DNSSEC
Testbed für Deutschland

Status: Vers: 1.0
Stand: 24. April 2009

Vervielfältigung und Verbreitung

Diese Version des Dokuments ist abgestimmt zwischen:

Braintec Netzwerk-Consulting GmbH
Bundesamt für Sicherheit in der Informationstechnik
eco - Verband der deutschen Internetwirtschaft e.V.
DENIC eG
Klute-Thiemann Informationstechnologie GmbH & Co. KG

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: dnssec@bsi.bund.de
Internet: http://www.bsi.bund.de

eco - Verband der deutschen Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln
Tel.: +49 (0) 221 70 00 48-0
E-Mail: info@eco.de
Web: http://www.eco.de/

DENIC eG
Kaiserstraße 75 – 77
60329 Frankfurt am Main
Tel: +49 (0) 69 27235-0
E-Mail: DNSSEC@denic.de
Internet: www.denic.de

Inhaltsverzeichnis

1 Zusammenfassung

DNSSEC ist ein möglicher Baustein zur Verbesserung der Sicherheit des Internets. Vor einer Einführung von DNSSEC gilt es jedoch, eine Reihe von technischen Fragestellungen zu adressieren und eine Anzahl von organisatorischen und wirtschaftlichen Punkten detailliert zu untersuchen.

DNSSEC steht als Verfahren zur Steigerung der Sicherung von Authentizität im DNS seit einiger Zeit zur Verfügung. Dennoch kommen die Akzeptanz und Einführung nur sehr schleppend voran. In Kapitel 2 (Hintergrund) sind mögliche Ursachen und Gründe für eine mangelnde Akzeptanz, noch bestehende Probleme und Schwierigkeiten sowie Handlungsoptionen und mögliche Fragestellungen aufgezeigt. Durch koordiniertes Vorgehen auf vielen Ebenen sollen die offenen Fragen bearbeitet und wenn möglich gelöst werden. Ziel ist es, eine potentielle Einführung von DNSSEC dadurch zu erleichtern und zu beschleunigen.

Es wird daher empfohlen, den Weg zu einer möglichen Einführung von DNSSEC durch eine Reihe von Maßnahmen zu flankieren:

- Einrichtung einer längerfristig angelegten Gesprächsrunde, durch die alle am Thema beteiligten Parteien miteinander in Kontakt stehen,
- Verabschiedung einer gemeinsamen Zielvereinbarung, in der sich alle Beteiligten zu einer aktiven Unterstützung eines DNSSEC-Testbeds bereit erklären,
- Aufbau eines Testbeds für DNSSEC für Anbieter und Nutzer des Internets in Deutschland,
- Dokumentation und begleitende Beobachtung des Testbeds,
- Erarbeitung eines gemeinsamen Abschlussberichts und Verabschiedung einer Empfehlung zum weiteren Vorgehen.

Im Rahmen der vorgenannten Maßnahmen soll in jedem Verfahrensstadium ergebnisoffen über das weitere Vorgehen diskutiert werden, was im Verlauf des Projekts zu Änderungen der Planungen und Ziele führen kann.

Bisherige Beteiligte an diesem Prozess sind BRAINTEC, BSI, DENIC, eco und Klute-Thiemann.

2 Hintergrund

Das Internet bildet heute eine zentrale Infrastruktur für das gesamte Wirtschaftsleben. Ohne die durch das Internet erbrachten Kommunikationsdienste sind viele tägliche Vorgänge sowohl im Geschäftsleben als auch im privaten Umfeld nicht mehr in der gewohnten Form möglich.

Private Nutzer und die Wirtschaft verlassen sich zunehmend darauf, dass das Internet funktioniert. Das Internet wird als Basis sowohl für private, öffentliche, unternehmensinterne als auch externe Kommunikation genutzt.

Meist geht der Nutzer auch davon aus, dass Daten unverfälscht und unverändert im Internet übertragen werden. Es werden ständig neue Anwendungen und Verfahren im Internet eingeführt. Eine große Zahl dieser Anwendungen und Verfahren verlässt sich auf eine zuverlässig funktionierende und korrekte DNS-Auflösung von Namen auf Adressen. Daneben gibt es eine ständig steigende Zahl von Anwendungen, die das DNS zusätzlich zum Ablegen und Abfragen weiterer Informationen nutzen. Dazu zählen unter anderem Verfahren zur SPAM-Bekämpfung und Sicherung des Mailverkehrs wie DKIM und SPF, die ihre Schlüssel im DNS ablegen, oder VoIP-Anwendungen wie Asterisk, die über ENUM aus dem DNS die Informationen zum Vermitteln von Telefongesprächen erhalten. Da bei vielen dieser An-

wendungen kein Benutzer mehr an der Interaktion beteiligt ist, hat die Verlässlichkeit des DNS-Systems hierbei eine noch höhere Bedeutung als beim Zugriff auf Webseiten, bei denen immer noch eine Prüfung des Inhalts durch den Anwender erfolgen kann.

Die breite Einführung von DNSSEC brächte durch die Sicherung der Datenintegrität eine Steigerung der Zuverlässigkeit im gesamten DNS. DNSSEC löst keinesfalls alle Probleme, aber schon allein die Sicherung der Übertragung zwischen DNS-Server und DNS-Resolver verringert mögliche Angriffspunkte und verbessert so die Gesamtsicherheit. DNSSEC ist aber nur *eine* Maßnahme zur Steigerung der Sicherheit im Internet, deswegen sollten auch regelmäßig mit den betroffenen Industriekreisen etwaige alternative oder anderweitige Ansätze erörtert werden, um sicherzustellen, dass DNSSEC tatsächlich über den Projektverlauf hinaus das Mittel der Wahl ist.

