



DNSSEC activities in DE

Peter Koch, DENIC eG

DNSSEC Workshop, ICANN 54

Dublin, 2015-10-21

The original news article



Am 30. Juni ist DNSSEC-Day

24.06.15



DNSSEC schließt eine elementare Sicherheitslücke der Internet-Infrastruktur - Webseiten-Abrufe lassen sich damit nicht mehr ohne Weiteres auf präparierte Server umleiten.

DNSSEC ist eine bedeutsame Technik, weil sie DNS-Daten, also essentielle Informationen, die zur Navigation im heutigen Internet gebraucht werden, kryptografisch gegen Fälschungen absichert. Potenzielle Nutznießer sind nicht nur Diensteanbieter wie Energieversorger, Banken oder der Tk-Sektor, sondern auch Anwender: **DNSSEC** stellt sicher, dass der Browser beim Abruf einer Online-Banking-Seite genau die Adresse bekommt, die der Anwender angefragt hat.

Im Kontrast zur Bedeutung steht die Verbreitung: Weltweit führend sind in dieser Hinsicht die Niederlande. Dort sind fast schon 50 Prozent aller Domains signiert, während DNSSEC in Deutschland bisher nicht flächendeckend in Gebrauch ist. Optimistisch stimmt jedoch, dass mit der Postbank ein erstes sicherheitskritisches Unternehmen seine Web-Seiten signiert hat.

Tools



iMonitor

[Netalyzr](#)

[Fernwartung](#)

[Netzwerk-Rechner](#)

[RFCs](#)

[Whois](#)

[Spam-Listen](#)

[Bandbreitenrechner](#)

[MAC-Adressen](#)

[Ping](#)

[Traceroute](#)

[IPv4-Adressen](#)

[DNS-Abfrage](#)

[Meine IP-Adresse](#)

[Punycode](#)

[Webcheck](#)

[IPv6-Adressen](#)

[Übersicht Tools](#)

Anzeige

AKTUELLE MELDUNGEN >>

DNSSEC-Day: Kleine Nachlese



02.07.2015

Das BSI, DENIC und heise online haben am 30. Juni im Rahmen des DNSSEC-Days die Vorteile der Technik vorgestellt und kritische Fragen diskutiert. Für manche unerwartet müssen neue Registrare Kunden künftig DNSSEC anbieten.

Internet-Verwaltung: Kampagne für anonyme Domain-Registrierung



01.07.2015

Über 6000 Nutzer fordern die Internet Corporation for Assigned Names and

The friendly reprint



Deploy360
Programme

[Home](#) | [English](#)



[Home](#)

[START HERE!](#)

[IPv6](#)

[DNSSEC](#)

[Other Topics](#)

[ION Conferences](#)

[Projects](#)

[Blog](#)

[About](#)

Wednesday, June 30, Is "DNSSEC Day" In Germany!

IPv6

[Overview](#)

[Basics](#)

[Case Studies](#)

[Other Sites](#)

[Security](#)

[Statistics](#)

[Training Resources](#)

« [DNSSEC, IPv6, MANRS, and More at ION Cape Town](#)

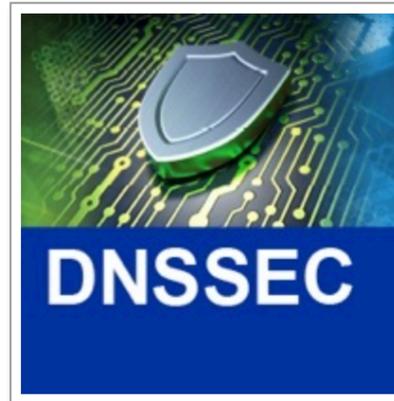
Wednesday, June 30, Is "DNSSEC Day" In Germany!

