Dienstes. Das FZI schlägt vor, eine interne Analyse mit dem Thema „Mehr Sicherheit im DNS-Betrieb“ vorzubereiten. [RFC 2870], [Househ], [Liu], [Chor].

4.6 Ausweg durch Secure DNS

Alle der aufgeführten Angriffsmöglichkeiten lassen sich erschweren durch sichere Administration des Dienstes und des Betriebssystemes. Zuverlässig zu verhindern sind sie jedoch nur mit Secure DNS.

4.7 Position der DENIC eG zu Secure DNS

„DENIC ist sich bewusst, dass es bzgl. DNSSEC eine Vorreiterrolle übernehmen muss, um den Einsatz des Sicherheitsprotokolls für *.de* voranzutreiben. Es bedarf allerdings eines Engagements von allen Beteiligten.“[42].

4.7.1 Empfehlungen

Neben der Investition in die eigene Betriebskompetenz (durch Testumgebungen und fachlich unterrichtete Administratoren und Operatoren) ist auch eine Unterstützung der DENIC Mitglieder (ISPs) angebracht, z.B. durch Schulungsmaßnahmen und technischen Support bei der Entwicklung und Anpassung der Applikationen für die Domainregistrierung. Eine Zusammenarbeit auf europäischer und internationaler Ebene mit anderen ccTLD- und gTLD-Domainregistrierungsstellen und Internetorganisationen ist notwendig.

4.7.2 DENIC-Studie

Im Jahr 2000 hat die DENIC eG zusammen mit der Secorvo Security Consulting GmbH durch die Erstellung einer Studie, den Einsatz von Secure DNS evaluiert [DENIC-Stud]. Die Studie geht sowohl auf rechtliche Anforderungen bei der Registrierung und Verwaltung der Domainnamen ein, als auch auf die vertraglichen Pflichten beim Betrieb. Diese Aspekte werden daher in unserer Analyse nicht untersucht.

In der Studie werden weiterhin detailliert die internen organisatorischen Prozesse für den DNS und DNSSEC-Betrieb beschrieben und sowohl technische als auch organisatorische Maßnahmen empfohlen, die sich am IT-Grundschutzhandbuch [GSHB] orientieren.

Der im Erstellungszeitraum der Studie existierende Protokollstandard war noch nicht ausgereift genug und somit zu diesem Zeitpunkt nicht einsetzbar. Grundlegende Mechanismen wurden in den letzten zwei Jahren nochmals überarbeitet. Dennoch sind die in der Studie gemachten Aussagen bzgl. Schlüsselmanagement und Policy sehr hilfreich.

4.8 Unterschiedliche Rollen im DNS-Betrieb

Secure DNS ist keine Anwendung, die DENIC alleine zur Verfügung stellen kann, um zukünftig eine sichere Namensauflösung zu gewährleisten. Vielmehr handelt es sich bei Secure DNS um mehrere Sicherheitsprotokolle zusammen mit einer PKI. Dies muss von den unterschiedlichen am DNS-Betrieb und der Anwendung Beteiligten unterstützt werden. Im einzelnen wären dies:

1. Endbenutzer: Je nachdem wie die Client-Software entwickelt wird, ist ein technisches Verständnis für Fehler- oder Sicherheitsmeldungen der Applikation notwendig[43].

[42] DENIC eG Geschäftsführerin Sabine Dolderer in einem Gespräch am 9.1.2003.

[43] Während der Benutzer sich bisher z.B. mit der folgenden Browser Fehlermeldung auseinandersetzen musste:

```
The following error was encountered:
Unable to determine IP address from host name for www.abcdefghijk.de
The dnsserver returned: Name Error: The domain name does not exist.
```

Könnte zukünftig die folgende Meldung eintreffen:

```
Verification of signature failed. Unable to determine the correct IP
address for the host www.abcdefghijk.de
The dnsserver returned:
```

2. Registrant (Domaininhaber): Auswahl der Option sicheres DNS beim Erwerb einer *.de*- Domain oder die Umstellung der gehaltenen Domains auf dieses Produkt. Dies kann mit Mehrkosten verbunden sein. Sicherlich ist nicht für jede „just for fun“-Domain eine Unterstützung durch DNSSEC notwendig.
3. Zonenadministrator: Dieser ist verantwortlich für die Publikation der Zoneninformationen: Der administrative Aufwand für den DNSSEC-Betrieb steigt.
4. Administrator (Nameserverbetreiber): Die Umstellung aller Nameserver und Resolver auf eine aktuelle Version, mag auf den ersten Blick als sehr aufwändig erscheinen. Es ist aber zu bedenken, dass die Nameserversoftware eine ständig zu pflegende Anwendung ist, die in regelmäßigen Abständen aktualisiert werden muss. Dies hat die Vergangenheit gezeigt, in der sehr häufig neue Patches gegen Angriffe und Softwarefehler der Nameserversoftware veröffentlicht wurden siehe z.B. Bind Vulnerabilities [BIND-Vul].
5. Reseller: Der Aufwand bei der Kundenauthentifizierung und beim Kontakt zum ISP wird höher. Eine Anpassung der organisatorischen Prozesse und Anwendungen ist erforderlich.
6. Registrar (ISP): Der Aufwand bei der Kundenauthentifizierung und beim Kontakt zu DENIC wird höher. Eine Anpassung der organisatorischen Prozesse und Anwendungen ist erforderlich.
7. Registry (DENIC): Im DNS-Betrieb wird höheres Update der Domaindaten notwendig. Die ISP’s müssen durch die Schulungsmaßnahmen unterstützt werden. Die Prozesse und Applikationen, die für die Domainregistrierung notwendig sind müssen angepasst werden. Für die Bereitstellung des Dienstes ist eine Investition in die Hardwareinfrastruktur und der Ausbau der Public Key-Infrastruktur notwendig.

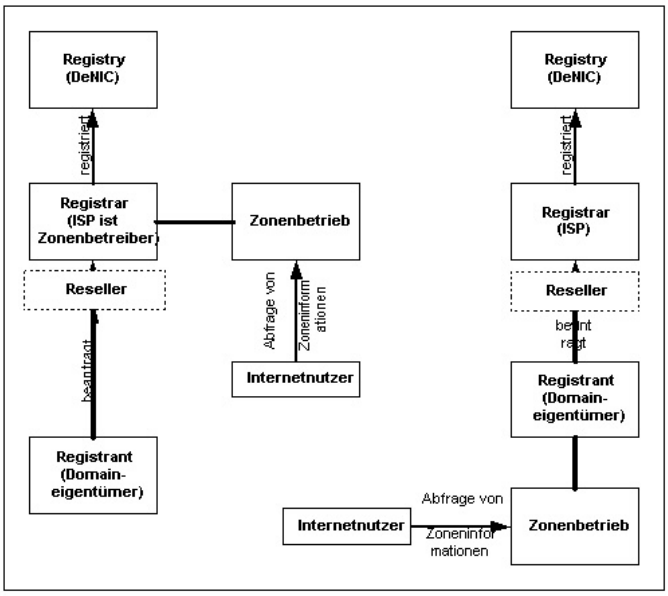


Abbildung 16: Unterschiedliche Rollen im DNS-Betrieb.

Abbildung 16 verdeutlicht die unterschiedlichen Rollen und zeigt auf, dass für den Zonenbetrieb sowohl der Domaineigentümer als auch der ISP zuständig sein kann.

Signature Error: The IP address can not dedicated reliably.

5 Sicherheitsprotokolle für DNS

5.1 Historie

Die Arbeit zu DNSSEC wurde bei einer IETF Konferenz 1993 [Galvin93] erstmals organisiert. Schon damals wurde die Entscheidung getroffen, DNS-Daten als öffentliche Informationen anzusehen und somit den Fokus für das Sicherheitsprotokoll auf die Datenintegrität und Authentizität zu legen.

Die Domain Name System Security Extensions (DNSSEC), welche auf diesen Ideen aufbauen, wurden zum ersten Mal 1997, als RFC 2065 und in überarbeiteter Form 1999 als RFC 2535, veröffentlicht. Zudem wurde 2000 der TSIG-Mechanismus RFC 2845 entwickelt, um Mechanismen zur Host-Authentifizierung anzubieten.

5.2 Entwurfsziele von DNSSEC

Das Hauptentwurfsziel von DNSSEC ist die Erweiterung des DNS-Protokolls nach RFC 1035, um Resolvern und Applikationen eine Überprüfung der DNS-Daten durch Authentifizierung und Datenintegrität zu ermöglichen. Unter anderem wird dadurch ein DNS-Poisoning verhindert.

5.3 Entwicklungsstand

5.3.1 Neue Resource Records, Header-Erweiterungen und Flags

Bei den DNSSEC-Extensions werden vier neue Resource Record (RR) Typen definiert: SIG, KEY, DS und NXT. Zudem wurde der OPT-Header um das DO-Bit erweitert und ein bisher leeres Feld im DNS-Header um die AD und CD Flags ergänzt. Diese Erweiterungen werden in den nachfolgenden Abschnitten näher erklärt.

5.3.2 DNSSEC Resource Record

Resource Records (RR) nach RFC 1035 umfassen die Daten einer DNS Zone und bestehen aus einem allgemeinen Teil, der den RR identifiziert (Name, Type, Class, TTL) und dem Datenteil (Länge der Daten, und die Daten).

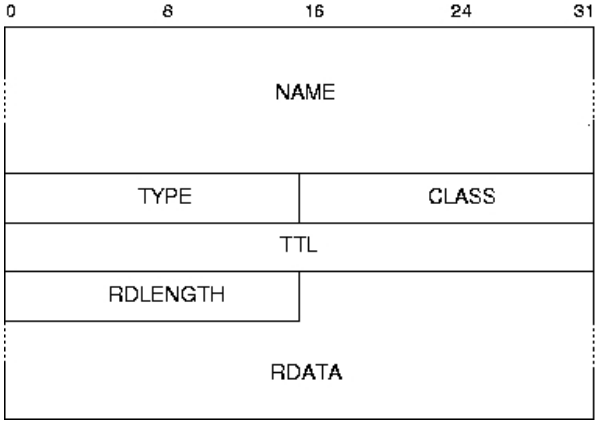


Abbildung 17 Aufbau eines DNS-Resource Records

NAME Eigentümer (des zughörigen DNS-Namensraums) zu dem dieser RR gehört

TYPE Ein 16-Bit Feld (signed integer), das den RR Typ bestimmt. Bei DNSSEC kommen hier KEY (25), SIG (24), NXT (30) und DS() hinzu.

CLASS Zwei Octette (signed integer), die die Klasse des RRs angeben. Typischerweise IN für Internet mit dem Wert 1.

TTL Ein 32 Bit langer positiver Integer, der angibt, wie lange dieser RR im Cache verweilt bevor er verfällt und neu angefordert werden muss.

RDLENGTH Ein vorzeichenloser 16 Bit Integer, der die Länge in Bytes des RDATA-Feldes angibt.

RDATA Dieses Feld enthält die Daten des Resource Records. Der Aufbau des Daten-Teils hängt vom TYPE ab.

Für zwei Resource Records ist es nicht sinnvoll in allen Werten von Namen, Class, Type und Datenfeld übereinzustimmen. Dennoch ist es möglich, dass zwei oder mehrere RRs den gleichen Namen, Class und Type aber unterschiedliche Daten haben. Solch eine Gruppe von RRs wird *Resource Record Set* (RRSet) genannt.

Beispiel:

```
drake.eid.fzi.de.     IN    A     141.249.248.7
gate.eid.fzi.de.      IN    A     141.249.248.7
```

5.3.2.1 KEY Resource Record

Der KEY Resource Record wird zur Speicherung eines Public Keys verwendet[44]. Bei DNSSEC hat jede "sichere" Zone mehrere (mindestens einen Key Signing Key und einen Zone Signing Key) Schlüsselpaare (öffentlicher und privater Schlüssel) [45]. Im KEY RR wird der öffentliche Schlüssel abgelegt. Der private Schlüssel wird geheimgehalten.

KEY RDATA Format

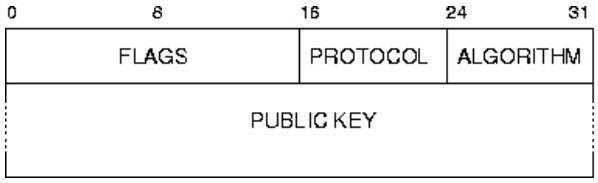


Abbildung 18: Aufbau des KEY-RDATA Feldes eines RRs

Ein Key-Record, der BIND-Konfiguration, sieht z.B. folgendermaßen aus:

```
fzi.de.  100 KEY 256 3 1 (
                          AQPBBstVnMAPxeEARO7UKaVwKUKAEjie6VKa
                          DpqrSyvLWE4byV/sr7gRZC4VuWCWfD6lXBxm
                          PZXZuDIhAYLSYWFuVhR35t94Wbn37/wcu/Wp
                          CCi8AcIj5Ik/CpCFyY0jKmH0LahuW5YdRNTy
                          gdew1jQOPg+/6lgJzfVRGDbnjdVfGQ==
```

[44] Ein erweiterter Einsatzbereich z.B. für IPSec oder TLS ist möglich.
[45] Die Unterscheidung von ZSK und KSK wird später noch näher erklärt.

```
                                ) ; key id = 45371
```

fzi.de ist der Domainname des Eigentümers, IN (Internet) der Typ und KEY die Klasse dieses Resource Records. Die danach folgenden Felder sind Teil des (KEY-)RDATA Feldes und haben folgende Bedeutungen:

FLAGS Ein 16 Bit langes Feld zum Setzen von Eigenschaften dieses KEY RRs. Das KSK-Flag im FLAGS-Feld zeigt an, ob es sich um ein Key Signing Key (KSK) oder ein Zone-Signing-Key (ZSK) handelt. In diesem Beispiel hat das FLAGS-Feld den Wert *256*.

PROTOCOL Dieses Octett Feld gibt an, für welches Protokoll dieser Record verwendet soll. *3* steht hier für DNSSEC, 1 für TLS, 2 für Email und 4 für IPSEC.

ALGORITHM Parallel zum SIG-RR wird hier der Algorithmus angegeben mit dem der Public Key verwendet werden soll. 1 steht hier für RSA/MD5.

PUBLIC KEY Der Public Key selbst. In Konfigurationsdateien wird der Public Key Base-64 codiert zur Darstellung des Keys mit ASCII-Text.

Die Key-ID wird nur in Konfigurationsdateien von Nameservern angegeben und wird durch das Berechnen einer Checksumme über den KEY-RR gebildet. Sie dient zur leichteren Identifizierung und Bennenung eines Schlüssels.

5.3.2.2 SIG Resource Record

Der "Signatur" SIG Resource Record (RR) dient zur Authentifizierung von Daten und ist der wesentliche Bestandteil der DNSSEC-Erweiterungen. Da die Public Key-Kryptografie rechenaufwändiger ist, wird anstelle eines einzelnen RRs die Authentifizierung eines RRsets von einem SIG RR durchgeführt, um so Rechenzeit zu sparen.

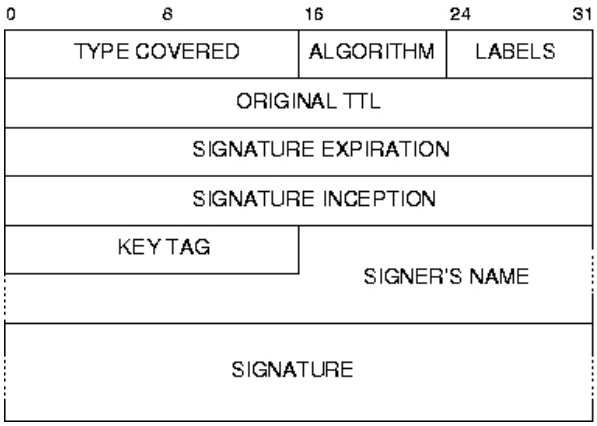


Abbildung 19: Aufbau des Signatur (SIG)-RDATA Feldes

Beispiel für einen authentifizierten KEY RR:

```
fzi.de.  100      SIG
                   KEY ; type covered
                   3     ; Algorithm
                   2     ; Labels
                   100 ; original TTL
                   20030425140814 ; Sig Expire
                   ( 20030326140814 ; Sig Inception
                   45371 ; key identifier
                   fzi.de. ; signers name
                   sJSncmJhSeZiAndvcbsqTUllJugExaHG974p
                   08Fy9JzzWRmJbwmB88EfLRXPzR/Rpp+Th/TX
                   j9veS5fdCSBuUGssAc4yLz5CvE//4R1XKzOc
                   Q8GJhYWSuzSQodbDAChgocjxD/0o3SvFShyp
                   HxQIAFZghPlSAYpbjQpytChFJE4= )
```

TYPE COVERED Gibt den Typ der Resource Records an, die diese SIG authentifiziert.

Im Beispiel wird der *KEY* Record abgedeckt.

ALGORITHM Nennt den Public Key-Algorithmus, der zur Erzeugung der Signatur verwendet wurde. Er hat den gleichen Wert wie das Algorithmus-Feld mit den dazugehörigen KEY RR. Hier ist mit 3 der DSA-Algorithmus angegeben.

LABELS Gibt die Anzahl der Labels, d.h. die Tiefe dieser Zone im DNS-Baum, an. `fzi.de` hat hier den Wert 3, wegen `de` und `fzi`.

Original TTL Dieses Feld ist Bestandteil des SIG RDATA-Feldes um zu vermeiden dass ein Angreifer die TTL der Signatur verändern kann. Da die SIGNATUR auch die Original TTL abdeckt ist sie unveränderbar.

Signature Expiration/Inception Die im SIG RR angegebene Signature ist von der Signature Inception bis zur Signature Expiration Zeit gültig. Diese werden in der Anzahl an vergangenen Sekunden seit dem 1. Januar 1970 GMT angegeben.

KEY TAG Identifiziert den KEY RR der den öffentlichen Schlüssel enthält.

SIGNERS NAME Der Domainname des öffentlichen Schlüssels, den ein Resolver oder Nameserver bei der Überprüfung der Signatur benutzen soll. Zusammen mit dem KEY TAG wird der öffentliche Schlüssel eindeutig identifiziert. Hier ist es der im Beispiel angegebene KEY mit *Key ID 45371* unterzeichnet von *`fzi.de`*.

Erzeugung der Signatur

Zur Erzeugung des SIGNATUR-Feldes im RDATA-Feld des SIG RRs wird zunächst

```
data = RDATA | Rrset
```

bestimmt, wobei RDATA die Daten des SIG RRs selbst sind und RRset das RRset ist, über das die Signatur gebildet wird. | bezeichnet hier die Konkatenation[46].

Es wird `data'` gebildet:

```
data' = hash(data)
```

[46] Das Aneinanderhängen von Strings, wird Konkatenation genannt

wobei hash eine Hashfunktion ist und schließlich

$$SIGNATUR = e_s\ (data')$$

berechnet wird, in der e eine Verschlüsselungsfunktion ALGORITHMUS mit privatem Schlüssel s ist.

Überprüfen der Signatur

Umgekehrt wird zur Überprüfung zunächst

$$h_1 = d_p\ (signatur)$$

gebildet, wobei d eine Entschlüsselungsfunktion (welche durch ALGORITHMUS bestimmt ist) mit öffentlichem Schlüssel p ist und dann

$$h_2 = hash(nachricht)$$

berechnet. Stimmen nun die beiden Ergebnisse h1 und h2 überein, so ist das RRset authentisch.

5.3.2.3 NXT Resource Record

Der NXT ("next") Resource Record wird benutzt um anzugeben, welche Resource Record Typen für einen Namen existieren und dient gleichzeitig als Zeiger auf den nächsten Domainamen einer Zone. Durch einen NXT RR vom letzten zum ersten Domainnamen einer Zone wird ein virtueller Ring erzeugt, durch den – mit Hilfe der entsprechenden SIG RRs - sicher festgestellt werden kann ob ein Name zu einer Zone gehört.

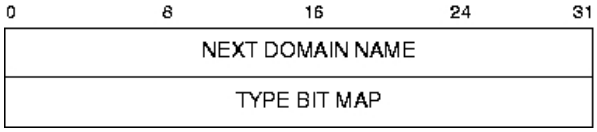


Abbildung 20: NXT Resource Record RDATA-Feld

Beispiel:

Die Domainnamen in *fzi.de* sind die folgenden (die RR werden zunächst lexikographisch sortiert):

```
fzi.de.            IN SOA ...
alice.fzi.de.      IN A   141.249.249.6
bob.fzi.de.        IN A   141.249.249.7
...

www.fzi.de.        IN A   141.249.249.2
```

alice.fzi.de kommt vor *bob.fzi.de.* Es ist *www.fzi.de* der letzte RR dieser Zone. Hieraus folgt z.B. folgender NXT Record:

```
alice.fzi.de.      NXT     bob.fzi.de. A SIG NXT
```

Dieser gibt an, dass *bob.fzi.de* (NEXT DOMAIN NAME) auf *alice.fzi.de* folgt und dass *bob.fzi.de* die Resouce Records A, SIG und NXT besitzt (TYPE BIT MAP).

