# deSEC

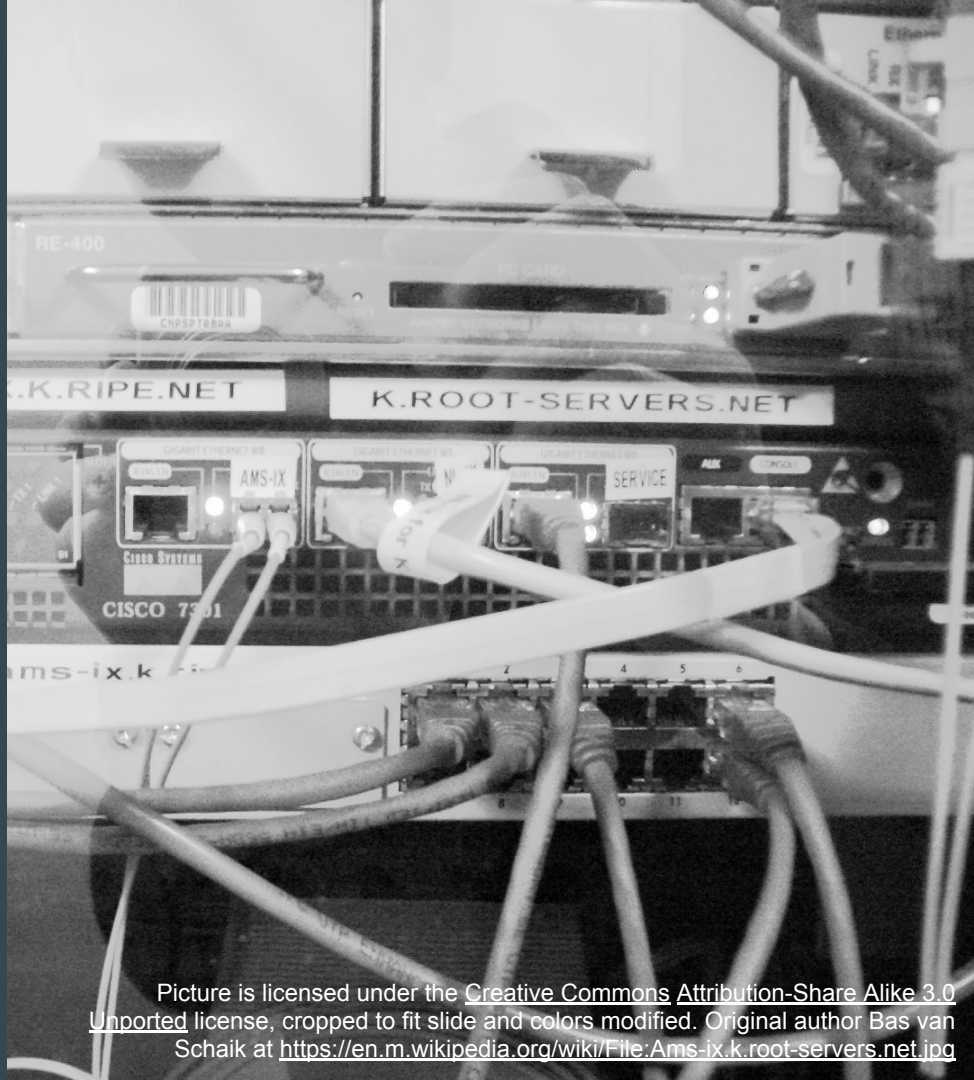
Free, Secure, and Easy DNS Hosting

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