2.1 Das Domain Name System (DNS)

2.1.1 Grundfunktionen

Das DNS (Domain Name System) ist ein verteiltes System zur Speicherung und Abfrage von Informationen im Internet. Die bekannteste Anwendung dient der Umwandlung von Namen in IP-Adressen. Neben dieser Grundfunktion wird das DNS noch zu einer Reihe anderer Abfragen genutzt, dazu zählen das Auffinden von Diensten wie Mailservern und Anmeldeservern, die flexible Abfrage von Rufnummern und den zugehörigen Servern und Diensten und anderes mehr. Die Verfügbarkeit und die Richtigkeit der Ergebnisse von DNS werden heute im Internet als gegeben betrachtet. Prinzipiell funktioniert das Internet auch ohne DNS, allerdings ist ein Verzicht auf Namen und Label und stattdessen die direkte Verwendung von numerischen IP-Adressen kaum vorstellbar. Ohne DNS müsste jeder Benutzer ständig IP-Adressen in seinem Browser oder in seiner Mail verwenden, was umständlich und fehleranfällig ist. IP-Adressen sind außerdem teilweise an den Provider gebunden und somit bei Serverwechsel/-umzug zwangsläufig Änderungen unterworfen. Das DNS basiert auf einer hierarchischen Server-Struktur, von der aus die Anfragen beantwortet werden. Diese Server stehen im Netz des Kunden oder beim Provider (für die lokale Zwischenspeicherung und die lokalen Netze), beim jeweiligen Anbieter von Diensten (für die Zielnetze), bei der jeweiligen Registry für TLDs (wie .de, .fr, .com, .net oder .org) sowie auf oberster Ebene bei den Betreibern der sogenannten root-Zone.

2.1.2 DNSSEC

Das DNS ist ein Protokoll, das selbst noch keine Maßnahmen zum Schutz seiner Inhalts-Daten enthält, insbesondere enthält es keine Sicherung der Daten gegen Veränderungen auf dem Transportweg oder in den durchlaufenden Servern und Caches. Verfälschungen können daher weder erkannt noch verhindert werden. Unter dem Namen DNSSEC wurden aus diesem Grund von der IETF eine Reihe von Erweiterungen und Ergänzungen standardisiert. DNSSEC ist zwar schon lange in der Entwicklung, eine weite Verbreitung und Einführung im Internet hat dieser Standard jedoch bisher noch nicht gefunden.

DNSSEC beschränkt sich ausschließlich auf die Quellenauthentisierung, das heißt auf die Sicherung des Pfades zwischen DNS-Servern und validierenden DNS-Klienten, wobei auch dazwischen liegende Server und Resolver mit ihren Caches mit in die Sicherheitskette eingeschlossen sind. Anhand der verwendeten Signatur lässt sich prüfen, ob die Daten von einer dazu berechtigten Stelle gesendet wurden. DNSSEC beinhaltet jedoch keine Vorgaben bezüglich einer Überprüfung der Authentizität der Identität der initial eingestellten Daten.

DNSSEC prüft Daten anhand von kryptografisch gesicherten Signaturen, die über die zu schützenden Daten errechnet werden und zusammen mit den Daten an den Client übertragen werden. Die Prüfung der Daten erfolgt dann im Client oder in dem davor liegenden Resolver gegenüber den zur jeweiligen

Zone passenden öffentlichen Schlüsseln. Diese Schlüssel können am einfachsten wiederum ebenfalls im DNS hinterlegt und abgerufen werden.

Dies ist dann optimal und ohne Bruch des Sicherheitsmechanismus möglich, da auch dieser Transfer mit Hilfe von DNSSEC abgesichert erfolgt und lediglich der für den Beginn der Kette notwendige Schlüssel (der Key der root) im Client fest hinterlegt oder per Konfiguration eingepflegt wird.

Solange die root noch nicht signiert ist, kann alternativ auch mit geeigneten Verteilungsfunktionen außerhalb von DNS für eine vertrauenswürdige Verteilung der benötigten Schlüssel gesorgt werden. Verschiedene Ansätze dazu sind derzeit noch in der Diskussion.

DNSSEC ist ein möglicher Baustein, um den Betrieb von DNS und damit einen Aspekt des Internets sicherer zu machen. DNSSEC hilft gegen Fälschungen und das Unterschieben falscher DNS-Daten, kann jedoch viele andere Probleme wie Domain-Hijacking, Phishing oder Manipulationen bei der Registrierung nicht verhindern. Die Vorteile von DNSSEC lassen sich auch erst dann komplett ausnutzen, wenn DNSSEC in der Fläche möglichst von jeder Hard-/Software und der überwiegenden Mehrheit der Resolver unterstützt wird. Bis dahin sind nur Teile nutzbar und Unsicherheiten, die durch den Bruch der Kette entstehen, zu überwinden.

2.2 Fragen und Probleme von DNSSEC

Hinsichtlich der Einführung von DNSSEC gibt es eine Reihe offener Fragen und Probleme technischer, organisatorischer oder ökonomischer Natur. Die folgenden Kapitel beleuchten diese Fragen und Probleme. Die Entwicklung von Lösungsansätzen und Antworten sind Thema des in Kapitel 3 vorgeschlagenen Testbeds.

2.2.1 Betrieb der Root-Zone und der root-Server

DNSSEC setzt für den reibungslosen und optimalen Betrieb eine vollständige Kette von Signaturen von der Spitze (root) bis zur jeweiligen zu sichernden Domain voraus. Da sich bei der Signierung der Root-Zone vielfältige politische Probleme, offene Verfahrensfragen und Diskussionen und daraus resultierend Verzögerungen ergeben haben, gibt es zwischenzeitlich Vorschläge, einen DNSSEC-Betrieb ohne signierte Root zu starten. Statt von einem zentralen signierten Punkt aus (der root), startet die Kette der Trust-Anchor mit einem oder mehreren auf einer öffentlichen Webseite bekanntgegebenen öffentlichen Schlüsseln oder DS-Records.

Von diesem von Hand konfigurierten Punkt aus können dann die Resolver alle unterhalb dieser Zonen liegenden weiteren Zonen mit DNSSEC erreichen. Ein automatisiertes Verfahren dazu findet sich zum Beispiel in RFC 5074 „DNSSEC Lookaside Validation (DLV)“. Eine andere Alternative sind eigene, oft skriptbasierte Verfahren zum Laden der Trust-Anchor, welche die Daten von einem vertrauenswürdigem Repository (z.B. IANA) laden.

