

# deSEC

...

Free, Secure, and Easy DNS Hosting

Peter Thomassen · Nils Wisiol · 7 May 2019 · Crypto Meetup Berlin

[{first name}@desec.io](mailto:{first name}@desec.io)

## Section 1

# DNS & DNSSEC

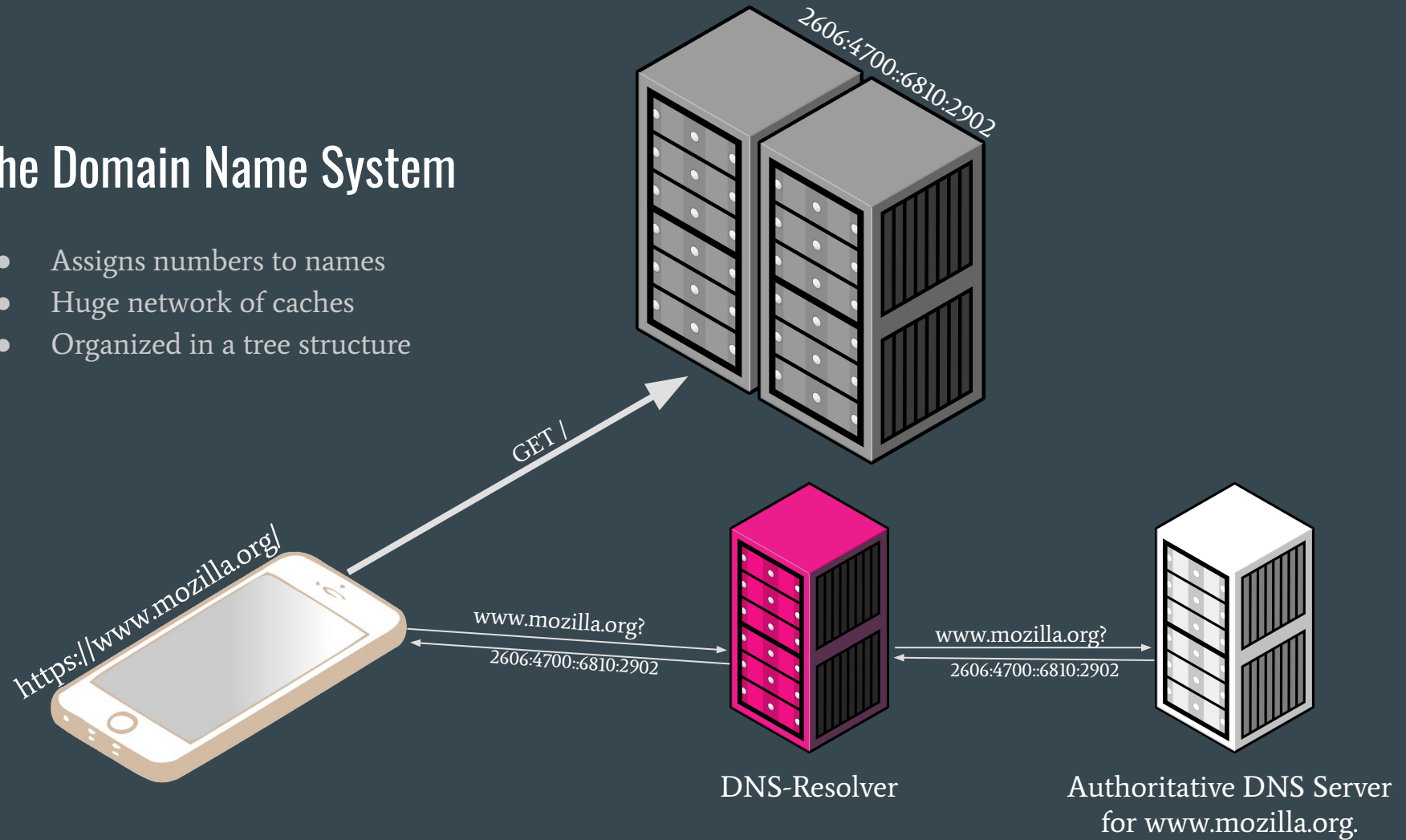
A Bird's-eye View



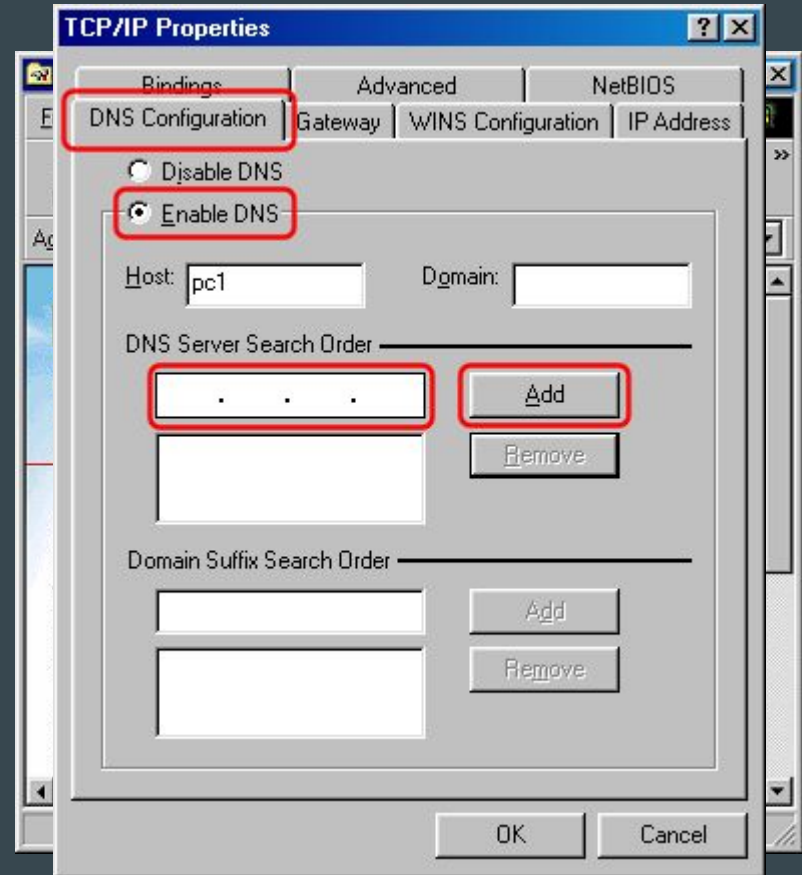
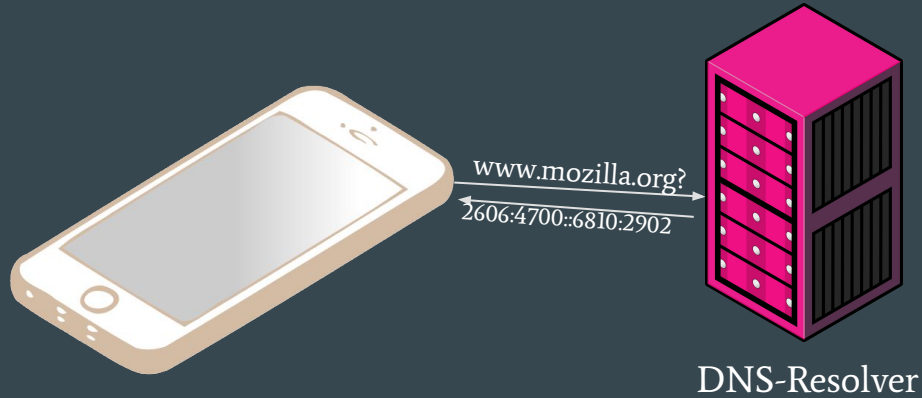
