



deSEC

...

Free, Secure, and Easy DNS Hosting

Nils Wisiol · 12.02.2019 · Datengarten/97 · CCC Berlin · deseq.io

Section 1

DNS & DNSSEC

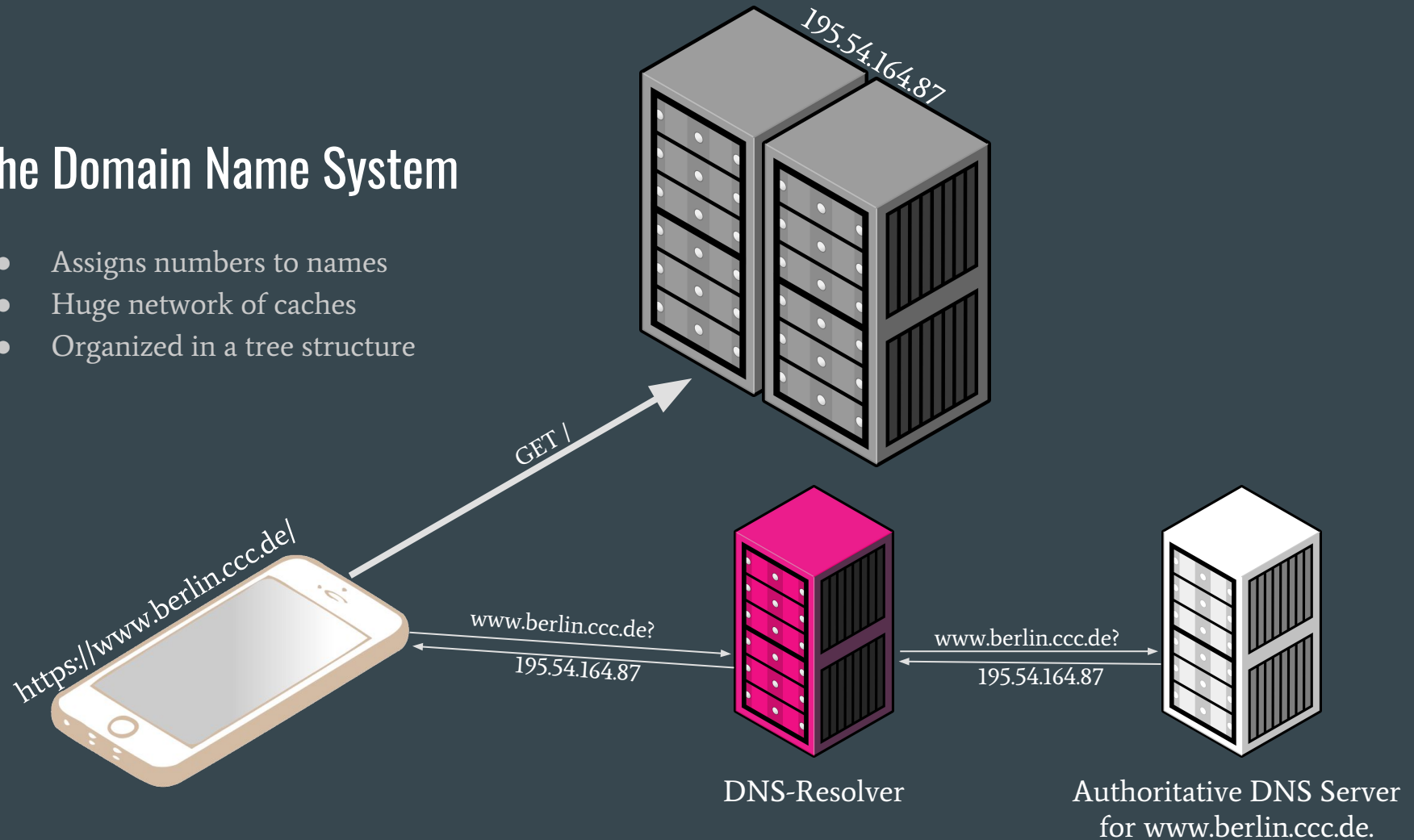
A Bird's-eye View



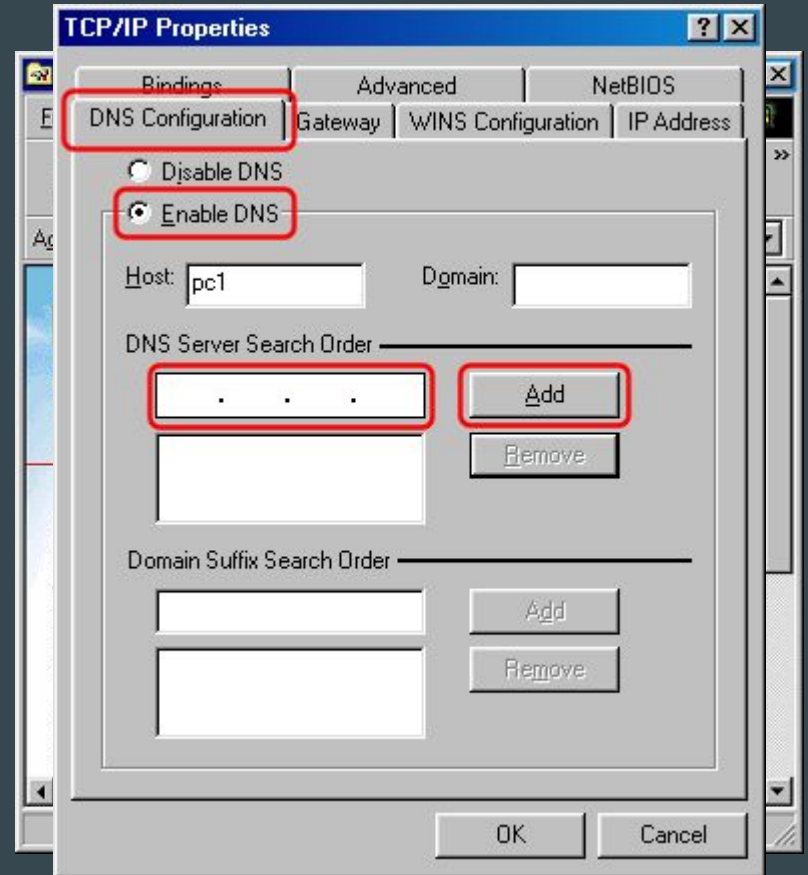
Picture is licensed under the Creative Commons Attribution-Share Alike 3.0 Unported license, cropped to fit slide and colors modified. Original author Bas van Schaik at <https://en.m.wikipedia.org/wiki/File:Ams-ix.k.root-servers.net.jpg>

