

deSEC

...

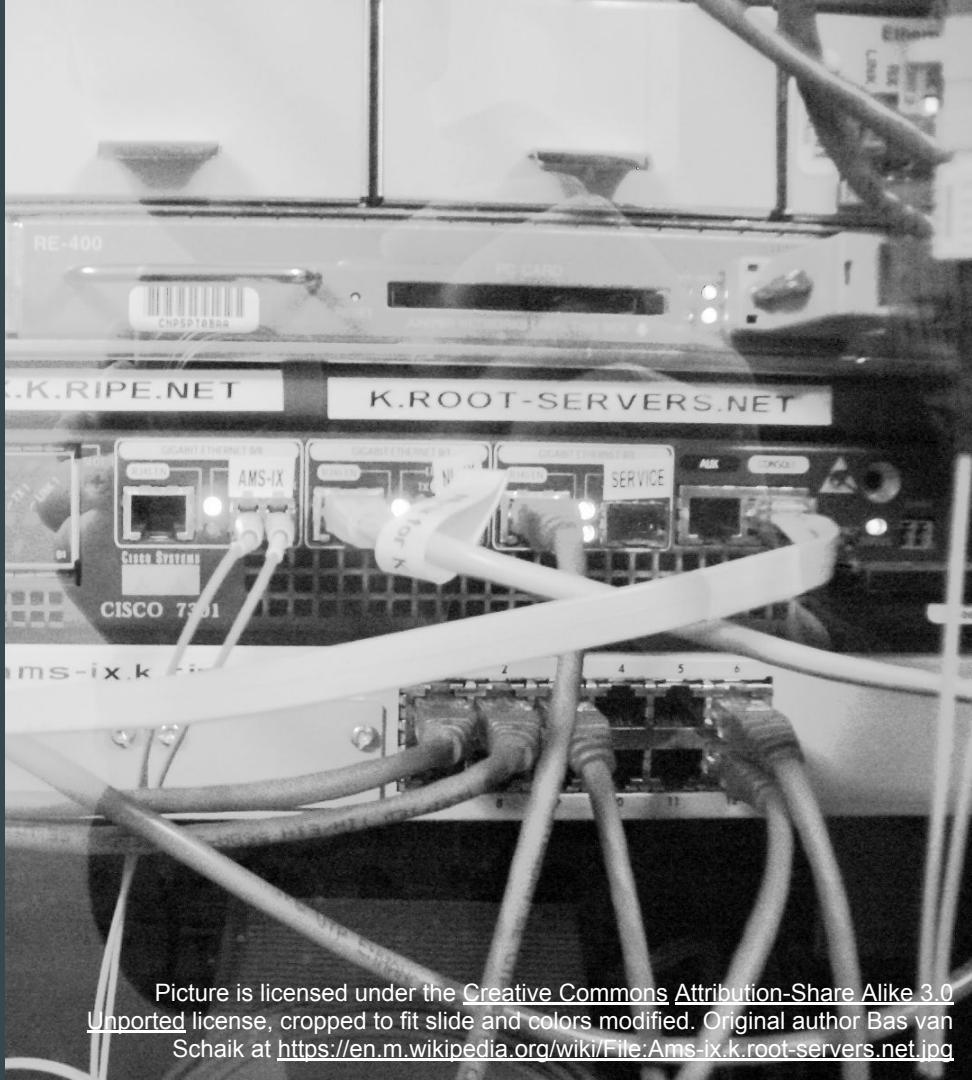
Free, Secure, and Easy DNS Hosting

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

Section 1

DNS & DNSSEC

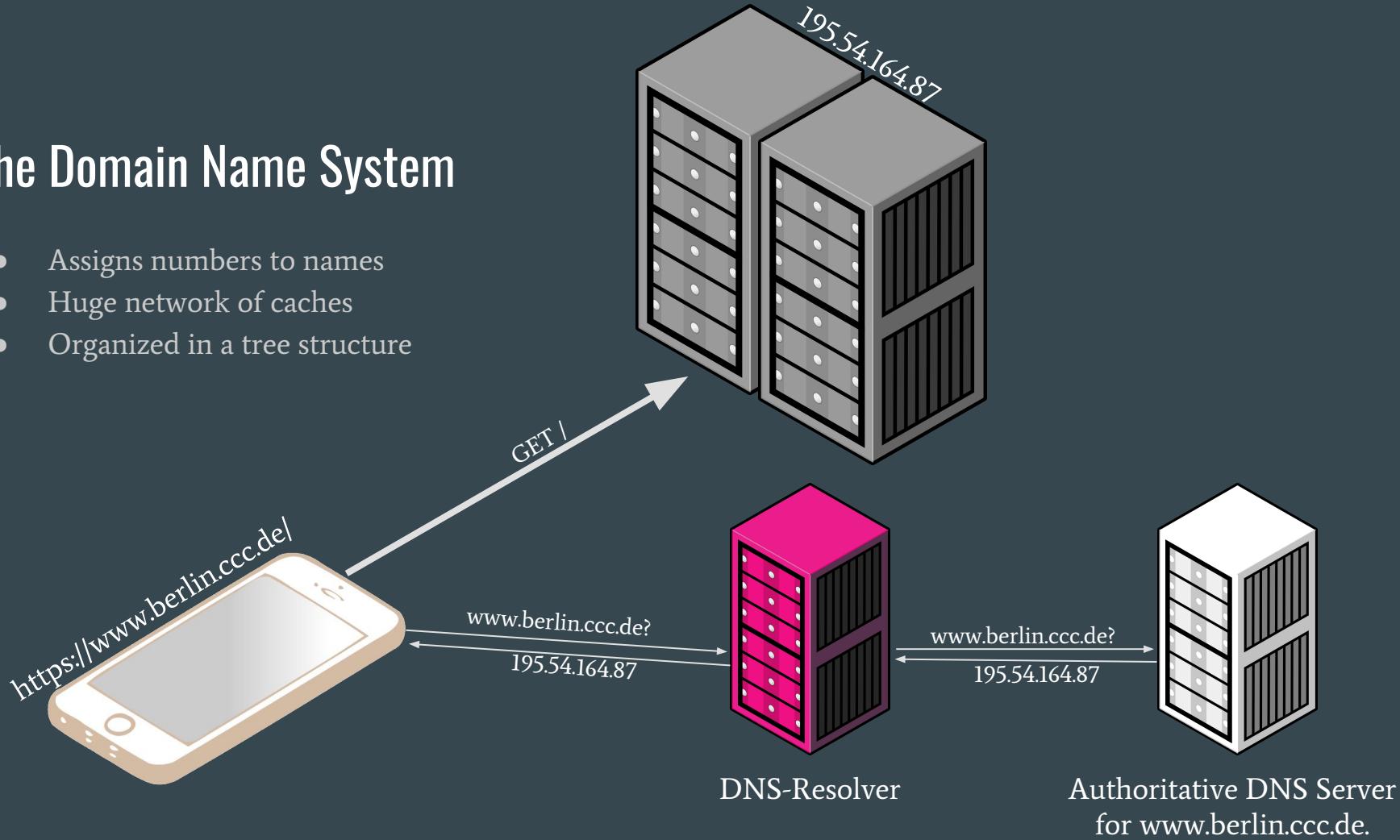
A Bird's-eye View



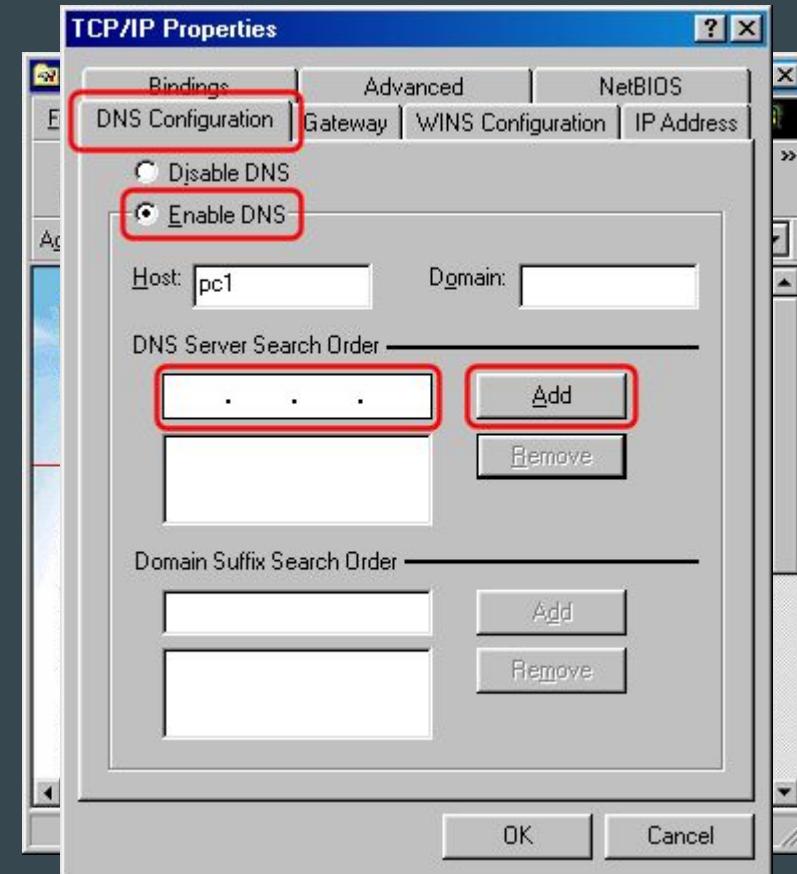
Picture is licensed under the [Creative Commons Attribution-Share Alike 3.0 Unported](#) license, cropped to fit slide and colors modified. Original author Bas van Schaik at <https://en.m.wikipedia.org/wiki/File:AmS-IX.k.root-servers.net.jpg>