Section 1

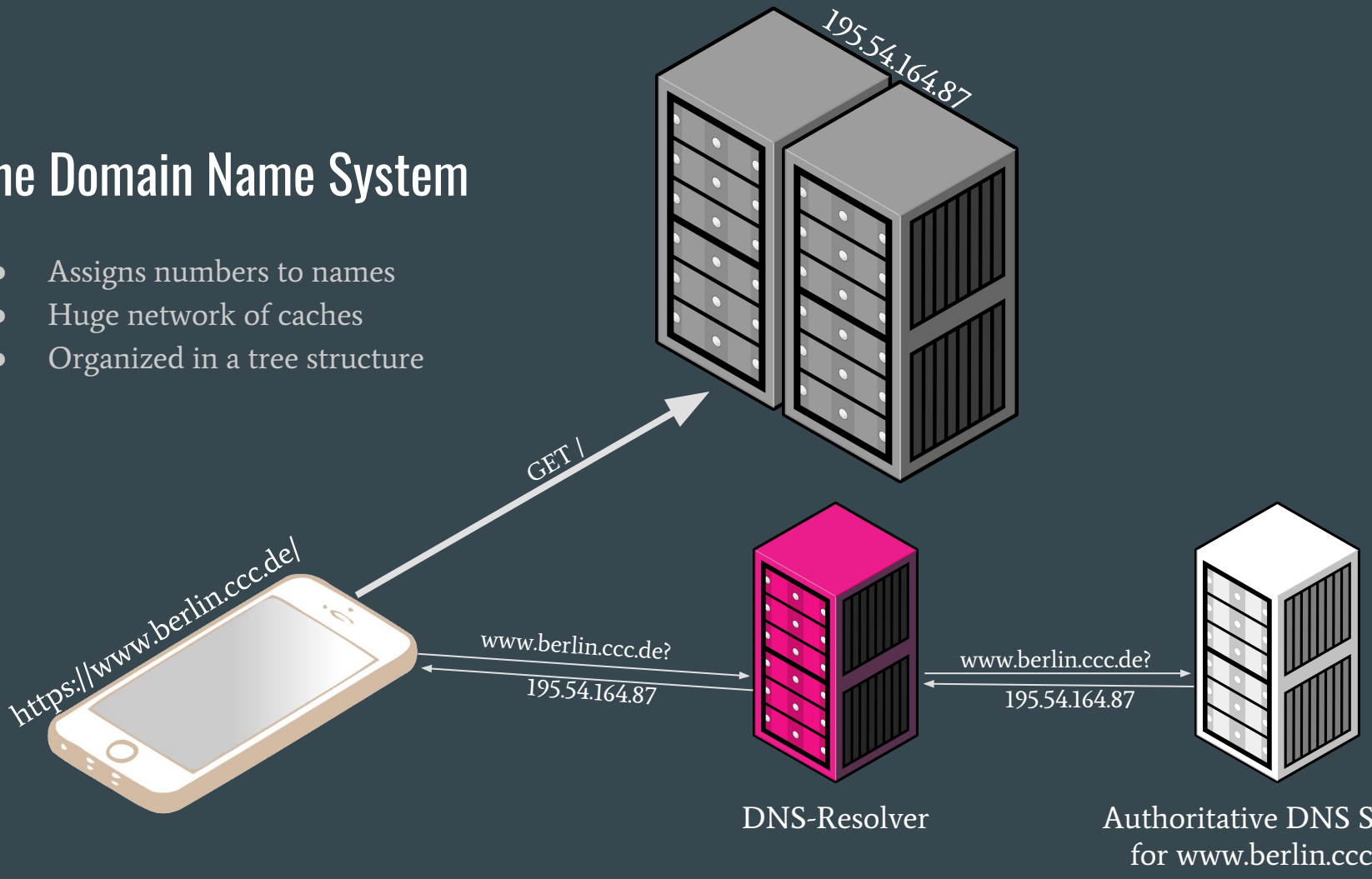
# DNS & DNSSEC

## A Bird's-eye View

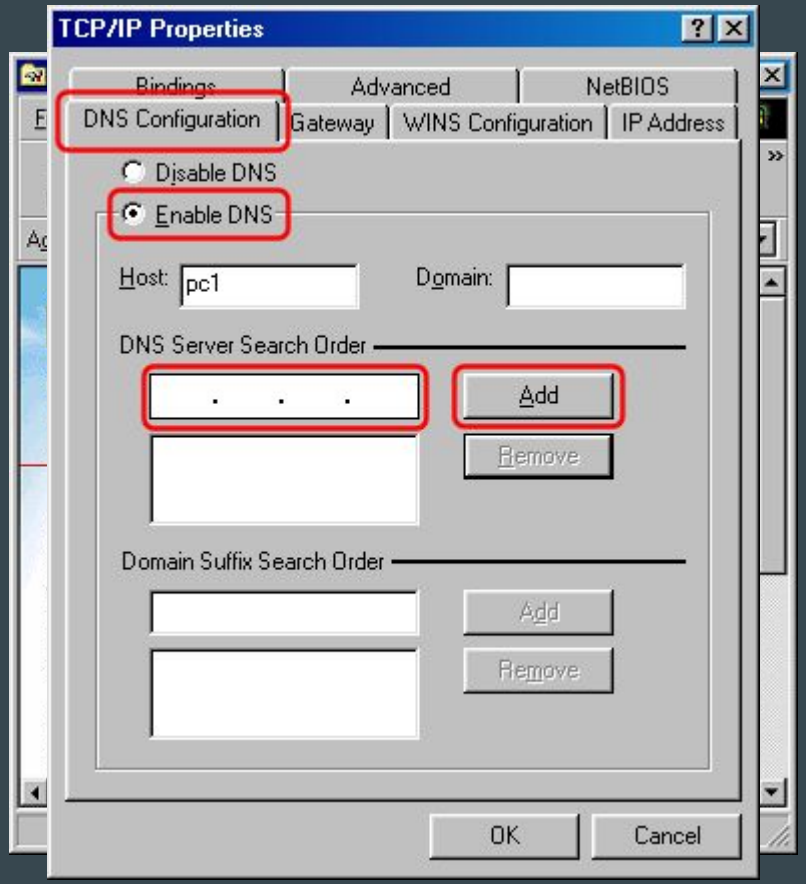