Picture is licensed under the [Creative Commons Attribution-Share Alike 3.0 Unported](https://creativecommons.org/licenses/by-sa/3.0/) license, cropped to fit slide and colors modified. Original author Bas van Schaik at <https://en.m.wikipedia.org/wiki/File:Ams-ix.k.root-servers.net.jpg>

# The Domain Name System

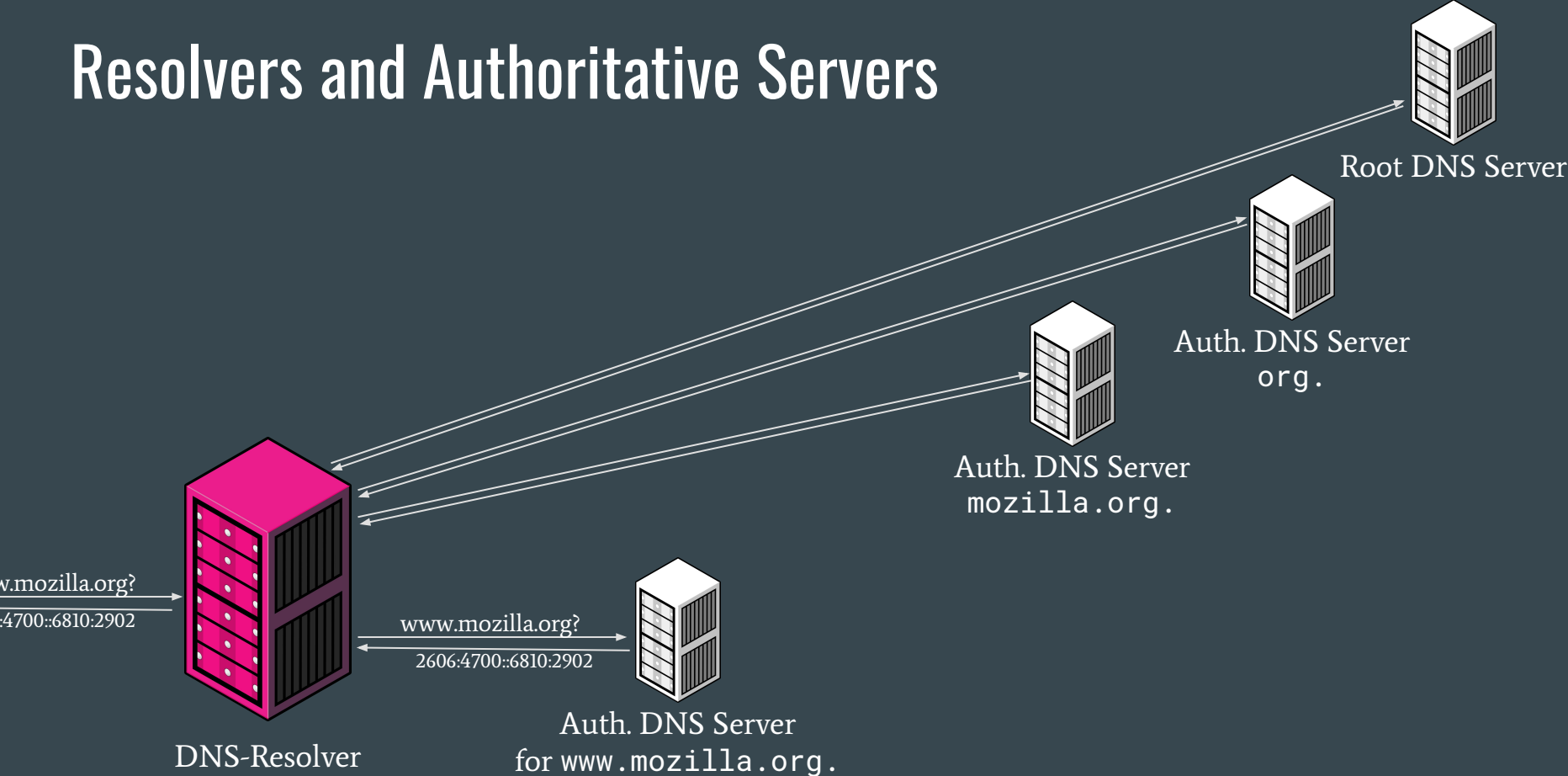
- Assigns numbers to names
- Huge network of caches
- Organized in a tree structure