The Domain Name System

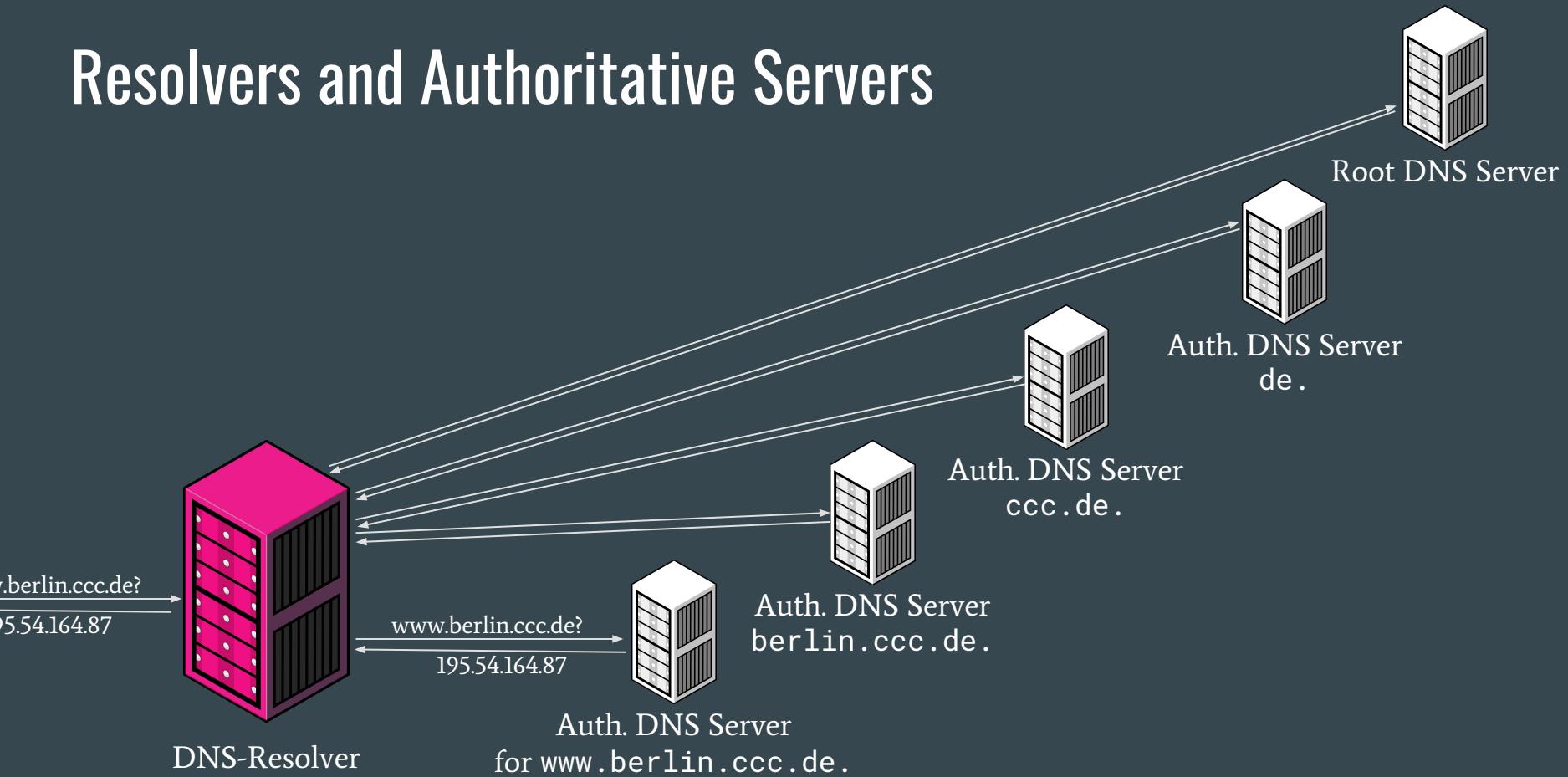
- Assigns numbers to names
- Huge network of caches
- Organized in a tree structure