Die Verwaltung des Inhaltes der Root-Zone wird derzeit von ICANN durchgeführt. Grundlage ist ein Vertrag (sog. IANA-Contract) mit dem DOC (US Departement of Commerce). ICANN/IANA nimmt die Daten von TLD-Betreibern entgegen und prüft diese. Danach werden die Daten zur Prüfung an das DOC weitergegeben und anschließend von Verisign (dem Betreiber des A-root-servers) in die Root-Zonen-Datei einpflegt und die Distribution an die anderen Root-Server-Betreiber veranlasst.

Mit DNSSEC und dem Signieren der Root-Zone kommen in diesem Bereich neue Funktionen hinzu. Die Root-Zone muss signiert werden. Die dazu notwendigen Schlüsselpaare müssen generiert und die öffentlichen Schlüssel in geeigneter Weise publiziert werden. Die Schlüssel müssen in regelmäßigen Abständen gegen neue ausgetauscht werden. Im Fall einer Kompromittierung muss ein Schlüsselwechsel

eingeleitet und durchgeführt werden. Regelmäßig muss der TLD-Betreiber die DS-Records mit den Hash-Werten ihrer aktuell gültigen Schlüssel übermitteln und diese in die Root-Zone übernommen werden. Ein Verfahren und die Definition der entsprechenden Zuständigkeiten sind zu erarbeiten.

2.2.2 Zusammenfassung für die Root-Zone

Die Erarbeitung der Verfahren für die Signierung der root ist für den langfristigen reibungslosen Betrieb von DNSSEC von hoher Bedeutung. Solange kein Ergebnis erzielt ist, können für den Testbetrieb lokale Trust-Anchor eingesetzt werden. Falls die Erarbeitung der Verfahren länger dauert oder eine Verteilung sinnvoll erscheint, stehen alternative Lösungen (zentrales Repository, DLV) zur Verfügung.

Zu betrachtende Fragestellungen:

- Wie kann ein geeignetes Verfahren zur Signierung der Root aussehen?
- Wie sehen die verschiedenen wechselseitigen Verantwortlichkeiten aus?
- Was für Worst-Case-Szenarien sind denkbar – Welche Handlungsoptionen gibt es?

2.3 Betrieb der Topleveldomain

Hinsichtlich der Ziele von DNSSEC hat die DENIC, als für .de zuständige Stelle, eine grundsätzlich positive Haltung. Für DENIC stehen die Betriebssicherheit, Robustheit und Verfügbarkeit des DNS an erster Stelle, gefolgt von Fragen der Wirtschaftlichkeit und insbesondere der Nutzerakzeptanz, welche wesentliche Kriterien für die Zielerreichung sind.

2.3.1 Registrierungssystem der TLD .de

Neben dem Betrieb der DNS-Server, ist eine zentrale Aufgabe die Haltung der dafür notwendigen Daten. Durch die Einführung von DNSSEC werden zusätzliche Datenfelder in den Datensätzen der einzelnen Domains benötigt. Das für die interne Speicherung der Domain-Daten verwendete Registrierungssystem muss dazu hinsichtlich der notwendigen DS-Records erweitert werden. Gleiches gilt für die Registry/Registrar-Schnittstelle und die damit verbundenen Prozesse. Weiterhin müssen die Backend-Prozesse zur Generierung der eigentlichen für die DNS-Server verwendeten Zonendaten entsprechend angepasst werden.

Die Erweiterungen der bestehenden Datenbank und der zugehörigen Interfaces sowie die damit verbundenen Umstellungen in den internen Abläufen müssen sorgfältig geplant werden. Zusätzlich zu den Erweiterungen sind neue interne Abläufe notwendig und müssen eingeführt werden. Beispiele dafür sind: Signierung der Zonendaten, Festlegung der Gültigkeitsdauer von Signaturen und Überwachung derselben, Generierung von Schlüsseln, Verfahren zum Schlüsselmanagement, Festlegung von Notfallprozeduren u.ä.

Neben den rein technischen Erweiterungen und dem Betrieb verursacht DNSSEC bei der unsachgemäßen Nutzung auch eine Reihe Seiteneffekte, wie z.B. die Nichterreichbarkeit einer Domain bei inkonsistenten DS-Records. Hier sind geeignete Verfahren und Maßnahmen zu entwickeln.

2.3.2 Nameserverbetrieb der TLD .de

Da die Nutzung von DNSSEC die Anforderungen an die eingesetzten Ressourcen hinsichtlich Kapazität, Bandbreite, CPU erheblich erhöht, ergeben sich für den Betrieb einer Top-Level-Domain daraus spezielle Anforderungen an die zum Betrieb genutzte Hard- und Software genauso wie an die Infrastruktur. Engpässe im aktuellen Betriebskonzept sind zu evaluieren und ggf. Lösungen dafür zu erarbeiten.

2.3.3 Zusammenfassung für die TLD

- Herausforderungen hinsichtlich Betriebssicherheit, Wirtschaftlichkeit und Nutzerakzeptanz müssen gelöst werden.
- Die Registry/Registrar-Schnittstelle muss geeignet erweitert werden.
- Die .de-Nameserverinfrastruktur muss entsprechend ausgebaut werden.
- Vor einem Beginn eines Produktivbetriebs müssen alle Komponenten auf ihre Stabilität im Massenbetrieb getestet werden.
- Trust-Anchor müssen an geeigneter Stelle veröffentlicht werden.
- Verfahren und Empfehlungen zur Schlüsselerzeugung, -verwaltung, -management und Keyrollover sind zu erarbeiten, zu testen und umzusetzen.
- Für potentielle Fehler im betrieblichen Umfeld müssen Lösungsvorschläge, FAQs, Schulungsmaterial, u.ä. erstellt und betriebliche Prozesse adaptiert werden.

2.4 Registrare

Registrare sind Dienstleister für Registrierungsdienste. Es handelt sich dabei typischerweise um reine Domainanbieter, Hostingfirmen oder auch ISPs. Einige bieten nur die reine Registrierungsdienstleistung an, andere bündeln diese mit zusätzlichen Dienstleistungen wie den Betrieb autoritativer Nameserver, Webseitenpräsenzen, Serverhosting für ihre Kunden, u.ä.