# The Domain Name System

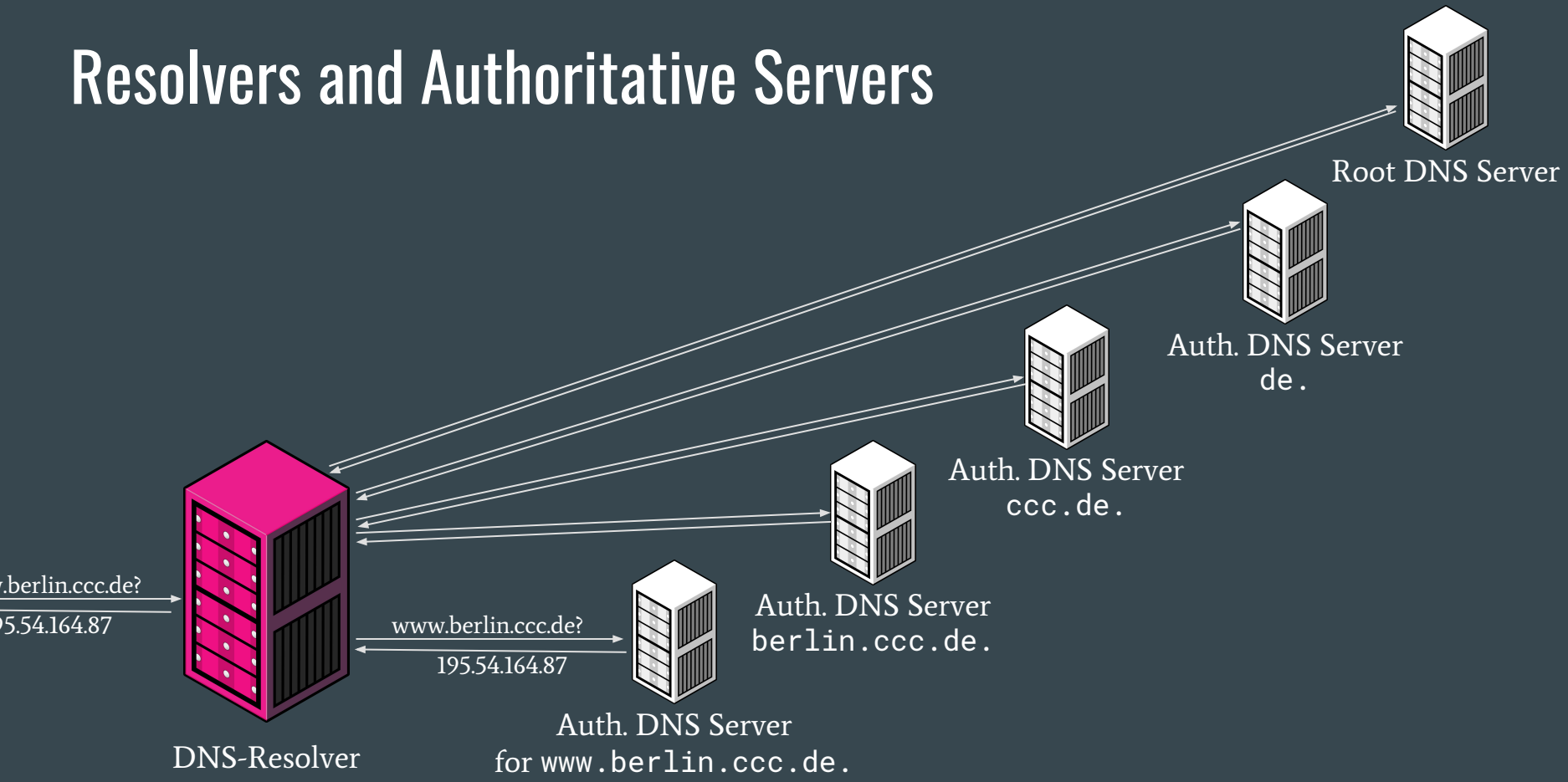
- Assigns numbers to names
- Huge network of caches
- Organized in a tree structure