The Domain Name System

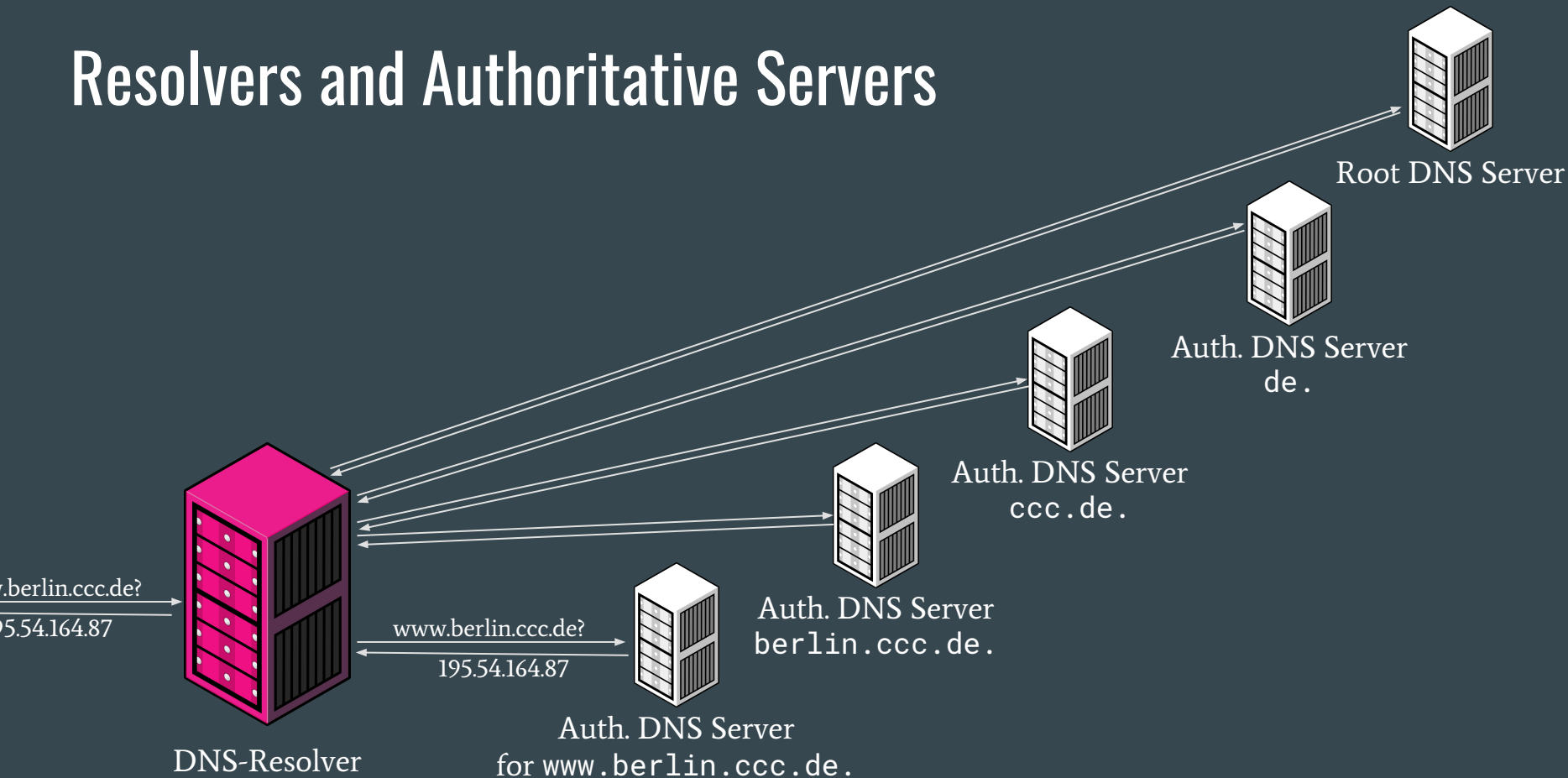
- Assigns numbers to names
- Huge network of caches
- Organized in a tree structure