Die Registrare müssen die für die interne Speicherung der Domain-Daten verwendeten Systeme um die notwendigen DS-Records erweitern. Gleiches gilt für daraus resultierende Änderungen an der Registry/Registrar-Schnittstelle sowie den damit verbundenen Prozessen. Weiterhin müssen sie, soweit sie Nameserverdienste anbieten, die Backend-Prozesse zur Generierung der eigentlichen Zonendaten entsprechend anpassen und entsprechende Vorkehrungen für den DNSSEC-Betrieb ihrer Nameserverinfrastruktur treffen. Letzteres beinhaltet auch den technischen Ausbau der Infrastruktur (Bandbreite, Rechnerkapazitäten, …).

Zusätzlich zu diesen Erweiterungen sind neue interne Abläufe notwendig. Sie müssen definiert und eingeführt werden. Beispiele sind: Signierung der Zonendaten, Festlegung der Gültigkeitsdauer von Signaturen und Überwachung derselben, Generierung von Schlüsseln, Verfahren zum Schlüsselmanagement, Festlegung von Notfallprozeduren u.ä.

Neben den rein technischen Erweiterungen und dem Betrieb verursacht DNSSEC bei der unsachgemäßen Nutzung auch eine Reihe Seiteneffekte, wie z.B. die Nichterreichbarkeit einer Domain bei inkonsistenten DS-Records. Hier sind geeignete Verfahren und Maßnahmen zu entwickeln.

2.4.1 Zusammenfassung für Registrare

- Herausforderungen hinsichtlich Betriebssicherheit, Wirtschaftlichkeit und Nutzerakzeptanz müssen gelöst werden.
- Die Registry-Schnittstelle, die internen Abläufe sowie die Kundenschnittstellen müssen erweitert werden.
- Bei eigenem DNS-Betrieb muss die Nameserverinfrastruktur muss entsprechend ausgebaut werden.
- Verfahren und Empfehlungen zur Schlüsselerzeugung, -verwaltung, -management und Keyrollover sind zu erarbeiten, zu testen und umzusetzen.
- Vor einem Beginn eines Produktivbetriebs müssen alle Softwarekomponenten auf ihre Stabilität im Massenbetrieb getestet werden.

2.5 Domaininhaber

Betreibt ein Kunde seine Domain ohne eigenen DNS-Server, so muss er einen Dienstleister mit dem DNS-Service beauftragen. Da in diesem Fall keine eigene DNSSEC-abhängige Hardware und Software betrieben wird, sind keine technischen Probleme zu erwarten bzw. DNSSEC-spezifische Herausforderungen vom jeweiligen Dienstleister (vgl. 2.4) zu lösen.

Viele Anwender, insbesondere Firmen oder Betreiber von größeren Server-Parks, betreiben für eigene Domains die Nameserver, statt sich als Kunde auf die Dienstleistungen eines externen Anbieters zu stützen. In diesen Fällen muss die selbst betriebene DNS-Infrastruktur DNSSEC entsprechend unterstützen.

Zusätzlich zu diesen Erweiterungen sind neue interne Abläufe notwendig. Sie müssen definiert und eingeführt werden. Beispiele sind: Signierung der Zonendaten, Festlegung der Gültigkeitsdauer von Signaturen und Überwachung derselben, Generierung von Schlüsseln, Verfahren zum Schlüsselmanagement, Festlegung von Notfallprozeduren u.ä.

2.5.1 Zusammenfassung für Domaininhaber

- Bei eigenem DNS-Betrieb muss die Nameserverinfrastruktur entsprechend ausgebaut werden.
- Verfahren und Empfehlungen zur Schlüsselerzeugung, -verwaltung, -management, Keyrollover aber auch Nameserverbetrieb sind zu erarbeiten.

2.6 Provider

Ein Provider (ISP) bietet seinen Kunden meist neben dem reinen Zugang zum Internet weitere Dienste an. Dazu zählen zentrale DNS-Server, die von den Kunden entweder direkt über die Resolver in ihren Endgeräten oder über ein dazwischen geschaltetes Gerät (DSL-Router oder Kabel-Router mit DNS-Cache) benutzt werden können.

Aktuell wird DNSSEC von vielen Endgeräten und -anwendungen noch nicht unterstützt. Es gibt daher Vorschläge, die DNS-Antworten in den Caching-Servern zu prüfen und nur die validierten DNS-Antworten an die Endkunden weiterzuleiten bzw. Antworten, bei denen die Validierung fehlschlägt, zu verwerfen.

Dieser Betriebsmodus ist durch den Einsatz geeigneter Soft- und Hardware zu unterstützen. Da wegen der hohen Zahl der eventuell betroffenen Kunden ein gewisses Risiko besteht, sind Fragen zu einer weichen Migration, Roll-Back-Möglichkeiten u.ä. zu adressieren.

Weiterhin bestehen Unsicherheiten, wie ein validierender Resolver mit negativen Ergebnissen umgehen soll. Bei dem aktuell präferierten Vorschlag werden Labels, die als zu einer DNSSEC-unterstützenden Zone gehörend erkannt werden (DS-Record ist vorhanden), auf eine korrekte Signatur geprüft. Kommt es bei dieser Prüfung zu einem Fehler, so wird der anfragenden Stelle ein Fehler (SERVFAIL oder auch NXDOMAIN oder Timeout) zurückgemeldet. Damit ist aber nicht zu erkennen, ob dieses Label wirklich nicht existiert oder ob bei der DNSSEC-Validierung ein Fehler entdeckt wurde. Diese Unklarheiten können zu verstärktem Aufwand bei Hotline und Support führen sowie eventuell Unsicherheiten bei der Haftung hervorrufen. Durch diese Änderung des DNS-Verhaltens verändert sich die Benutzererwartung. Hier sind geeignete Anpassungen und Maßnahmen zu entwickeln und ggf. Informationen für die Nutzer bereitzustellen.