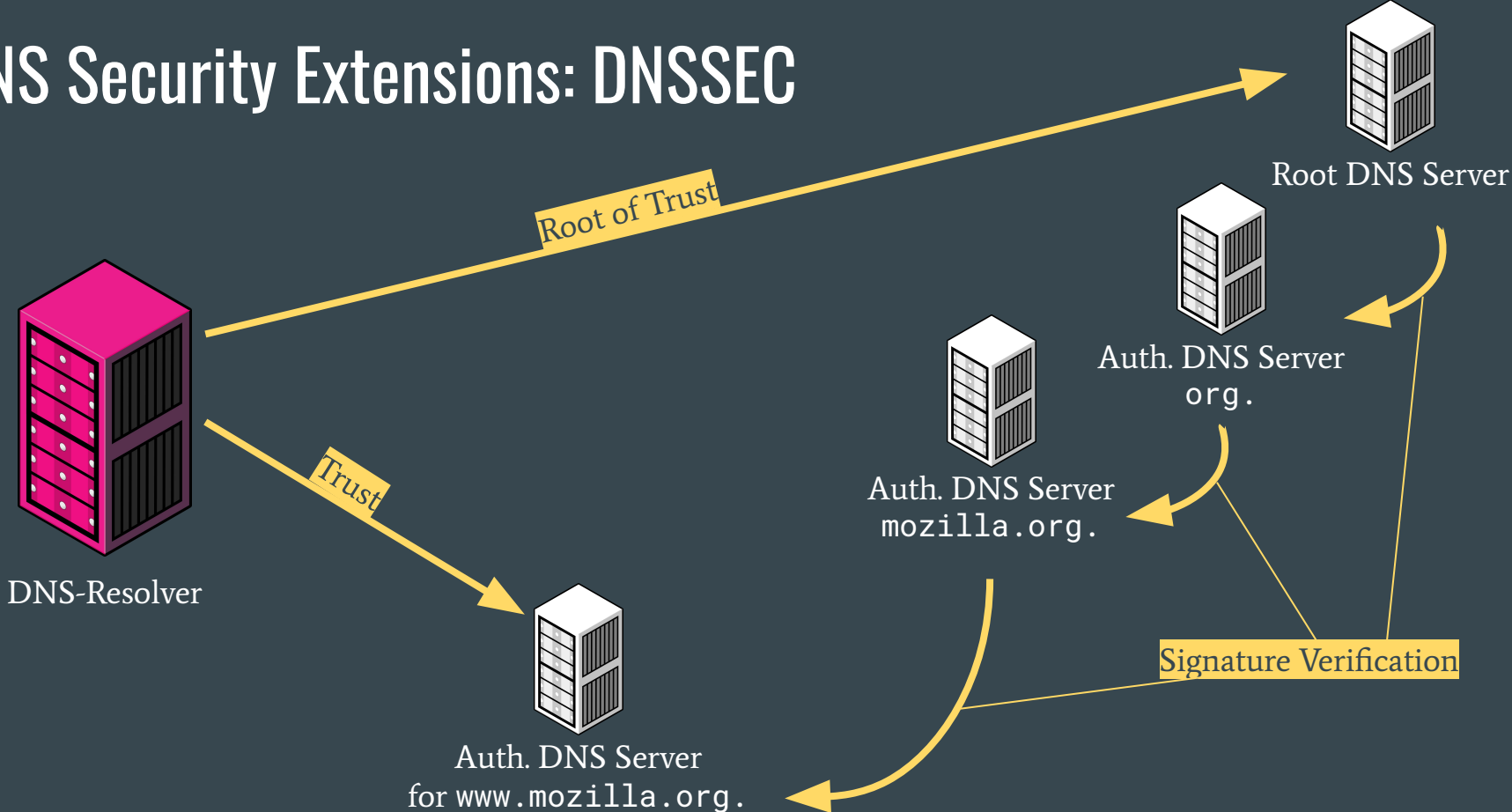
# Clients and DNS Resolvers



# Resolvers and Authoritative Servers

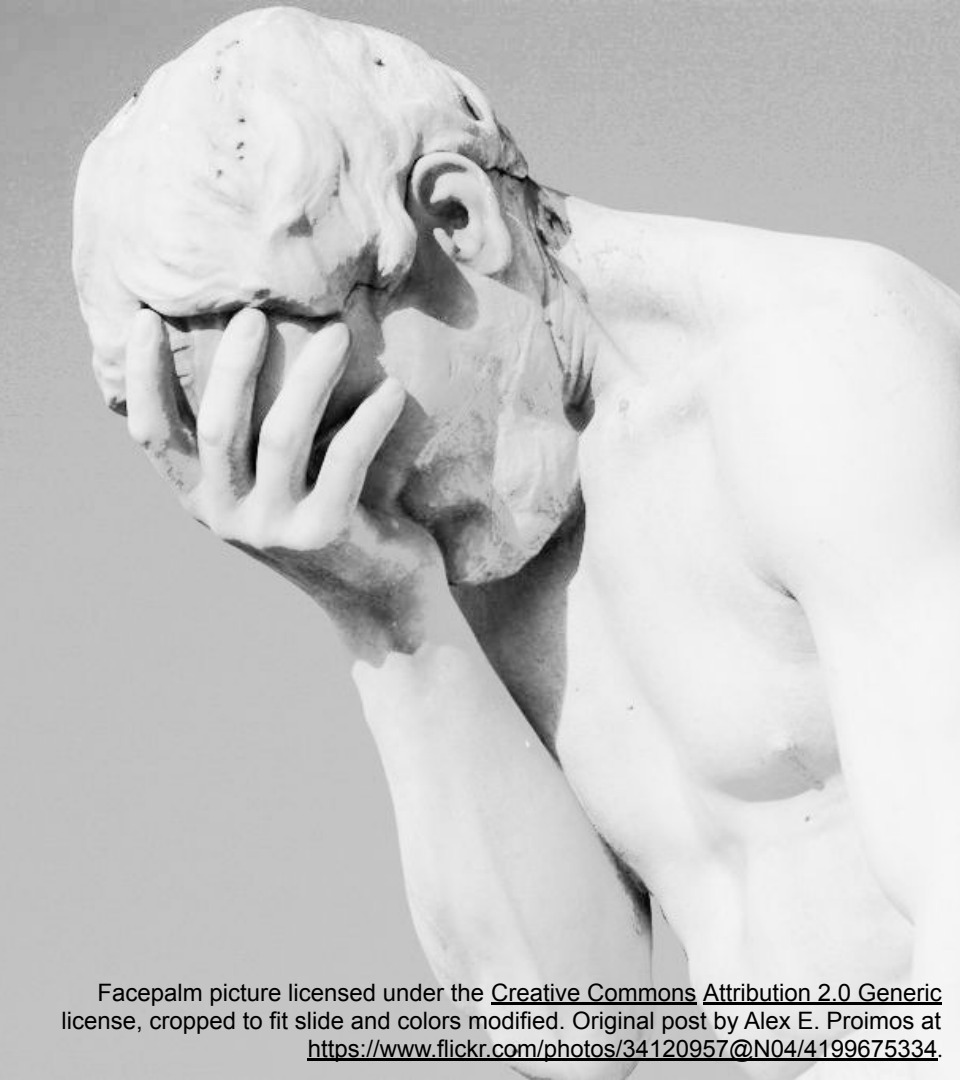


# DNS Security Extensions: DNSSEC



## 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	TTL	<input type="text" value="86400"/>	hostname	<input type="text" value="ns5.a4a-dns.de"/>	email	<input type="text" value="root@ns5.a4a-dns.de"/>
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="nils-wisiol.de"/>	IN NS	<input type="text" value="ns5.a4a-dns.de"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="nils-wisiol.de"/>	IN NS	<input type="text" value="ns6.a4a-dns.de"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="nils-wisiol.de"/>	IN A	<input type="text" value="178.63.189.70"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="www.nils-wisiol.de"/>	IN A	<input type="text" value="178.63.189.70"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="*.nils-wisiol.de"/>	IN A	<input type="text" value="178.63.189.70"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="nils-wisiol.de"/>	IN MX	<input type="text" value="10"/> <input type="text" value="sn4b.de"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="mail.nils-wisiol.de"/>	IN A	<input type="text" value="178.63.189.74"/>	remove <input type="checkbox"/> ?