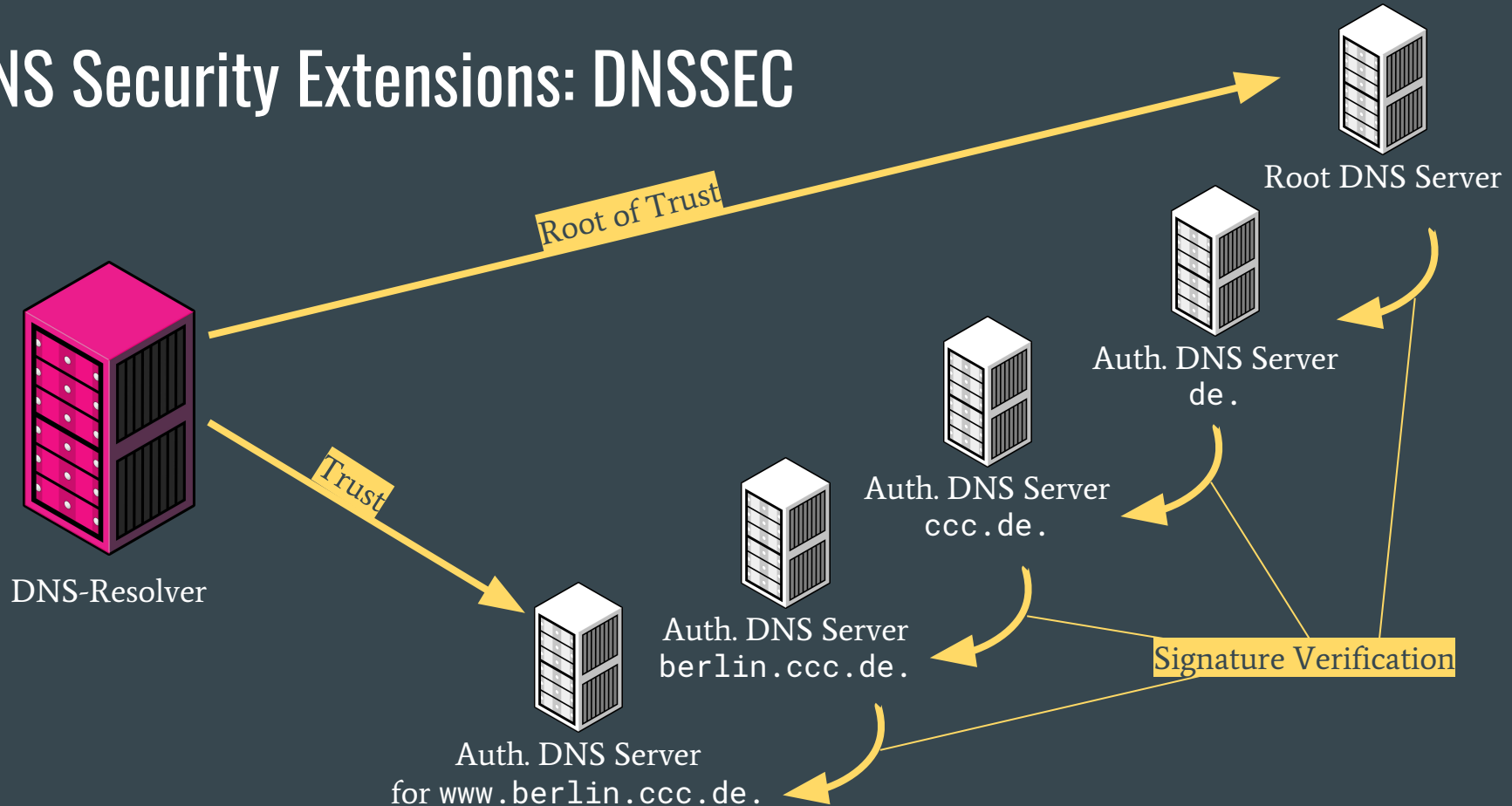
Clients and DNS Resolvers



Resolvers and Authoritative Servers

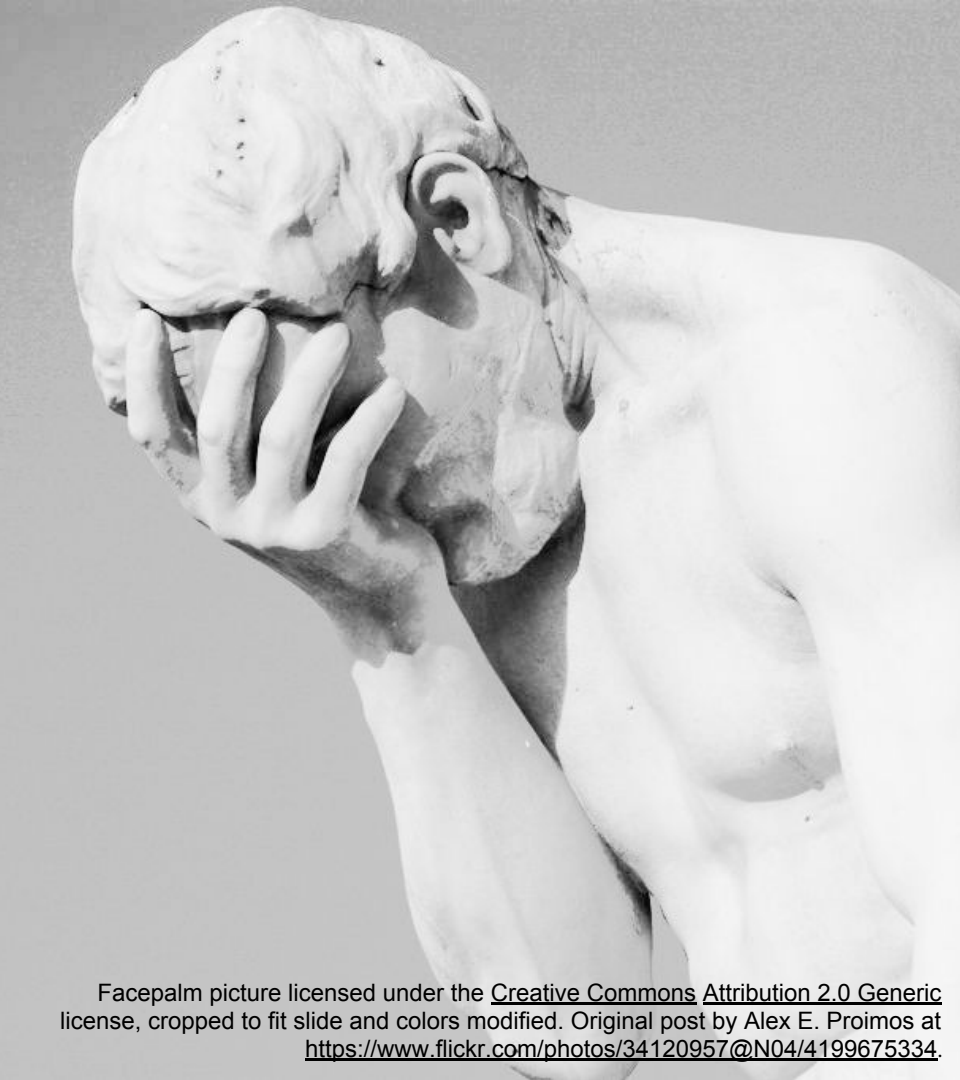


DNS Security Extensions: DNSSEC



Section 2

The State of DNS Security and Usability



Facepalm picture licensed under the [Creative Commons Attribution 2.0 Generic](https://creativecommons.org/licenses/by/2.0/) license, cropped to fit slide and colors modified. Original post by Alex E. Proimos at <https://www.flickr.com/photos/34120957@N04/4199675334>.

Einstellungen

Domainverwaltung

DNS Verwaltung

DNS ändern

DNS löschen

DNS Lookup

Nameserver Verwaltung

Handle Verwaltung

nTLD Vorreservierung

Produktseite

Logout: enita0001

nils-wisiol.de (changed: 2015-03-20 14:19:47)

SOA Data

TTL86400▼hostnamens5.a4a-dns.deemailroot@ns5.a4a-dns.de

Resource Record

TTL86400▼nils-wisiol.deIN NSns5.a4a-dns.deremove ?

Resource Record

TTL86400▼nils-wisiol.deIN NSns6.a4a-dns.deremove ?