Da eine flächendeckende Verfügbarkeit von validierenden Resolvern in den Endgeräten erst in einigen Jahren zu erreichen ist, sollte über alternative Mechanismen, die dem Anwender die Informationen über fehlgeschlagene Validierungen bereitstellen können, nachgedacht werden.

2.6.1 Zusammenfassung für Provider

- Die Eignung von Software und Hardware muss im Einzelfall geprüft und bewertet werden. Das geplante Testbed soll die Möglichkeit bieten, auch Tests für Massendaten vorzunehmen.
- Für folgende Fragen könnte ein Leitfaden zum Umgang mit DNSSEC erarbeitet werden und Antworten liefern:
  - Wie sollen mit DNSSEC als unsicher erkannte Einträge in geschützten Zonen behandelt werden (via NXDOMAIN oder SERVFAIL o.a.)?
  - Wie unterscheidet man echte von DNSSEC gefundene Probleme von eigenen Konfigurationsfehlern?
  - Soll man Anwender auf einen DNSSEC-Fehler hinweisen? Wenn ja, wie soll dies geschehen?
  - Soll man den Inhaber oder technischen Kontakt einer als fehlerhaft gekennzeichneten Domain auf die Probleme hinweisen? Wie? Wer?
  - Wie erkennt man Konfigurationsfehler eines Administrators und unterscheidet diese von echten, durch einen Angriff hervorgerufenen Meldungen?
- Die auf dem Markt verfügbaren Geräte für Endkunden (DSL-Router, Kabel-Modems und ähnliche Netzanschlussgeräte) sollen auf ihre Tauglichkeit für DNSSEC geprüft und die Resultate öffentlich dokumentiert werden.

2.7 Software

Hersteller für Hard- und Software sind in ihrer Produktplanung meist relativ stark von der Nachfrage ihrer Kunden bestimmt. Für DNSSEC existiert derzeit keine entsprechende Nachfrage, da das Protokoll für die meisten Endanwender keinen unmittelbaren Nutzen zeigt. Allerdings wird von Seiten einiger potentiell betroffenen Anbieter im Internet ein Bedarf nach Verbesserungen signalisiert, wie sie z.B. DNSSEC bietet.

2.7.1 DNS-Server

Die Anzahl der voneinander unabhängigen Entwicklungen im DNS-Bereich ist relativ klein. Es beschäftigt sich nur eine kleine Anzahl von Firmen mit DNS-Software und vermarktet diese. Die folgende Tabelle gibt eine aktuelle Übersicht.

Hersteller	Produkt	DNSSEC Support	Anwendungs-bereich	Relevanz und Verwendung
ISC	BIND inklusive Resolver + Library)	Ja	TLD, große Zonen, kleine Zonen	.de,Unix-Systeme, Referenzprodukt
Nominum	Nominum Authorative Name Server und Caching Name Server	Ja	Caching-Resolver	Große Zugangsprovider
NL net Labs	NSD	Ja	TLD	.de, .nl
NL net Labs	Unbound	Ja	Caching-Resolver	relativ neues Produkt
NeuStar	UltraDNS	Nein	TLD und große Zonen	.org, .info, .mobi, .asia, .biz, .tel
D.J. Bernstein	DJBDNS	Nein	Große Zonen, kleine Zonen	Weit verbreitet bei kleineren Zonen auf Linux-Systemen

Hersteller	Produkt	DNSSEC Support	Anwendungs-bereich	Relevanz und Verwen-dung
SECURE64	Secure64 DNS Authori-ty	Ja	Große Zonen	
Microsoft	Microsoft DNS-Server (ab Servicepack 1 für Windows Server 2008)	Ja	Große Zonen, kleine Zonen	Weite Verbindung in mit-telständischen und klei-nen Betrieben
Microsoft	Microsoft Resolver (ab Servicepack 1 für Windows Server 2008)	Ja	Caching-Resolver	Endsysteme
DEBIAN + Open Source	DNSMASQ	Nein	Resolver, Cache und Forwarder für kleine Systeme	DEBIAN, Linux-Systeme, CPE-Systeme, u.a. Link-sys
PowerDNS BV	PowerDNS	Nur als Slave	Große Zonen, kleine Zonen	

Die permanente Weiterentwicklung des Standards sowie die fehlende Nachfrage wurde lange Zeit von den meisten Herstellern von Software als Hauptgrund für die zögerliche Umsetzung genannt. Da es wenig Erfahrung im produktiven Umfeld gibt, ist Betriebserfahrung nur im kleineren Umfeld und aus dem Testbetrieb bekannt. Hier sind noch mehr Betriebserfahrung und weitere Tests erforderlich.

Die Entwickler von DNS-Software sind eine relativ kleine und gut überschaubare Gruppe von Softwareentwicklern. Typisch sind intensive und oftmals sehr persönlich geführte Diskussionen um oft nur winzige Änderungen und Verbesserungen am Protokoll. Durch den engen Kontakt lassen sich aber auch effizient schnelle Entwicklungsschritte realisieren.

2.7.2 Software für Blackboxes (CPE-Router usw.)

Die bei Endkunden in großer Zahl eingesetzten Routern (DSL-Router, Kabel-Modems mit Routern und ähnliche Geräte) bieten meist neben anderen Funktionen auch DNS-Dienste an. Teilweise handelt es sich dabei um einfache DNS-Proxies, die Anfragen immer an vorkonfigurierte DNS-Server des jeweiligen ISP weiterleiten. Daneben existieren eine Reihe von Geräten (zum Beispiel von Linksys oder D-Link), die DNS-Anfragen zusätzlich aus einem internen Cache beantworten und Anfragen über direkt am Router angeschlossene und über DHCP konfigurierte Geräte geben.

Zwei Untersuchungen (Von Nominet siehe http://download.nominet.org.uk/DNSSECcpe/DNSSEC-CPE-Report.pdf und der Schwedischen Registry siehe http://iis.se/docs/Routertester_en.pdf) zeigen die oft noch fehlende DNSSEC-Unterstützung bei Geräten dieser Anwendungsklasse. Da diese Untersuchungen bei der Geräteauswahl auf ihren jeweiligen Heimatmarkt ausgerichtet waren, scheint es sinnvoll, für Deutschland eine entsprechende Studie durchzuführen.