Da *www.fzi.de* der letzte Name ist folgt,

```
www.fzi.de.     NXT   fzi.de. A SIG NXT
```

der durch den NXT-Record auf den ersten Resource Recod *fzi.de* der Zone den virtuellen Ring schließt.

Findet ein Lookup auf den nicht existierenden A-Record von *gibtsnicht.fzi.de* statt, so wird der NXT-RR zurück geliefert, der lexikografisch auf *gibtsnicht.fzi.de* folgt. Dies wäre im Beispiel *www.fzi.de*. Mit einem zugehörigen SIG RR wird folglich die Nichtexistenz eines Namens bzw. RRs bestätigt. Wird ein neuer RR in die Zone eingefügt, so muss nicht nur ein SIG RR für diesen RR eingefügt werden, sondern auch die Vorgänger- und Nachfolger-RRs. Deren Signaturen müssen neu erzeugt werden.

5.3.2.4 DS Resource Record

Der DS Resource Record wird zur Identifizierung der Schlüssel benutzt, die die Sub-Zone zur Selbstsignierung (Zone Signing Key) ihrer eigenen KEY RRsets benutzt. Ein DS RRset begleitend zu einem NS RRset deutet darauf hin, dass die delegierte - bzw. die Sub-Zone kryptografisch signiert und sicher ist.

Das RDATA-Feld des DS RRs

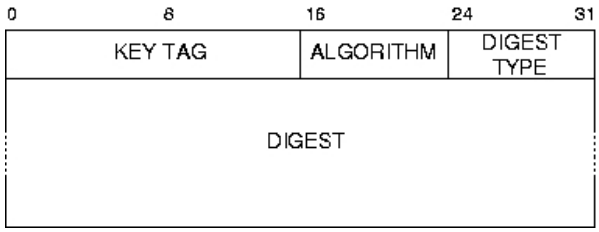


Abbildung 21: Deligation Signer (DS) Aufbau

KEY TAG Zur Identifizierung des KEY RRs der Sub-Zone.

ALGORITHM Gibt den Algorithmus des beim KEY RR verwendeten Schlüssels an.

DIGEST Berechnet sich aus

```
DIGEST = hash ( FQDN des KEY RR | KEYRRrdata )
```

wobei `hash` eine Hash-Funktion DIGEST TYPE ist und sich über

```
KEYRRrdata = Flags | Protocol | Algorithm | Public Key
```

der entsprechenden KEY RRs ergibt.

5.3.2.5 Modifizierung des OPT pseudo-RR

Der "Extension Mechanisms for DNS EDNS0" nach RFC 2671, erlaubt durch das Anhängen eines OPT pseudo-RRs in der Additional Section eines DNS-Paketes, einem Client den DNSSEC-Servern seine Fähigkeiten bezüglich der DNSSEC-Unterstützung mitzuteilen. Weitere Optionen (wie z.B. maximale UDP-Paketgröße) können ebenfalls angegeben werden (dies wird durch RFC 3225 definiert). Der OPT-RR ist ein pseudo-RR, da dieser keine DNS-Daten sondern Transport-Level-Nachrichten austauscht. Da der pseudo RR nicht gecached werden muss, benutzt man das TTL-Feld des RRs für die Flags.

Werden DNSSEC-Server eingesetzt, so besteht die Möglichkeit, dass auch nicht DNSSEC-fähigen Clients diese Server anfragen und Antworten erhalten, die sie nicht verstehen. Hierdurch wird unnötig Netzlast erzeugt. Im schlimmsten Fall wird, wenn die maximale DNS-UDP-Paketgröße von 512 Bytes [RFC 1035] überschritten wird, eine TCP-Verbindung aufgebaut.

Daher wurde nach RFC 3225, im OPT pseudo-RR (nach RFC 2671), ein „DNSSEC „OK-Bit“, eingeführt[47], das für den Client vorgesehen ist um aufzuzeigen, dass DNSSEC-Security Resource Records akzeptiert werden.

Das Hinzufügen des OPT-RRs mit gesetztem DO-Bit bei einer Anfrage an einen DNS-Server führt dazu, dass in der Antwort - neben den Standard RRs nach RFC 1035 - auch die RRs nach RFC 2535 und Erweiterungen gesendet werden. Dabei soll DNSSEC-sichere Auflösung verwendet werden. Ein OPT-RR am Ende einer Antwort bestätigt die DNSSEC-Fähigkeit des Servers und zeigt das Vorhandensein von DNSSEC-RRs im Antwortpaket.

5.3.3 DNS-Header Modifizierungen

Um weitere Resolver-spezifischen Informationen versenden zu können, wurde im DNS-Header nach RFC 1035 das Z(ero) Feld (3 Bit Länge) neu definiert. Es besteht nun aus dem Z(ero)-Feld und den Flags AD (Authentic Data) und CD (Checking Disabled). Nicht-DNSSEC fähige Server oder Resolver ignorieren bzw. setzen dieses Feld auf Null, wodurch der Header nicht vergrößert werden muss und die Rückwärtskompatibilität erleichtert wird.

5.3.3.1 Authentic Data Flag

Das Authentic Data (AD) Flag im DNS-Header zeigt an, dass alle zurückgelieferten RRs im DNS-Antwortpaket kryptografisch geprüft wurden und somit authentisch sind. Dementsprechend ist das AD-Flag nicht gesetzt, wenn das Antwortpaket "unsichere" Daten enthält. Besteht zwischen Resolver und angefragtem rekursiven Nameserver ein Vertrauensverhältnis, so kann eine entsprechende Applikation durch das Abfragen dieses Flags feststellen, ob die zurückgelieferten Daten sicher sind. Resolver, die keine DNSSEC-Unterstützung besitzen, ignorieren dieses Flag, da es im DNS-Protokoll nach RFC 1035 nicht beachtet wird. Ein Nameserver setzt das AD-Flag im Antwortpaket nur, wenn im Anfrage-Paket das DO-Flag im OPT-RR gesetzt wurde.

5.3.3.2 Checking Disabled Flag

Dieses Flag wird vom Resolver gesetzt und zeigt an, ob dieser DNSSEC- Authentifizierung vom angefragten Nameserver verlangt. Der angefragte Nameserver kann, muss

[47] Hierfür wurde das DO-Flag-Feld verwendet. Nach RFC 2671 ist dies das leere TTL-Feld (Z-Feld) des RRs.

aber nicht eine DNSSEC-Authentifizierung, durchführen wenn das CD-Flag gesetzt ist. Trifft dies zu, so wird es auch in der Antwort gesetzt um anzuzeigen, dass keine Authentizitätsprüfung vom Resolver verlangt wurde.

5.3.3.3 Notwendigkeit von Key Signing Key und Zone Signing Key

Aufgaben der Schlüssel

Im Rahmen einer Protokolländerung wurde in DNSSEC eine Unterscheidung in KSK und ZSK eingeführt [Del-Sig]. Die beiden Schlüssel bzw. Schlüsselpaare haben unterschiedliche Aufgaben und sollen den Verwaltungsablauf in DNSSEC vereinfachen, da der Zonenbetreiber den Signaturschlüssel für die Zone (ZSK) selbst ändern kann, ohne den Schlüssel bei der übergeordneten Instanz erneut zertifizieren zu lassen. Dies ändert die Aufgaben und Möglichkeiten der einzelnen Schlüssel wie folgt:

Key Signing Key

Der öffentliche Teil des Key Signing Key (KSK) - genauer dessen Hashwert - wird von der Parent-Zone signiert. Der entstehende DS Record stellt die Verbindung im Baum dar. Der KSK ist für eine Gültigkeit von ca. 1 Jahr vorgesehen und sollte daher über die notwendige kryptografische Stärke verfügen. Genauere Vorschläge siehe unten. Mit seiner Hilfe wird der eigentlich verwendete Signaturschlüssel der Zone Signing Key (ZSK) zertifiziert. Da mit dem KSK nur der ZSK unterzeichnet wird, erzeugt seine Anwendung, selbst bei täglicher Neuerstellung der Zertifikate, kein Performanceproblem.

Der KSK muss viel größer gewählt werden als der ZSK. Doppelte Schlüssellänge bedeutet 8-fachen Zeitaufwand. Je länger der Schlüssel eingesetzt wird, desto größer ist die Wahrscheinlichkeit einer Kompromittierung (z.B. Schlüsseldiebstahl).

Auf Client-Seite müssen Signaturen mit dem KSK immer dann überprüft werden, wenn der vollständige Vertrauenspfad bis zur Parent-Domain hin überprüft werden soll. Ein langer KSK führt daher beim Client zu Verzögerungen. Durch Verwendung kurzer öffentlicher Schlüssel kann dem entgegengewirkt werden. Sobald mehrere Rechnernamen aus der Domain angeführt werden, ist die Überprüfung des KSK nur einmal erforderlich.

Zone Signing Key

Der ZSK wird regelmäßig (meist täglich) eingesetzt, um alle Records der Zone zu signieren. Durch dieses hohe Aufkommen an Signaturen ergibt sich hier vielfach die Notwendigkeit, auf (relativ) kurze Schlüssel zurückzugreifen, um die notwendige Performance zu erreichen. Daten werden vor der Signatur erst gehashed, daher ist die Zonengröße nicht unbedingt relevant. Aus kryptografischer Sicht müssen die ZSKs nicht ganz so sicher wie die KSKs sein, da die von ihnen signierten Daten eine maximale Gültigkeitsdauer von wenigen Tagen (dem Zeitraum zwischen Signatur-Anfangszeitpunkt und Endzeitpunkt der unterzeichneten Resource Records) besitzen. Dennoch ist es auch hier erstrebenswert, die Rahmenbedingungen des Signaturgesetzes (Kapitel 6.3) einzuhalten. Wenn sie kryptografisch schwächer gewählt werden, so sollten sie regelmäßig gewechselt werden (ca. monatlich).

Lebensdauer und Bitlängen der Schlüsseln und Zertifikate

Da es inzwischen rechtliche Rahmenbedingungen für elektronische Signaturen gibt, sollte sich die Länge der verwendeten Schlüssel an den dort spezifizierten Längen orientieren. Diese schreiben für eine Gültigkeit bis Ende 2006 eine Mindestlänge von 1024 Bit für RSA und DSA vor [SigG, SigV, Algo-02]. Empfohlen ist jedoch eine Länge von 2048 Bit. Es würde sich anbieten, den langfristigen Schlüssel KSK mit einer Länge von 2048 Bit zu wählen, während die Länge von 1024 Bit des ZSK, der bezüglich seiner Performance kritisch ist, ausreicht. Diese Werte übertreffen die von [RFC 1541] gefor-

derten Mindestwerte, führen aber bei dem aktuellen Stand der Rechnertechnik nicht zu unlösbaren Performanceproblemen.

Ein Beispiel für die Gültigkeitsperiode der Schlüsseln und der durch sie signierten Daten könnte wie unten beschrieben aussehen. Zu beachten ist hierbei, dass normativ das Gültigkeitsmodell noch festzulegen ist. Das Kettenmodell, das nur die Gültigkeit der jeweiligen Zertifikate zum Erstellungszeitpunkt fordert, hat Vorteile in der Ausfallsicherheit des Gesamtsystems. Demgegenüber hat das Schalenmodell, bei dem zum Überprüfungszeitpunkt alle Zertifikate in der Hierarchie gültig sein müssen, Vorteile bei der einfacheren Durchsetzung unterschiedlicher Policies. Hier sollte im Rahmen der internationalen Normung ein Standard gesetzt werden. Für die verwendeten Schlüssel ergibt sich eine Unterscheidung zwischen deren Verwendungsdauer und dem Gültigkeitszeitraum der aktuellen Zertifikate. So kann ein Schlüssel zwar langfristig ausgelegt sein, aber vom übergeordneten ZSK jeweils nur kurzfristig zertifiziert werden. Dies ist nur scheinbar ein Widerspruch, da hier der gleiche langfristige Schlüssel immer nur kurzfristig als gültig bestätigt wird.

Nach [RFC 2541] ergeben sich folgende Gültigkeitsdaten:

- KSK von 13 Monate
- ZSK von 36 Tage
- Time To Live der Records 4 Tage

5.3.3.4 Caching der RR

Resource Records, die eine gültige Signatur besitzen und der Gültigkeitszeitraum (Zeitraum vom Anfangszeitpunkt der Signaturerstellung bis zum Endzeitpunkt) noch nicht überschritten ist, dürfen von einem sicherheitsunterstützenden Resolver gecached werden. Hierbei muss der Gültigkeitszeitraum der Signatur berücksichtigt werden, wenn die TTL festgelegt wird. Schwierigkeiten können entstehen, wenn die eigene Uhr des Resolvers falsch eingestellt ist.

5.4 Einsatz von Kryptografie-Hardware

Der private Schlüssel sollte nach Möglichkeit offline gehalten werden. Sofern kein dynamisches Update eingesetzt wird, ist das Signieren der RR problemlos möglich. Der private Schlüssel (ZSK) wird auf einem abgesicherten Computer ohne permanenten Netzwerkzugang gespeichert. Zur Erzeugung von neuen Signaturen, wird eine Netzwerkverbindung auf einem bestimmten Port aufgebaut. Alle anderen Ports sind über eine Firewall zu sperren. Die benötigten Daten werden z.B. von einer Datenbank angefordert. Sind die Signaturen erstellt, können die Daten auf den Nameserver übertragen werden.

Der KSK, der viel seltener eingesetzt wird, kann durch weitere Sicherheitsmaßnahmen wie z.B. Vier-Augen-Prinzip gesichert werden.

Für das Szenario Dynamic Update ist eine offline Haltung des privaten Schlüssels, wegen der benötigten ständigen Verfügbarkeit nicht möglich. Hier ist das Konzept von ZSK und KSK von großem Vorteil. Der KSK kann offline gehalten werden, während der ZSK online benötigt wird. Nur für den privaten Anteil des ZSK könnte der Einsatz von kryptografischer-Hardware von Vorteil sein. Allerdings sind derzeit noch keine Lösungen am Markt, die mit diesen Signaturen arbeiten können. Mittels DNSSEC ist es nicht vorgesehen die Integrität eines Zonentransfers zu schützen. Zusätzliche Mechanismen wie TSIG, SIG(0) oder IPsec sind notwendig und werden nachfolgend vorgestellt.

5.5 Protokollweiterentwicklung zum Schlüsselaustausch

Der in RFC 2535 definierte Protokollstandard für den Schlüsselaustausch ist mittlerweile durch verschiedene weitere RFC's und Drafts geändert und ergänzt worden. Die Mechanismen für den Schlüsselaustausch zwischen Parent[48] und Child[49] [Rollover] erwiesen sich in der Praxis als undurchführbar[50].

Als Alternative wurde vorgeschlagen, die Parent-Signatur des Schlüssels der untergeordneten Zone (Child-Key) nur in der Parent-Zone zu speichern, wo auch der Signaturschlüssel aufbewahrt wird [Gieben].

Aber auch dieser Entwurf brachte noch eine Reihe von möglichen Problemen mit sich. Daher wurde der Vorschlag durch einen Draft „Delegation Signer" [Del-Sig] abgelöst. Dieser Draft ist in seiner Entwicklung schon weit fortgeschritten und – aufgrund der Akzeptanz bei einem großen Teil der Entwicklergemeinde – sehr vielversprechend Es wird unter Experten davon ausgegangen, dass sich dieser Draft in der nächsten Zeit durchsetzen und in den Status eines RFC's erhoben wird. Weitere Anzeichen für die Akzeptanz des DS RR sind: Die derzeitige Entwicklerversion von ISC-BIND (bind-9.3.0s20021217) unterstützt das DS RR. Weiter wird in einigen Testumgebungen unter Voraussetzung dieser neuen Mechanismen gearbeitet.

Sollte der DS Draft in den RFC Status erhoben werden, dann würde dies einen Meilenstein in der Standardisierung des DNSSEC-Protokolls bedeuten. Das DS RR beeinflusst die darunter liegenden organisatorischen Prozesse in erheblichem Maße. Bei der Beschreibung der organisatorischen Prozesse in Kapitel 7 setzen wir ebenfalls die Verwendung des DS RR voraus. Allerdings ist durch diese Änderung im Protokoll eine Abwärtskompatibilität zu früheren Versionen des Nameservers und des Resolvers nicht mehr gegebenen. Dies ist ein Bruch mit einer wichtigen Tradition des Protokolls. Dies bedeutet, dass die Betreiber der DNS-Infrastruktur zu gegebener Zeit auf neue Versionen der Nameserversoftware umstellen müssen. Andere Softwarehersteller haben dieses Feature noch nicht implementiert zumindest der Name Service Daemon NSD vom Ripe NCC sollte in Kürze eine Unterstützung bieten.

5.6 Handhabung großer Zonen

DNSEC erfordert einen größeren Einsatz an Ressourcen bei der Erzeugung und Bereitstellung der Zone als DNS. Besonders für Registries mit sehr großen Zonen wie Verisign (*.com* über 21 Millionen) Einträge oder DENIC (*.de* über 6 Millionen Einträge) ergeben sich hier Schwierigkeiten für den operativen Betrieb.

Es wurde ein Verfahren mit Namen Opt-In [Opt-In] Vorgeschlagen, welches vorsieht neben den kryptografisch gesicherten Delegation an sichere Zonen auch kryptografisch ungesicherte Delegationen an unsichere Zonen vorzunehmen.

Um eine sichere Delegation für unsignierte Zonen vorzunehmen, bedarf es eines hohen kryptografischen Aufwandes. Dies gilt vor allem, wenn die Daten der RR für die unsichere Delegation auch noch häufig geändert werden. Durch Opt-In kann der Zonenad-

[48] Englisch Parent – Deutsch Elternteil. Wir verwenden auch Parent im deutschen da Elternteil umständlich wäre und Eltern nicht korrekt den Sachverhalt ausdrücken würde.

[49] Wir verwenden Child-Zone synonym für Sub-Zone aufgrund der Gebräuchlichkeit in der Literatur.

[50] Das ursprüngliche Austauschszenario [Rollover] ist: den Key RR und die Parent-Signatur darüber in der Child-Zone vorrätig zu halten (und u.U. noch in der Parent-Zone). Dies bringt verschiedene Komplikationen beim Schlüsselaustausch mit sich:

- das erneute Unterzeichnen durch den Parent wird schwierig
- ein angestoßener Schlüsselaustausch wird sehr kompliziert
- ein spontaner (unscheduled) Schlüsselaustausch wird praktisch unmöglich.

ministrator unsichere Zonen aus der NXT-Kette herausnehmen. Dies verringert den Aufwand der Bereitstellung des Zonefiles besonders für große Registries.

Die Argumente die gegen Opt-In sprechen, sind die steigende Komplexität der Software und die Reduzierung der Sicherheit durch die Delegation an unsichere Zonen.

Mittlerweile liegen auch erste Erfahrungen zum Test des Verfahrens vor [Opt-In WS].

5.7 Übersicht der Änderungen

Eine Liste mit derzeit im Draft Status[51] befindlichen Protokolländerungen wird von der IETF gepflegt[52]. Die Protokollweiterentwicklung wird intensiv auf der Namedroppers-Liste der IETF geführt. Das Ablaufdatum ist in Klammern angefügt, um den Entwurfstatus hervorzuheben. Sofern die Drafts im vorangegangen Text noch nicht beschrieben wurden, werden sie nachfolgend kurz erläutert. Die wichtigsten sind im Einzelnen:

5.7.1 Drafts

DNSSEC

[EDNS1] Extensions to DNS (EDNS1), (15-AUG-02).

Die „Extension Mechanisms for DNS (EDNS0)“, welche in RFC 2671 beschrieben sind, erweitertern die Nachrichtengröße des DNS-Protokolls von 512 Bytes auf 1289 Byte für UDP Pakete. DNSSEC benötigt diese Erweiterungsmechanismen, da durch die Verwendung von KEY, SIG und NXT Records eine erheblich erweiterte Nachrichtengröße notwendig wird.

EDNS1 verwendet den EDNS Erweiterungsmechanismus um erweiterte Labels, Typen und die Möglichkeit mehrere Fragen bei einer Anfrage zu stellen.