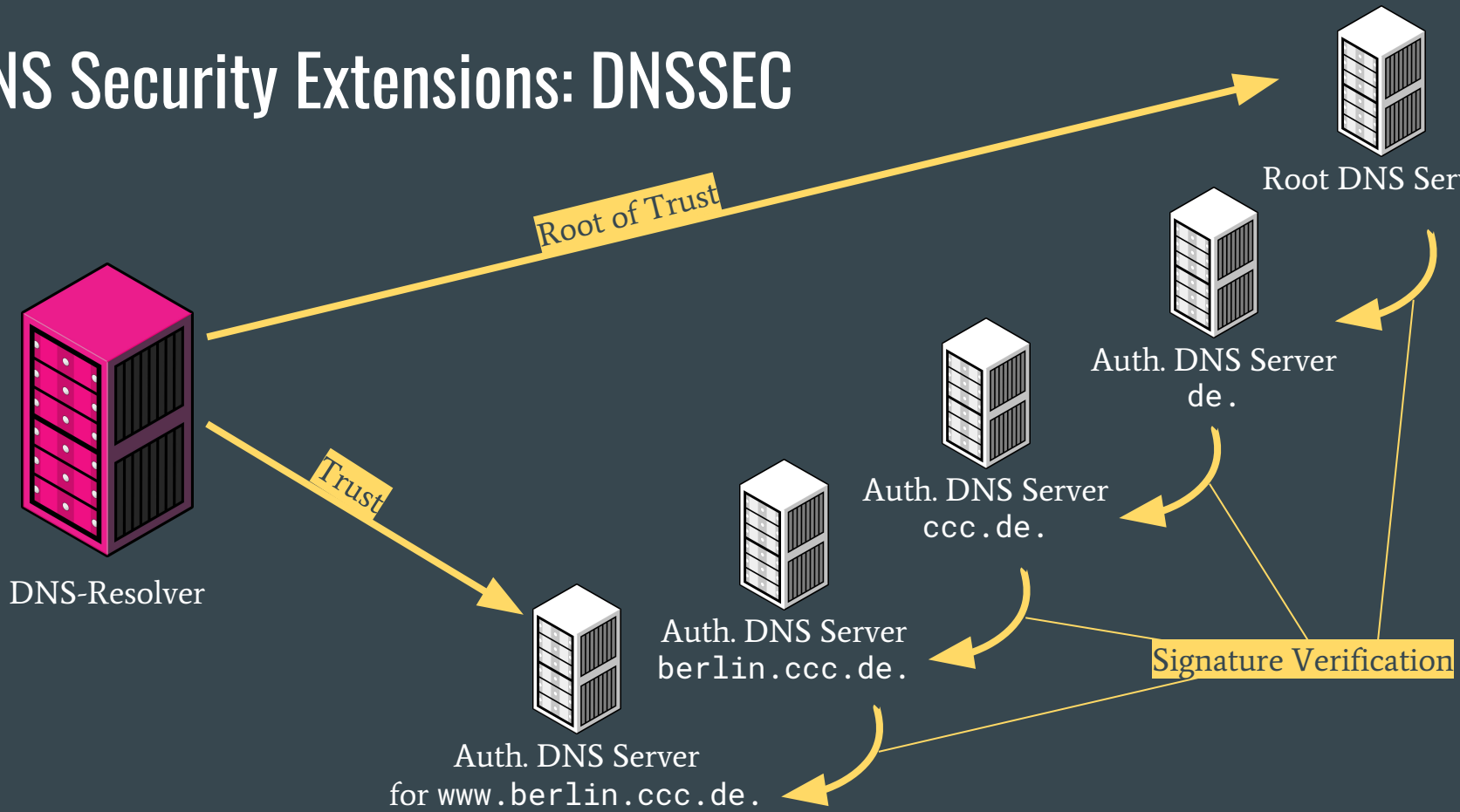
# Clients and DNS Resolvers

# Resolvers and Authoritative Servers