Viele Hersteller unterstützen aufgrund der mangelnden Nachfrage kein DNSSEC in ihren Geräten. Auch besteht bei den Providern, die diese Geräte oftmals kostenlos oder für einen geringen Betrag zur Verfügung stellen, nur geringe Motivation zusätzliche Features zu unterstützen. Ein großes Problem stellt deswegen die große installierte Basis von Geräten bei Endkunden dar, die überwiegend keinerlei Unterstützung für DNSSEC enthalten, und nur umständlich nachrüstbar sind.

2.7.3 Software für Endgeräte

Mit zusätzlicher Software kann DNSSEC unterstützt werden. Eine Sammlung weiterer Software (Plugins für Browser, Erweiterung für WWWCache, SQUID oder ähnliche Software) sollte erstellt werden. Fehlende Software kann ggf. entwickelt und als Open Source zur Verfügung gestellt werden.

2.7.4 Zusammenfassung Software

- Software, welche DNSSEC unterstützt, sollte gelistet und ihre jeweilige Verwendbarkeit dokumentiert werden. Bei Defiziten können die Hersteller kontaktiert und darauf hingewiesen werden.
- Für den deutschen Markt sollten die verfügbaren Geräte für Kunden (DSL-Router, Kabel-Modems und ähnliche Netzanschlussgeräte) auf ihre Tauglichkeit für DNSSEC geprüft und die Resultate dokumentiert werden. Bei Defiziten können die Hersteller kontaktiert und darauf hingewiesen werden.
- Für im Markt stark verbreitete Geräte sollte auch über die Verfügbarkeit von Updates und die Nachrüstbarkeit informiert werden.
- Lücken von Softwareunterstützung sollten dokumentiert werden.
- Für schwierigere oder komplexere Anwendungen könnten Dokumentationen und HowTo-Anleitungen erstellt werden.

2.8 DNSSEC in Firmen und für Endkunden

Für die Anwendung von DNSSEC in Firmennetzen und zuhause gibt es keine allgemeine Lösung, da vieles vom konkreten Anwendungsfall, der Größe der Unternehmung oder des Netzes und natürlich auch vom Sicherheitsbedürfnis abhängt.

Trotzdem sollten für diese Bereiche die entsprechenden Möglichkeiten beschrieben und Alternativen dokumentiert werden. Viele Überlegungen aus den vorherigen Kapiteln gelten aber analog bzw. lassen sich auf die lokale Nutzung extrapolieren.

2.8.1 Zusammenfassung DNSSEC in Firmen und für Endkunden

- Frei verfügbare deutschsprachige Information über DNSSEC sollte erstellt werden.
- Langfristig sind beim Endanwender oder zumindest bei größeren Firmennetzen ausreichende Informationen über den Einsatz und die Wirkungsweise von DNSSEC notwendig.

3 Testbed

Um die in Abschnitt 2 beschriebenen offenen Punkte zu adressieren, haben sich die Beteiligten verständigt, ein Testbed zu DNSSEC in Deutschland zu etablieren. Das Testbed soll allen Betreibern von DNS-nahen Anwendungen aber auch Interessierten offen stehen. Erzielte Ergebnisse sollen ebenfalls öffentlich sein.

Ziele des Testbeds sind ein gemeinsames Verständnis der Technologie zu fördern, Anwendungserfahrung zu sammeln und Lösungen zu erarbeiten. Themen im Einzelnen sind:

- die Identifizierung von Schwachstellen und Erarbeitung von Lösungen oder Lösungsansätzen,
- die Identifizierung technischer Probleme und deren Lösung,
- die Identifizierung wirtschaftlicher Probleme und Erarbeitung von Lösungsvorschlägen,
- die Identifizierung psychologischer und anderer Hindernisse und
- die Bereitstellung einer realen DNS-Umgebung, um allen Beteiligten und Interessierten Tests und Erfahrungen in einer produktionsnahen Umgebung zu ermöglichen

Im Testbed soll der gesamte Themenkomplex DNSSEC in Deutschland bearbeitet werden, wobei alle Dienste und Funktionen untersucht werden, die notwendig sind, um das Internet in Deutschland zu betreiben. Insbesondere werden dabei die Top-Level-Domain .de und der Namensbereich unterhalb der TLD betrachtet. Als zu untersuchende Bereiche wurden identifiziert:

- DNS-Root (IANA,ICANN, root-Server-Operator), bzw. TAR/DLV-Betreiber
- Registrierungssystem für die Toplevel-Domain .de (DENIC eG)
- Nameserverbetrieb für die Toplevel-Domain .de (DENIC eG)
- Kommunikation mit dem Registrierungssystem und den Endkunden (DENIC-Mitglieder, Registrare, Dienstleister bei Domainregistratur, DENIC),
- Betreiber von autoritativen Secondlevel Nameservern (DENIC-Mitglieder, Registrare, ISPs, größere Endanwender, …)
- Betreiber von Caching-Name-Servern, Forwarding-Nameservern (Zugangsprovider, ISPs, größere Endanwender) und
- Betreiber von Resolvern, Zugangsroutern u.ä.. (Administratoren in Unternehmen und Endnutzer)

Neben den technischen und organisatorischen Fragestellen sollen begleitend zum Testbed die Fragen nach den ökonomischen Auswirkungen und der Marktakzeptanz von DNSSEC beantwortet werden. Die Ergebnisse sollen – gegebenenfalls unter Einschluss von Erfahrungen im Ausland – in die weiteren Planungen eingestellt werden.

Aus den Ergebnissen soll ein gemeinsamer Abschlussbericht erstellt werden. Dabei sollen mindestens folgende Punkte adressiert werden:

- Dokumentation, Bewertung und Auswirkung von gefundenen Ergebnissen,
- Identifizierte Probleme sowie Lösungsvorschläge, Alternativlösungen und Umgehungen,
- Bewertung der Erfahrungen und Beobachtungen aus den produktionsnahen Tests,
- Erstellung einer gemeinsamen Empfehlung zum weiteren Vorgehen.