Want to learn about **DNSSEC** and **DANE** auf Deutsch? On Wednesday, June 30, 2015, a group of organizations in Germany will be streaming live a session called "DNSSEC Day" from 14:00 to 18:00 CEST (UTC+2). Information can be found at:

heise.de/netze/dnssec-day

They say the exact link for the live stream will be published there before the start. The agenda indicates the four-hour live stream will be broken into four parts:

- DNSSEC: Wofür man die Technik braucht. wie sie in Grundzügen funktioniert



Follow Us



Recent Posts

[Wednesday, June 30, Is "DNSSEC Day" In Germany!](#)

[DNSSEC, IPv6, MANRS, and More at ION Cape Town](#)

[Live TODAY – DNSSEC Workshop Streaming From ICANN53 in Buenos Aires](#)

[Watch Live TODAY – DNSSEC For Everybody: A Beginner's Guide at ICANN53](#)

[Congratulations to Argentina On](#)

The inspiring *loyal opposition*



golem.de
IT-NEWS FÜR PROFIS

HOME TICKER VIDEO ABO

TOP-THEMEN: E3 2015 Windows 10 Auto Apple NSA Google mehr...

Suchen

IMHO

DNSSEC ist gescheitert

PR für ein totes Protokoll: Am heutigen 30. Juni wird der DNSSEC-Day begangen. Dabei ist das Protokoll in seiner heutigen Form nahezu nutzlos - und wird es wohl auch bleiben.

Das DNSSEC-Protokoll ist ein inzwischen über 20 Jahre alter Ansatz, um die Sicherheit im Domain Name System (DNS) zu verbessern. Doch durchsetzen konnte sich das Protokoll nie, bis heute ist ein praktischer Nutzen nahezu nicht vorhanden. Dafür gibt es eine Reihe von Gründen - und realistischerweise ist kaum damit zu rechnen, dass sich das irgendwann ändert. DNSSEC ist ein veraltetes, gescheitertes Konzept, das man am besten beerdigen sollte.

Doch ungeachtet seiner Erfolglosigkeit hat DNSSEC einige Fans. Praktisch jedes Mal, wenn auf Golem.de oder anderswo ein Artikel über die Probleme mit TLS-Zertifikaten und Zertifizierungsstellen berichtet wird, fordern Kommentatoren, dass man endlich das auf DNSSEC aufbauende DANE einsetzen müsse, um Zertifikate abzusichern. Das BSI, die für .de-Domains zuständige Denic und der Heise-Verlag haben für [den heutigen 30. Juni einen DNSSEC-Day ausgerufen](#), nach ihren Angaben *"eine Aktion zur Förderung der Internetsicherheit"*.



DNSSEC ist aus heutiger Sicht total veraltet und bringt wenig Vorteile. (Bild: [Oxfordian Kissuth/Wikimedia Commons/CC by-sa 3.0D](#))

Artikel: **IMHO**
DNSSEC ist gescheitert

Inhalt:

- DNSSEC auf Clients praktisch nicht vorhanden
- Schwache Krypto und Reflection-Angriffe
- DNSSEC wird kaum von großen Internetkonzernen unterstützt

Datum: 30.6.2015, 10:24

Autor: Hanno Böck

Themen: DNS, Denic, Ican, Server-Applikationen, Verschlüsselung, Server, Technologie, Applikationen, Internet, Security

Teilen:

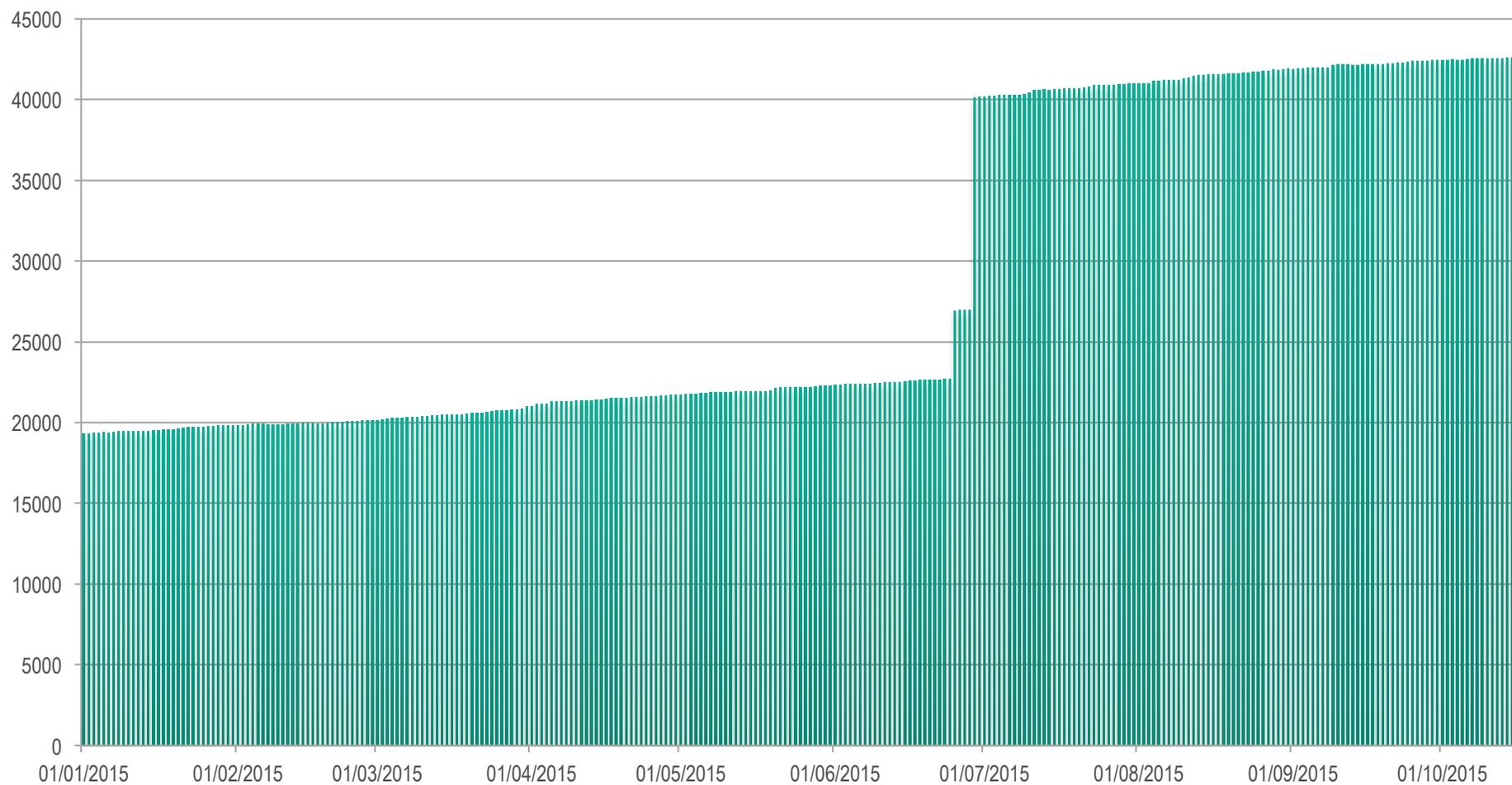


DNSSEC Day – What was it about?