Resource Record	TTL	<input type="text" value="86400"/>	<input type="text" value="nils-wisiol.de"/>	IN MX	<input type="text" value="20"/> <input type="text" value="sn7b.de"/>	remove <input type="checkbox"/> ?
ADD Resource Record	TTL	<input type="text" value="86400"/>	<input type="text"/>	IN	<input type="text" value="A"/> <input type="text" value="priority(MX,SRV)"/>	<input type="text"/>

*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"

Show page:  
(1 | 2 | 3 | 4 | 5 | 6)

	<b>Id</b>	<b>Name</b>	<b>Type</b>	<b>Content</b>	<b>Priority</b>	<b>TTL</b>
 	3	berlin.de	SOA	berlin.de. 2018120600 6040 864 3600000 6040		360
 	147	berlin.de	NS	berlin.de	0	360
 	149	localhost-berlin.de	NS	localhost-berlin.de	0	360
 	11	server-berlin.de	NS	server-berlin.de	0	360
 	13	www-berlin.de	NS	www-berlin.de	0	360
 	15	av-berlin.de	A	127.0.0.39	0	360
 	17	am-berlin.de	A	127.0.0.178	0	360
 	19	app-berlin.de	CNAME	app-berlin.de	0	360
 	21	data-powersoft-berlin.de	CNAME	data-powersoft-berlin.de	0	360
 	35	www-powersoft-berlin.de	A	127.0.0.15	0	360
 	23	localhost-berlin.de	A	127.0.0.7	0	360
 	25	localhost-berlin.de	A	127.0.0.63	0	360
 	27	localhost-berlin.de	A	127.0.0.31	0	360
 	97	localhost-berlin.de	A	127.0.0.159	0	360
 	105	localhost-berlin.de	A	127.0.0.135	0	360
 	371	localhost-berlin.de	A	127.0.0.191	0	360
 	29	localhost-berlin.de	CNAME	localhost-berlin.de	0	360
 	31	localhost-berlin.de	A	127.0.0.97	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, marian.margraf}@fu-berlin.de