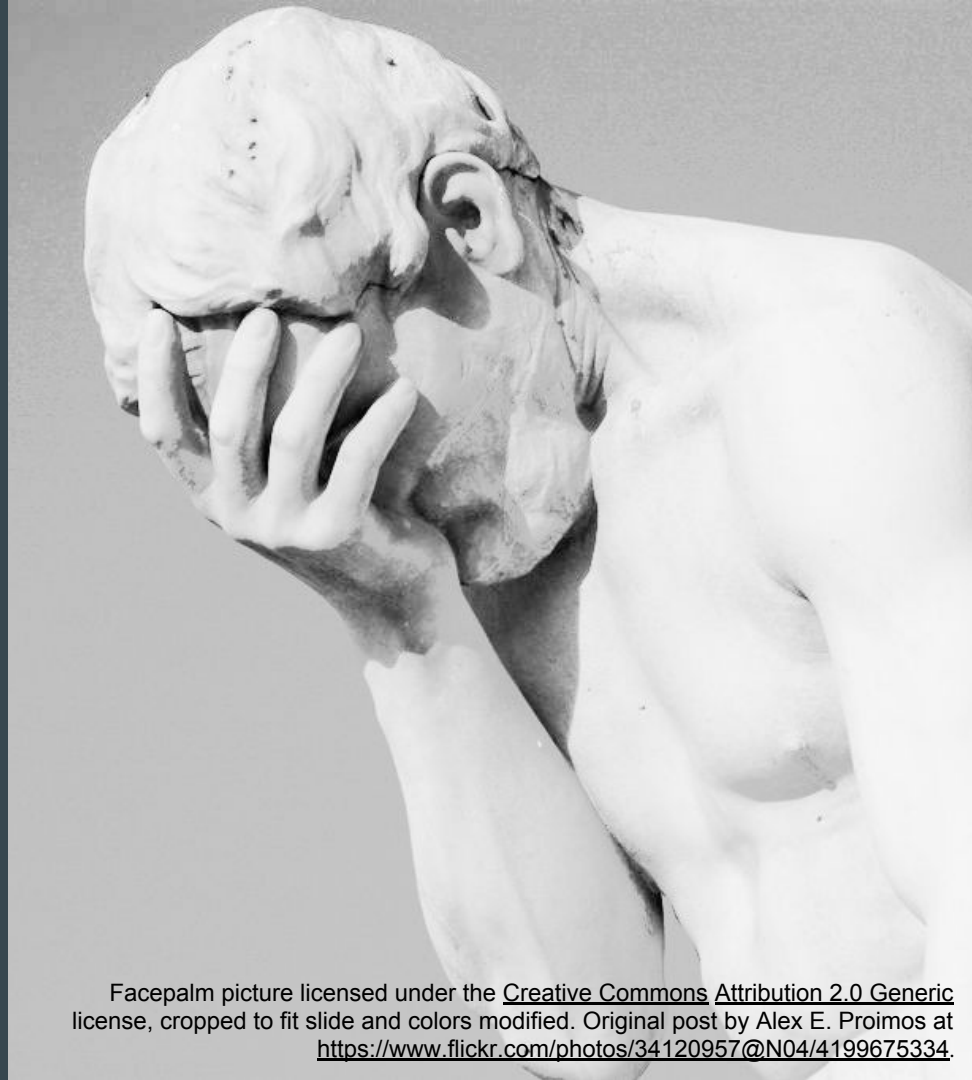


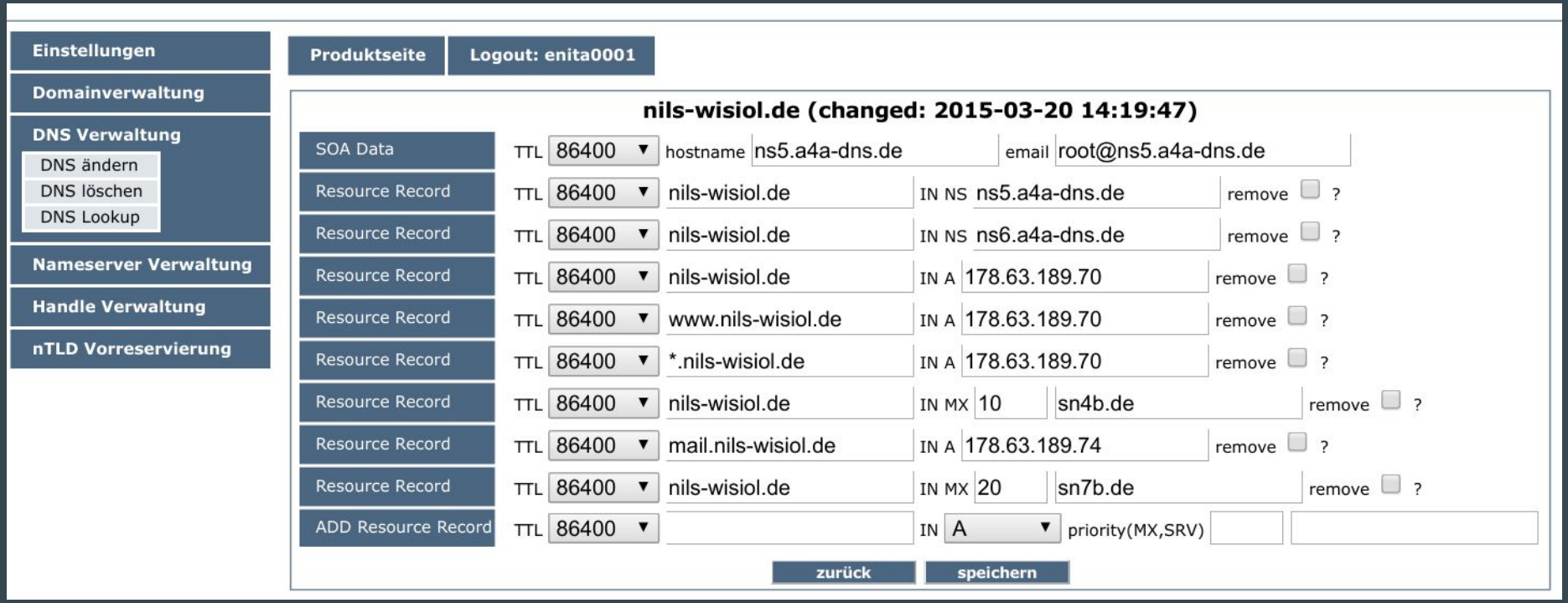
# DNS Security Extensions: DNSSEC



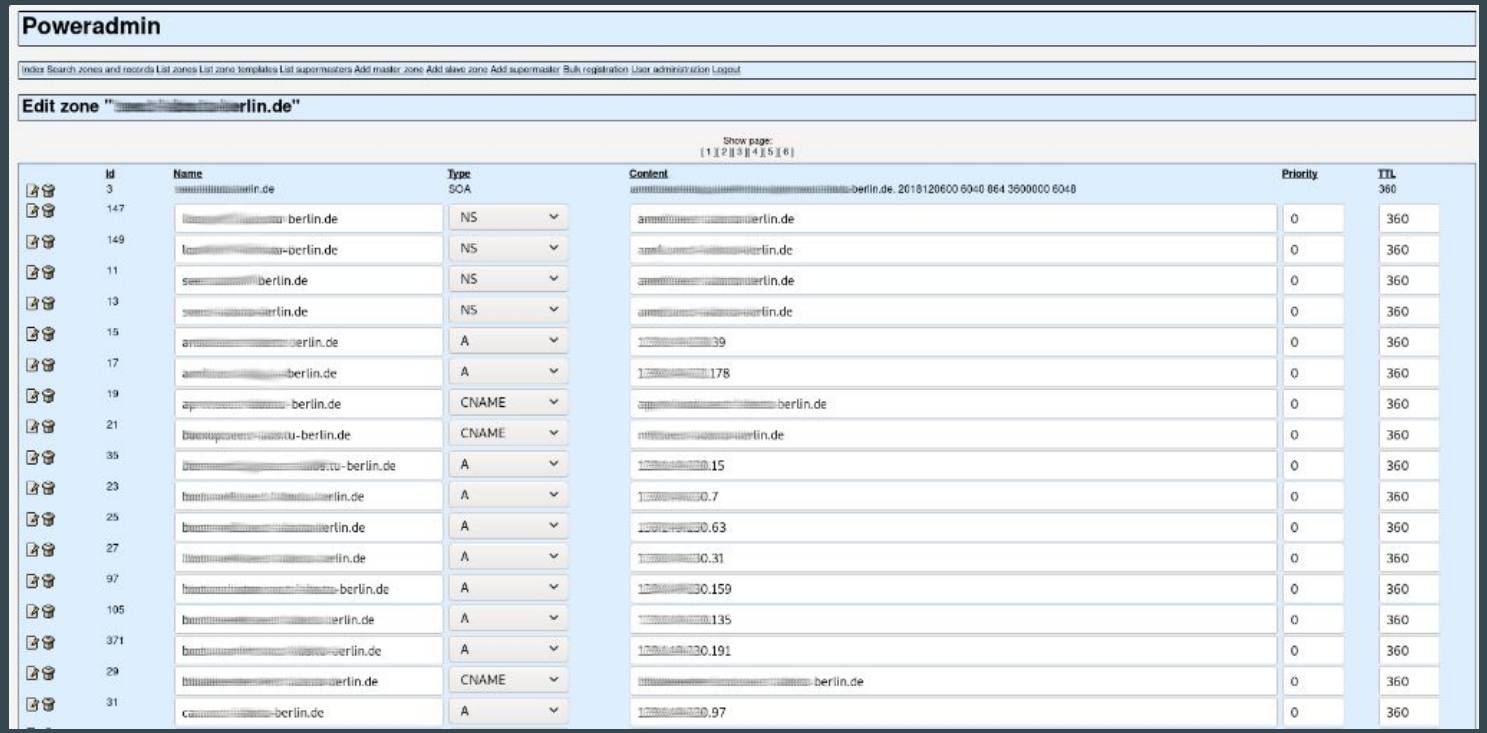