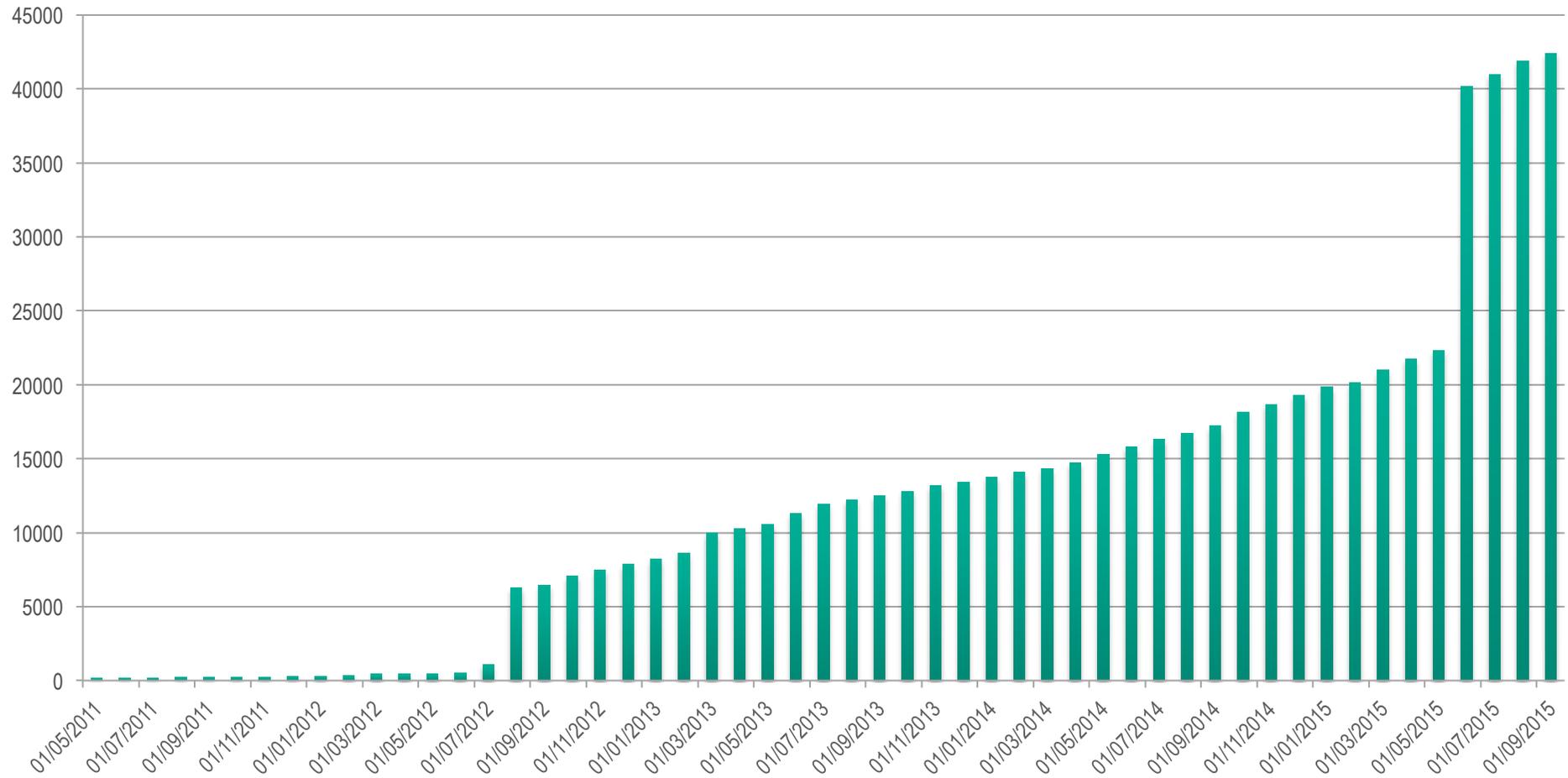


- Organized jointly
 - Heise Media
 - BSI (Fed. Inst. For Information Security)
 - DENIC
 - DANE practitioners
- 4 hours live video panel discussion
 - Questions injected
 - Myths busted
 - Complexity questioned: KSK/ZSK split, automated rollovers
- Background articles
 - Including lists of registrars/resellers