*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*

### 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

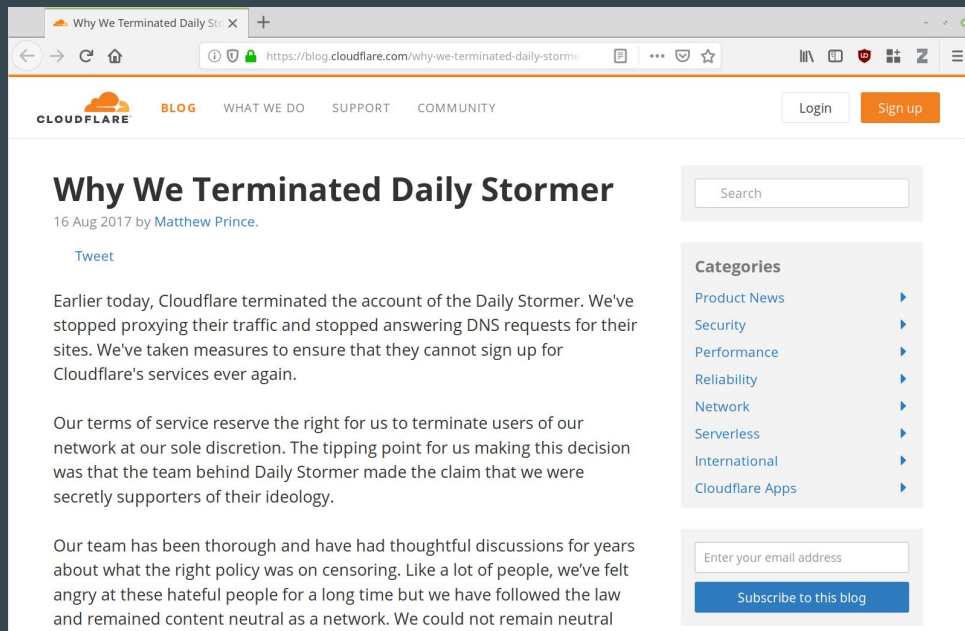
### 1 INTRODUCTION

Before a connection to a named Internet host (e.g. [www.fu-berlin.de](http://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

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



The screenshot shows a web browser window with the URL <https://blog.cloudflare.com/why-we-terminated-daily-stormer>. The page header includes the Cloudflare logo, navigation links for 'BLOG', 'WHAT WE DO', 'SUPPORT', and 'COMMUNITY', and buttons for 'Login' and 'Sign up'. The main content area features the article title '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. A 'Tweet' link is visible below the title. On the right side, there is a search bar, a 'Categories' list with links to Product News, Security, Performance, Reliability, Network, Serverless, International, and Cloudflare Apps, and a subscription form with an email input field 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

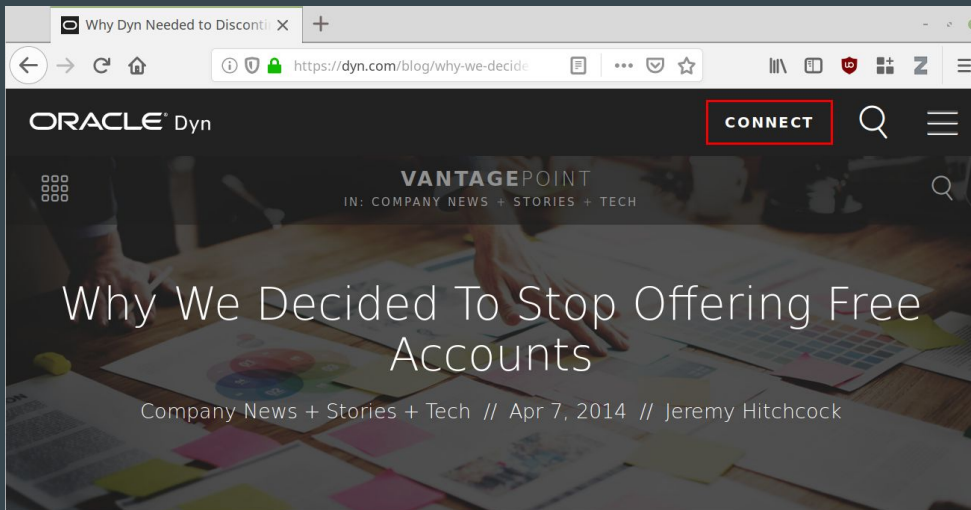
Search

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

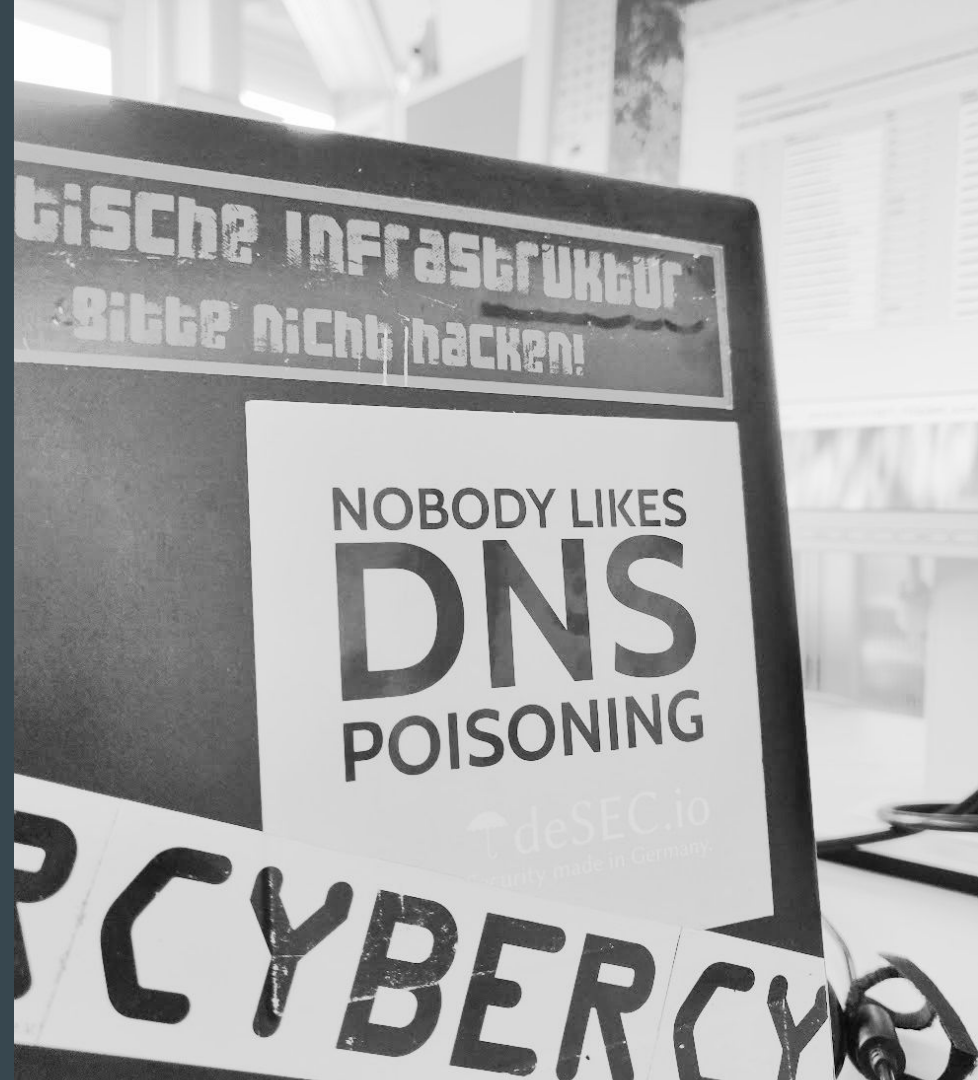
- **Usability**
  - API access
  - Convenience features like search and replace
  - Flexibility in record types and TTLs
- **Security**
  - DNSSEC
- **Organization**
  - Data protection
  - European laws
  - Free open-source software
  - Low cost hosting