3.1 Maßnahmen im Testbed

Bei der folgenden Liste von Maßnahmen handelt es sich nicht um eine abschließende Liste, sondern um einzelne Punkte zu denen bereits Einigkeit erzielt wurde. Die Liste kann um weitere sinnvolle Punkte ergänzt werden.

3.1.1 Aufbau DNS-Test-Infrastruktur bei DENIC

DENIC wird für Testzwecke eine dedizierte parallele Infrastruktur für die autoritativen Nameserver der TLD .de einrichten. Das .de-Registry/Registrar-Interface wird um die DNSSEC-Funktionalität erweitert und danach wird die signierte .de-Zone aus diesen Daten erstellt und in dieser parallelen DNS-Struktur bereitgestellt. Den Registraren wird damit ein erweiterter Zugang zum .de-System zur Verfügung gestellt, über den sie konfigurerbar selbst ebenfalls DNSSEC nutzen und anbieten können. Über die adaptierte Schnittstelle kann die Übergabe von Signaturen erfolgen. Registrare können damit den Prozess der internen Generierung von Signaturen und die Weitergabe an die Registry testen. Parallel dazu werden automatisierte Verfahren für Key-Rollover und Schlüsselwechsel im Notfall nach einer Kompromittierung erarbeitet und testweise erprobt. Durch die Bereitstellung der parallelen Infrastruktur können Provider (oder Endkunden) mittels ihrer Resolver auf das Testbed zugreifen. Dazu muss bei diesen Resolvern DNSSEC aktiviert und manuell der Trust-Anchor des DENIC konfiguriert sowie ein Forward auf einen der Server im Testbed eingetragen werden.

3.1.2 Test von Endgeräten

Am Markt gibt es wenig Information zu DNSSEC-geeigneten Geräten. Viele der Zugangsgeräte wie ADSL- oder Kabel-Router, welche gleichzeitig als DNS-Forwarder, DHCP-Server und teilweise noch als Hub oder Wireless-LAN-Router verwendet werden, unterstützen DNSSEC nicht oder nur bedingt.

Das BSI wird daher eine Studie durchführen, um hier mehr Transparenz im Markt zu erzeugen. Als Beispiel dienen Untersuchungen aus Schweden (DNSSEC Tests of Consumer Broadband Routers, Joakim Åhlund & Patrik Wallström, 2008) und England (Test Report: DNSSEC Impact on Broadband Routers and Firewalls, Nominet, 2008).

3.1.3 Aufbau und Signierung einer sicheren Domain

Um Erfahrungen im realen Betrieb zu sammeln, wird eine zentrale Domain in öffentlicher Hand (zum Beispiel bund.de oder auch die für den Zugang zu de-mail benötigten Domains) signiert und die öffentlichen Schlüssel dazu passend bekannt gegeben werden. Ein Test der Signierung und der Validierung wäre dann für alle interessierten Parteien möglich.

3.1.4 Kooperation mit anderen Betreibern

Da international viele Gruppen an der Bereitstellung von DNSSEC arbeiten, soll der Erfahrungsaustausch gestärkt werden. Vertreter dieser Organisationen, die in dem Bereich DNSSEC arbeiten, wie Verisign, Afilias, IIS oder ISC sollen deswegen auch zu den geplanten Gesprächsrunden eingeladen werden.

3.1.5 Aufbau und Verteilung von Know-how

Da DNSSEC für viele an der Umsetzung Beteiligte noch relatives Neuland darstellt, ist eine zentrale Sammlung von Know-how sinnvoll. Die Erstellung eines deutschsprachigen DNSSEC-HowTo kann dazu verwendet werden, das Wissen und die Erfahrungen zu sammeln und zu verbreiten.
Im Testbed gewonnene Erfahrungen und entstandene Dokumentationen der Umsetzung können für andere hilfreich sein. Die dort verwendeten Betriebsparameter und Testwerte sollten dokumentiert und veröffentlicht werden.

Regelmäßige DNSSEC-Gesprächsrunden sollen dafür sorgen, dass ein permanenter Erfahrungsaustausch stattfindet.

4 Projektplan

Das Projekt wird von BSI, eco und DENIC gemeinsam koordiniert und zum Projektfortschritt werden regelmäßige Abstimmungsrunden durchgeführt.

Die Zeitangaben bei den einzelnen Schritten basieren auf Schätzungen. Zuverlässige und belastbare Zeiten können erst im Gespräch mit den jeweils ausführenden Teilnehmern erhoben werden. Die angegebenen Startdaten beziehen sich auf einen angenommenen Beginn der Aktivitäten am 1.7.2009.

Beginn	Maßnahme	Dauer	Verantwortlich		
			BSI	eco	DENIC
24.4.2009	Diskussion BSI, eco, DENIC – Finalisierung Abstimmungspapier	4 W	B	B	B
2.7.2009	Intitiales Meeting zum Thema für alle am Thema aktiven Teilnehmer (DENIC, Registrare, Provider, Vertreter der Behörden, Vertreter der Anbieter) - Sensibilisierung der Teilnehmer - Motivation zur Teilnahme - Planung des weiteren Vorgehens		B	B	D