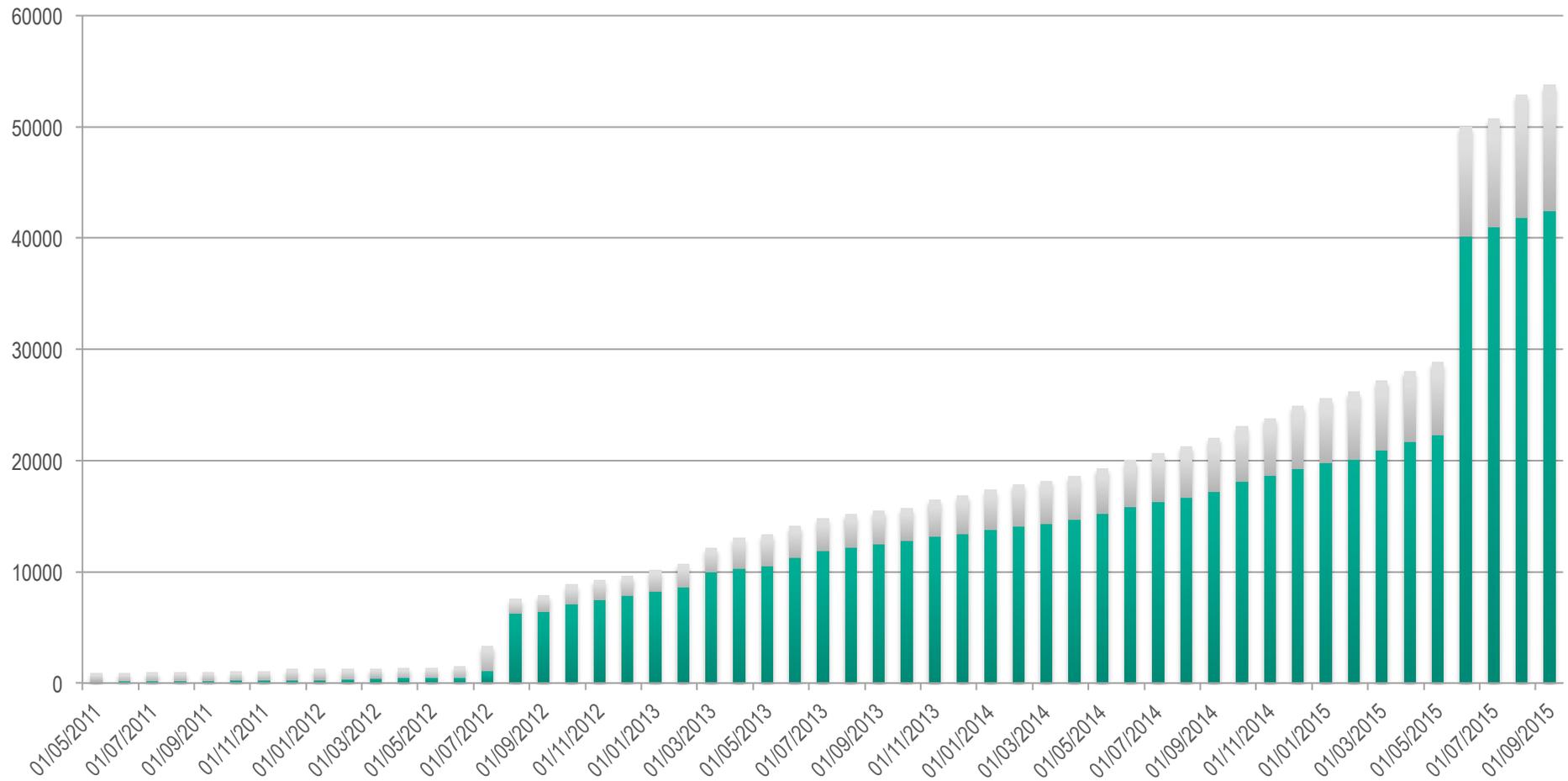
DE DNSSEC domain growth 2015



DE DNSSEC domain growth *ab urbe condita*



Signed vs registered DE domains – mysterious potential



DNSSEC – Who does it?



- Some registrars
 - Full service variant
- Some resellers
 - Used to be smaller ones (50-100 domains)
 - More recently those in the three/four digit range
- „Geeks“
- Security aware companies, sometimes
 - few banks
- Email providers -> DANE!

DNSSEC – What else did we do?



- Added support for elliptic curve crypto
 - GOST, ECDSA/P-256, ECDSA/P-384
 - now cover all current (non deprecated) IETF defined algorithms
- Due to cautious pre delegation checks



Danke!

Q/A

pk@DENIC.DE