Resource Record

TTL86400▼nils-wisiol.deIN A178.63.189.70remove ?

Resource Record

TTL86400▼www.nils-wisiol.deIN A178.63.189.70remove ?

Resource Record

TTL86400▼*.nils-wisiol.deIN A178.63.189.70remove ?

Resource Record

TTL86400▼nils-wisiol.deIN MX10sn4b.deremove ?

Resource Record

TTL86400▼mail.nils-wisiol.deIN A178.63.189.74remove ?

Resource Record

TTL86400▼nils-wisiol.deIN MX20sn7b.deremove ?

ADD Resource Record

TTL86400▼IN A▼priority(MX,SRV)

zurück

speichern

Before we started deSEC, this is how I had to manage my DNS records

Poweradmin						
Index Search zones and records List zones List zone templates List supermasters Add master zone Add slave zone Add supermaster Bulk registration User administration Logout						
Edit zone "berlin.de"						
<div>Show page: 123456</div>						
	Id	Name	Type	Content	Priority	TTL
	3	berlin.de	SOA	berlin.de. 2018120600 6040 864 3600000 6040		360
	147	berlin.de	NS	berlin.de	0	360
	149	tu-berlin.de	NS	berlin.de	0	360
	11	sen-berlin.de	NS	berlin.de	0	360
	13	berlin.de	NS	berlin.de	0	360
	15	berlin.de	A	139	0	360
	17	berlin.de	A	178	0	360
	19	ap-berlin.de	CNAME	ap-berlin.de	0	360
	21	berlin.de	CNAME	berlin.de	0	360
	35	tu-berlin.de	A	15	0	360
	23	berlin.de	A	7	0	360
	25	berlin.de	A	63	0	360
	27	berlin.de	A	31	0	360
	97	berlin.de	A	159	0	360
	105	berlin.de	A	135	0	360
	371	berlin.de	A	191	0	360
	29	berlin.de	CNAME	berlin.de	0	360
	31	berlin.de	A	97	0	360

Another way to do it



Open Access

Open Journal of Web Technologies (OJWT)
Volume 5, Issue 1, 2018

<http://www.ronpub.com/ojwt>
ISSN 2199-188X

Hijacking DNS Subdomains via Subzone Registration: A Case for Signed Zones

Peter Thomassen, Jan Benninger, Marian Margraf

Freie Universität Berlin, Takustr. 9, 14195 Berlin, Germany
{peter.thomassen, jan.benninger, marian.margraf}@fu-berlin.de

ABSTRACT

We investigate how the widespread absence of signatures in DNS (Domain Name System) delegations, in combination with a common misunderstanding with regards to the DNS specification, has led to insecure deployments of authoritative DNS servers which allow for hijacking of subdomains without the domain owner's consent. This, in turn, enables the attacker to perform effective man-in-the-middle attacks on the victim's online services, including TLS (Transport Layer Security) secured connections, without having to touch the victim's DNS zone or leaving a trace on the machine providing the compromised service, such as the web or mail server. Following the practice of responsible disclosure, we present examples of such insecure deployments and suggest remedies for the problem. Most prominently, DNSSEC (Domain Name System Security Extensions) can be used to turn the problem from an integrity breach into a denial-of-service issue, while more thorough user management resolves the issue completely.

TYPE OF PAPER AND KEYWORDS

Regular research paper: DNS, security, domain, subdomain, zone, man in the middle, TLS certificate, ACME DNS

1 INTRODUCTION

Before a connection to a named Internet host (e.g. www.fu-berlin.de) can be established, it is necessary to determine the IP address associated with the host name. This lookup is done using the Domain Name System

with a myriad of Internet access providers maintaining their own caches. Thus, the correct operation of an authoritative DNS service is a non-trivial task.

Furthermore, while being initially intended and still primarily used for IP lookups, the DNS has been seeing growing use for other domain related purposes [10]. A

When we started deSEC, this is how we were able to take over DNS zones and issue Let's Encrypt certificates for a couple of zones hosted by affected providers

*This is how we let US companies
decide what's acceptable speech
and what is not*

The screenshot shows a web browser window displaying a blog post on the Cloudflare website. The browser's address bar shows the URL <https://blog.cloudflare.com/why-we-terminated-daily-stormer>. The Cloudflare logo and navigation links (BLOG, WHAT WE DO, SUPPORT, COMMUNITY) are at the top. The article title is "Why We Terminated Daily Stormer" by Matthew Prince, dated 16 Aug 2017. The article text discusses Cloudflare's decision to terminate the account of the Daily Stormer website. On the right side, there is a search bar, a list of categories with arrows, and a subscription form with a "Subscribe to this blog" button.

Why We Terminated Daily Stormer

16 Aug 2017 by [Matthew Prince](#).

[Tweet](#)

Earlier today, Cloudflare terminated the account of the Daily Stormer. We've stopped proxying their traffic and stopped answering DNS requests for their sites. We've taken measures to ensure that they cannot sign up for Cloudflare's services ever again.

Our terms of service reserve the right for us to terminate users of our network at our sole discretion. The tipping point for us making this decision was that the team behind Daily Stormer made the claim that we were secretly supporters of their ideology.

Our team has been thorough and have had thoughtful discussions for years about what the right policy was on censoring. Like a lot of people, we've felt angry at these hateful people for a long time but we have followed the law and remained content neutral as a network. We could not remain neutral

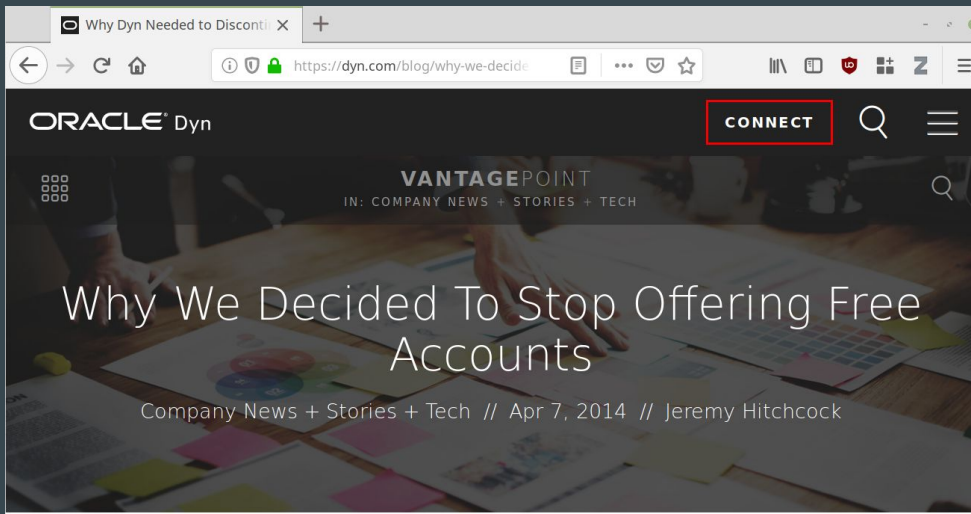
Search

Categories

- [Product News](#)
- [Security](#)
- [Performance](#)
- [Reliability](#)
- [Network](#)
- [Serverless](#)
- [International](#)
- [Cloudflare Apps](#)