Im EDNS-Header wird das DO Bit gesetzt (RFC 3225), welches die Bereitschaft signalisiert DNSSEC-Records zu empfangen. Daher muss ein Nameserver, der DNSSEC-fähig ist, den EDNS-Mechanismus unterstützen.

[AD-Bit] Redefinition of DNS AD bit, (28-JUN-02).

Der Draft ändert die Bedeutung des AD Bit (Authenticated Data) aus RFC2535. Das AD Bit wird jetzt nur gesetzt, wenn in der Antwort die Signatur kryptografisch überprüft wurde oder wenn der Server autoritativ für die Daten ist und zudem berechtigt, das Bit aufgrund seiner Policy zu setzen.

[Del-Sig] Delegation Signer Resource Record, (04-DEC-02).

Siehe Kapitel siehe Abschnitt 5.5.

[Opt-In] DNSSEC Opt-In, (27-Feb-03).

[51] Draft Status bedeutet, dass dies Vorschläge für potenzielle RFC's sind, die von der Entwicklergemeinde diskutiert und bewertet werden. Diese Draft's werden ständig überarbeitet und haben nur eine Gültigkeitsdauer von 6 Monaten. Daher sollten sie auch nicht zitiert werden.

[52] http://www.ietf.org/ids.by.wg/dnsext.html

Siehe Kapitel siehe Abschnitt 5.6.

[KSK-Flag] KEY RR Key-Signing Key (KSK), (08-JAN-03).

Mit dem DS RR wurde das Konzept des key-signing eingeführt. Während des Schlüsselaustauschs mit dem Parent besteht die Notwendigkeit, zwischen ZSK und KSK zu unterscheiden. Für die Kennzeichnung des KSK wird ein Flag vorgeschlagen.

TKEY (Transaction Key)

[TKEY] TKEY Secret Key Renewal Mode, (25-SEP-02).

Eine Protokollerweiterung – ein neuer Mode im TKEY-Protokoll [RFC 2930], für den Ablauf des regelmäßigen Wechsels der geheimen Schlüssel, wird vorgeschlagen.

[DHS] Storage of Diffie-Hellman Keys in the DNS, (31-MAY-02).

Zur Speicherung von Diffie-Hellmann Schlüsseln soll der KEY RR verwendet werden.

Überblick

[Roadmap] DNS Security Document Roadmap, (05-FEB-03).

Die Vorschläge zur DNS-Sicherheit bestehen aus einer Reihe von Sicherheitsprotokollen. Die Roadmap versucht einen Überblick über die verschiedenen Vorschläge und die dazugehörigen Dokumente zu geben.

[Intro] DNS Security Introduction and Requirements, (05-FEB-03).

Überblick über die Domain Name System Security Extensions (DNSSEC).

[Threats] Threat Analysis Of The Domain Name System, (07-NOV-02).

Mögliche Angriffe gegen DNS werden vorgestellt, gegen die DNSSEC Schutz bietet.

Applikationkeys

[SSH-DNS], [IPSEC]

Das Problem des zuverlässigen Schlüsselaustausches haben viele Applikationen. Durch den CERT-RR wird ein Resource Record spezifiziert, mit dem Zertifikate für Applikationen wie SSH und IPSEC über DNSSEC ausgetauscht werden können.

5.7.2 RFC's

Nachfolgend sind die RFC's aufgelistet die den Standard RFC 2535 für DNSSEC ändern bzw. erweitern. Das angegebene Datum kennzeichnet jeweils den Zeitpunkt der Veröffentlichung:

TSIG

[RFC 2845] Secret Key Transaction Authentication for DNS (TSIG), May 2000.

Mittels symmetrischer Kryptografie soll ein Schutz des Zonentransfers erreicht werden. Außerdem kann mit TSIG eine Authentifikation des Clients bei Dynamic Update Prozessen erreicht werden.

TKEY

[RFC 2930] Secret Key Establishment for DNS (TKEY RR), Sept. 2000.

Transaktionsschlüssel, die für TSIG verwendet werden, müssen manuell zwischen Resolver und Server konfiguriert werden. Mit dem TKEY RR kann dieser Prozess automatisiert werden.

SIG(0)

[RFC 2931] DNS Request and Transaction Signatures (SIG(0)s), Sept. 2000.

Es wird Public Key-Kryptografie (RSAMD5, RSASHA1, DSA) eingesetzt, um Anfragen und Antworten zu authentifizieren. Dies ist auch zum Schutz des Zonentransfers geeignet.

Dynamic Update

[RFC 3007] Secure Domain Name System (DNS) Dynamic Update Nov. 2000.

Beim secure Dynamic Update wird gewährleistet, dass nur autorisierte Teilnehmer Änderungen an den Zonendaten vornehmen können. TSIG oder SIG(0) werden eingesetzt.

DNSSEC

[RFC 3130] Notes from the State-Of-The-Technology: DNSSEC, June 2001.

Bericht eines DNS-Security Meetings während der 49th IETF Konferenz.

[RFC 2929] Domain Name System (DNS) IANA Considerations, Sept. 2000.

Die von der IANA vergebenen Parameter für DNS werden aufgeführt.

[RFC 3008] Domain Name System Security (DNSSEC) Signing Authority, Nov 2000.

Ein überarbeitetes Model der Domain Name System Security wird vorgeschlagen.

[RFC 3090] DNS Security Extension Clarification on Zone Status, March 2001.

RFC 2535 wurde überarbeitet und verschiedene Begriffe klarer definiert.

[RFC 3110] RSA/SHA-1 SIGs and RSA KEYs in the DNS, May 2001.

Beschrieben wird das Verfahren, wie RSA/SHA1 SIG Resource Records(RRs) zu erzeugen sind.

[RFC 3225] Indicating Resolver Support of DNSSEC, Dec. 2001.

DNSSEC-Server dürfen die DNSSEC-RR nur dann automatisch bei der Antwort mit einbeziehen, wenn der Resolver vorgibt, die RR auch zu verstehen. Hierzu ist ein neues Bit im DNS-Header vorgesehen, das EDNS0 Bit. Dies drückt explizit aus, dass der Client das DNSSEC-Protokoll unterstützt. Bezeichnet wird das Bit auch als DO-Bit (DNSSEC OK Bit).

Aus dem RFC lässt sich folgern, welche Sicherheitsunterstützung von einem Client erbracht werden muss, der zu einer verlässlichen Namensauflösung beitragen soll: Das Fehlen von DNSSEC-Daten bei gesetztem DO-Bit darf nicht dahingehend interpretiert werden, dass keine DNSSEC-Daten für diese Zone verfügbar sind.

Will der Client der Sicherheitsunterstützung Rechnung tragen, muss dieser solche Daten ablehnen. Sobald DNS und DNSSEC parallel angeboten werden, ergibt sich folgendes Problem: Wird eine zurückgegebene Nachricht derart manipuliert, dass sowohl das DO Bit als auch die DNSSEC-Informationen entfernt werden, ist die DNSSEC-Unterstützung nutzlos, wenn der Client auf die DNS-Informationen zugreift.

[RFC 3445] Limiting the Scope of the KEY Resource Record out, Dec. 2002.

Der Einsatz der DNS KEY Resource Record (RR) wird auf die Domain Name System Security Extensions beschränkt.

Weitere RFC's und Drafts sind verfügbar, die im thematischen Umfeld von Secure DNS sind bzw. Bezug darauf nehmen, wie z.B. IPv6,. Eine Umfangreiche Liste ist unter [WG] verfügbar.

5.8 Neue Anforderungen durch DNSSEC

Die Erweiterung des herkömmlichen DNS-Dienstes zum DNS-Dienst mir Sicherheitsunterstützung durch das Protokoll DNSSEC, ist aus unterschiedlichen Gesichtpunkten erheblich aufwändiger.

1. Hardware

   Die Zoneninformationen vergrößern sich um einen Faktor 5-7 [TEST-NL]. Zu jedem RR, für den ein Server autoritativ ist, kommt ein SIG-RR und ein NXT-RR hinzu. Außerdem sind noch KEY-RR in der Zone vorhanden. Bei kleinen Zonen ist dies unproblematisch. Bei großen Zonen oder einer Vielzahl an Zonen können jedoch Grenzen erreicht werden. Bei einer Zonendatei größer als 4Gbyte sind beispielsweise die Hauptspeicheranforderungen so groß, dass eine Server Architektur mit 64-Bit verwendet werden muss.

2. Adminstration

Neue Aufgaben entstehen wie beispielsweise die Schlüsselerzeugung und Schlüsselverwaltung.

Weitere Anforderungen an den Betrieb treten auf: Beispielweise müssen Primary und Secondary dieselben Zeitkoordinaten besitzen. TSIG Nachrichten haben eine Default Lebensdauer von 5 min. Wenn die Zeit nicht synchron ist, werden die TSIG Nachrichten zurückgewiesen.

3. Operating

   Der DNS-Dienst ist derzeit bei den zentralen Nameserver ein 7*24 Stunden Betrieb. Um auf Störungen in angemessener Kürze reagieren zu können, wird meist eine Notfallhotline angeboten. Auch die für den Ernstfall angewiesenen Operatoren müssen über die neuen Schadensszenarien bestens unterrichtet sein. Notfallmaßnahmen müssen zur Verfügung stehen und sollten durch Planspiele abgedeckt sein.

4. Software

   ISC-BIND: Derzeit ist nur die Entwicklerversion der Software ISC-BIND in der Lage, den vorgeschlagenen Standard anzubieten. Dies wird sich aber ändern, sobald die Standardisierung abgeschlossen ist. Auch die anderen Anbieter von Nameserver und Resolver Software sind hier gefordert.

   Operationale Software im Betrieb: Registry, Registrar müssen ihre Applikationen erweitern und anpassen, damit sie die neuen Szenarien bearbeiten können.

   Clientseitige Unterstützung: Die Resolver Bibliothek muss DNSSEC unterstützen.

5. Prozesse

   Die Prozesse müssen die neuen Protokollanforderungen erfüllen und ergänzen, z.B. für den Fall, dass Schlüsselaustauschmechanismen oder die Schlüsselsperrung nicht im Protokoll enthalten sind.

5.9 Server Interoperabilität

Mittlerweile gibt es eine ganze Reihe an DNS-Server-Software. Sowohl Open Source als auch kommerzielle Produkte sind am Markt vertreten. Einen Überblick zusammen mit technischen Details und Installationshinweisen einiger ausgewählter Produkte gibt [Knowles][53]. Die bekanntesten Produkte sind in Tabelle 8 dargestellt.

Produkt	Lizenz	Secure DNS Unterstützung
ISC-BIND Version 8.2.3, 9.2.2),	Opensource	DNSSEC, TSIG Secure Dynamic Update (RFC 3007)
Microsoft 2000 DNS + Active Directory	Kommerziell	Secure Dynamic Update GSS-TSIG
Microsoft Server	Kommerziell	Secure Dynamic Update

[53] Ein interessanter Überblick darüber welches Nameserver-Produkt die gTLDs und ccTLDs einsetzen wird in der Präsentation ebenfalls gegeben.

Produkt	Lizenz	Secure DNS Unterstützung
+ Active Directory		DNSSEC (eingeschränkt)
UltraDNS	Kommerziell	nein
PowerDNS	GPL	nein
Incognito	Kommerziell	DNSSEC
Djbdns/tinydns	« Dont ask Dan »	nein
Ripe NCC Nsd	BSD-Lizenz	DNSSEC Kein Dynamic Update
Nominum	Kommerziell	DNSSEC

Tabelle 8: Vergleich unterschiedlicher Nameserversoftware

In Bezug auf obengenannte Beispiele werden unterschiedliche Sicherheitseigenschaften diskutiert und deren Eignung für Secure DNS vorgestellt.

1. ISC-BIND

   Das Internet Software Consortium (ISC) http://www.isc.org/ ist eine non-profit Gesellschaft. Sie hat die Aufgabe der Entwicklung und Pflege von Softwareprodukten, die für den Produktionsbetrieb geeignet sind. Verschiedene Open Source Software wird als Referenz Implementierung von fundamentalen Internet Protokollen bereitgestellt.

   Berkeley Internet Name Domain ist die am weitesten verbreitetste Software zum Betrieb eines DNS-Servers, mittlerweile ist diese Software schon 14 Jahre im Einsatz. Die Implementierung neuer Eigenschaften geht eng einher mit der Protokollstandardisierung. ISC-BIND ist quasi die Referenzimplementierung des DNSSEC-Protokolls. Bei allen unseren praktischen Untersuchungen hinsichtlich Secure DNS wurde ISC-BIND eingesetzt.

   Für die aktuellsten Protokollvorschläge muss auf die Entwicklerversion zurückgegriffen werden. Beispielsweise wird Sig(0) erst ab Version 9.3.0 unterstützt (die gegenwärtige Produktionsversion ist 9.2.2). Von einem Einsatz für die Produktionsumgebung muss bei dieser Version abgesehen werden.

2. Windows 2000 DNS

   Der Windows DNS-Server galt bisher als sehr sicher [Burns]. Es sind einige spezielle Sicherheitseigenschaften integriert, die allerdings nur im Zusammenspiel mir Active Directory verfügbar sind[54]. Dies macht den Einsatz aber proprietär. Probleme entstehen z.B. bei den Access Control Listen oder wenn „Nicht Windowsmaschinen“ am Dynamic Update Prozess teilnehmen sollen.

3. Windows Server 2003 family

   Eine einfache Unterstützung von DNSSEC findet statt. Ein Secondary-DNS-Server kann DNSSEC-Zonen anbieten. Weder die Erzeugung von Signaturen noch deren Überprüfung ist möglich. Secure Dynamic Update ist nur mit Active Directory Unterstützung durchführbar [Win2003].

[54] Der Einsatz nur im Zusammenspiel mit Active Directory wird auch von der NSA empfohlen. NSA, “Windows 2000 Security Recommendation Guide”, http://nsa2.www.conxion.com/win2k/index.html as of 7/30/01.

4. Djbdns

   Die Software gilt als sehr sicher. Für das Auffinden von Sicherheitslöchern ist ein Preis von 500$ ausgesetzt[55]. Als etwas eigenwillig erweisen sich die Konfiguration und Installation. Eine weitere Besonderheit ist, dass das Zonentransferprotokoll nicht unterstützt wird und eigene Anwendungen (remote sync) dafür bereitgestellt wird.

   DNSSEC Unterstützung:

   Keine DNSSEC Unterstützung, solange das Protokoll nicht fertig gestellt ist und kein konkreter Einsatzplan vorliegt [6].

5. nsd http://www.nlnetlabs.nl/nsd/

   Ein neuer, vielversprechender Nameserverdämon (name server daemon - nsd) wurde vom Ripe NCC entwickelt. Durch spezielle Eigenschaften ist er nur für bestimmte Einsatzgebiete (z.B. als Root- oder TLD-Server) geeignet. Es handelt sich um einen authoritative-only Server, der keine Rekursion, kein Caching, keine Dynamic Update und keine Zonentransfers unterstützt. Dafür wird DNSSEC angeboten und auf Sicherheit und Performance wert gelegt.

6. PowerDNS http://www.PowerDNS.com

   Authoritative-only Server ohne DNSSEC-Unterstützung

7. UltraDNS http://www.ultradns.com/,

   Bei UltraDNS handelt es sich um einen organisierten DNS-Service, den ein Drittanbieter als Dienstleistung erbringt. Auch DNSSEC-Services sind geplant [4].

8. Nominum http://www.nominum.com/

   Nominum's Chief Scientist ist Paul Mockapetris[56]. Es werden zwei Produkte angeboten:

   1. Nominum Foundation™ Autoritativer Nameserver mit DNSSEC-Unterstützung
   2. Nominum Foundation™ Caching Nameserver, unterstütz die kryptografische Überprüfung der DNSSEC RR.

9. Incognito

   DNS Commander mit einem komfortablen Interface zur Verwaltung der Zoneninformationen und DNS Diagnostic Tool. DNSSEC-Unterstützung[57].

10. Weitere bekannte Opensource Produkte sind:

    - MaraDNS http://www2.maradns.org
    - CustomDNS http://customdns.sourgeforge.net
    - Lbnamed www.stanford.edu/~ripel/lbnamed

[55] http://cr.yp.to/djbdns/guarantee.html
[56] Erfinder des DNS.
[57] http://www.incognito.com/products/DNSCommander/Enterprise/index.asp
http://www.circleid.com/articles/2551.asp

5.10 Client-seitige Unterstützung von DNSSEC

Für einen erfolgreichen Einsatz von Secure DNS ist es notwendig, dass die Nameserver die sicheren Zonen anbieten. Aber auch die Resolver und Client-Applikationen müssen das Protokoll unterstützen.

Aufgrund des Hinzufügens neuer Resource Records und modifizierte DNS-Header, sind auch auf der Resolver-Seite Veränderungen notwendig. Client-seitige Unterstützung des DNSSEC-Protokolls ist derzeit noch nicht vorhanden.

Da die notwendigen Funktionen noch nicht in den Resolverbibliotheken implementiert sind, existieren folglich auch keine Applikationen, die eine DNSSEC-unterstützte Namensauflösung anbieten.

In einer FZI-internen Studie wird untersucht, inwieweit die DNSSEC-Erweiterung einer ausgewählten Client-Applikation möglich ist. Als Applikation wurde der SQUID-Proxy ausgewählt.

Eine weitere Studie zur Unterstützung der Client-Systeme ist geplant. Da nicht abzusehen ist inwieweit Hersteller das DNSSEC-Protokoll in ihre Anwendungen integrieren, wird die Entwicklung eines **DNSSEC-Proxy** vorgeschlagen. Dieser soll die DNSSEC-Anfragen und Antworten bearbeiten und im Fehlerfall (z.B. Signatur Error), die Namensauflösung nicht durchführen. Der Benutzer erhält eine Information. Dieser Proxy hätte auch den Vorteil, dass er für alle Anwendungen regelt, wie im Fehlerfall zu verfahren ist. Ein einheitliches Ausgabeinterface sowie eine definierte Policy für die Verwendung von DNSSEC ist erforderlich. Dies würde auch verhindern, dass der Benutzer eine solche Meldung einfach durch „wegklicken“ ignoriert. Signaturfehlermeldungen müssen hier vom Anwender ernster genommen werden als die bekannten Meldungen über abgelaufene Zertifikate oder unbekannte Zertifizierungsstellen. Die Praxis zeigt, dass unbedachte Benutzer Webseiten trotz solcher Warnungen besuchen.

5.11 Unterschiedliche Einführungsebenen

Es gibt unterschiedliche Einführungsebenen für Secure DNS.

1. Root
2. Top-Level Domainebene (gTLD, ccTLD)
3. Domainebene (Intranet)

Weiter gibt es verschiedene Anwendungsszenarien. Wie oben beschrieben, unterscheiden wir Authentizität, Integrität und Vertraulichkeit. Dies wird durch die Verwendung von DNSSEC, TSIG, und Sig(0) gewährleistet. Welche Probleme stellen sich bei der Einführung auf den einzelnen Ebenen und welcher Sicherheitsgewinn wird dadurch erreicht?

- Root

  Das Problem eines globalen Deployments von DNSSEC wurde bereits auf einigen Mailinglisten diskutiert und ein Draft-Dokument ist vorhanden [Ihren].

- Top-Level Domainebene

  Hier sind die Probleme ähnliche wie auf der Root-Ebene nur um einige Größenordnungen kleiner und bei den cc-TLDs mit nationalem Charakter.

  TSIG könnte ohne größeren technischen Aufwand eingesetzt werden, um die Kommunikation zwischen Primary und Secondary abzusichern. Hier eignen sich auch proprietäre Verfahren, sofern diese auf wirksamen Sicherheitsprotokollen

aufsetzen. Für den Zonentransfer könnte z.B. auch scp[58], rsync[59] eingesetzt werden.

- Intranet

  Das Know How für den Einsatz von DNSSEC im Intranet , bei z.B. hostbasierten Services ist derzeit bei fast allen DNS-Administratoren noch nicht vorhanden. Es werden vom Ripe NCC Kurse angeboten. Adressiert sind diese Kurse aber an die ISPs. Zum Einsatz auf Intranetebene könnte vorteilhaft TSIG und Sig(0) zur Anwendung kommen.