§ 24 Abs. 1 UrhG

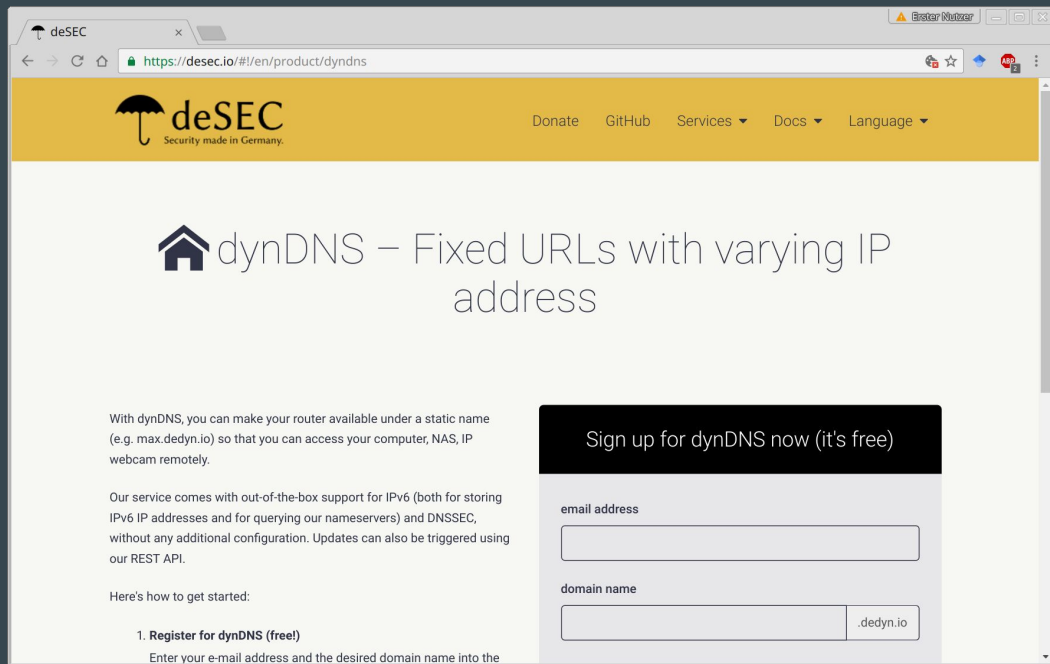
## Section 3

# deSEC: DNS Hosting for Everyone





# Home Use: Permanently Free Dynamic DNS



The screenshot shows a web browser window with the URL `https://desec.io/#/en/product/dyndns`. The page features the deSEC logo (an umbrella) and the text "Security made in Germany." in the top navigation bar. Below the navigation bar, the main heading reads "dynDNS – Fixed URLs with varying IP address". The page content includes a description of the service, its features (IPv6 support, DNSSEC, REST API), and a "Sign up for dynDNS now (it's free)" button. A registration form is visible with fields for "email address" and "domain name" (with ".dedyn.io" as a suggestion).

deSEC  
Security made in Germany.

Donate GitHub Services Docs Language

## dynDNS – Fixed URLs with varying IP address

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.

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.

Here's how to get started:

- 1. Register for dynDNS (free!)**  
Enter your e-mail address and the desired domain name into the



The screenshot shows the FRITZ!Box web interface for configuring Dynamic DNS. The page has a blue header with the "FRITZ!Box" logo and navigation links for "Abmelden", "Ansicht: Experte", "Inhalt", and "Hilfe". Below the header, there are tabs for "USB-Speicher", "Fernwartung", "Dynamic DNS", "VPN", and "IPv6". The "Dynamic DNS" tab is active, showing a configuration page with a dropdown menu for "Anbieter" set to "Benutzerdefiniert" and a button for "Neuen Domainnamen anmelden". 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".

## FRITZ!Box

Abmelden Ansicht: Experte Inhalt Hilfe

USB-Speicher Fernwartung **Dynamic DNS** VPN IPv6

können Anwendungen und Dienste, für die in der FRITZ!Box-Firewall Portfreigaben eingerichtet wurden, unter anderem aus dem Internet erreicht werden, obwohl sich die öffentliche IP-Adresse der FRITZ!Box mit jeder