Enter your email address

[Subscribe to this blog](#)



This is how a popular dynamic DNS service closed in 2014

For the last 15 years, all of us at Dyn have taken pride in offering a free version of our Dynamic DNS Pro product. What was originally a product built for a small group of users has blossomed into an exciting technology used around the world.

That is why with mixed emotions we announced the end of that free hostname program today, officially turning down on May 7th.

Of course, the big question when these things happen is, “Why?”

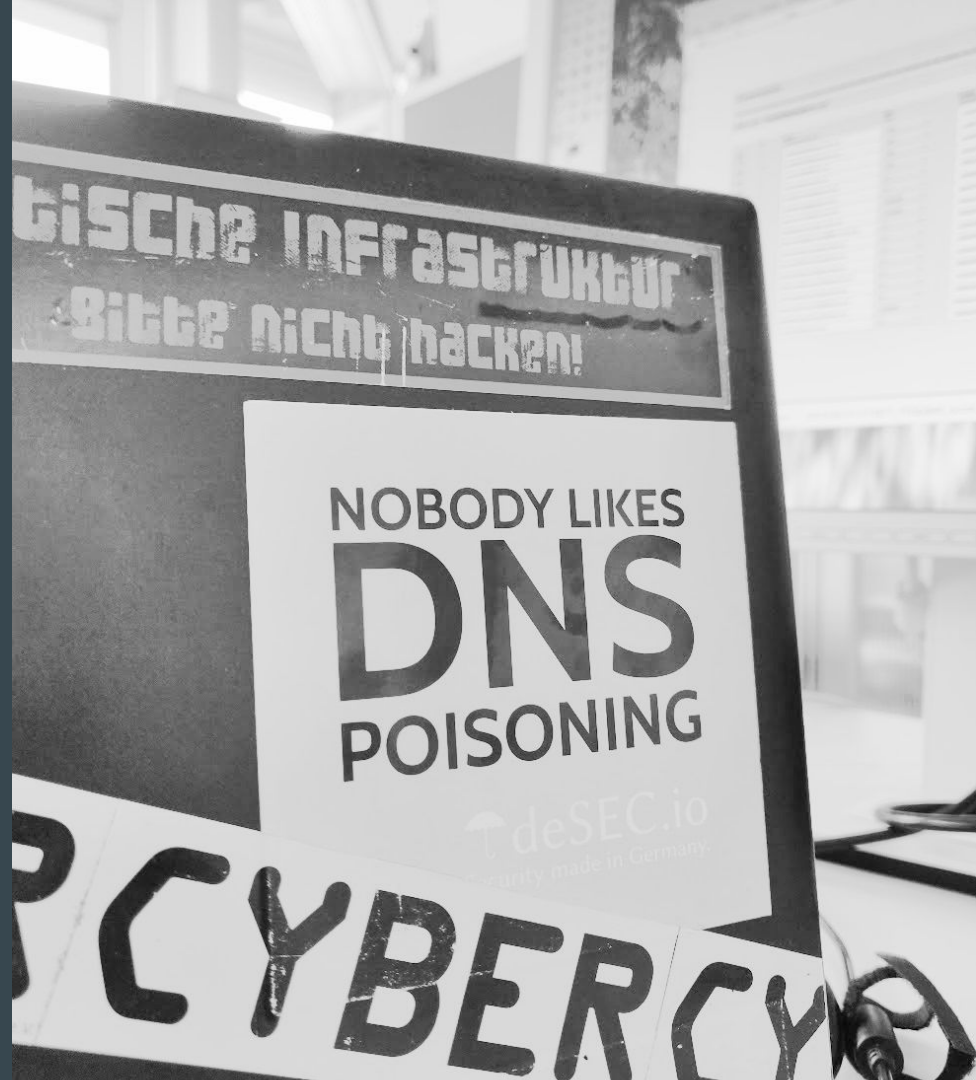
— We have an obligation to have the cleanest DNS network possible. There is a danger to a free infrastructure and over the years, we have seen mixed results from our freemium model. We have seen an increase in abuse and a portion of users violating our trust, so we felt closing this down was the most responsible action we

Things That are Desperately Missing

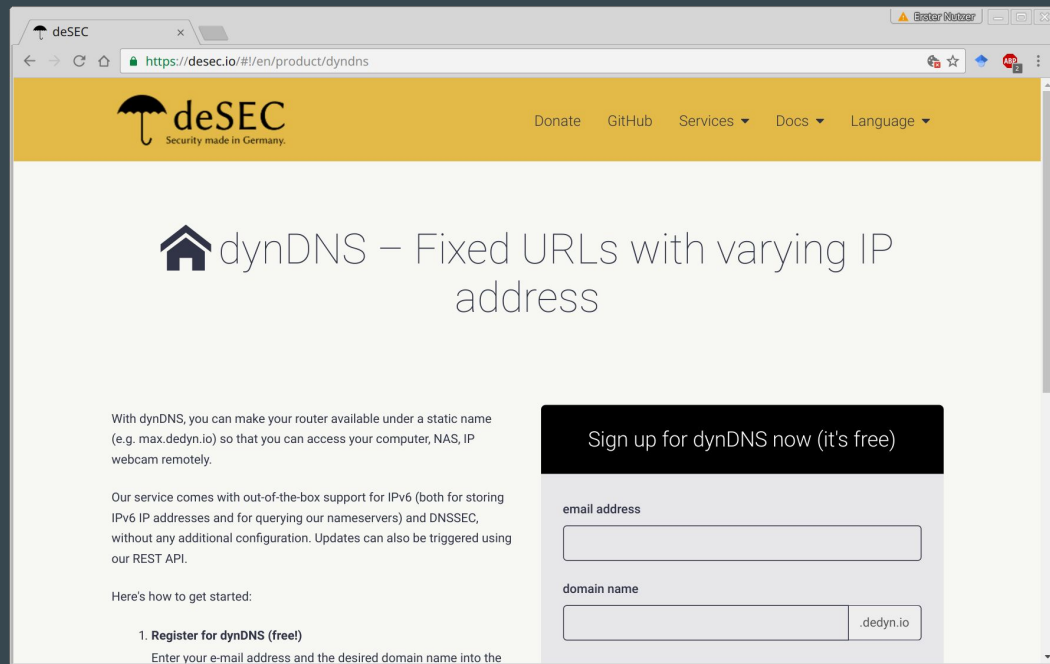
- **Usability**
 - API access
 - Convenience features like search and replace
 - Flexibility in record types and TTLs
- **Security**
 - DNSSEC
- **Organization**
 - Data protection
 - European laws
 - Free open-source software
 - Low cost hosting