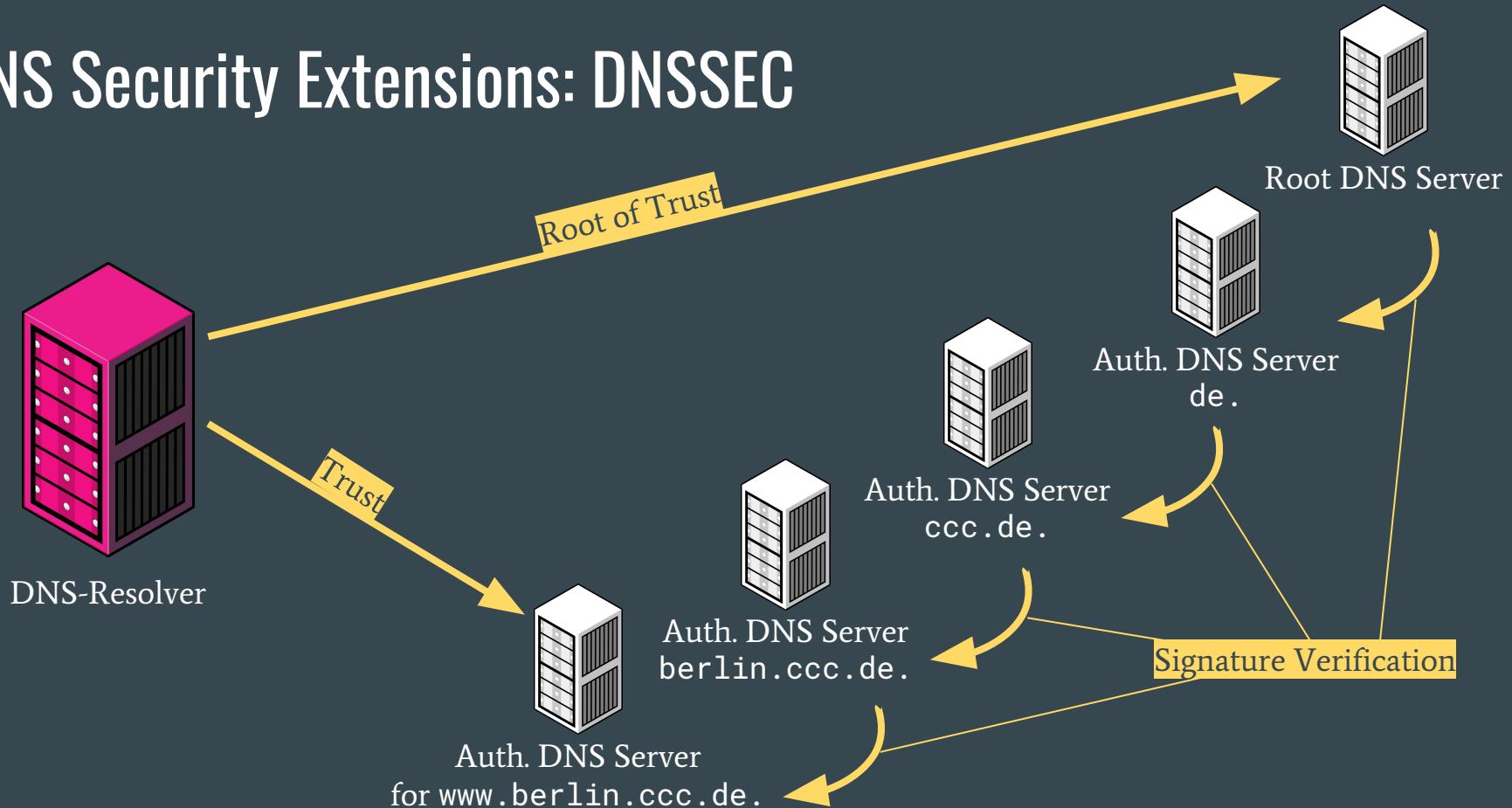
Clients and DNS Resolvers



Resolvers and Authoritative Servers

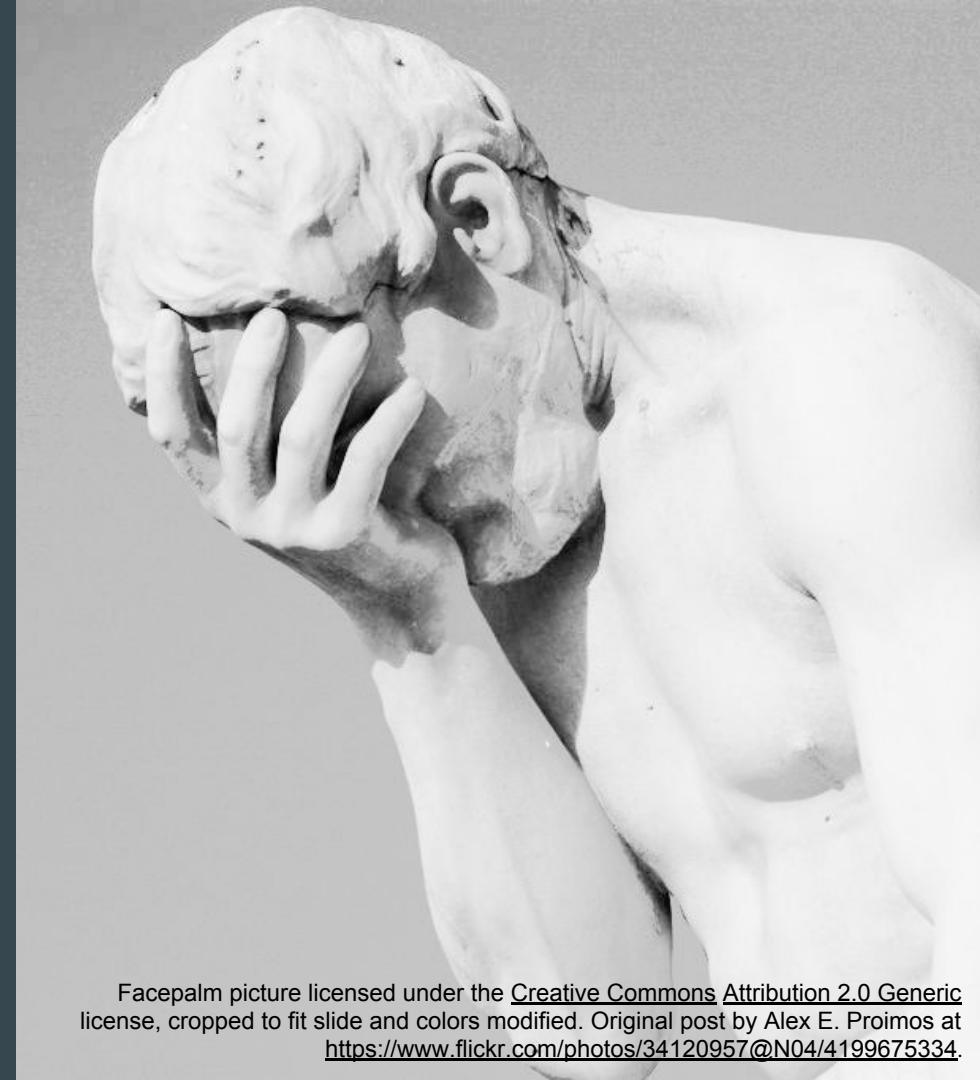


DNS Security Extensions: DNSSEC



Section 2

The State of DNS Security and Usability



Facepalm picture licensed under the [Creative Commons Attribution 2.0 Generic](#) 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	TTL	86400	▼	hostname	ns5.a4a-dns.de	email	root@ns5.a4a-dns.de		
Resource Record	TTL	86400	▼	nils-wisiol.de	IN NS	ns5.a4a-dns.de	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	nils-wisiol.de	IN NS	ns6.a4a-dns.de	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	nils-wisiol.de	IN A	178.63.189.70	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	www.nils-wisiol.de	IN A	178.63.189.70	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	*.nils-wisiol.de	IN A	178.63.189.70	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	nils-wisiol.de	IN MX	10	sn4b.de	remove	<input type="checkbox"/> ?
Resource Record	TTL	86400	▼	mail.nils-wisiol.de	IN A	178.63.189.74	remove	<input type="checkbox"/> ?	