Beginn	Maßnahme	Dauer	Verantwortlich		
			BSI	eco	DENIC
	- Erste Vorstellung der Rahmenplanung des Testbeds - Erste Verteilung von Actionitems Einholen der Bereitschaft von Registraren, Providern und interessierten „Early-Usern“, am Testbetrieb aktiv mitzuarbeiten				
07 2009	Übersicht über die in Deutschland verbreiteten Endgeräte, ADSL- und Kabelrouter und ihre DNSSEC-Eignung erstellen - Auswahl der im Test zu betrachtenden Geräte - Test und Auswertung der Ergebnisse - Kontakte und Gespräche mit Herstellern zur Lösung der im Test aufgetretene Probleme - Veröffentlichung eines Ergebnisdokuments	6 M	D		
07 2009	Sammlung von Software mit spezieller DNSSEC-Unterstützung (optionales Zusatzprojekt) - Sammlung von existierender Software mit DNSSEC-Erweiterungen (Browser-Plugins, Anzeigemodule, SQUID-Erweiterungen, Mailserver-Erweiterungen, usw.) - Kontakte und Gespräche mit Herstellern zur Lösung der im Test aufgetretene Probleme - Erstellung von Modulen mit deutscher Bedienoberfläche - Test und Erprobung von Endanwender-Software - Test und Auswertung der Ergebnisse - Veröffentlichung eines Ergebnisdokuments				
07 2009	Betrachtung ökonomischer Auswirkungen und Marktrelevanz von DNSSEC, ggf. Erstellung Studie.	8 M	(D)	(D)	
07 2009	Aufbau einer produktiven DNSSEC-Testumgebung - Bereitstellung der parallelen Server-Struktur für DNSSEC für .de	8 M			D
07 2009	Aufbau einer produktiven DNSSEC-Testumgebung - Erweiterung der Registry/Registrar-Schnittstelle für DS-Records	8 M			D
07 2009	Bei am Testbed teilnehmenden Registraren mit DNS-Service: Implementierung von Werkzeugen zum Signieren von gehosteten Domains - Erweiterungen für Schlüssel in den Kundendatenbanken - Erweiterung des Benutzerinterfaces zur Verwaltung von DNSSEC (Ein- und Ausschalten, Key-Rollover) - Hosten von signierten Domains (eventuell auf paralleler DNSServer-Struktur) - Übergabe von DS-Records an die DENIC	18 M			K

Beginn	Maßnahme	Dauer	Verantwortlich		
			BSI	eco	DENIC
07 2009	Bei am Testbed teilnehmenden Registraren ohne DNS-Service: - Erweiterungen für DS-Records in den Kundendatenbanken - Erweiterung des Benutzerinterfaces zur Eingabe von DS-Records durch die Kunden - Übergabe von DS-Records an die DENIC - Zusätzlich ist die Teilnahme von einzelnen (großen) Endkunden mit Signierung entsprechender Zonen sinnvoll (siehe auch Abschnitt 5.2.3)	18 M			K
12 2009	Zweites Meeting zum Thema für alle am Thema aktiven Teilnehmer (DENIC, Registrare, Provider, Vertreter der Behörden, Vertreter der Anbieter) - Berichte vom Stand der Aktivitäten und Implementierungen von verschiedenen Teilnehmern - Präsentation von Zwischenergebnissen		B	B	K
01 2010	Nutzung der produktiven DNSSEC-Testumgebung durch ISPs: - Implementieren eines parallelen validierenden Zweigs von Caching-Nameservern - Umlenken von Anwendern auf das Testbed	12 M		K	
07 2010	Drittes Meeting zum Thema für alle am Thema aktiven Teilnehmer (DENIC, Registrare, Provider, Vertreter der Behörden, Vertreter der Anbieter) - Berichte vom Stand der Aktivitäten und Implementierungen von verschiedenen Teilnehmern - Präsentation von Zwischenergebnissen		B	B	K
12 2010	Viertes Meeting zum Thema für alle am Thema aktiven Teilnehmer (DENIC, Registrare, Provider, Vertreter der Behörden, Vertreter der Anbieter) - Berichte vom Stand der Aktivitäten und Implementierungen von verschiedenen Teilnehmern - Präsentation von Ergebnissen - Sammlung der Punkte und Empfehlungen zur Erstellung des Abschlussberichts		B	B	K
1.1.2011	Auswertung der Testergebnisse Erstellung des Abschlussberichts	3 M	B	B	K
Q2 2011	Fünftes Meeting zum Thema für alle am Thema aktiven Teilnehmer (DENIC, Registrare, Provider, Vertreter der Behörden, Vertreter der Anbieter) - Präsentation und Diskussion des Abschlussberichts sowie des weiteren Vorgehens		B	B	K

B = Beteiligung
K = Koordination
D = Durchführung

5 Abkürzungen und Begriffsdefinitionen

DKIM	DomainKeys Identified Mail, ein Verfahren, bei dem die Herkunft von Mails durch Prüfung von Signaturen im Mailheader an Hand von im DNS hinterlegten Schlüsseln verifiziert wird DNS - Domain Name System
IANA	Internet Assigned Numbers Authority, Zentralstelle für die Vergabe von IP-Nummern, Protokoll-Nummern und AS-Nummern. Ist bei ICANN angesiedelt aufgrund einer vertraglichen Regelung mit dem US Departement of Commerce.
ICANN	Internet Corporation for Assigned Names and Numbers, Zentralstelle des Internets für die Koordination zwecks Adressierung eineindeutiger Nummern und Namen im Internet.
IETF	Internet Engineering Taskforce, entwickelt Internetprotokolle und erarbeitet Standards für den Betrieb des Internets
Provider	Anbieter von Anschlüssen an das Internet.
Registrant	Inhaber einer Domain, der diese über den Registrar bei der Registry anmeldet. Der Registrant kann eigene autoritative Nameserver für eine Domain betreiben oder diesen Dienst von Dritten (ISP, Registrar) beziehen.
Registrar	Dienstleister bei Domainregistratur, hat Kontakt mit dem Domaininhaber, übernimmt die Registrierung einer Domain bei der zuständigen Registry, betreibt teilweise auch als zusätzliche Dienstleistung den Nameservice für Domains
Registry	Zentrale Einrichtung, die Domains einer oder von mehreren Top-Level-Domains verwaltet. Sie nimmt Registrierungen von Domains von Registraren und teilweise auch direkt vom Domaininhaber entgegen. Die Registry betreibt eine Datenbasis, in der alle zu einer Domain notwendigen Daten enthalten sind. Aus der Datenbasis werden die Zonendaten für den Betrieb der autoritativen Nameserver der Zone erzeugt.
SPF	Sender Policy Framework, ein Verfahren, bei dem an Hand von im DNS hinterlegten Schlüsseln und Policy-Beschreibungen die Herkunft von Mails geprüft werden kann
TLD	Top Level Domain, ein Name (Label) im DNS, der auf der obersten Ebene der Hierarchie steht (Beispiele: .de, .com, .eu oder .net)
Zone	Bereich im DNS, der die Daten einer Domain umfasst, die als Einheit verwaltet werden.