Section 3

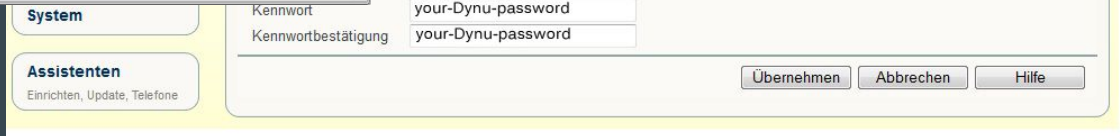
deSEC: DNS Hosting for Everyone



Home Use: Permanently Free Dynamic DNS

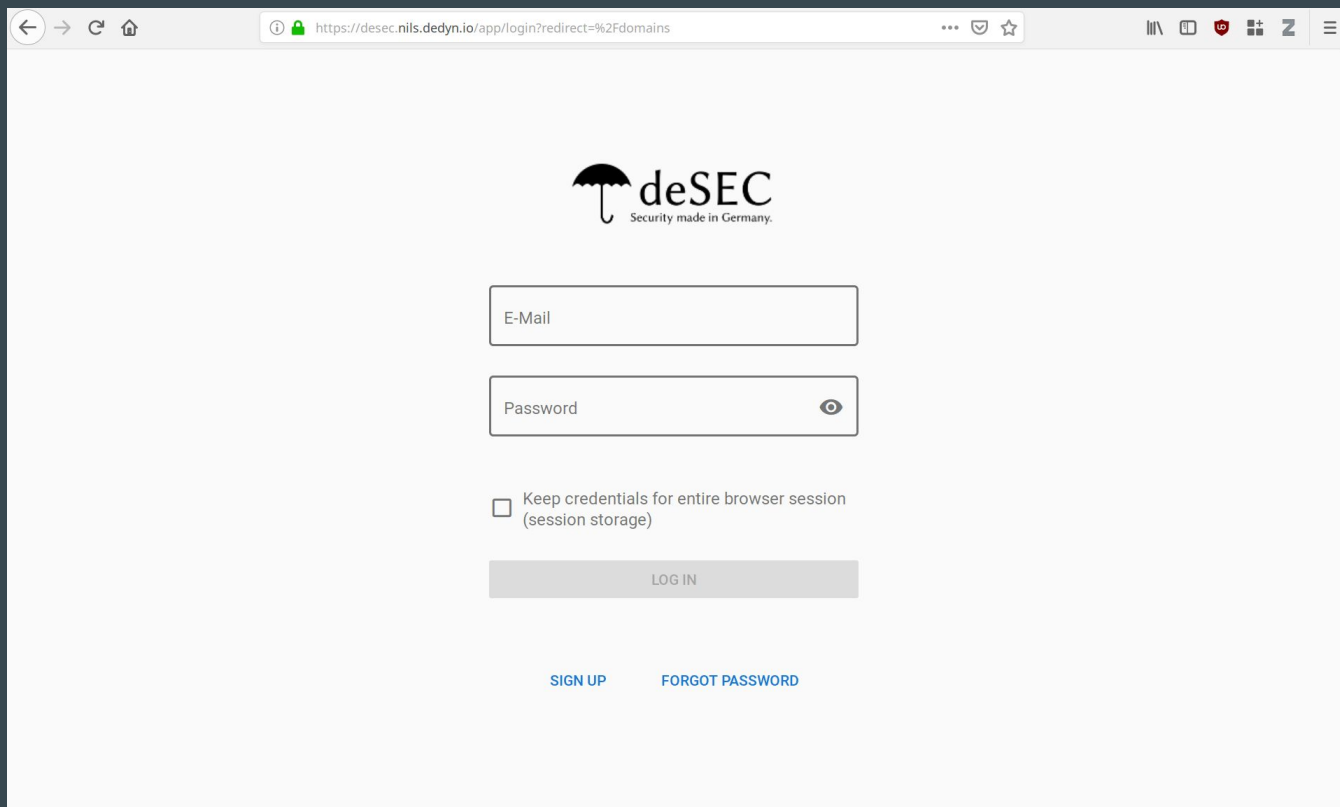


The screenshot shows the deSEC website in a web browser. The URL is <https://desec.io/#/en/product/dyndns>. The page features the deSEC logo (an umbrella) and the tagline "Security made in Germany." in the header. Navigation links include "Donate", "GitHub", "Services", "Docs", and "Language". The main heading is "dynDNS – Fixed URLs with varying IP address". Below this, there is a paragraph explaining the service: "With dynDNS, you can make your router available under a static name (e.g. max.dedyn.io) so that you can access your computer, NAS, IP webcam remotely." Another paragraph states: "Our service comes with out-of-the-box support for IPv6 (both for storing IPv6 IP addresses and for querying our nameservers) and DNSSEC, without any additional configuration. Updates can also be triggered using our REST API." A section titled "Here's how to get started:" includes a numbered list: "1. Register for dynDNS (free!)" followed by the instruction "Enter your e-mail address and the desired domain name into the". A black registration box is overlaid on the page with the text "Sign up for dynDNS now (it's free)". It contains two input fields: "email address" and "domain name", with ".dedyn.io" pre-filled in the domain name field.