Resource Record	TTL	86400	▼	nils-wisiol.de	IN MX	20	sn7b.de	remove	<input type="checkbox"/> ?
ADD Resource Record	TTL	86400	▼		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

Show page:
[1][2][3][4][5][6]

Id	Name	Type	Content	Priority	TTL
3	soa.berlin.de	SOA	soa.berlin.de. 2018120600 6040 864 3600000 6048	0	360
147	ns.berlin.de	NS	ns.berlin.de	0	360
149	ns2.berlin.de	NS	ns2.berlin.de	0	360
11	www.berlin.de	NS	www.berlin.de	0	360
13	www2.berlin.de	NS	www2.berlin.de	0	360
15	a.berlin.de	A	172.217.178.39	0	360
17	a2.berlin.de	A	172.217.178.1	0	360
19	ap.berlin.de	CNAME	ap.berlin.de	0	360
21	bmcup.berlin.de	CNAME	bmcup.berlin.de	0	360
35	bmcup2.berlin.de	A	172.217.178.15	0	360
23	bmcupold.berlin.de	A	172.217.178.7	0	360
25	bmcup.berlin.de	A	172.217.178.63	0	360
27	bmcup.berlin.de	A	172.217.178.31	0	360
97	bmcup.berlin.de	A	172.217.178.159	0	360
105	bmcup.berlin.de	A	172.217.178.135	0	360
371	bmcup.berlin.de	A	172.217.178.191	0	360
29	bmcup.berlin.de	CNAME	bmcup.berlin.de	0	360
31	can.berlin.de	A	172.217.178.97	0	360