[58] http://www.openssh.com/
[59] http://rsync.samba.org/features.html

6 PKI –Aspekte für Secure DNS

6.1 Grundlagen PKI

Unter einer Public Key-Infrastruktur (PKI) versteht man die Infrastruktur, die im Hintergrund zur Verfügung stehen muss, um das Public Key-Verfahren für verschiedene Applikationen einzusetzen. An eine solche PKI sind in Abhängigkeit der Sicherheitsbedürfnisse verschiedene Anforderungen zu stellen, um eine Sicherheitsunterstützung zu erreichen.

Eine detaillierte Übersicht über eine Public Key-Infrastruktur und die dazugehörigen Prozesse ist in [Austin] beschrieben.

Bei der Verwendung der Sicherheitsprotokolle für Secure DNS sind zwei unterschiedliche Aspekte hinsichtlich einer Integration in eine Public Key-Infrastruktur von Interesse. Zum einen stellt sich die Frage welche PKI-Technik ausgewählt werden soll, um Zertifizierungsdienstleistungen anzubieten, zum anderen benötigt die Bereitstellung der Protokolle DNSSEC, TSIG, Sig(0) eine Einbettung in eine PKI, die innerhalb der Protokolle nicht vollständig spezifiziert ist.

Kapitel 6.2 bis 6.6 untersucht die von DENIC betriebenen CA-Dienstleistungen vor dem Hintergrund bestehender standardisierter Regelungen. Hierbei wird ein Vergleich zu signaturgesetzkonformen PKIs angestellt. Wenngleich die Anforderungen im DNS-Bereich nicht an die einer qualifizierten Signatur nach SigG heranreichen, wird dennoch eine Anlehnung an die entsprechenden Standards empfohlen.

In Kapitel 6.7 werden die Grundprozesse einer PKI vorgestellt und daraufhin analysiert, inwieweit diese von Secure DNS unterstützt werden. Eine Beschreibung der organisatorischen Abläufe mit PKI-Unterstützung wird in Kapitel 7 vorgenommen.

6.2 CA-Dienstleistungen für die Domain Registrierung

Diese Dienstleistungen sind nicht primär in den DNS-Betrieb eingebunden. Sie unterstützen den Betrieb jedoch, indem über sie die Generierung und Wartung der im DNS zu veröffentlichenden Daten abgesichert wird. Eine Kompromittierung der Verfahren an dieser Stelle kompromittiert daher direkt die im DNS veröffentlichten Daten unabhängig von ihrer Absicherung durch DNSSEC. Die Anforderungen an die Integrität und Authentizität der ausgetauschten Daten sind an dieser Stelle daher relativ hoch.

6.2.1 Authentisierung der Beteiligten

Wie in Kapitel 4.8 beschrieben, gibt es unterschiedliche Parteien im DNS-Betrieb. Wir betrachten diese unter dem Gesichtpunkt der gegenseitigen Authentifizierung. Diese ist bezüglich einer verbindlichen Identifikation für die unterschiedlichen Abläufe erforderlich.

6.2.1.1 ICANN – DENIC

Müssen beispielsweise die Daten des Primary geändert werden, ist ein Kontakt zwischen DENIC und ICANN notwendig. In diesem Fall, wird ein unsigniertes Template vom administrativen Ansprechpartner (Sabine Dolderer) oder technischen Ansprechpartner (DENIC-operations) der DENIC, an ICANN gesendet. Daraufhin wird von ICANN das Template an den eingetragenen admin-c und tech-c der TLDs zur Gegen-

bestätigung an beide Kontakte zurückgeschickt. Danach wird nochmals eine Bestätigung versandt. Gegebenenfalls gibt es noch weitere Nachfragen. Ist alles geklärt, erfolgt der Eintrag.

Aufgrund der hohen Konstanz der Einträge der TLDs erfolgt diese Kommunikation sehr selten. Hinzu kommt, dass die beteiligten Parteien oft in regelmäßigem persönlichen Kontakt stehen und anfallende Änderungen daher auch vorab über getrennte Wege kommuniziert werden.

6.2.1.2 DENIC - ISP

PGP-Verfahren

Schon seit längerer Zeit wurde von DENIC die Einführung eines Authentifikationsverfahrens -basierend auf PGP-Signaturen[60] - für die Mitglieder geplant. Dieses Verfahren machte es erforderlich, alle Prozesse, die für die Domainverwaltung genutzt werden und die Kommunikation zum ISP betreffen, anzupassen. Die entsprechenden Schnittstellen mussten auch auf Applikationsseite der ISPs implementiert werden. Diese Umstellung erforderte auf beiden Seiten einen größeren technischen Aufwand, wodurch Verzögerungen verursacht wurden. Der technische Beirat entschied, die PGP-Lösung bis zum 1.12.2002 anzubieten. Seit diesem Zeitpunkt werden keine herkömmlichen Anträge mehr unterstützt.

Als Verfahren wird PGP in der Version 5 eingesetzt. Es wir mit einer Schlüssellänge von 1024 Bit gearbeitet. Die Schlüsselerzeugung findet seitens der ISP statt. Der öffentliche Schlüssel wird von DENIC signiert. Die Übertragung geschieht per Email, zur Überprüfung wird der Schlüsselhashwert telephonisch abgeglichen. DENIC tritt an dieser Stelle als CA für die derzeit 183 Mitglieder auf. Die Schlüssel werden im Dateisystem gespeichert unter dem Benutzeraccount, der die Programme zur automatischen Bearbeitung der Domainaufträge verwaltet. Zugriff auf diesen Account haben bei DENIC die Hostmaster. Eine Personalisierung des Schlüssels findet nicht statt. Er ist dem Hostmasteraccount zugeordnet.

Die Kommunikation geschieht über signierte Emails. Das Format der Anträge und das Verfahren ist proprietär.

6.2.1.3 ISP - Zonenadministrator

Geschäftskunden von ISPs haben meist persönliche Ansprechpartner. Auf beiden Seiten gibt es berechtigte Personen, die Anträge stellen bzw. diese entgegennehmen.

6.2.1.4 ISP – Kunden

In der Regel findet das folgende Szenario statt: Der Kunde meldet sich beim Provider an. Neben Name, Anschrift, Emailadresse wird auch die Bankverbindung erfasst. Der Provider besitzt daher ausreichende Daten, um den Kunden zu identifizieren. Spätere Kontakte nach der Etablierung dieses Geschäftsverhältnisses, finden in der Regel über Kundennummer und Passwort über eine Webschnittstelle statt. Bei besonderen Aufträgen wie z.B. dem Providerwechsel, muss eine Unterschrift vom Domaineigentümer vorliegen. Dies geschieht über die Briefpost oder auch über Fax.

[60] Pretty Goog Privacy, The International PGP Home Page, http://www.pgpi.org/

6.2.2 Einbettung in den europäischen und internationalen Kontext

Für die Domainregistrierung gibt es mittlerweile standardisierte Verfahren. Unter anderem EPP [EPP] und NSI RRP [RFC 2832]. EPP wird von der IETF Arbeitsgruppe Provisioning Registry Protocol (provreg) weiterentwickelt.

Das EPP-Protokoll verwendet 3 Sicherheitsmechanismen:

1. Zugriffskontrolle durch einen Filter für IP-Adressen
2. SSL-Verschlüsselung des Kommunikationskanals. Hier kommen X.509 Zertifikate zum Einsatz
3. Sitzungsauthentifikation durch Benutzername und Passwort

Das EPP Protokoll wird z.B. von Afilias (www.afilias.info) eingesetzt. Mittelfristig möchte DENIC auch EPP anbieten.

6.3 Rahmenbedingungen des Signaturgesetzes

CA-Dienstleistungen werden als besonders sicherheitsrelevante Prozesse betrachtet. Eine übergeordnete Autorität ordnet durch ein digitales Zertifikat dem Antragsteller einen eindeutigen Namen zu (distinguished name). Wären die Prozesse, Algorithmen und Verfahren hinter diesem Zertifizierungsprozess unsicher, könnte der digitale Ausweis angezweifelt werden und wäre somit wertlos. Mittlerweile gibt es rechtliche Rahmenbedingungen [SigG, SigV] für elektronische Signaturen in Deutschland[61]. Diese geben vor, wie eine digitale Signatur, die auf einer bestimmten Zertifikatsklasse beruht, rechtlich zu behandeln ist. Bei der Verwendung von qualifizierten elektronischen Signaturen, die auf qualifizierten elektronischen Zertifikaten beruhen, lässt sich im Extremfall sogar eine Rechtsverbindlichkeit der erzeugten Signaturen ableiten, die der handschriftlichen Unterschrift gleichgestellt ist.

Die technischen Normen, die die Erstellung und Ausgabe von Signaturen und Zertifikaten regeln, werden in [SigI] beschrieben. Die darin vorgeschlagenen Schlüssellängen und Algorithmen gelten zum gegenwärtigen Zeitpunkt als sicher und sind so gewählt, dass sie mit hoher Wahrscheinlichkeit für einen bestimmten Zeitraum zuverlässig zu verwenden sind [Algo-01, Algo-02]. Daher erscheint es sinnvoll, sich bei der Auswahl der Verfahren, Parameter und der Algorithmen, auf diese Empfehlungen zu stützen, auch wenn die Rechtskomponente nicht zur Anwendung kommt.

6.3.1 Aufgaben einer CA nach SigG/SigV

Im folgenden werden die Aufgaben eines Betreibers einer CA nach dem deutschen Signaturgesetz bzw. der Signaturverordnung aufgeführt.

Der Betreiber muss bei der RegTP die Tätigkeit als CA beantragen und sich von einer Bestätigungsstelle (z.B. TÜV-IT) überprüfen bzw. akkreditieren lassen. Hierbei wird nachgewiesen, dass die Aufgaben einer CA zuverlässig und fachkundig durchgeführt werden können. Kontrolliert wird das Sicherheitskonzept des Betreibers, das ist im Einzelnen:

Übersicht über die Ablauforganisation der Zertifizierungstätigkeit

Übersicht über eingesetzte Produkte, Hard- und Software zur Zertifizierung

Technische sowie organisatorische Maßnahmen, zur Absicherung der Zertifizierungsarbeit

[61] Auch auf europäischer Ebene gibt es entsprechende Rahmenbedingungen. Am 19.1.2000 wurde die **Richtlinie 1999/93/EG** im Amtsblatt der Europäischen Gemeinschaft veröffentlicht und trat somit in Kraft.

Maßnahmen zur Sicherstellung des Betriebs in Notfällen

Maßnahmen zur Überprüfung des eingesetzten Personals auf Zuverlässigkeit

Abschätzung & Bewertung eventuell verbleibender Sicherheitsrisiken

Der Betreiber ist für seine Zertifizierungen haftbar. Eine Deckungsvorsorge von mindestens 250.000 € muss bereitgestellt werden.

Sämtliche Vorgänge im Zusammenhang mit der Zertifizierungstätigkeit müssen dokumentiert werden.

Die im Betrieb eingesetzten Hard- und Software Komponenten müssen nach dem Signaturgesetz zertifiziert worden sein.

Bei der Zertifizierung eines Antragsteller muss der Betreiber folgendes beachten:

Ein Antragsteller muss sich nachweisbar identifizieren, beispielsweise durch persönliches Erscheinen unter Vorlage des Personalausweises bzw. anhand eines „digitalen Ausweises“ - ein nach dem Signatur-Gesetz qualifiziertes Zertifikat.

Der Inhalt eines auszustellenden Zertifikats ist vom Gesetz festgelegt. Es enthält:

Name des Inhabers oder ein ihm eindeutig zuzuordnendes Pseudonym

Der Signaturprüfschlüssel inkl. Name des verwendeten Algorithmus sowie die dafür wichtigen Parameter

Laufende Nummer des Zertifikats

Beginn und Ende der Zertifikat-Gültigkeit

Eventuelle Einschränkungen für die Benutzung des Zertifikats und antragstellerspezifische Attribute, z.B. berufsbezogene Attribute

Angaben zu möglichen Vertretungen des Antragstellers

Vor Ausstellen des Zertifikats muss der Betreiber als CA den Antragssteller über sämtliche Details im Umgang mit dem Zertifikat und digitalen Signaturen belehren und sich überzeugen, dass vom Antragsteller nur qualifizierte Hard- und Software eingesetzt wird.

Wird das Zertifikat zu einem späteren Zeitpunkt fertiggestellt, so muss es dem Antragsteller vom Betreiber persönlich übergeben werden.

Der Betreiber hat als CA ein öffentliches Verzeichnis aller von ihm ausgestellten Zertifikate zu führen.

Alte Zertifikate, d.h. Zertifikate, die gesperrt oder „ausgelaufen“ sind, müssen noch mindestens weitere 30 Jahre vom Betreiber gespeichert werden.

Es muss ein 24h Service zur Sperrung von Zertifikaten verfügbar sein. Ein Zertifikat ist unverzüglich auf Antrag des Inhabers zu löschen.

Für den Betrieb einer CA gelten die allgemeinen Bestimmungen des Datenschutzes. Demzufolge dürfen nur für den Betrieb als Zertifizierungsstelle zweckdienliche Daten von Antragstellern gesammelt und gespeichert werden. Grundsätzlich bedarf jedwede Datenerhebung der Zustimmung des Betroffenen.

6.3.1.1 Erzeugen von qualifizierten digitalen Signaturen

Hierbei ist zu beachten, dass sämtliche Hard- und Software-Komponenten nach dem Signaturgesetz zertifiziert sind.

6.4 Best Practice Sicherheit für die DENIC-CA

Es ist aus organisatorischen und finanziellen Gründen für DENIC wenig sinnvoll, signaturgesetz-konforme qualifizierte Dienste anzubieten. Die im Signaturgesetz und in entsprechenden Gesetzesverordnungen vorgeschriebenen Maßnahmen sind kurz- und mittelfristig für den Einsatz als CA für DNS-Dienste zu aufwendig, zu teuer und wenig zweckmäßig. Vielmehr sollte eine „best practice“ Lösung zum Einsatz kommen, die durch die Vorschriften und Maßnahmen des Signaturgesetzes angeleitet ist.

Wie im Signaturgesetz vorgeschrieben, macht es für jede CA durchaus Sinn, ein systematisches Sicherheitsmanagement einzuführen, auf den Einsatz sicherer Hard- und Software zu achten, sowie zuverlässig neue Zertifikate für Antragsteller, Provider bzw. Zonenverwalter, zu erstellen. Im Folgenden werden die an den Vorgaben des Signaturgesetzes angelehnten Anforderungen für Sicherheitsmanagement, Hardware und Software, auf das DENIC angewendet[62].

6.4.1 Sicherheitsmanagement

- **Sicherheitskonzept** DENIC muss die komplette Ablauforganisation und Zertifizierungstätigkeit dokumentieren und von einer qualifizierten Stelle überprüfen lassen, beispielsweise durch renommierte Security-Consulting Unternehmen, die für die Erstellung eines Audits zertifiziert sind. Dabei sollte das Ergebnis sein, dass DENIC die Tätigkeit als CA für den Betrieb Secure DNS fachkundig, sicher und zuverlässig ausüben kann. Die Sicherheit sämtlicher Tätigkeiten soll durch das Einhalten eines Sicherheitskonzepts („Security-Policy“) gewährleistet werden. Diese Policy beschreibt neben strategischen Zielen zum sicheren Umgang mit dem Internet oder dem firmeneigenen Netz („Netzwerk-Policy“) und den Schutz eines jeden Aspekts, der mit den Aktivitäten als CA zusammenhängt. Auch untergeordnete CAs bei den ISPs sollten ein Sicherheitskonzept vorlegen, das den vom DENIC spezifizierten Mindestanforderungen genügt.
- **Risikomanagement** Im Rahmen eines Risikomanagements werden Risiken wie beispielsweise Fehlbenutzung der CA-Software, externe oder interne Angriffe auf Schlüssel oder Kommunikationsverbindungen, Hard- und Software-Fehler als Bedrohungen identifiziert. Aus solchen Bedrohungen lassen sich – z.B. anhand des IT-Grundschutzhandbuches – sehr praktische Maßnahmen ableiten, die solche Bedrohungen abwenden oder minimieren. Diese Maßnahmen müssen in die Praxis umgesetzt werden. Anhand des DENIC DNS-Betriebs wurde in der Vergangenheit eine Bestimmung der Sicherheitsanforderungen durchgeführt [DENIC-Stud].
- **Notfall-Pläne** Nicht immer können im Vorfeld Absicherungen gegen sämtliche potenzielle Gefahren eingesetzt werden. Daher müssen die trotz der schützenden Maßnahmen verbleibenden Risiken erkannt und eingeschätzt werden. Es ist von entscheidender Bedeutung, dass „für den Fall der Fälle“ Notfall-Pläne bereit stehen, so dass ein u.U. eingeschränkter Betrieb noch möglich ist.

[62] Standardsicherheitsanforderungen, wie das IT-GSHB vorsieht wurden bei DENIC bereits bestimmt und die enstprechneden Maßnahmen umgesetzt [DENIC-DFN].

- **Security Management** DENIC sollte ein Security-Management einführen, dass kontinuierlich diesen Prozess der Sicherheits-Realisierung durch
  - Erkennen von Gefahren
  - Implementierung von Gegenmaßnahmen
  - Identifikation von Restrisiken

  überwacht.
- **Haftung** Für seine neue CA-Tätigkeit ist DENIC entsprechend verantwortlich und muss gegenüber Providern oder Zonen-Betreibern die Verantwortung übernehmen. Das Signaturgesetz verpflichtet zu einer Deckungsvorsorge von mindestens 250.000 €, die bereitgestellt werden muss. Inwieweit DENIC als „nicht-akkreditierte" CA entsprechend finanzielle Absicherung benötigt bzw. braucht, muss noch überprüft werden. Gegenstand und Umfang der Haftung sollten dennoch klar geregelt werden.
-

6.4.2 Auswahl geeigneter Hard- und Software

Die im Betrieb eingesetzten Hard- und Software Komponenten müssen höchsten Sicherheitsansprüchen genügen. Ideal wäre der Einsatz von gesetzes-konformen zertifizierten Produkten. Da diese jedoch erwartungsgemäß für den automatisierten Einsatz bei DENIC und bei den Providern nicht in Frage kommen, müssen am Markt befindliche Lösungen eingesetzt werden, die eine einfache Anpassung an ihr Einsatzfeld ermöglichen und trotzdem ein hohes Maß an Sicherheit bieten. Prinzipiell sollte von „Bastel-Lösungen" möglichst abgesehen werden. Der Einsatz von Hardware Sicherheits- Modulen (HSM) - wie Chipkarten - hat beispielsweise gegenüber der bisherigen rein softwarebasierten PGP-Methode den Vorteil, dass der geheime Schlüssel das Chipkarte HSM nicht verlassen kann. Der Rechner, auf dem die PGP-Signaturen erstellt werden, ist hingegen ständig von bekannten oder noch unbekannten Schwachstellen seines Betriebssystems und der eingesetzten Software bedroht.

6.4.3 Zertifizieren eines Providers bzw. Zonenverwalters

- Bei der Zertifizierung eines neuen Antragssteller ist die Authentizität sicher festzustellen. Ein Antragsteller, das ist im Normalfall ein Provider oder der Verwalter einer Zone, muss sich nachweisbar bei DENIC identifizieren. Sinnvoll wäre hier persönliches Erscheinen unter Vorlage des Personalausweises zur Überprüfung der Identität. Weniger sicher sind Telefonate oder Emails.
- Das von DENIC ausgestellte Zertifikat muss Informationen enthalten, die notwendig für den weiteren Betrieb des Inhabers im regulären DNSSEC-Betrieb sind.

Name des Inhabers oder ein ihm eindeutig zuzuordnendes Pseudonym

Der Signaturprüfschlüssel inkl. Name des verwendeten Algorithmus sowie die dafür wichtigen Parameter

Laufende Nummer des Zertifikats

Beginn und Ende der Zertifikat-Gültigkeit

Eventuelle Einschränkungen für die Benutzung des Zertifikats und antragsteller-spezifische Attribute, z.B. berufsbezogene Attribute

Angaben zu möglichen Vertretungen des Antragstellers

- Vor Ausstellen des Zertifikats muss DENIC als CA den Antragssteller über sämtliche Details im Umgang mit Zertifikat und digitalen Signaturen belehren. Zweckmäßig ist darüber hinaus, den Providern/Zonenverwaltern beratend zur Seite zu stehen. Denkbar wäre, dass DENIC für die Provider ein Komplett-Paket aus Hard- und Software für den Umgang mit DNSSEC anbietet. Dadurch wäre sichergestellt, dass auch auf Provider-Seite nur qualifizierte Komponenten zur Signatur/DNSSEC eingesetzt werden.
- Die Leistungen, die DENIC erbringt, müssen genau festgelegt und Tarife dafür bestimmt werden.
- Als CA ist es Aufgabe von DENIC, ein Verzeichnis aller von ihm ausgestellten Zertifikate zu führen.
- Alte Zertifikate, d.h. Zertifikate, die gesperrt oder „ausgelaufen“ sind, sollten noch eine bestimmte Zeit vorgehalten werden. Das Signaturgesetz schlägt dafür 30 Jahre vor. Ein angemessener Zeitraum muss festgelegt werden.
- Es muss ein 24h Service zur Sperrung von Zertifikaten verfügbar sein. Ein Zertifikat ist unverzüglich auf Antrag des Inhabers zu löschen.