The screenshot shows the FRITZ!Box web interface. The top bar is blue with the "FRITZ!Box" logo. Navigation links include "Abmelden", "Ansicht: Experte", "Inhalt", and "Hilfe". Below the top bar, there are tabs for "USB-Speicher", "Fernwartung", "Dynamic DNS", "VPN", and "IPv6". The "Dynamic DNS" tab is selected. The main content area explains that applications and services can be accessed from the Internet using a static IP address. It includes a section for "benutzen" (usage) and a "Neuen Domainnamen anmelden" button. Below this, there are input fields for "your-hostname", "your-Dynu-username", "your-Dynu-password", and "your-Dynu-password" (repeated). At the bottom, there are buttons for "Übernehmen", "Abbrechen", and "Hilfe".

Professional Use: Good-Looking Web Management App



A screenshot of a web browser displaying the login page for deSEC. The browser's address bar shows the URL `https://desec.nils.dedyn.io/app/login?redirect=%2Fdomains`. The page features the deSEC logo, which consists of a black umbrella icon and the text "deSEC" with the tagline "Security made in Germany." below it. The login form includes two input fields: "E-Mail" and "Password". The "Password" field has a toggle icon (an eye) on its right side. Below these fields is a checkbox labeled "Keep credentials for entire browser session (session storage)". A grey "LOG IN" button is positioned below the checkbox. At the bottom of the page, there are two links: "SIGN UP" and "FORGOT PASSWORD".

deSEC
Security made in Germany.

E-Mail

Password

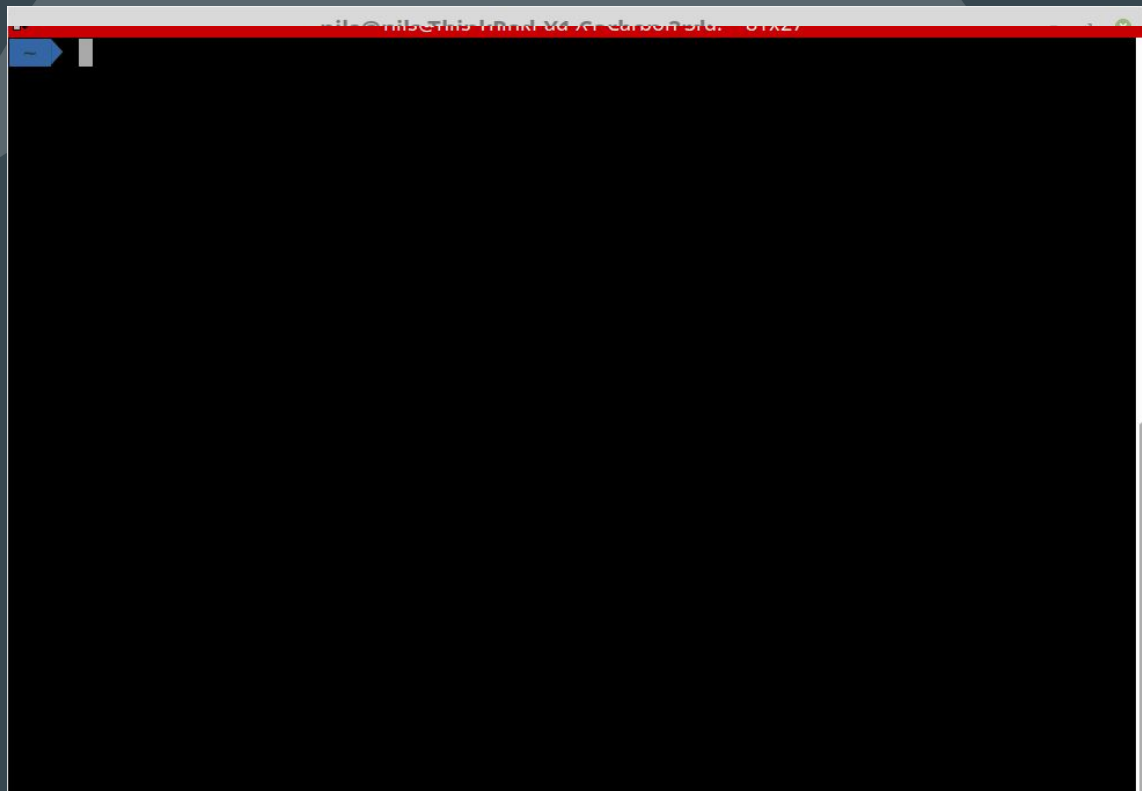
☐ Keep credentials for entire browser session (session storage)

LOG IN

[SIGN UP](#) [FORGOT PASSWORD](#)

Power Use: Easy API Access

- Open to everyone
- Only email-address needed
- Extensive documentation at desec.readthedocs.io
- Support for almost all record types and TTLs
- Automatic DNSSEC for everything
- Let's Encrypt Support, TLSA tools, PGP key, etc. can be build on top



4%

of websites use DNSSEC

19%

of Internet users validate DNSSEC
signatures

Global Delivery, Local Cryptography

- Global anycast network for rapid responses to queries
- Local storage of cryptographic keys



Organisational and Legal

- Based in Berlin
- All source code and discussions on <https://github.com/desec-io/>
- Not-For-Profit *Verein* is underway
- Sponsoring for permanently free hosting is planned
- Built-in data protection



Things That We Can Fix

- **Usability**
 - API Access ✓
 - Convenience features like search and replace planned
 - Flexibility in record types and TTLs ✓
- **Security**
 - DNSSEC ✓
- **Organization**
 - Data protection ✓
 - European laws ✓
 - Free open-source software ✓
 - Low cost hosting ✓