Another way to do it



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, marijan.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

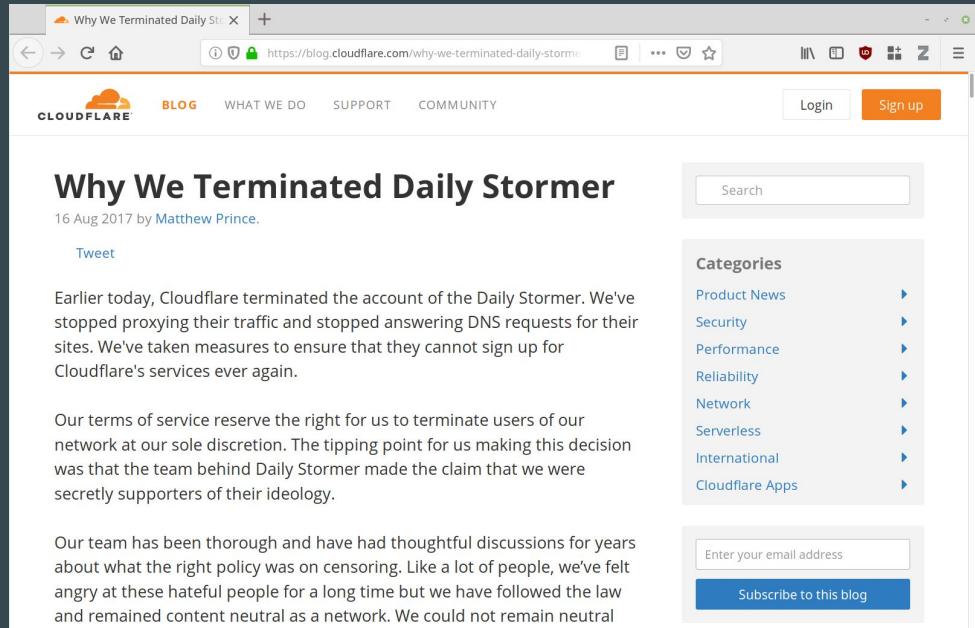
Before a connection to a named Internet host (e.g. www.fu-berlin.de) can be established, it is necessary to determine the IP address associated with the host name. This lookup is done using the Domain Name System

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 displaying a Cloudflare blog post. The title of the post is "Why We Terminated Daily Stormer", written in a large, bold, black font. Below the title, the date "16 Aug 2017" and the author's name "Matthew Prince" are visible. To the right of the main content, there is a sidebar with a "Categories" section containing links to "Product News", "Security", "Performance", "Reliability", "Network", "Serverless", "International", and "Cloudflare Apps". At the bottom of the sidebar, there is a form for entering an email address and 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

Categories

- Product News
- Security
- Performance
- Reliability
- Network
- Serverless
- International
- Cloudflare Apps

Enter your email address

Subscribe to this blog

Why Dyn Needed to Discontinu X +

https://dyn.com/blog/why-we-decide

ORACLE Dyn

VANTAGE POINT
IN: COMPANY NEWS + STORIES + TECH

CONNECT

SEARCH

SEARCH

Why We Decided To Stop Offering Free Accounts

Company News + Stories + Tech // Apr 7, 2014 // Jeremy Hitchcock



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?"

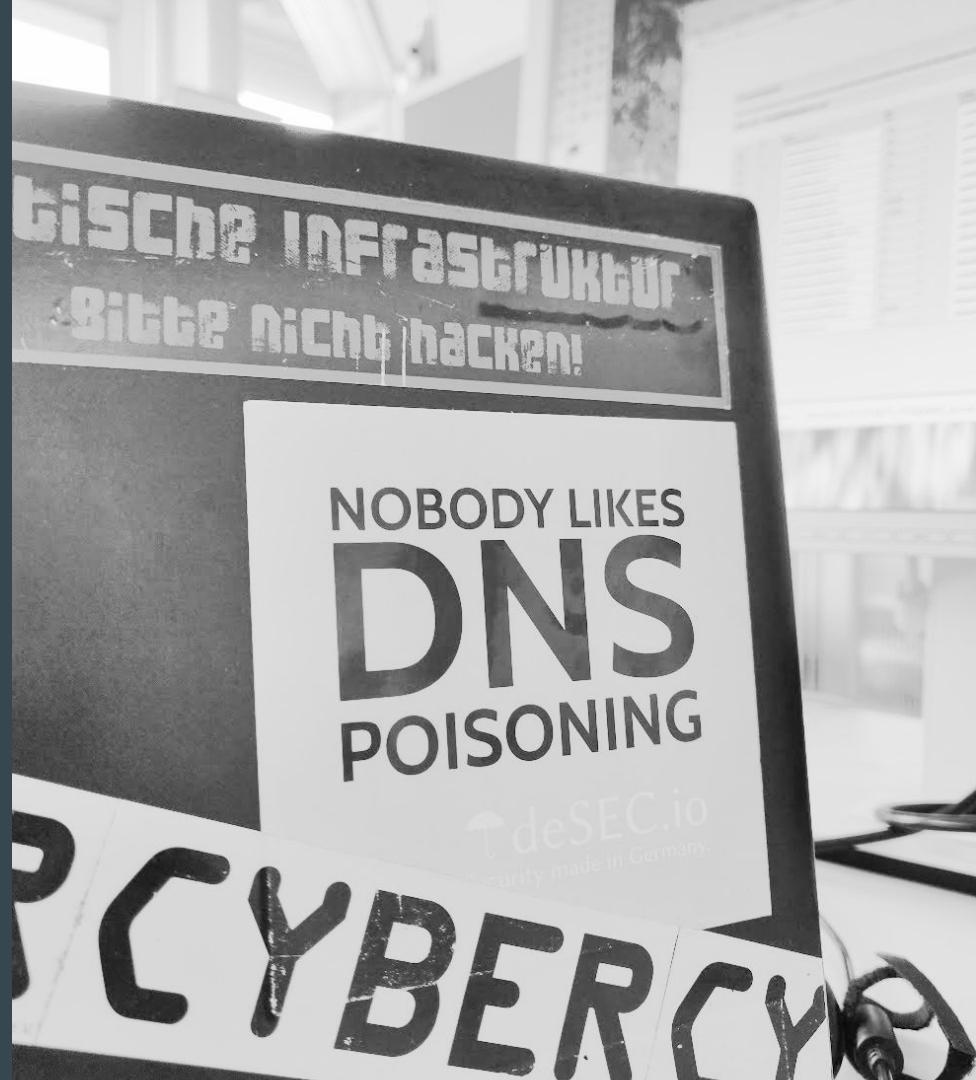
– We have an obligation to have the cleanest DNS network possible. There is a danger to a free infrastructure and over the years, we have seen mixed results from our freemium model. We have seen an increase in abuse and a portion of users