benutzen

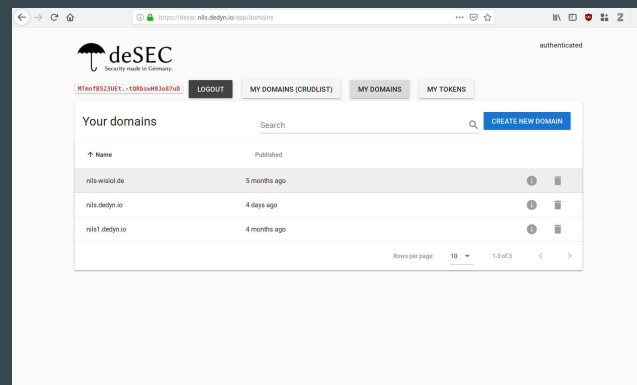
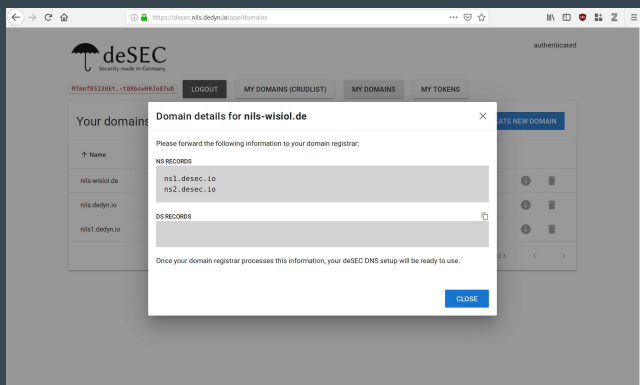
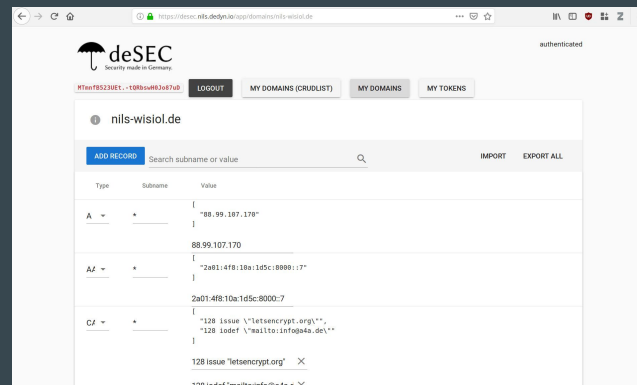
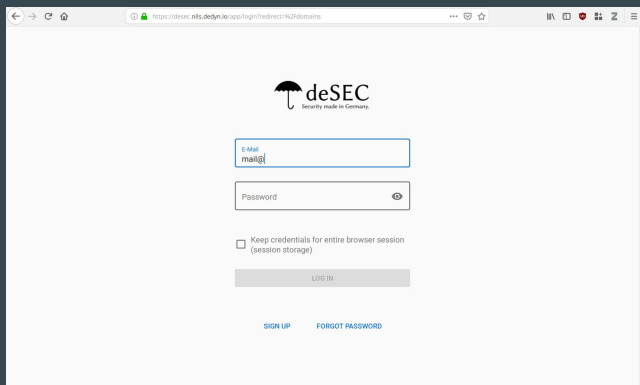
Idendaten für Ihren Dynamic DNS-Anbieter an.

Anbieter: **Benutzerdefiniert**

Kennwort

Kennwortbestätigung

# 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](https://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 built on top



# Live Demo

Get Your Laptops Out

<https://dnslookup.online>

<https://dnsquery.org/>

4%

of websites use DNSSEC

19%

of Internet users validate DNSSEC  
signatures

**Under .de.,**

**1%**

of zones use DNSSEC

**In Germany,**

**46%**

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*
- 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

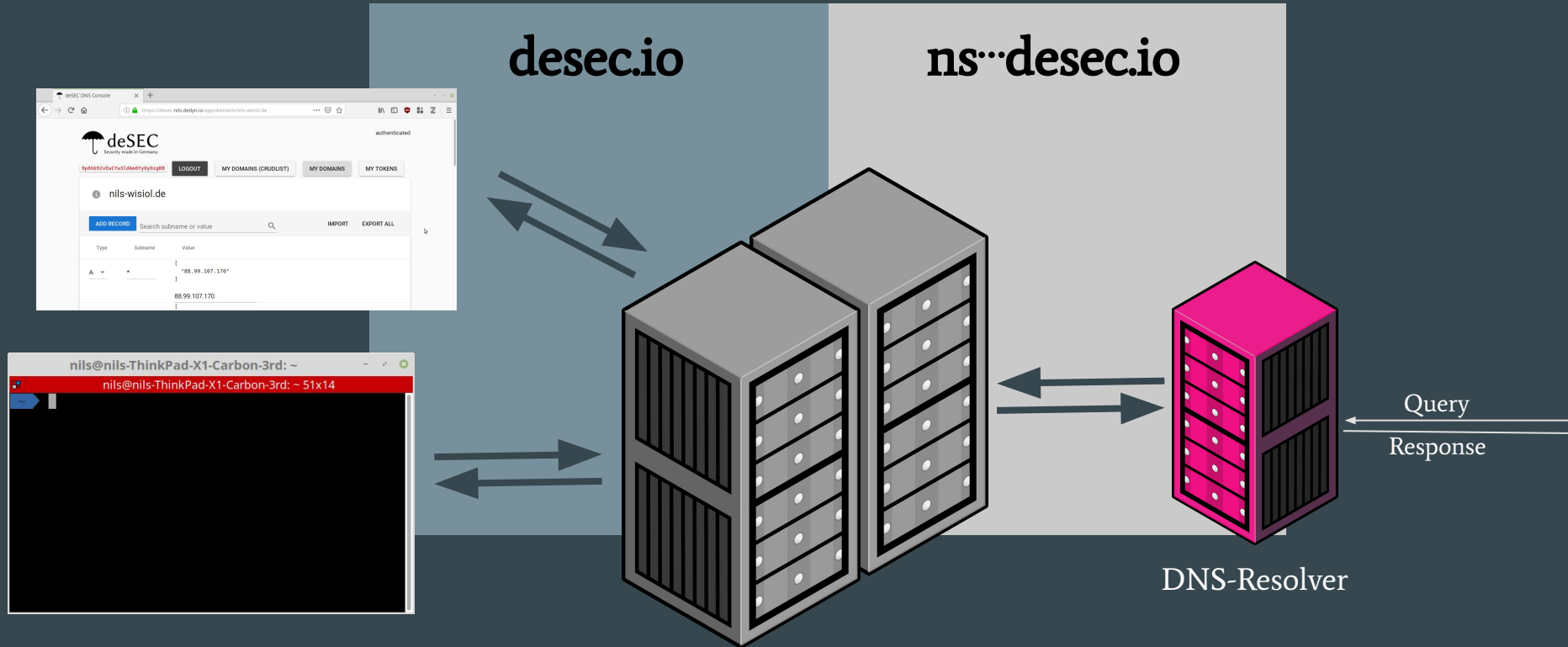
  static:
    build: static
    image: desec/dedyn-static:latest
    networks:
      - rearwww
    logging:
      driver: "syslog"
      options:
        tag: "desec/static"
      restart: unless-stopped