6.4.4 Datenschutz

Als Betreiber einer CA gelten die allgemeinen Bestimmungen zum Datenschutz. Demzufolge dürfen nur für den Betrieb als Zertifizierungsstelle zweckdienliche Daten von Antragstellern gesammelt und gespeichert werden. Grundsätzlich bedarf jedwede Datenerhebung der Zustimmung des Betroffen.

6.5 DNSSEC CA

Die eigentliche DNSSEC CA ist auch ein wichtiger Bereich. Sie sollte vom Prinzip her ähnlich wie die Betriebs-CA aufgesetzt werden. Auch hier ist es wichtig, Sicherheitskonzepte zu definieren, über die den Endkunden eine gewisse Qualität der CA zugesichert wird. Auch bei dieser CA ist keine Konformität zur Signaturgesetzgebung erforderlich. Dennoch dürfte der Gesamtprozess davon profitieren, wenn sich die Prozesse und Algorithmen am Signaturgesetz orientieren. Erschwerend kommt hier dazu, dass es sich um eine mehrstufige CA handelt, da jeder Anbieter einer gesicherten Zone gleichzeitig dort als CA fungiert. In diesem Zusammenhang wird es auf Dauer unverzichtbar sein, die Zonenbetreiber auf die Einhaltung eines Sicherheitskonzeptes zu verpflichten. Gibt es kein minimales Sicherheitskonzept, auf das untergeordnete Zonenbetreiber verpflichtet werden, so besteht die Gefahr, dass das gesamte System über einzelne unsichere Domänen diskreditiert wird.

Die Anlehnung der Algorithmen und Schlüssellängen an das Signaturgesetz sollte einerseits gegenwärtig keine unzumutbaren technischen Probleme erzeugen. Andererseits schafft die Nähe zum Signaturgesetz das notwendige breite Vertrauen in die eingesetzten Algorithmen.

6.6 Einordnung

6.6.1 PGP versus PEM

Sowohl PGP als auch PEM[63] sind bewährte Standards um mittels elektronischer Signaturen die Sicherheit in Kommunikationsprozessen zu unterstützen.

Die Unterschiede zwischen beiden Verfahren bestehen vor allem im Vertrauenskonzept. Bei X.509 liegt ein hierarchisches Modell mit übergeordneter CA zugrunde, die das Vertrauen ausspricht. Mit deren öffentlichen Schlüssel kann von allen Beteiligten die Vertrauenskette überprüft werden. Bei PGP hingegen spricht man von einem „Web of Trust“. Die Benutzer in diesem Modell unterschreiben ihre Schlüssel gegenseitig. Die Nachteile, die bei einer großen Benutzergruppe entstehen – z.B. beim Rückruf der Schlüssel, der allen Beteiligten bekannt gegeben werden muss – kommen hier nicht zum Tragen, da der Anwendungsbereich eine abgeschlossene Benutzergruppe darstellt, die auch nicht untereinander kommuniziert. Kommunikation findet nur zwischen DENIC und den ISPs statt. Beide Verfahren sind daher für den Einsatz geeignet.

Ein weiterer wichtiger Punkt ist die zukünftig vermutlich zunehmende Kommunikation im Rahmen von Secure DNS, mit dem A-Root-Server-Betreiber. Bisher verläuft ein Kontaktszenario zum Wechsel von Primary- oder Secondary-Daten für *.de* wie in Abschnitt 6.2.1.1 beschieben.

Es ist davon auszugehen, dass sich an diesen Szenarien einiges ändern wird, sofern Schlüssel bzw. Records, wie das DS RR für Secure DNS, zwischen der Root und den Registries (Betreiber der TLD-Nameserver) ausgetauscht werden. Hier wäre dann das Augenmerk auf möglichst internationale Standards zu legen, um eine internationale Interoperabilität zu erreichen. Hierfür steht seit kurzem ein Standard zur Verfügung [ISIS-MTT][64]. Siehe auch [PKIX], Interoperabilität [DUD 4/99, 9/01]

6.6.2 Alternative: Outsourcing

Lösungen basierend auf PGP als auch auf X.509 Zertifikaten sind am Markt vertreten. Beispielsweise werden von der DFN-PCA die Verfahren PGP, PEM (X.509v1), S/MIME sowie SSL (X.509v3) unterstützt [DFN-PCA].

Eine Übersicht über akkreditierte CAs nach dem deutschen Signaturgesetz wird unter [PKI-Page] gepflegt.

Als Alternative zum von DENIC eigens eingesetzten CA-Betrieb bietet sich das Outsourcing dieser Dienstleistungen zu Trust-Centern an. Unternehmen wie die Telekom oder das TC-Trustcenter übernehmen die Authentifizierung und das Ausstellen von Zertifikaten für DENIC und Provider. Sie können außerdem Chipkarten Hardware zur Verfügung stellen. DENIC kann so mit seinen Providern eine von qualifizierten „Fachmännern“ bereitgestellte und gewartete Public Key-Infrastruktur benutzen. Routinearbeiten wie Schlüsselwechsel, Sperren von Zertifikaten oder gar Ausnahmesituationen wie kompromittierte Schlüssel übernimmt ein externes Trustcenter.

[63] PEM ist ein Betriebsmodell für die Nutzung von Zertifikaten, welches auf der Grundlage von X.509-Zertifikaten arbeitet
[64] Die Herausgabe der vereinheitlichten “ISIS-MTT-Spezifikationen für Interoperabilität und Testsysteme" ist der erste Schritt eines mehrstufigen Projekts, in dem bisherige Erfahrungen mit internationalen Standards gekoppelt werden sollen. Qualifizierte Signaturen gemäß Signaturgesetz und Formvorschriften im Privat- und Verwaltungsrecht sind dabei ebenso berücksichtigt wie die Spezifikation von Sicherheitsfunktionen für Secure E-Mail mit unterschiedlichen Sicherheitsniveaus.

6.7 Einbettung von DNSSEC in eine PKI

Die PKI-Komponenten, Verfahren und Prozesse, die für die Identifikation der Kommunikationspartner und der darauf aufbauenden sicheren Prozesse zum Austausch von Daten notwendig sind, werden an dieser Stelle nicht näher beschrieben. Im folgenden setzen wir einen zuverlässigen Zertifizierungsprozess voraus, um unsere Szenarien darauf zu stützen.

Es werden die für die Secure DNS notwendigen wesentlichen PKI-Prozesse aufgeführt und vorgeschlagen, wie diese realisiert bzw. abzubilden sind. Eine teilweise ausführlichere Darstellung ist in der [DENIC-Stud] enthalten.

6.7.1 Regulärer Betrieb

Schlüsselmanagement

DENIC delegiert in der *.de* Zone die Autorität für die Second-Level Domain an die betreffenden Nameserver. Für die Pflege der Zonendaten ist der in den Domaindaten eingetragene Zonenansprechpartner zuständig. Dieser ist meistens identisch mit dem technischen Ansprechpartner, der für den Serverbetrieb und dessen Sicherheitsbelange zuständig ist. Eine Delegation an DENIC ist, da hier über 6 Millionen Domains verwaltet werden, nicht praktikabel. Es könnten lediglich Empfehlungen ausgesprochen werden. Ansprechpartner für die Pflege der Zonendatei ist der Zonenansprechpartner (zone-c). Der Aufgabenbereich des zone-c wird durch DNSSEC erweitert.

Zu den neuen Aufgaben gehört u.a. die **Schlüsselgenerierung**. Software, die DNSSEC unterstützt, wird ähnlich wie dies bei ISC-BIND der Fall ist, auch Werkzeuge zur Schlüsselgenerierung enthalten. Die Schlüsselgenerierung muss vom Zonenadministrator vorgenommen werden, um das Prinzip der Vertraulichkeit zu wahren. Würde eine Dritte Instanz diese erzeugen, müsste gewährleistet werden, dass der private Schlüssel nicht dem Dritten für eine weitere Verwendung zur Verfügung steht. Ein solches Verfahren ist aufwändig und müsste zertifiziert sein. Die Schlüsselgenerierung sollte offline erfolgen und der private Schlüssel muss sicher verwahrt werden. Für diese **Schlüsselspeicherung** bietet sich ein PSE[65] oder ein kryptografisches Hardwaremodul an z.B. basierend auf Smartcards. Eine Verwendung dieser Lösungen ist besonders für die Transaction und Request Signaturen und für Secure Dynamic Update Szenarien interessant, da hier die Schlüssel online gehalten werden müssen. Für beide Speichermedien sind derzeit keine Schnittstellen zu ISC-BIND vorhanden. Diese Anbindung müsste evaluiert werden.

Die **Schlüsselzertifizierung** findet im Zonefile statt. Hier sind die RR durch eine Signatur der ausstellenden Instanz kryptografisch gesichert. Eine Signatur über einem Resource Record kann daher zusammen mit weiteren Zoneninformationen als ein Zertifikat angesehen werden. In Tabelle 9 sind die Begriffe X.509 Zertifikat und SIG RR in einer DNNSEC Zone gegenübergestellt.

[65] PSE – Personal Security Environment, Software nach pkcs12 [PKCS] für die Ablage von Schlüsseln und Zertifikaten.

X.509	SIG RR in DNSSEC-Zone
Version	Protokollversion steht nicht in der Zone.
Serien Nummer	Serien Nummer der Zone
Aussteller (Issuer)	Übergeordnete Zone (Domainname in der Zeile des SOA RR)
Gültigkeitszeitraum	Zeitraum zwischen Anfangs- und Endzeitpunkt der Signaturgültigkeit
Subjekt (des zu zertifizierenden Objektes)	Domainname der delegierten Zone
Öffentlicher Schlüssel	DS Record als Verweis auf den öffentlichen Schlüssel
Signaturschlüsselparameter	Signaturschlüsselparameter
Revocation URL	Definition von Mechanismen außerhalb des Protokolls
Signatur Algorithmus	Siehe Signaturschlüsselparameter
Signatur des Ausstellers	Signatur des Ausstellers unter den einzelnen Rrsets
Verweis auf Zertifikat des Ausstellers	Im SIG RR ist der Aussteller angegeben
Anwendungsbereich	Anwendungsbereich des Schlüssels[66]

Tabelle 9: Vergleich X.509 Zertifikat mit DNSSEC-Zone

Die Hierarchie von der Root über die Top-Level Zone zur delegierten Domain, wird bei der Namensauflösung durchlaufen. In derselben Weise geschieht auch die **Schlüsselverteilung** der öffentlichen Schlüssel, die für die Verifikation der Signaturen notwendig ist. Der DS Record in der delegierten Zone kennzeichnet eindeutig den Key Signing Key (KSK) in der delegierten Zone. Dieser Record ist unterschrieben mit dem privaten Zonenschlüssel. Wird der DS Record mit seinem Verweis auf den KSK der delegierten Zone akzeptiert (d.h. seine Unterschrift als gültig verifiziert), dann findet sich der KSK in der delegierten Zone. Mittels des KSK kann die Unterschrift unter dem Zone Signing Key (ZSK) überprüft werden. Der ZSK letztlich unterzeichnete die RR. Die unterschriebenen Resource Records sind ebenfalls in der Zone enthalten. Nach Überprüfung deren Signatur ist die gesuchte Information verfügbar.

Die **Schlüsselverteilung** findet über das DNS statt. Daher ist keine separate Verteilung notwendig (z.B. durch einen Verzeichnisdienst). Schwierigkeiten bereitet die Konfiguration der Endanwendungen (Resolver). Diese müssen mit dem sicheren Einstiegsschlüssel (trusted key) vorkonfiguriert werden. Die Schlüssel, die unterhalb der trusted keys liegen, werden über die DNS-Anfragen erhalten. Durch die Delegation an die untergeordnete Zone ist jede Subzone für die Verteilung ihrer öffentlichen Schlüssel selbst zuständig.

Die statische Konfiguration macht ein deployment von Secure DNS in der Anfangsphase aufwändig, da sämtliche Resolver mit dem trusted key vorkonfiguriert werden müssen. Auch der potenziell mögliche Schadensfall, dass gerade der sicherere Einstiegs-

[66] Im Protokollfeld des Schlüssels könnten weiter Einsatzgebiete wie TLS, Email, IPSec angegeben werden.

punkt „die Root“ kompromittiert wird, stellt die DNS-Betreiber bisher vor sehr schwierige Probleme [Ihren].

Eine interessante Idee ist es, Tools für die automatische Überprüfung des trusted keys der Resolver zu entwickeln, und diese außerhalb des DNS bereitzustellen [DENIC-Stud].

Das Problem des **Schlüsselwechsels** wird sich durch die Einführung des DS RR verringern. Die Schlüssel sind nun in der delegierten Zone selbst gespeichert. Außerdem ist durch Verwendung von KSK und ZSK eine Änderung des DS Records weniger häufig vorgesehen.

Wird beispielsweise der Schlüssel der Parent-Zone gewechselt, so führt dies dazu, dass alle RR neu zu unterschreiben sind und die Zone neu erstellt werden muss. Dies bedeutet, dass eine neue Zertifizierung vorgenommen werden muss. Die zu zertifizierenden Daten bleiben jedoch dieselben.

Wechselt im anderen Fall die Child-Zone ihren Schlüssel, dann muss der DS RR an den Parent übermittelt werden. Der Parent zertifiziert diesen. Diese Kommunikation geschieht - wie vorgeschlagen - out-of-band mit PKI-Mechanismen. Bei früheren Protokollvorschlägen [RFC 2535] gab es Entwürfe, die einen automatischen Schlüsselwechsel innerhalb von DNSSEC unterstützt haben. [Rollover].

Einen **Schlüsselrückruf** bzw. **Schlüsselsperrung** gibt es im DNSSEC-Protokoll nicht. Mechanismen wie Certificate Revocation Lists (CRLs) sind nicht vorgesehen. Wird jedoch ein Schlüssel aus der Zone gelöscht, dann ist nach Ablauf der Time To Live (TTL) der Schlüssel auf dem Resolver nicht mehr vorhanden. Es ist daher empfehlenswert, die TTL möglichst klein zu wählen.

Unter **Schlüsselanwendung** verstehen wir die Erzeugung von Signaturen mit dem privaten Schlüssel bzw. die Überprüfung der Signaturen der RR mit dem öffentlichen Schlüssel. Die Erzeugung der Signaturen sollte offline erfolgen. Im besten Fall werden die Daten an ein Hardwaremodul gesendet. Der private Schlüssel kann das Hardwaremodul nicht verlassen. Bei den Verfahren TSIG und SIG(0) müssen die Schlüssel online gehalten werden. Umso empfehlenswerter ist hier die Verwendung eines Kryptomoduls. Das Verfahren der **Schlüsselanwendung/Schlüsselzugriffs** und die Signierung der Daten muss vollautomatisch durchgeführt werden können. Dies ist bei der großen Anzahl an Aufträgen eine Grundvoraussetzung. Größenordnungen für die Verwendungszeiten, Algorithmen und Länge der eingesetzten Schlüssel, sind in Abschnitt 5.3.3.3 beschrieben.

6.7.2 Schadensfall, Kompromittierung

In derselben Weise, wie DENIC delegiert, kann es in der Subzone zu weiteren Delegationen kommen. Zu beachten ist, dass je höher man sich in der Hierarchie befindet, desto größer ist die Betriebsverantwortung, da mit einer **Schlüsselkompromittierung** immer auch die Delegation der darunter liegenden Zonen unsicher wird. Da die privaten Schlüssel der untergeordneten Zonen jedoch nicht in der Parent-Zone verfügbar sind, müssen bei einer Kompromittierung der Parent-Zone weder die Zonenschlüssel der Subzone neu erstellt noch die DS Records neu berechnet werden. Es ist aber genau zu prüfen, ob nach der Neugenerierung der Schlüssel, die Daten, die zur Generierung der Zone herangezogen werden, im Vorfeld manipuliert wurden.

Für den Fall des Schlüsselverlustes, sind auch **Schlüsselwiederherstellungsmaßnahmen** (Key Recover) zu planen. Gerade für Schlüssel, die als sogenannte „trusted keys“ den Einstieg in das Secure DNS-System erlauben, sind solche Mechanismen notwendig, da ein Verlust der zugehörigen privat Key eine Neuverteilung der Schlüssel

erfordern würde. Am Ende der Hierarchie in den Blättern des Baumes, kann von Key Recovery Maßnahmen abgesehen werden. Im Verlustfalle sind neue Schlüssel zu erzeugen. Über die organisatorischen Prozesse ist der Verweis auf die neuen Schlüssel an die übergeordnete Zone zu übermitteln.

Für einen **Wiederanlauf** ist der **Schlüsselwechsel** genau zu planen. Bei einer Kompromittierung könnte der Schlüsselwechsel über die zugrunde gelegte PKI erfolgen. Diese ist mit großer Wahrscheinlichkeit zu dem betreffenden Zeitpunkt intakt, da sie unabhängig betrieben wird. Im Falle einer Störung des PKI-Betriebs hat dies auf der anderen Seite für Secure DNS die Folge, dass die update Mechanismen für die RR nicht mehr durchgeführt werden können. Szenarien die die Dauer bis zum Wideranlauf des Betriebs abschätzen und die schnelle Durchführung unterstützen, sind notwendig.

7 Organisatorische Prozesse

Eine vollständige Beschreibung der organisatorischen Prozesse kann im Rahmen dieser Studie nicht durchgeführt werden. Neben der Schwierigkeit, dass viele Protokollvorschläge erst als Entwürfe existieren und übergreifende Prozesse noch nicht aufeinander abgestimmt sind, besteht eine detaillierte Prozessanalyse immer auch in der Berücksichtigung der realen Gegebenheiten bei DENIC und den ISPs. Die Prozesse müssen mit einer sehr großen Sorgfalt entworfen und adaptiert werden. Dies setzt umfangreiche praktischen Erfahrungen voraus. Hier soll die Komplexität einzelner Szenarien veranschaulicht werden, damit ein tieferes Verständnis für Secure DNS erreicht werden kann.

Wir unterscheiden wie in Kapitel 5 beschrieben

1. DNSSEC (Verwendung von asymmetrischer Kryptografie)
2. Secret Key Transaction Authentication -TSIG (mittels symmetrischer Kryptografie)
3. DNS Request and Transaction Signatures SIG(0) (asymmetrische und symmetrische Kryptografie-Verfahren)

Die Verfahren werden im folgenden exemplarisch, zum Teil auch diagrammatisch dargestellt. Die Abbildungen und Beschreibungen sind stark vereinfacht.

7.1 Übermittlung der DNS-Datensätze

DENIC stellt den ISPs verschiedene Abläufe zur Verfügung, um Domainnamen zu registrieren und die dafür notwendigen Daten zu pflegen. Pflegen bedeutet hier: Neue Daten eintragen, ändern, löschen. Diese Abläufe setzen auf der DENIC PKI auf.

7.1.1 Szenario 1: Übermittlung des DS Resource Record an Parent

Das Verfahren zur Änderung des DS Records, wie er im Verfahren Delegation Signer vorgeschlagen, könnte ähnlich wie die Pflege der anderen DNS-Datensätze ablaufen. Zu berücksichtigen ist, dass Änderungen an diesem Record aufgrund seiner Wichtigkeit für die Authentifikation der Zone vorrangig behandelt werden sollten. Gerade im Falle einer Kompromittierung eines Schlüssels aus der Child-Zone ist es erforderlich, schnell einen neuen gültigen DS Eintrag zu erzeugen und an die Parent-Zone zu übermitteln.

7.2 DNSSEC

7.2.1 Szenario 2: Die Child Zone wird sicher

In der Abbildung 22 ist dargestellt, welche Schritte ablaufen müssen, damit die Child - Zone sicher angeboten werden kann.