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

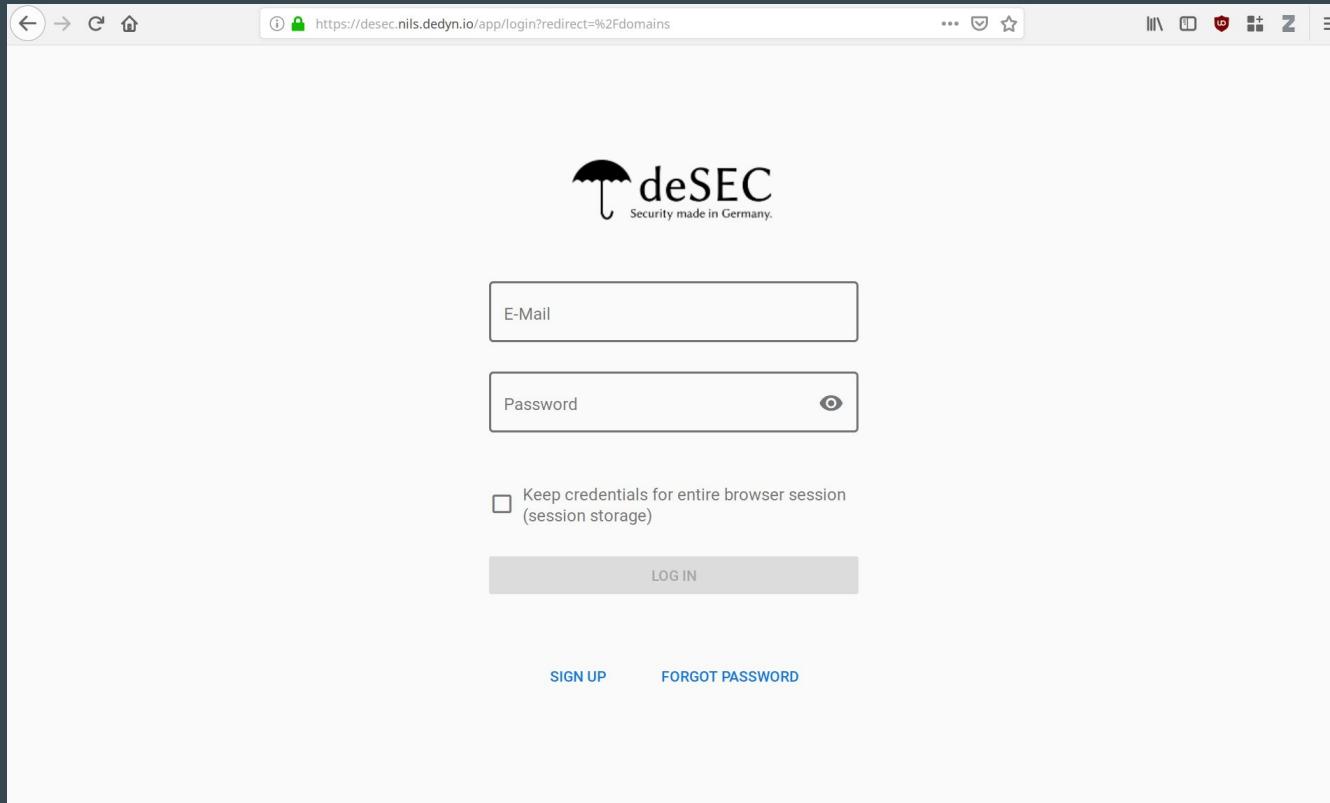
deSEC: DNS Hosting for Everyone



Home Use: Permanently Free Dynamic DNS

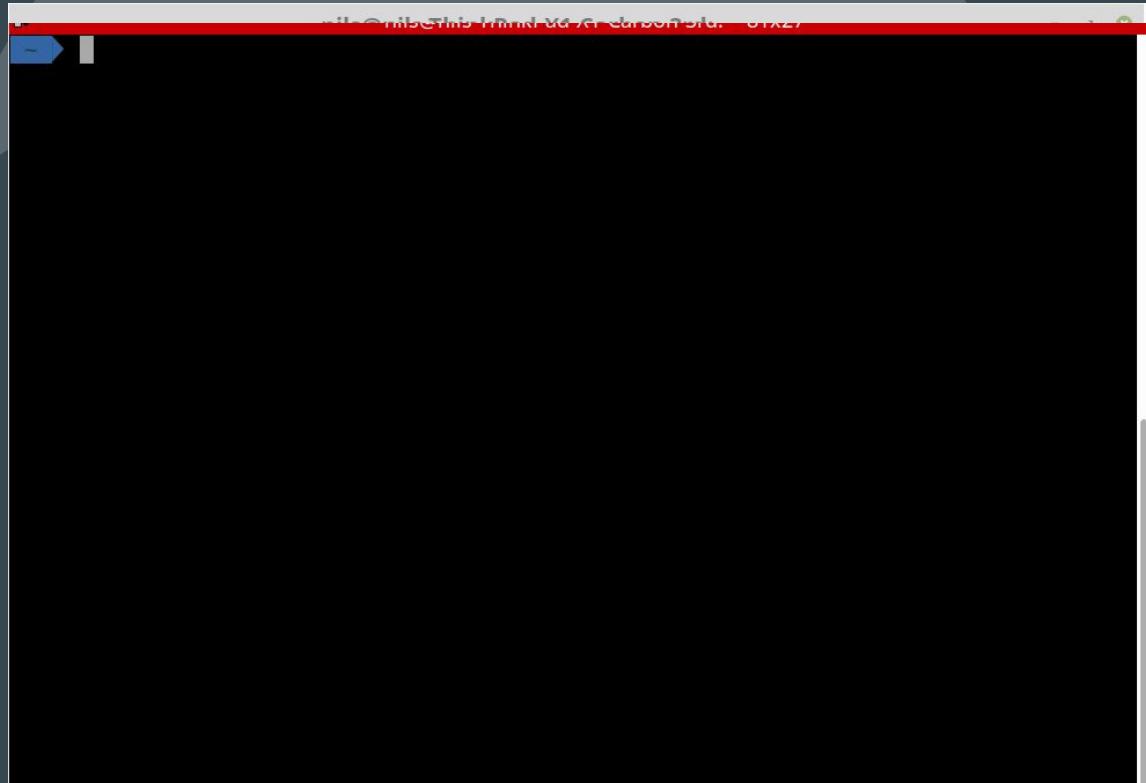
The image shows two screenshots side-by-side. On the left is the deSEC website at <https://desec.io/#!/en/product/dyndns>. The page features a yellow header with the deSEC logo and navigation links for Donate, GitHub, Services, Docs, and Language. The main content area has a house icon and the text "dynDNS – Fixed URLs with varying IP address". Below this is a "Sign up for dynDNS now (it's free)" button with input fields for "email address" and "domain name". A note below the form states: "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 note below that says: "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 "Here's how to get started:" section with a "1. Register for dynDNS (free!)" link and a note: "Enter your e-mail address and the desired domain name into the" is also present. On the right is a screenshot of the FRITZ!Box configuration interface under the "Dynamic DNS" tab. The top navigation bar