  dbapi:
    build: dbapi
    image: desec/dedyn-dbapi:latest
    volumes:
      - dbapi_mysql:/var/lib/mysql
    environment:
      - DESECSTACK_IPV4_REAR_PREFIX16
      - DESECSTACK_DBAPT_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_pans
    networks:
      - rearlord
    logging:
      driver: "syslog"
```



# Public Interfaces: HTTP, DNS

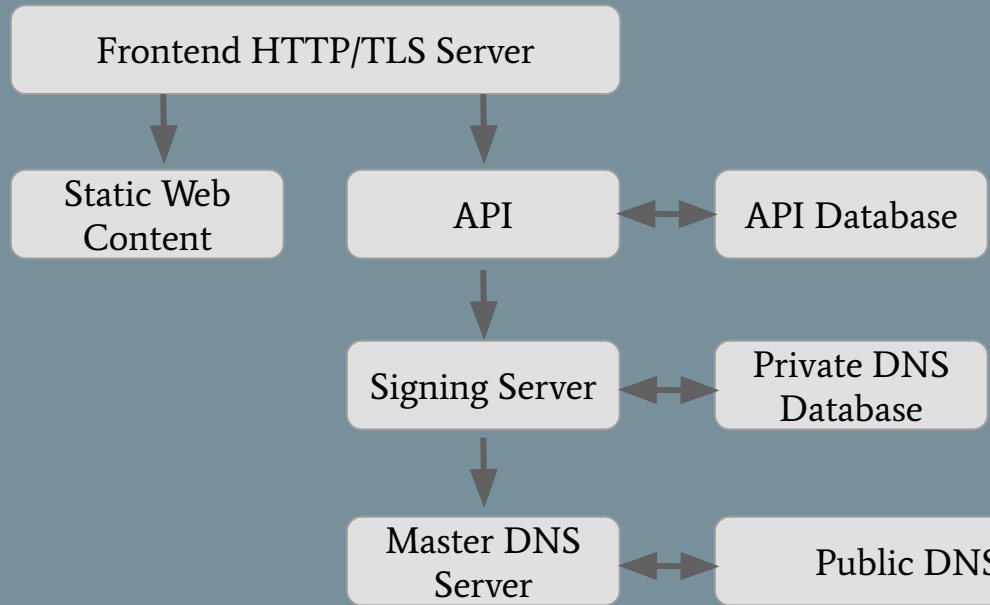


# Internal Structure



desec.io 

ns.desec.io 



# We're Launching in July 2019

The screenshot shows a web browser displaying the GitHub project dashboard for 'Launch'. The browser's address bar shows the URL 'https://github.com/de...'. The page header includes navigation links for 'Code', 'Issues 28', 'Pull requests 3', 'Projects 1', 'Wiki', 'Pulse', and 'Community'. The main content area features a Kanban board with two columns: 'To do' (12 items) and 'In progress' (2 items). Each item is a card representing a GitHub issue, with a title, issue number, creator, and status tags.

**To do**

- Abuse Scenario: Email and System Load** (#185 opened by nils-wisio) **api** **bug** **prio: medium**
- Allow users to delete their account** (#151 opened by peterthomassen) **api** **enhancement** **prio: high**
- CORS Headers** (#87 opened by nils-wisio) **enhancement** **help wanted**
- Decouple Unlocking from REST API** (#162 opened by nils-wisio) **bug**
- Rate Limit Signups** (#160 opened by nils-wisio)
- Sign Docker Images** (#158 opened by nils-wisio)
- Add curl examples to docs** (#99 opened by nils-wisio) **docs** **prio: low**

**In progress**

- Blacklisting of public and already registered suffixes** (#88 opened by peterthomassen) **enhancement** **prio: low**
- review `write\_rrsets` into pieces, maybe refactor** (#97 opened by nils-wisio) **enhancement** **prio: medium**

# Thank You

<https://desec.io/>

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

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

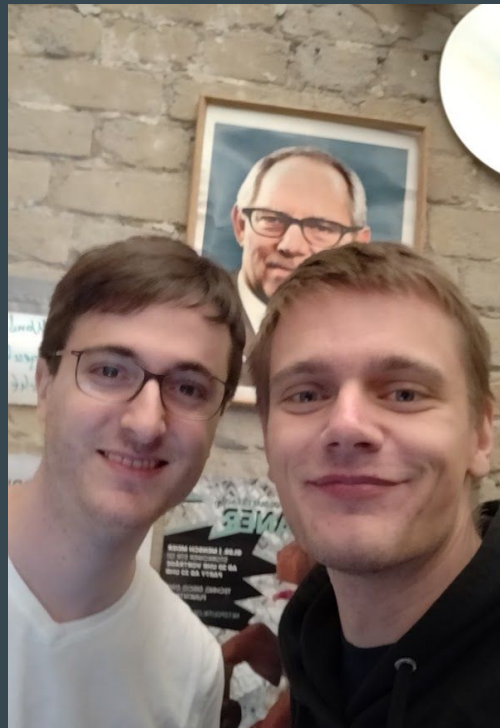
7 May 2019 · Crypto Meetup Berlin

deSEC

Dr. Peter Thomassen

Nils Wisiol

Donations kindly accepted: we take code and money



# Discussion

- Abuse scenarios
  - Free, anonymous zones
  - Blocking in some applications on public-suffix level?
- Security of private user data and keys
- Threats in misconfiguration of DNS servers
- DDoS