1. Child und Parent: Für die zum Einsatz kommenden Schlüssel muß jeweils ein Schlüsselpaar zur Erstellung der Zonensignaturen und ein Schlüsselpaar für die Schlüsselsignaturen[67] erzeugt werden. Diese müssen in regelmäßigen, festgelegten Zeiträumen (siehe Abschnitt 5.3.3.3) erneuert werden. Der Zonenschlüssel wird durch den Schlüsselsignaturschlüssel unterschrieben. Der Prozess der Erzeugung neuer Schlüssel vereinfacht sich durch das Konzept von Key Signing Key und Zone Signing Key. Dieser Prozess muss weniger häufig durchgeführt werden.
2. Child: Die Resource Records werden z.B. aus einer Datenbank geholt und unterschrieben. Der DS Record wird berechnet. Das Zonefile besteht aus allen Resource Records. Der DS RR wird an den Parent übertragen. Dies findet „out of band“ statt. Das bedeutet, dass keine Mechanismen des DNSSEC-Protokolls eingesetzt werden. Die Übertragung geschieht abgestützt auf die DENIC PKI.
3. Parent: Das Zonenfile, in dem die Delegation für die Child Zone stattfindet, wird mit dem neuen DS Record erzeugt. Nach jeder Änderung der Zonendaten muss die Zone neu erstellt und unterschrieben werden. Die Serien Nummer wird um eins erhöht, damit die Secondary-Server die Zone laden. Es erfolgt eine Benachrichtigung (Notify) an den Child-Nameserver, wenn der Prozess beendet ist. Ebenso geht eine Benachrichtigung an die Secondarys. Die Zone mit kryptografisch gesicherter Delegation steht bereit.
4. Child: Der Child Nameserver lädt die Zone und informiert seine Secondary. Der Zustand: Childzone ist sicher, ist erreicht.

Anmerkung: Es sind weitere Prozesse vorzusehen, um den Gültigkeitszeitraum der SIG RR zu verwalten. Es sollte vermieden werden, dass sich RR mit überschrittener Ablaufzeit für die Signatur in der Zone befinden. Daher müssen die Werte, der TTL und der Signaturgültigkeit aufeinander abgestimmt werden.

[67] Key signing key und Zone signing key.

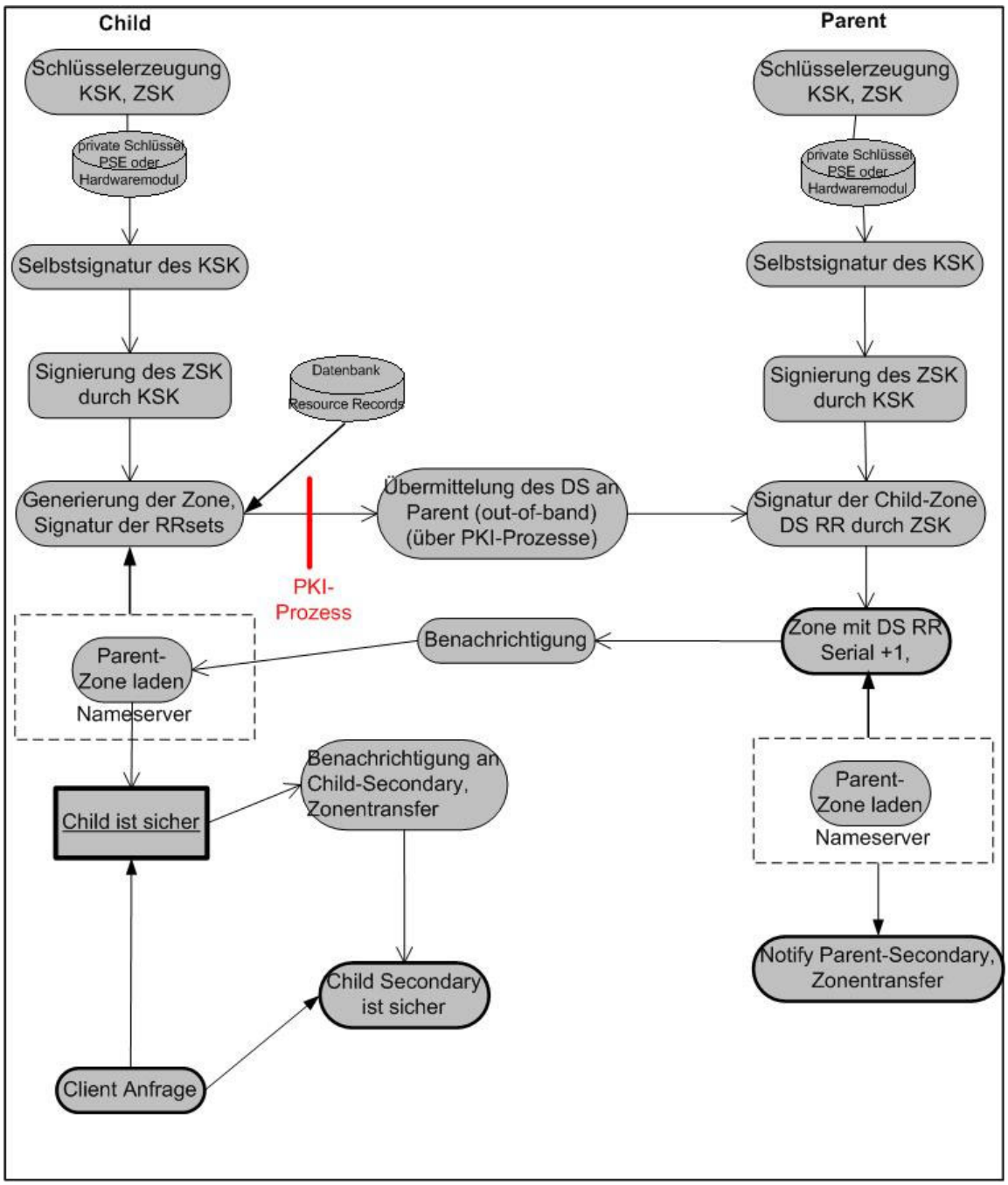


Abbildung 22: Child-Zone wird sicher

7.3 Secret Key Transaction Authentication

Um einen Zonentransfer innerhalb der Mechanismen, wie sie das DNS-Protokoll bietet, abzusichern, wird TSIG vorgeschlagen. Es läuft folgendes Szenario ab.

1. Erzeugung eines geheimen symmetrischen Schlüssels.
2. Konfiguration des Primary-Nameservers mit dem geheimen Schlüssel.
3. Der Primary hat einen sicheren Status.
4. Übertragung des geheimen Schlüssels. Hierbei muss ein sicherer Kanal gewählt werden. z.B. mittels Email und PGP Verschlüsselung oder scp. Die Übertragung geschieht out-of-band mittels der PKI-Prozesse.
5. Konfiguration des Secondary-Nameservers mit dem geheimen Schlüssel.
6. Der Secondary ist bereit für den Zonentransfer.
7. Eine Benachrichtigung, dass der Secondary bereit ist für den Zonentransfer, wird an den Primary geschickt.
8. Wird die Zone neu erzeugt, dann muss die Zonenseriennummer um eins erhöht werden. Die Zone wird danach vom Nameserver neu geladen.
9. Der Primary hält die Zone vor.
10. Benachrichtigung an Secondary, daraufhin erfolgt der Zonentransfer durch den Secondary.
11. Der Secondary hält die Zone vor.
12. Primary und Secondary bieten dieselbe Zone an.
13. Client-Anfragen nach den Resource Records sind jetzt möglich.

Anmerkungen:

Ein Konsistenzcheck der Zone auf dem Secondary ist nicht notwendig, da eine korrekte Entschlüsselung garantiert, dass die Daten während der Übertragung nicht manipuliert werden konnten. Für die Konsistenz der Daten hat der Primary Sorge zu tragen.

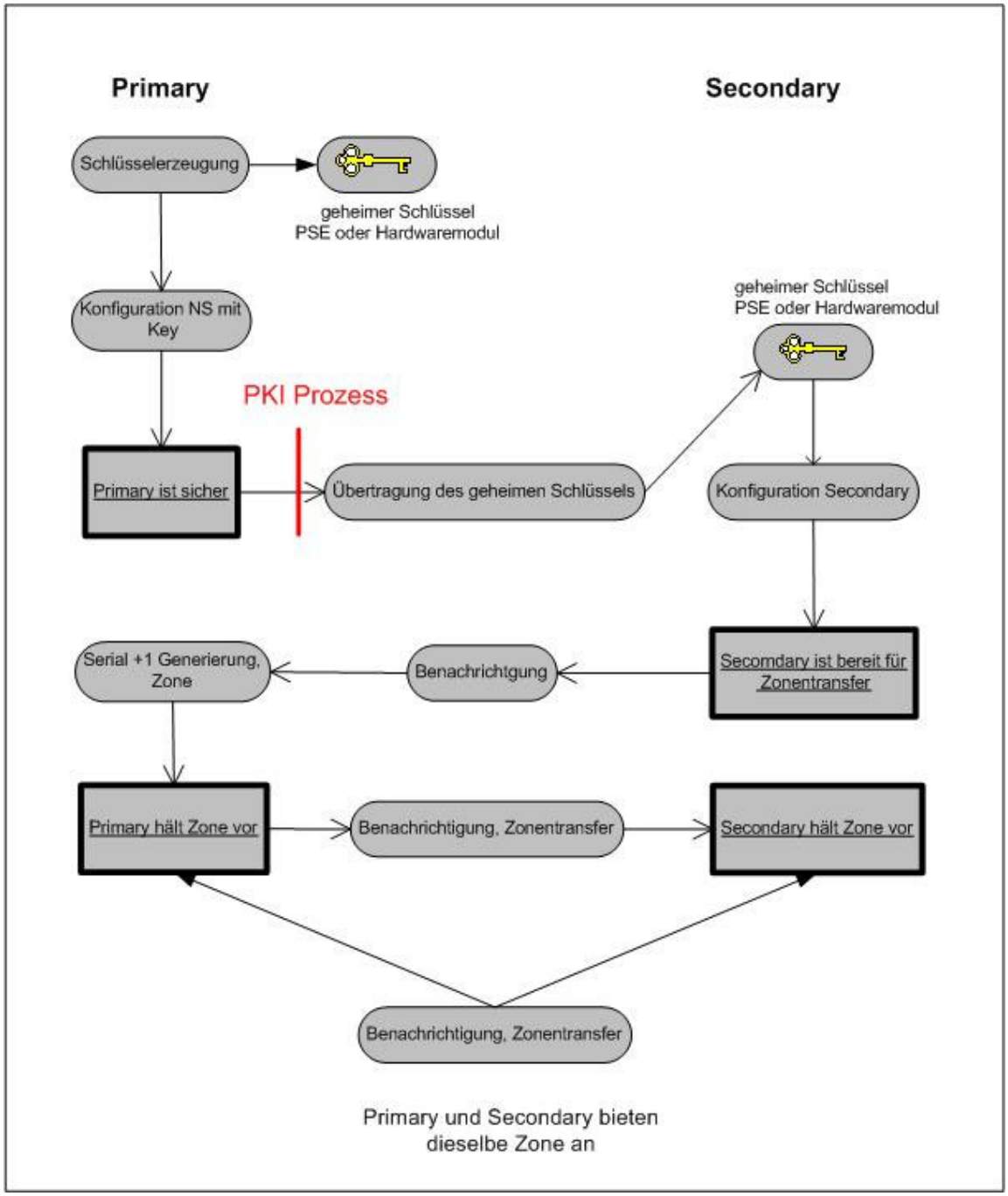


Abbildung 23: Zonentransfer mit Transaktionssignaturen

7.3.1 Szenario 3: Kompromittierung des geheimen Schlüssels

Als Sicherungsmöglichkeiten für die geheimen Schlüssel, stehen unterschiedliche Möglichkeiten (PSE oder Kryptohardwaremodul) zur Verfügung. Dennoch kann ein Schadensfall nicht ausgeschlossen werden. Es kann sich sowohl um eine Kompromittierung der privaten asymmetrischen Schlüssel handeln, als auch um den des symmetrischen Verfahrens.

Der Ablauf ist der folgende:

1. Ausgangspunkt ist der sicherer Betrieb.
2. Unterschiedliche Möglichkeiten der Kompromittierung müssen in Betracht gezogen werden.
3. Nach einer Kompromittierung ist der Betrieb unsicher.
4. Erst wenn die Kompromittierung erkannt wird, können Maßnahmen ergriffen werden.
5. a) Benachrichtigung an Secondary für den Fall, dass die Kompromittierung auf dem Primary-Server vorfiel.

   b) Benachrichtigung an Primary für den Fall, dass die Kompromittierung auf dem Secondary-Server vorfiel.
6. Ablauf von Szenario 2 bzw. 3, um wieder in den Status „sicherer Betrieb“ zu gelangen

Anmerkungen:

Spezielle Notfallkonzepte sind notwendig, die garantieren, dass Szenario 2 und 3 auch im Kompromittierungsfall schnell durchgeführt werden können. Z.B. sollte ein Ersatzschlüssel vorliegen um nicht erst out-of-band einen neuen Schlüssel übertragen zu müssen. Weiter muss es Kriterien geben, wie mit dem Secondary zu verfahren ist, falls auf dem Primary eine Kompromittierung vorliegt. Dieser sollte keine Zoneninformationen mehr verbreiten, bis er neue Daten vorliegen hat.

Eine Schlüsselkompromittierung darf in Bezug auf die Vertraulichkeit der Zoneninformationen als eher unkritisch eingeschätzt werden. Eine kritische Situation entsteht dann, wenn die Möglichkeit der Änderung der Zoneninformationen besteht.

Darüber hinaus muss die Ursache geklärt werden. Wie konnte es zu der Kompromittierung des geheimen Schlüssels kommen.

1. Liegt ein Angriff auf das Betriebssystem vor, so ist dies auch bezüglich anderer potenzieller Angriffsziele höchst kritisch.
2. Wurde der Schlüssel z.B. aus Unachtsamkeit publiziert, dann können hieraus zwar Bedrohungen entstehen, sodass ein Schlüsselaustausch angeraten ist. Das Risiko ist aber als geringer als das mit 1. verbundene einzustufen.

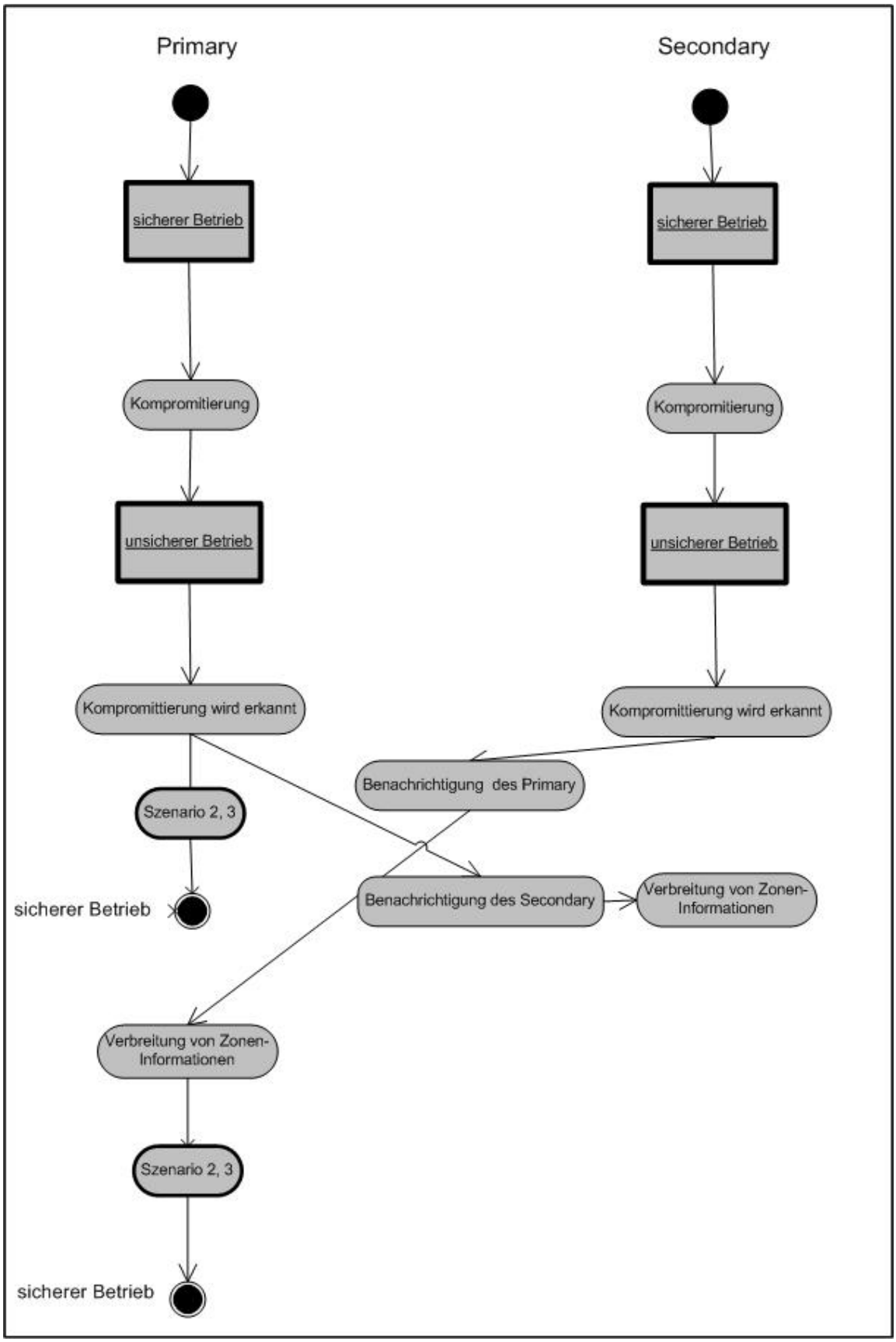


Abbildung 24: Kompromittierung des geheimen Schlüssels

7.3.2 TKEY Erneuerung

Der Draft „TKEY Secret Renewal Mode“ [TKEY] beschreibt detailliert, wie ein automatisierter Schlüsselwechsel für die Transactions und Request Signaturen ablaufen könnte. Szenarien, die auf diesen Vorschlägen aufbauen, sind für den operativen Betrieb sehr wichtig.

7.4 DNS Request and Transaction Signatures SIG (0)

Der Dynamic Update Prozess wird immer wichtiger durch den Einsatz des Dynamic Host Configuration Protocol (DHCP). Dieses Verfahren wird teilweise von den ISPs eingesetzt. Auf der DENIC-Seite könnte durch den Einsatz von Dynamic Update Mechanismen der Service für die unmittelbare Bereitstellung der eingetragenen Zoneninformationen verbessert werden. Für beide Einsatzgebiete wird Secure Dynamic Update empfohlen.

7.5 Sicherer Einstiegspunkt

Als sicheren Einstiegspunkt bezeichnet man die Stelle im Domainnamensbaum, zu der überprüfte DNSSEC-Schlüssel zur Verfügung stehen. Dieser Einstiegspunkt kann in jedem Zweig des Baumes liegen. Die Kommunikationspartner, die ihren Resolver mit dem öffentlichen Teil dieser Schlüssel vorkonfigurieren, können die Zonendaten, die durch den privaten Schlüssel unterschrieben sind, verifizieren. An welcher Stelle im DNS-Baum Schlüssel zur Verfügung stehen, hängt vom Grad des DNSSEC-Deployments ab. Organisatorisch abgedeckt werden muss die Verteilung und Überprüfung der „trusted keys“.

Im besten Fall gibt es nicht verschiedene Einstiegspunkte für die einzelnen Zweige des DNS-Baumes, sondern die Wurzel des Baumes wird sicher. Alle darunter liegenden Signaturen können dann bis zu der obersten Hierarchie zurückverfolgt werden[68].

[68] Die Initialisierung des Vertrauens kann ähnlich gesehen werden, wie die Initialisierung der Namensauflösung durch den Eintrag der Root Server bei der Konfiguration der Nameserver.

8 Kompetenz DNSSEC

8.1 Zeitraum Protokollstandardisierung

Der aktuelle Stand der Protokollstandardisierung wird stark kontrovers diskutiert. Dies deuten schon die Zitate auf Seite 2 an. Auf die Frage, wann der abschließende Standard für DNSSEC vorliegen würde, heißt es unter Protokollentwicklern etwas spöttisch: „In sechs Monaten“. Schon einige dieser „sechs Monate“ sind zwischenzeitlich vergangen. Es kann nicht davon ausgegangen werden, dass dieser Zeitraum eingehalten werden kann.