includes "Abmelden", "Ansicht: Experten", "Inhalt", and "Hilfe". The "Dynamic DNS" tab is selected. The main content area shows fields for "Benutzerdefiniert" (User-defined), "Neuen Domainnamen anmelden" (Register new domain name), "your-hostname", "your-Dynu-username", "your-Dynu-password", and "your-Dynu-password" (repeated). A "Kennwort" (Password) and "Kennwortbestätigung" (Password confirmation) field are also present. A "System" tab is visible at the bottom left, and a "Assistenten" (Assistant) tab is visible at the bottom right.

Professional Use: Good-Looking Web Management App



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



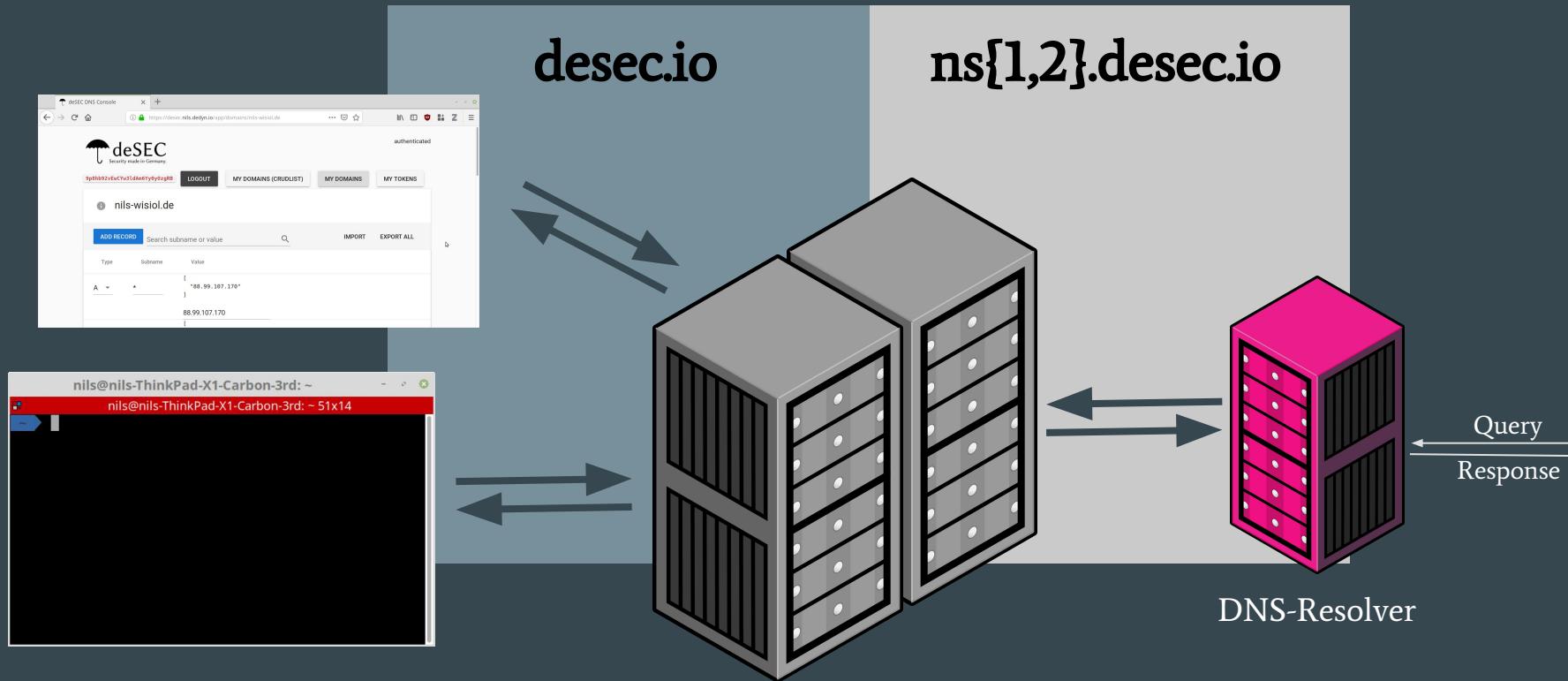
```
www:
  build: www
  image: desec/dedyn-www:latest
  ports:
    - "80:80"
    - "443:443"
  volumes:
    - ${DESECSTACK_WWW_CERTS}:/etc/ssl/private:ro
    - ./www/html:/usr/share/nginx/html:ro
    - webapp_dist:/usr/share/nginx/html/app:ro
  environment:
    - DESECSTACK_DOMAIN
    - DESECSTACK_WWW_CERTS
    - 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:
      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:
    "cyslog"
```