Section 4

Technical Solution

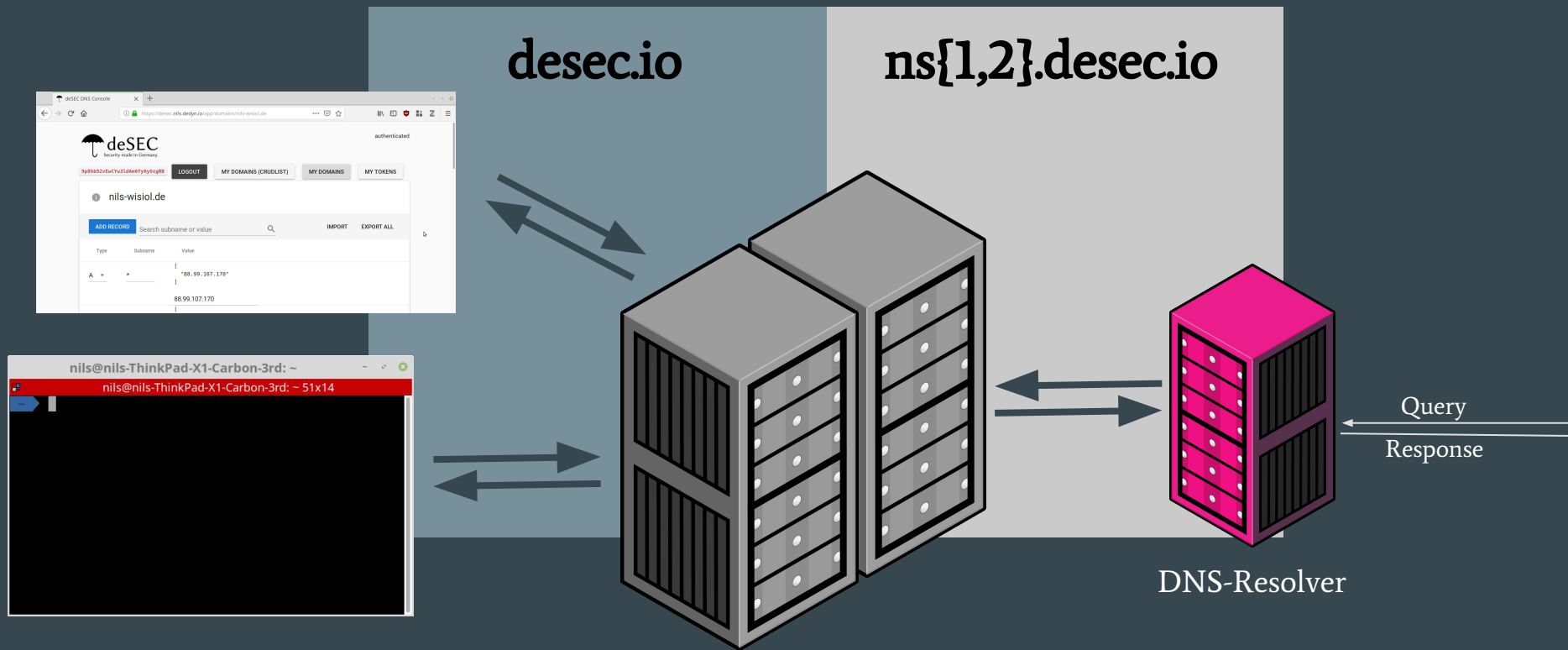
```
services:
  www:
    build: www
    image: desec/dedyn-www:latest
    ports:
      - "80:80"
      - "443:443"
    volumes:
      - ${DESECSTACK_WWW_CERTS}:/etc/ssl/private:ro
      - ./www/html:/usr/share/nginx/html:ro
      - webapp_dist:/usr/share/nginx/html/app:ro
    environment:
      - DESECSTACK_DOMAIN
      - DESECSTACK_WWW_CERTS
      - DESECSTACK_API_DEV=0
      - DESECSTACK_API_PROD=1
    depends_on:
      - static
      - api
    mac_address: 06:42:ac:10:00:80
    networks:
      front:
        ipv4_address: ${DESECSTACK_IPV4_REAR_PREFIX16}.0.128
        ipv6_address: ${DESECSTACK_IPV6_ADDRESS}
      rearwww:
    logging:
      driver: "syslog"
      options:
        tag: "desec/www"
      restart: unless-stopped

  static:
    build: static
    image: desec/dedyn-static:latest
    networks:
      - rearwww
    logging:
      driver: "syslog"
      options:
        tag: "desec/static"
      restart: unless-stopped

  dbapi:
    build: dbapi
    image: desec/dedyn-dbapi:latest
    volumes:
      - dbapi_mysql:/var/lib/mysql
    environment:
      - DESECSTACK_IPV4_REAR_PREFIX16
      - DESECSTACK_DBAPI_PASSWORD_desec
    networks:
      - rearapi2
    logging:
      driver: "syslog"
      options:
        tag: "desec/dbapi"
      restart: unless-stopped

  dblord:
    build: dblord
    image: desec/dedyn-dblord:latest
    volumes:
      - dblord_mysql:/var/lib/mysql
    environment:
      - DESECSTACK_IPV4_REAR_PREFIX16
      - DESECSTACK_DBLORD_PASSWORD_pdns
    networks:
      - rearlord
    logging:
      driver: "syslog"
```

Public Interfaces: HTTP, DNS



Internal Structure

desec.io



ns{1,2}.*.desec.io

Frontend HTTP/TLS Server

Static Web
Content

API

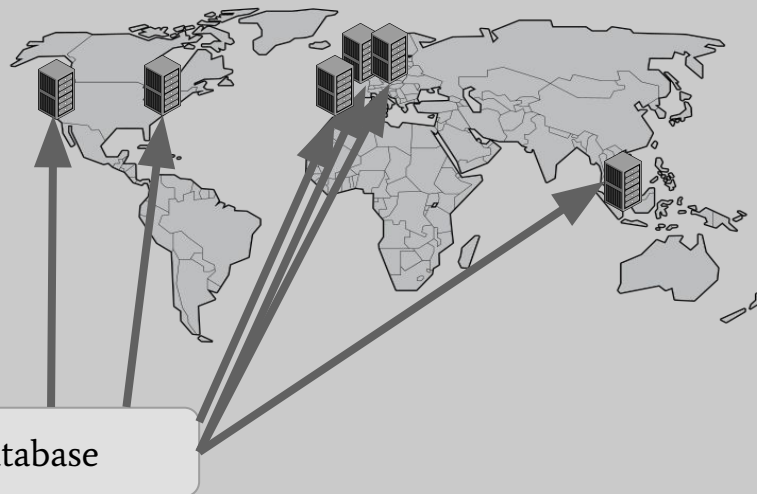
API Database

Signing Server

Private DNS
Database

Master DNS
Server

Public DNS Database



Thank You

<https://desec.io/>

<https://github.com/desec-io/>

Excited? Sign up for our mailing list at desec.io!

12.02.2019 · Datengarten/97 · CCC Berlin

deSEC

Dr. Peter Thomassen

Nils Wisiol

Donations kindly accepted: we take money and code