Geht man davon aus, dass das DS RR akzeptiert wird und die Standardisierung fortgeschrieben werden kann, kann dies als Meilenstein gesehen werden. Dieser Standard würde sich für eine Erprobung des Protokolls und eines Test der organisatorischen Abläufe eignen. Ein Zeitraum von 12 Monaten bis zum Erreichen dieses Punktes scheint durchaus realistisch. Vorarbeiten in diesem Zeitraum sind empfehlenswert. Letztlich sind die organisatorischen Prozesse diejenigen, die langfristig getestet, implementiert und umgesetzt werden müssen. Hierzu ist von DENIC und den ISPs eine Kompetenz Secure DNS aufzubauen.

8.2 Vorgehensmodell

Auf DNSSEC kann nicht einfach umgeschaltet werden! Vielmehr muss durch einen längeren Testbetrieb ein technisches und organisatorisches Wissen erlangt werden, bei dem alle möglichen Szenarien ausgiebig erprobt werden. Beispielsweise auch der extrem unwahrscheinliche Fall der Rootschlüsselkompromittierung und des darauf folgenden Wiederanlaufs. Zur Erreichung dieser Fähigkeit gibt es zwei sich ergänzende Ansätze. Beide sollten parallel verfolgt werden.

8.2.1 Lokale Testumgebungen

Zur Erprobung der neuen Softwaremöglichkeiten für den DNS-Betrieb und zur Entwicklung der Applikationen sind experimentelle Testumgebungen der einzelnen Provider und DENIC zu verfolgen, um spezifische Problemstellungen zu analysieren und Erfahrungen zu gewinnen. Von Interesse wären bspw.:

- Möglichkeit der Schlüsselspeicherung in Spezialhardware
- Kontrollmechanismen zur Verhinderung des NXT-Chaining[69]
- Erprobung neuer Verfahren wie Secure Dynamic Update
- Dauer der Erzeugung von großen Zonen
- Nameserver Lastverhalten
- Evaluierung der Möglichkeiten zum Schutz vor DoS-Angriffen
- Erweiterung der Applikationen
- Test von neuen Protokollmechanismen wie z.B. Opt-In
- Test von kryptografischer Hardware für die Schlüsselspeicherung

[69] Durch Einführung des NXT RR wird es möglich, schrittweise durch die Zone zu laufen und somit einen Zonentransfer durchzuführen.

8.2.2 Aufbau einer Schattenzone de.de

Um im Zusammenspiel der DNS-Betreiber den erweiterten DNS-Betrieb zu testen, könnte eine Schattenzone *.de.de*. aufgebaut werden. Darin sollte ein Teil der *.de*-Zone für ausgewählte Provider signiert angeboten werden. Die Provider selbst haben die Möglichkeit, ihre sicheren Zonen in diese Zone einzuhängen.

Fragen, die bei einem Testbetrieb von Interesse sind:

- Antwortzeiten
- Webinterface bzw. Erprobung neuer Protokolle (EPP) bei der Schnittstelle Registry - Registrar
- Kombination von sicheren und unsicheren Zonen im Betreib.
- Gestaltung und Erprobung der neuen organisatorischen Prozesse
- Ausbau PKI
- Erprobung der Applikationen

Der Auflösungsprozess wird umfangreicher, da zusätzlich zur Rückgabe des gewünschten RR eine Signaturüberprüfung durchgeführt werden muss. Hierfür ist der öffentliche Schlüssel des Unterzeichners notwendig. Sofern dieser Schlüssel nicht bekannt und vertrauenswürdig ist, muss er von einer vertrauenswürdigen dritten Instanz unterzeichnet sein. Diese Unterschrift muss vom Resolver überprüft werden.

8.3 Testumgebungen

Aktuell werden verschiedene größere Testumgebungen mit unterschiedlichen Zielsetzungen betrieben. Neben organisatorischen Abläufen werden spezielle Protokollerweiterungen sowohl für DNSSEC als auch für die Registrar-Registry Schnittstelle untersucht.

8.3.1 Verisign DNSSEC-Service

Der von VeriSign's Applied Research Department betriebene DNSSEC-Pilot [Verisign] ist ein eigenständiges Forschungsprojekt.

Über ein webbasiertes Interface wird der Zugriff auf die Domaindaten durch eine erweiterte Version des RRP[70] ermöglicht. Dieses gibt den Registraren die Möglichkeit, ihre Schlüssel für die delegierten Domains selbst zu verwalten. Die Änderungen werden auf den DNSSEC-Server überspielt, der von VeriSign betrieben wird. Bei dem Demonstrator wird das von VeriSign vorgeschlagene Opt-In Verfahren eingesetzt.

Interessierte Registrare sind zur Teilnahme aufgefordert.

8.3.2 SECREG experiment in .nl

Von Miek Gieben wurde für die NLnetLabs and SIDN.nl (Stichting Internet Domeinregistratie Nederland) eine Registry aufgesetzt. Für niederländische Domainbesitzer ist es möglich, eine Domain unterhalb *nl.nl* zu registrieren. Der Betreib läuft seit November 2002. In diesem Teilbaum wird das DNSSEC-Protokoll unter Verwendung der DS RR-Technik eingesetzt. Opt-In wird nicht unterstützt. Die Zone ist 300 MByte groß und wird

[70] RRP ist ein Protokoll für die Registrierung von Second-Level-Domainnamen zwischen Registry Registrar. Es wurde von Network Solution (NSI) entwickelt, und ist in [RFC 2832] standardisiert.

täglich signiert. Derzeit sind 133 sichere Domains enthalten. Die Interaktion mit der Zertifizierungsstelle geschieht über ein Webfrontend [SECREG].

8.3.3 USC/ISI DNSSEC-Testbed

Unter der Adresse http://fmeshd.nge.isi.edu/ wird von der University of Southern California und dem Information Science Institute eine Testumgebung betrieben. Zum Zeitpunkt der Datenerhebung waren die angegebenen Adressen http://www.ds.isi.edu/ und http://www.sigz.net/ nicht erreichbar.

8.3.4 CARIN

Nicht mehr in Betrieb

Ausgehend von den organisatorischen Prozessen der Schlüsselspeicherung nach RFC 2535 wurde eine Testumgebung aufgesetzt. Die Ergebnisse sind im Draft [Massey] veröffentlicht. Die Ergebnisse sind aufgrund des frühen Stadiums des Protokolls größtenteils veraltet. Die Testumgebung ist nicht mehr in Betrieb.

8.4 Policy beim DNSSEC-Betrieb

Ein Ziel innerhalb der verschiedenen Testumgebungen ist es, Erkenntnisse über die Erstellung von Betriebsrichtlinien zu gewinnen. Insbesondere sollten Sicherheitsleitlinien erstellt werden, die die wesentlichen Punkte des Betriebes in Bezug auf Sicherheit und Abläufe regeln. In dieser Policy muss eine Gratwanderung zwischen Übersichtlichkeit und Detaillierung gefunden werden. Eine zu detaillierte Beschreibung bewirkt, dass die Darstellung unübersichtlich wird. Eine nicht hinreichend genaue Beschreibung führt dagegen zu Unsicherheit auf allen Seiten.

Eine entsprechende Policy sollte auf alle Fälle zu folgenden Punkten Aussagen treffen:

Detailspezifikation zur PKI

Algorithmen

Schlüssellängen

Gültigkeitszeiträume

Betriebskonzept

Schutzmaßnahmen für die beteiligten Rechner

Schutzmechanismen für kryptografische Schlüssel

Schlüsselmanagement

Notfallkonzept

Verhalten bei (Verdacht auf) Schlüsselkompromittierung

Strategien bei Kompromittierung eines Rootschlüssels

Roll-Out

Verteilung der Root-Schlüssel an die Resolver

Sicherstellung der Sicherheitskonzepte für untergeordnete Server

Protokolle zur Zonenregistrierung

8.5 Empfehlung

Der normale DNS-Betrieb wird durch Secure DNS um eine große Zahl an neuen komplexen Abläufen erweitert. Hinzu kommen neue Techniken und höhere Anforderungen an die Leistungsfähigkeit der Server. Hierfür ist im Vorfeld einer Einführung eine Secure DNS-Kompetenz aufzubauen.

Die Einführung von DNSSEC ist gegenwärtig noch nicht möglich. Die Gründe sind:

- Nicht abgeschlossen Standardisierung
- Keine DNSSEC-Software für den Produktionsbetrieb vorhanden
- Fehlende Resolver-Unterstützung
- Bisher noch keine Client-Applikationen
- Erfahrungen im Realbetrieb fehlen

Diese Probleme sind lösbar. Einige Arbeitsgruppen arbeiten an der Umsetzung. Die aktive Teilnahme an diesen Arbeitsgruppen ist notwendig, um gegenseitig Erfahrungen auszutauschen und an den Ergebnissen zu partizipieren. Nicht jede Fragestellung muss von DENIC selbst gelöst werden. Aber schon die Umsetzung von bekannten Abläufen setzt ein großes Maß an Know-how voraus. Für die Teilnahme an einer Testumgebung sind die ISPs zur Mitarbeit aufgefordert. Die Mitarbeit erfordert zum einen Interesse an der neuen Technik, zum anderen muss Zeit investiert werden. Dies bedeutet auch ein zusätzliches finanzielles Engagement. Die Notwendigkeit zum Aufbau einer solcher Testumgebung sollte daher gut begründet und der Nutzen klar herausgestellt werden. Beispielsweise könnte DENIC neue Abläufe wie Secure Dynamic Update evaluieren und im Rahmen von Secure DNS-Schulungsmaßnahmen durchführen, bei denen die Vorteile der neuen Protokolleigenschaften an die Provider weitergegeben werden.

8.6 Zeitraum

Um die Sicherheit des DNS-Betriebes zu erhöhen und letztlich Secure DNS zu unterstützen, könnte der folgende Zeitplan verfolgt werden.

Kurzfristig (1-6 Monate)

Verbesserung der Sicherheit im DNS-Betrieb durch:

Bereitstellung von Dokumentationsmaterialien (Anleitungen für die sichere Nameservice Administration, Baustein DNS-Server für das Grundschutz Handbuch)

Administratorschulungen

Informationsveranstaltung zu geplanten Secure DNS-Einführung

Analyse und Empfehlung von alternativen Nameserversoftwareprodukten

Mittelfristig (1-24 Monate)

Ausbau der DENIC PKI

Planung der Prozesse

Experimentelle Testumgebungen mit unterschiedlichen Fragestellungen

Aufsetzung einer Schattenzone *.de.de* zusammen mit ISPs

Unterstützung von TSIG und SIG(0) in der Anwendung

Langfristig

Nachdem DENIC und ISPs durch den Betrieb einer Schattenzone *de.de* ausreichend Know How im Betrieb der DNSSEC-Server und Infrastruktur aufgebaut haben und die organisatorischen Abläufe bereit stehen, ist ein Zustand erreicht, bei dem alle Beteiligten bereit für Secure DNS sind.

9 Problemfelder

9.1 Neue Verwundbarkeiten

DNSSEC macht DNS verwundbar gegen eine neue Klasse von DoS, welche auf der Ausnutzung der kryptografischen Operationen der sichereren Nameserver und Resolver beruhen.

Gegen die in Kapitel 4 vorgestellten Angriffe bietet Secure DNS ausreichenden Schutz. Es ergeben sich aber durch den Einsatz der neuen Protokolle auch neue Angriffsmöglichkeiten. Über die Sicherheitserweiterungen hinaus gibt es weitere Änderungsvorschläge für das DNS-Protokoll. Beispielsweise wurden:

- neuen Resource Records für die Abbildung des Telephonnummerraumes in das DNS definiert,
- Vorschläge zur Ablage von DNS-fremden Schlüsseln und Zertifikaten in der Zone implementiert
- und die Einführung von Internationalen Domainnamen vorbereitet.

Mit diesen Erweiterungen ergeben sich auch neue Herausforderungen für die Sicherheit. Das Thema IDN wird mit einigen anderen Problemfeldern exemplarisch vorgestellt.

Neue Verwundbarkeiten durch DNSSEC

Zonentransfer durch den NXT RR

Ein bisher ungelöstes Problem stellt der NXT-Record dar. Es ist durch diesen Record möglich, einen Zonentransfer zu erzwingen. Durch den NXT-RR wird von einem existierenden Namen auf den alphabetisch nächsten verwiesen. Der Zone wird so eine vorschriftsmäßige Ordnung aufgezwungen. Ein Angreifer kann nacheinander alle RR abfragen um alle Namen in einer Zone zu erhalten. Hierzu sind bereits Tools im Internet verfügbar [Walker].

Informationen die mit DNSSEC gesichert werden, bürgen für Authentizität und Integrität, sind jedoch öffentlich. Während DNS so konzipiert ist, dass Informationen öffentlich zugänglich sind, kann beobachtet werden, dass viele Zonenbetreiber auf diese Eigenschaft mittlerweile gerne verzichten, und wegen zu häufigem Missbrauch bzw. zu hohem Netzlastvolumen ihre Zonendaten nur noch für die eigenen Secondary-Nameserver bereit stellen.

Bisher wird dieses Problem kaum diskutiert. Es ist aber davon auszugehen, dass sich bei einem realen Einsatz die DNS-Betreiber lautstark zu Wort melden um diese Protokolleigenschaft abzulehnen.

Die Verwendung des NXT RR könnte den unerwünschten Effekt haben, dass die Zoneninformationen wieder für verschiedenste Angriffe (Spam, Distributed Denial of Service (DDOS)), zur Verfügung steht.

Eine Möglichkeit der Abhilfe bot der NO-RR [NO-RR], dieser Ansatz wurde aber wieder verworfen.

Komplexität

Mittlerweile ist ISC-BIND Version 9.2.2 auf 336.243 Zeilen Code angewachsen. Dies erhöht in erheblichem Maße die Verwundbarkeit, wie Veröffentlichungen der jeweils aktuellsten Bugs belegen. Eine Faustregel ist, dass die Anzahl an Fehlern proportional

zum Quadrat der Codezeilen eines Programmes ist. Neue Protokollmöglichkeiten eröffnen auch neue Möglichkeiten der Serververwundbarkeit durch Softwarefehler. Zum DNSSEC-Protokoll wurden bereits die folgenden Schwachstellen veröffentlicht: „sigdiv0 bug“, „tsig bug", „nxt bug", „sig bug" [BIND-Vul].

Client-Applikationen

Für den Einsatz von Secure DNS ist die Verfügbarkeit von Client-Applikationen notwendig. Während auf der Unix/Linux-Seite die Entwicklung transparent verläuft und beobachtet, angeregt und unterstützt werden kann, ist es auf der Microsoft-Seite schwer, an die notwendigen Informationen zu gelangen, die eine Beurteilung ermöglichen. Mittlerweile sieht die Entwicklung der DNS-Server Software von Microsoft eine teilweise Unterstützung des DNSSEC-Protokolls vor. Die Eigenschaften der nächsten Serverversion und insbesondere die Frage nach der zukünftigen Client-Unterstützung konnte im Rahmen dieser Studie nicht geklärt werden. Sollte Microsoft zukünftig auf andere Sicherheitsmechanismen als DNSSEC setzen, könnte das die Verbreitung des Protokolls ernsthaft einschränken. Einen Ausweg könnte der in Kapitel 5.10 vorgestellte DNS-Proxy darstellen.

Angriffe auf das Betriebssystem

Angriffe auf das Betriebssystem des Nameservers geschehen häufig über fehlerhaft programmierte Anwendungen (Buffer Overflows). Daher ist es zu empfehlen, einen „Nameservice only“-Betrieb auf dem Server zu fahren. Leider werden oft überflüssige Dienste auf einem Nameserver bereitgestellt wie in Abbildung 15: Auswertung Portscan dargestellt wurde.

Denial of Service

Die Root-Server waren in der Vergangenheit immer wieder ein begehrtes Ziel von DoS-Angriffen. Secure DNS trägt nicht zum Schutz gegen diese Art des Angriffes bei. Im Gegenteil, Angriffe durch DoS werden sogar leichter möglich, da das Protokoll erheblich mehr Ressourcen in Anspruch nimmt.

Wie bedrohlich diese Angriffe sind, hat sich jüngst (Januar 2003) gezeigt, als der Wurm SQLSlammer[71] in wenigen Minuten große Teile des Internets befiel.

Eine konkrete Möglichkeit des DOS-Angriffs besteht über die Dynamic Update Schnittstelle. Ein Angreifer kann hier die Ressourcen eines DNS-Servern in Anspruch nehmen, indem Updates öfter als notwendig an den Nameserver geschickt werden mit der Aufforderung eine Signatur zu erstellen.

Internationalisierte Domains

Immer lauter wird der Ruf nach den sogenannten Internationalen Domainnamen[72]. Bei diesen handelt es sich um eine Erweiterung des bisherigen Zeichensatzes für Domainnamen (alphanumerische Zeichen zusammen mit dem Bindestrich, 37 Stück) auf den Unicode Zeichensatz mit 95.221 Zeichen aus den unterschiedlichsten Schriftensystemen. Um das DNS-System nicht ändern zu müssen, werden Unicode-Domainnamen in DNS-konforme Namen umgewandelt mit Hilfe des Punycode Algorithmus. Problematisch an der Verwendung von IDN könnte sein, dass es einfach möglich ist, homographisch identische Domainnamen zu registrieren, die nichts miteinander zu tun haben und die daher zu unterschiedlichen IP-Adressen gehören. Beispielsweise lassen sich die russisch/kyrillischen Buchstaben „c“ und „o“ nicht von ihren lateinischen Entsprechungen unterscheiden. Schon jetzt ist hin und wieder zu beobachten, dass von cleveren Webseitenanbietern Domainnamen verwendet werden, die auf den ersten Blick de-

[71] http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/pab-27.01.03-000/default.shtml&words=Wurm
http://www.ripe.net/ttm/worm/, http://www.unicode.org, http://www.ietf.org
[72] http://www.i-d-n.net

nen bekannter Seiten recht ähnlich sind. Beispielsweise `H0mebanking.de` anstelle von `Homebanking.de`. Die Möglichkeiten dazu werden durch die Einführung von IDN sicherlich zunehmen und ernstzunehmender Missbrauch ist zu erwarten[73]. Auch die Verwendung von Zertifikat-basierten Ansätzen ist hier nicht unbedingt eine Lösung.

Ein sehr konservativer Standpunkt könnte sein, Unicode-Zeichensätze grundsätzlich abzulehnen, damit Domainnamen international benutzt werden können. Sonst besteht die Gefahr, dass Benutzer außerhalb des jeweiligen Kulturkreises die fremden Schriftsymbole nicht kennen und deshalb solche Namen im Browser auch nicht aufrufen können

Eine Empfehlung wäre eine Verwendung von IDN mit vorwiegend lokalem Bezug im betreffenden Sprachraum. Überregional sollte die Umschreibung mittels des ASCII-Zeichensatzes – wie bisher – zum Einsatz kommen.

***https* als Alternative**

Für die Client-Server-Authentifikation werden mittlerweile immer häufiger X.509 Zertifikate eingesetzt. Sofern das Zertifikat der ausgebenden Instanz (CA) im Client–Browser integriert ist, werden Serverzertifikate von Webseiten als vertrauenswürdig akzeptiert. Die Integration des öffentlichen Schlüssels der ausgebenden Zertifizierungsstelle in den Webbrowser Netscape oder Microsoft Internet Explorer ist mit hohen Kosten verbunden, weshalb auch einige Web CA-Anbieter die manuelle Integration des Zertifikates vom Benutzer in den Browser erwarten. Das erste Verfahren besitzt verschiedene Schwächen (s.u.), das zweite Verfahren ist abzulehnen, da es einen sehr gut informierten Internetbenutzer voraussetzt, der genaue Kenntnisse der einzelnen Schritte und insbesondere ihrer Sicherheitsüberprüfung besitzt.

Die Akzeptanz des Zertifikates der ausgebenden CA durch den Benutzer setzt eine unabhängige Überprüfung des öffentlichen Schlüssels oder des Fingerprints (z.B. SHA1[74]), voraus. Die Veröffentlichung könnte über eine Webseite oder in den Printmedien geschehen. Dies wird im allgemeinen vom Benutzer nicht nachgeprüft. Auch bezüglich der Güte des Zertifikates bedarf es tiefergehender Recherchen auf Benutzerseite. Zertifizierungsstellen können mit sehr unterschiedlicher Policy betrieben werden. Daher ist nicht auszuschließen, dass einige nur eine schwache Identifizierung von ihren Kunden und deren Organisationen verlangen beziehungsweise die Berechtigung der Ausstellung eines Serverzertifikates für eine bestimmte Domain nur unzureichend überprüfen. Webzertifikate, die einerseits für Sicherheit bürgen aber auf der anderen Seite fehlerhafte Informationen über eine Firma liefern, könnten so ein Sicherheitsrisiko darstellen. Der Einsatz dieser Technologie verlangt ein aktives Bemühen des Benutzers, um die Wirksamkeit zu gewährleisten.