Public Interfaces: HTTP, DNS



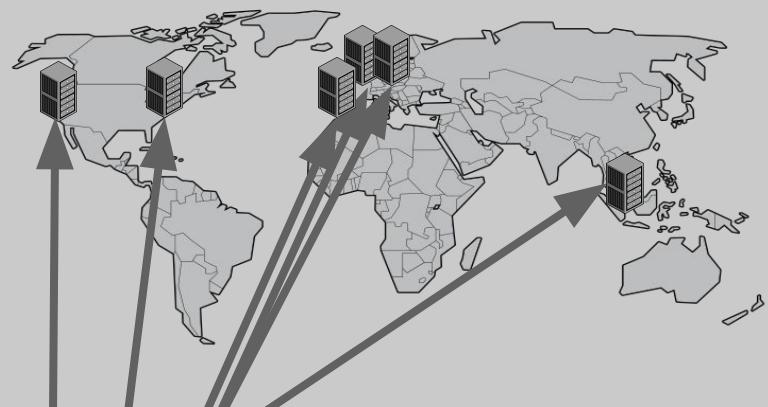
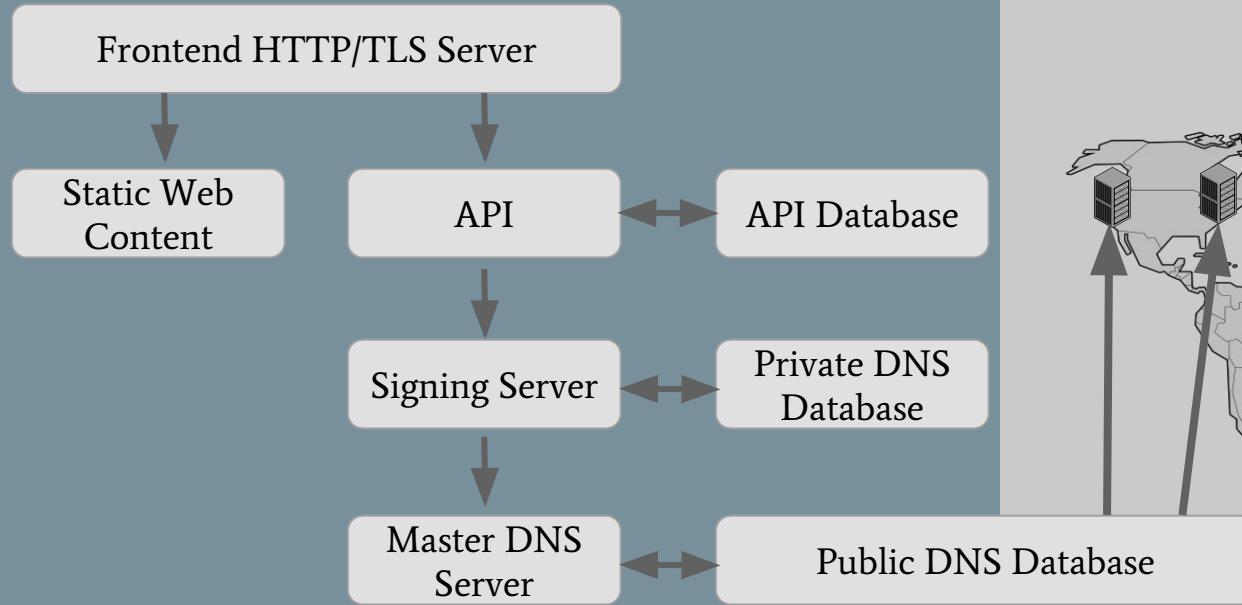
Internal Structure

HTTP
↓

desec.io 



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



Thank You

<https://desec.io/>

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

Excited? Sign up for our mailing list at [desec.io!](https://desec.io/)

12.02.2019 · Datengarten/97 · CCC Berlin

[deSEC](#)

Dr. Peter Thomassen

Nils Wisiol

Donations kindly accepted: we take money and code