In vielen Szenarien wird https aus Aspekten der Sicherheit schon äußerst gewinnbringend eingesetzt. Beispielsweise verwenden viele Firmen starke Authentifizierungsmechanismen im Intranet. Dies hat aber nur einen beschränkten Anwendungsbereich. Kommunikationsprotokolle wie POP3, IMAP4 oder SMTP können über SSL abgesichert werden. Bei anderen ist es nicht möglich auf diese Sicherheitsunterstützung aufbauen. Es müssen deshalb spezielle Maßnahmen für Ihren Schutz in Betracht gezogen werden. Beispielsweise kann die Vertraulichkeit und Integrität bei der Email-Kommunikation durch den Einsatz von PGP geschützt werden, für die korrekte Zustellung aber ist das

[73] DNS-Chaos befürchtet wegen multilingualer Domains.
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-01.11.02-000/
DENIC führt neue Regeln für Domain-Namen ein. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/ad-25.02.02-000/
http://www.icann.org/committees/idn/idn-keyword-paper.htm
Internationalisierte Domains: Ohrfeige für VeriSign. http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-28.01.03-012/

[74] Secure Hash Standard 1. http://www.rsasecurity.com/rsalabs/faq/3-6-5.html

nicht von Nutzen. Auch hier steht die Namensumwandlung der am Transport beteiligten Computer am Anfang. Durch DNSSEC kann diese korrekt gewährleistet werden.

10 Zusammenfassung

E-Commerce und E-Government werden zukünftig immer mehr an Bedeutung gewinnen. Wenn bisher schwache Mittel zur Authentifikation der Kommunikationsserver ausreichend waren, könnten sich diese schon heute oder morgen als ungenügend herausstellen, da sie einfach zu überwinden sind und davon auszugehen ist, dass diese Verwundbarkeit immer häufiger genutzt wird. Secure DNS bietet hier Abhilfe.

DNSSEC als sicheres Kommunikationsprotokoll ist jedoch nur sinnvoll, wenn die umgebenden Mechanismen, Infrastruktur und Prozesse ebenfalls auf Sicherheit ausgerichtet sind. Bei gleichmäßiger Belastung bricht jeweils das schwächste Glied in einer Kette.

Daher sind die Prozesse zur Domainregistrierung und zum Betrieb der DNS-Infrastruktur von fundamentaler Bedeutung. Diese Prozesse existieren bereits, müssen aber in Erwartung der neuen Anforderungen ausgebaut werden. Als Fundament steht hier die DENIC Public Key Infrastruktur im Hintergrund.

Ein DNSSEC-Projekt zum jetzigen Zeitpunkt würde ein großes Engagement hinsichtlich DENIC und Internet Service Provider bis zum Anwender voraussetzen. Es erscheint hier günstiger, mit anderen Infrastrukturbetreibern und DNS-Experten in regionalen und überregionalen Arbeitsgruppen Vorbereitungen zu treffen. Mittelfristig ist zu empfehlen, durch experimentelle Testumgebungen die Kompetenz für die Bereitstellung und den Betrieb einer sicheren *.de* Zone zu erlangen. Langfristig sollte DNSSEC für einen Teil der *.de-Zone* angeboten werden.

Anhang

A Abkürzungsverzeichnis

AXFR	Zonentransfer
ADMIN-C	Administrativer Kontakt
BIND	Berkley Internet Name Daemon
DBS	Datenbank System
DHCP	Dynamic Host Configuration Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CCTLD	Country Code Top-Level Domain
CENTR	Council of European National Top Level Domain Registries
CRL	Certificate Revocation List
DE	Deutsches Länderkürzel [RFC 1591]
DENIC	Deutsches Network Information Center
DSA	Digital Signature Algorithm
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DoS	Denial of Service
EPP	Enhanced Provisioning Protokoll
FZI	Forschungszentrum Informatik
FQDN	Fully Qualified Domain Name
GSHB	Grundschutz Handbuch
GSS-API	Generic Security Service API
GTLD	Generic Top-Level Domain
IANA	Internet Assigned Numbers Authority
IDN	Internationalized Domain Names
ICANN	Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IRTF	Internet Research Task Force
KK	Konektivitätskoordination
MD5	Message Digest 5
MX	Mailexchange
NS	Nameserver

PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PSE	Personel Security Environment
REG	Registrierung
RFC	Request For Comment
RRP	Registry Registrar Protocol
RR	Resource Record
RSA	Rivest Shamir Adleman
RIPE NCC	Réseaux IP Européens Network Coordination Centre
RIR	Regional Internet Registry
SCP	Secure Copy
SHA1	Secure Hash Standard 1
SIG	Signature RR
SIG(0)	Transaction signature
SOA	Start of Authority
SSL	Secure Socket Layer
TCP / IP	Transmission Control Protocol / Internet Protocol
TECH-C	Technischer Ansprechpartner
TKEY	Transaction Key
TSIG	Secret Key Transaction Authentication for DNS
TTL	Time To Live
ISP	Internet Service Provider
UPD	User-Datagram-Protokoll
URL	Uniform Resource Locater
WG	Working Group
ZONE-C	Zonen Ansprechpartner

B Anglizismen

Nachfolgend werden einige häufig im Text verwendeten Anglizismen vorgestellt. Diese sind in der Fachsprache so gebräuchlich, dass sie synonym zu deutschen Wörtern eingesetzt werden oder sogar längere Beschreibungen bestimmter Sachverhalte ersetzen. Sowohl in der Schriftsprache als auch in der Umgangssprache sind sie anzutreffen.

Answer Section	Antwort Abschnitt
Application	Anwendung
Best practice	Optimales Verfahren
Bottom up	Von unten nach oben
Cache	Speicher
Certificate Authority	Zertifizierungsstelle
Child-Zone	Sub-Zone
Country code)	Länder Code
Denial of Service	Einschränkung der Betriebsfähigkeit eines Servers
Deployment	Einsatz
Domain	Teilbaum im DNS
E-Commerce	Elektronischer Handel
E-Government	Elektronische Regierungsdienstleistungen
File	Datei
Hosting	Betrieb von Servern
Hostmaster	Der für den Betreib zuständige Mitarbeiter
Hostnames	Computername
Nameserver	Für die Namensauflösung zuständiger Computer
Non-profit	Gemeinnützig
Outsourcing	Ausgliederung von Produkten oder Dienstleistungen an Externe
Out-of-band	Außerhalb des Protokolls
Parent	Elternteil
Patch	Softwarekorrektur
PGP	Pretty Good Privacy
PEM	Privacy Enhancement for Internet Electronic Mail
Primary	Autoritativer NS, der seine Daten aus einer DB oder Datei bezieht
Poisoning	Vergiften
Policy	Leitlinie
Privat Key	Privater Schlüssel

Public Key	Öffentlicher Schlüssel
Registrar	Registrierung beantragende Stelle
Registry	Registrierungsstelle
Resouce Record	Datensatz der Quelle
Response	Antwort
Reverse Mapping	Rückwärtsauflösung (IP-Adresse -> Hostnamen)
Secondary	Erhält seine Daten vom Primary-NS. Ebenfalls autoritativ.
Secure DNS	Verschiedene Sicherheitsprotokolle zusammen mit infrastrukturellen Maßnahmen
Spoofing	Manipulieren, fälschen
Support	Unterstützung
Subdomain	Weitere Untergliederung einer Domain
Tools	Werkzeuge
Top-Level Domain	Domain dirket unterhalt der Root.
Trusted Keys	Vertrauenswürdige Schlüssel
Logfile	Protokolldatei, Programmausgaben werden dorthin geschrieben.
Reseller	Wiederverkäufer
Revocation	Rückruf
Poisoning	Vergiftung
Pollution	Verschmutzung
Query	Anfrage
Lame delegationen	Lahme Delegation

C Quellenverzeichnis

Zitate

[1] Paul Wilson, Director General, APNIC, ATLANTA--(BUSINESS WIRE), Nov. 17, 2002. http://www.isc.org/ISC/news/pr-11172002.html

[2] Paul Mockapetris, Defending the DNS and its Future. http://www.nominum.com/content/documents/defending_dns_future.pdf

[3] P. Steadman Preventing Future Attacks: Alternatives In DNS Security Management, November 20, 2002. http://www.circleid.com/articles/2551.asp,

[4] Carolyn Duffy Marsan, *Network World* DNS security upgrade promises a safer "Net"*, 10/16/00.* http://www.nwfusion.com/news/2000/1016dnsec.html

[5] Bert Hubert, Mailingliste [Pdns-users] DNSSEC, May 27, 2002. http://mailman.powerdns.com/pipermail/pdns-users/2002-May/000052.html

[6] D.J.Bernstein, DNS forgery. *http://cr.yp.to/djbdns/forgery.html*

[7] Paul Vixie, IETF mailinglist namedropper, 2002.11.21.

[8] Miek Gieben, November 2002. http://secreg.nlnetlabs.nl/about.shtml

[9] Peter Eisenhauer, DNS-Administrator, Schlund & Partner , Gespräch am 14.01.2003.

Literatur

[Afilias] Aflilias, Global Registry Service. FAQ protocol. http://www.afilias.info/faqs/for_registrars/protocol

[Albitz] P. Albitz & Cricket Liu, DNS und Bind 4. Auflage, O'Reilly 2002.

[Algo-01] geeigneten Kryptoalgorithmen gemäß § 17(1) SigG 2001, § 17(2) SigV 1997 in Verbindung mit 1. SigVÄndV 2000 vom 05.07.2001. http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/39.pdf

[Algo-02] Geeigneten Kryptoalgorithmen gemäß § 17(1) SigG 2001, § 17(2) SigV 1997 in Verbindung mit 1. SigVÄndV 2000 vom 15.04.2002. http://www.dfn-pca.de/bibliothek/sigg/germany/krypto-algorithmen-2002-04-15.pdf

[Austin] Tom Austin, PKI, Wiley & Sins, Inc., 2001

[Bellovin95] Bellovin, S., "Using the Domain Name System for System Break-Ins", Proceedings of the Fifth Usenix Unix Security, Symposium, June 1995.

[BIND-Vul] Bind Vulnerabilities. http://www.isc.org/products/BIND/bind-security.html

[BINDv9] BIND 9 Administrator Reverence Manual, ISC 2001. http://www.nominum.com/content/documents/bind9arm.pdf

[BirthAtt] Cert CCVulnerability Note VU#457875. http://www.kb.cert.org/vuls/id/457875

[Burns] Vivian Burns, Windows 2000 DNS Security, http://www.giac.org/practical/Vivian_Burns_GCNT.doc

[Caching] How to Measure the Performance of a Caching DNS Server, Nominum, Inc., 2002. http://www.nominum.com/content/documents/CNS_WP.pdf

[Chor] L. S. Chor, DNS Security Considerations and the Alternatives to BIND, Okt. 2. 2001. http://www.sans.org/rr/DNS/alternatives.php

[Davidowicz] Diane Davidowicz, Domain Name System Security. 1999. http://compsec101.antibozo.net/papers/dnssec/index.htm l

[DENIC-DFN] M. Sanz, S. Kelm, Einsatz von DNSSEC in der Domain .de, 8. Workshop „Sicherheit in vernetzten Systemen“, DFN, 15/16 Mai 2001.

[DENIC-Int] DENIC interne Dokumentation der Prozessabläufe.

[DENIC-P] Pressemitteilung DENIC vom 6. August 2002, DENIC baut Nameserver-Netz für die DE-Zone aus. http://www.denic.de/doc/DENIC/presse/nameserver.html

[DENIC-Stat] Internet Statistiken. http://www.denic.de/DENICdb/stats/index.html

[DENIC-Stud] S. Kelm et al., Einsatz von Secure DNS bei DENIC. 26. 10. 2000.

[DENIC-TB] DeNIC eG Tätigkeitsbericht 1999, 2000, 2001, 2002.

[DFN-PCA] DFN, Policy Certification Authority. http://www.dfn-pca.de/

[DUD-4/99] Datenschutz und Datensicherheit (DuD), Public Key Infrastrukturen. April, 1999.

[DUD-9/01] Datenschutz und Datensicherheit (DuD), PKI-Interoperabilität, September 2001.

[DynUpd] Secure dynamic DNS, Jan. 2002. howto http://ops.ietf.org/dns/dynupd/secure-ddns-howto.html

[EPP] Extensible Provisioning Protocol, Expires: July 29, 2003 http://www.ietf.org/internet-drafts/draft-ietf-provreg-epp-08.txt

[Galvin93] Design team meeting summary message posted to dns-security@tis.com mailing list by Jim Galvin on 19 November 1993.

[GSHB] Grundschutz Handbuch, BSI 2002, http://www.bsi.de/gshb/deutsch/menue.htm

[Househ] A. Householder, B. King, CERT/CC, Securing an Internet Nameserver Aug. 2002. http://www.cert.org/archive/pdf/dns.pdf

[ISIS-MTT] ISIS-MTT Specifications for Interoperability and Test Systems, Version 1.02. http://www.t7-isis.de/ISIS-MTT/isis-mtt.html

[Knowles] Brad Knowles Domain Name Server Comparison. Januar 2003. http://www.shub-internet.org/brad/papers/dnscomparison/

[Liu] Securing an Internet Nameserver, 2000. http://www.acmebw.com/resources/papers/securing.pdf

[Massey] D. Massey, T. Lehman, and E. Lewis. "DNSSEC” Implementation in the CAIRN, Testbed". https://keys.cairn.net/,

http://www.ietf.org/proceedings/99nov/I-D/draft-ietf-dnsop-dnsseccairn-00.txt,

[Res-Vul]. Application-Level-Security Vulnerability in the Domain Name System, 2002. Nominum, Inc.

http://www.nominum.com/content/documents/DRV_whitepaper2.pdf

[RFC 1422] S. Kent, Privacy Enhancement for Internet Electronic Mail, 1993.

[RFC 2832] NSI Registry Registrar Protocol (RRP) Version 1.1.0, May 2000.

[RFC 2026] S. Bradner, The Internet Standards Process -- Revision 3, October 1996.

[RIR] Daniel Karrenberg et al., RIPE-NCC;Development of the Regional Internet Registry System,

http://www.ripe.net/ripencc/about/regional/rir-system.html

[Schiffman] Mike Schiffma, Bound by Tradition, A Samplin of the Security Posture of the Internet's DNS Server, , Feb. 2003.

[Schneier] Bruce Schneier Applied Cryptography. Second Edition. John Wiley & Sons, 1996.

[SECREG] SECREG experiment in .nl. http://secreg.nlnetlabs.nl/about.shtml

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (SigG), Bundesgesetzblatt Teil I Nr. 22 vom 21. Mai 2001.

[SigI] Spezifikation zur Entwicklung interoperabler Verfahren und Komponenten nach SigG/SigV, Stand Juli 1999. http://www.bsi.bund.de

[SigV] Verordnung zur elektronischen Signatur. BGBl. I S.3074.

[PKCS] Public Key Cryptography Standard.

http://www.rsasecurity.com/rsalabs/pkcs/

[PKI-Page] The PKI-Page von Stefan Kelm, Eine ausführliche Linksammlung zum Thema PKI, Kryptografie, digitale Signatur, Zertifikate, Zertifizierungsinstanzen. http://www.pki-page.org/

[PKIX] Public Key-Infrastructure (X.509) (pkix).

http://www.ietf.org/html.charters/pkix-charter.html

[TCP IP] C. Hunt TCP/IP Network Administration, 2nd Edition. December 1997.

[TEST-NL] Testresults at NlnetLabs. http://www.nlnetlabs.nl/dnssec/

[Verisign] Applied Research DNSSEC Pilot site,

http://www.dnssec.verisignlabs.com

[Walker] DNSSEC Walker (maintained by Simon Josefsson).

http://josefsson.org/walker/

[WG] DNS Extensions (dnsext),

http://www1.ietf.org/html.charters/dnsext-charter.html

Domain Name System Operations (dnsop)

http://www.ietf.org/html.charters/dnsop-charter.html

[Win2003] New features for DNS with the Microsoft® Windows® .NET Server 2003 family.

http://www.microsoft.com/technet/prodtechnol/windowsnetserver/proddocs/datacenter/sag_DNS_ovr_NewFeatures.asp

[X509] International Telecommunication Union: Information Technology – Open System Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509; Juni 1997.

Drafts zu DNSSEC

[SSH-DNS] W. Griffin, J. Schlyter. Using DNS to securely publish SSH key fingerprints.

[App-Key] J. Schlyter, Storing application public keys in the DNS.

[IPSEC] M. Richardson, A method for storing IPsec keying material in DNS.

[Renewal] Y. Kamite, M. Nakayama, TKEY Secret Key Renewal Mode.

[Gieben] Miek Gieben, Ted Lindgreen, Parent's SIG over child's KEY.

[NO-RR] S.A. Josefsson, Authenticating denial of existence in DNS with minimum disclosure.

[Rollover] M. Andrews, D. Eastlake, Domain Name System (DNS) Security Key Rollover.

[EDNS1] Paul Vixie, Extensions to DNS (EDNS1).

[AD-Bit] Olafur Gudmundsson, Brian Wellington, Redefinition of DNS AD bit.

[Del-Sig] Olafur Gudmundsson, Delegation Signer Resource Record.

[Opt-In] Mark Kosters, Roy Arends, DNSSEC Opt-In.

[Opt-In WS] Notes of the OPT-IN workshop, Amsterdam Jan 21-23, 2003. http://www.ripe.net/DISI/optin-workshop/

[KSK-Flag] Edward Lewis, Olaf Kolkman, Jacob Schlyter, KEY RR Key-Signing Key (KSK) Flag.

[TKEY] Masaya Nakayama, Y Kamite, TKEY Secret Key Renewal Mode.

[DHS] D. Eastlake.Storage of Diffie-Hellman Keys in the Domain Name System (DNS).

[Roadmap] Scott Rose, DNS Security Document Roadmap.

[Intro] D. Massey, M. Larson, S. Rose, R. Arends. DNS Security Introduction and Requirements.

[Ihren] Root, J. Ihren, An Interim Scheme for Signing the Public DNS.

[Threats] D. Atkins, R. Austein, Threat Analysis Of The Domain Name System.

RFCs zu DNS

[RFC] RFC Übersicht zu DNS und DNSSEC. http://www.nominum.com/standards.php

[RFC 0921] Domain Name System Implementation Schedule, 1984.

[RFC 1031] Milnet Name Domain Transition, 1987.

[RFC 1034] Domain Names - Concepts and Facilities, 1987.

[RFC 1035] Domain Names - Implementation and Specification, 1987.

[RFC 1535] A Security Problem and Proposed Correction With Widely Deployed DNS Software, 1993.

[RFC 1591] Domain Name System Structure and Delegation, 1994.

[RFC 1713] Tools for DNS debugging, 1994.

[RFC 1912] Common DNS Operational and Configuration Errors, 1996.

[RFC 1918] Address Allocation for Private Internets, 1996.

[RFC 2181] Clarifications to the DNS Specification, 1997.

[RFC 2182] Selection and Operation of Secondary DNS Servers, 1997.

[RFC 2308] Negative Caching of DNS Queries (DNS NCACHE), 1998.

[RFC 2535] Domain Name System Security Extensions, 1999.

[RFC 2541] DNS Security Operational Considerations, 1999.

[RFC 2761] Extension Mechanisms for DNS (EDNS0), 1999.

RFCS zu DNSSEC

[RFC 2845] Secret Key Transaction Authentication for DNS (TSIG), May 2000.

[RFC 2929] Domain Name System (DNS) IANA Considerations, Sept. 2000.

[RFC 2930] Secret Key Establishment for DNS (TKEY RR), Sept. 2000.

[RFC 2931] DNS Request and Transaction Signatures (SIG(0)s), Sept. 2000.

[RFC 3007] Secure Domain Name System (DNS) Dynamic Update, Nov. 2000.

[RFC 3008] Domain Name System Security (DNSSEC) Signing Authority, Nov 2000 .

[RFC 3090] DNS Security Extension Clarification on Zone Status, March 2001.

[RFC 3110] RSA/SHA-1 SIGs and RSA KEYs in the Domain Name System (DNS), May 2001.

[RFC 3225] Indicating Resolver Support of DNSSEC, Dec. 2001.

[RFC 3445] Limiting the Scope of the KEY Resource Record out, Dec. 2002.

[RFC 3123] A DNS RR Type for Lists of Address Prefixes (APL RR), June 2001.

[RFC 2870] Root Name Server Operational Requirements, June 2000.