Section 2

# The State of DNS Security and Usability






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




*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*

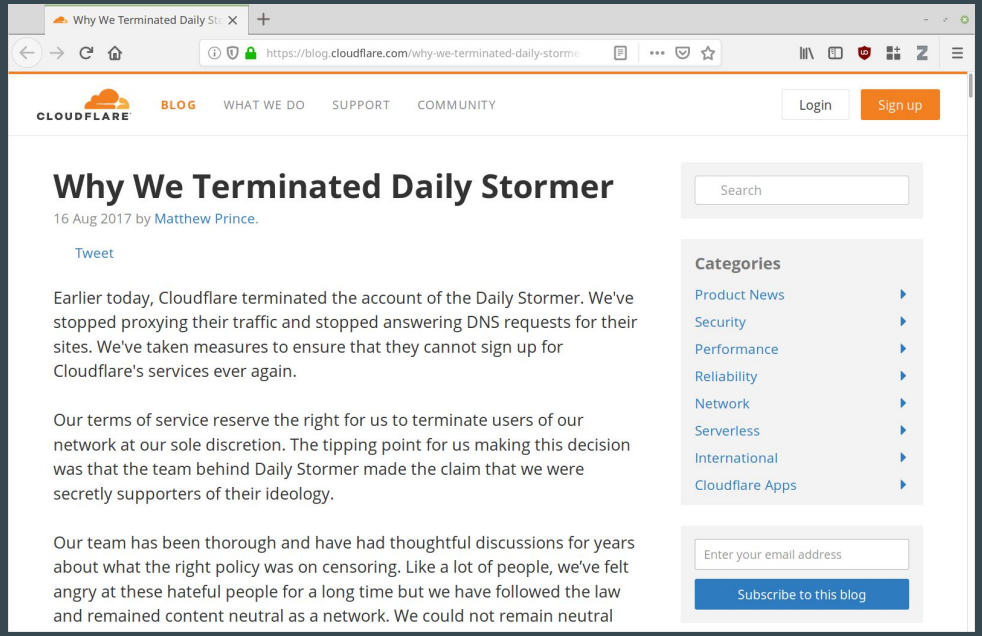
## 1 Introduction

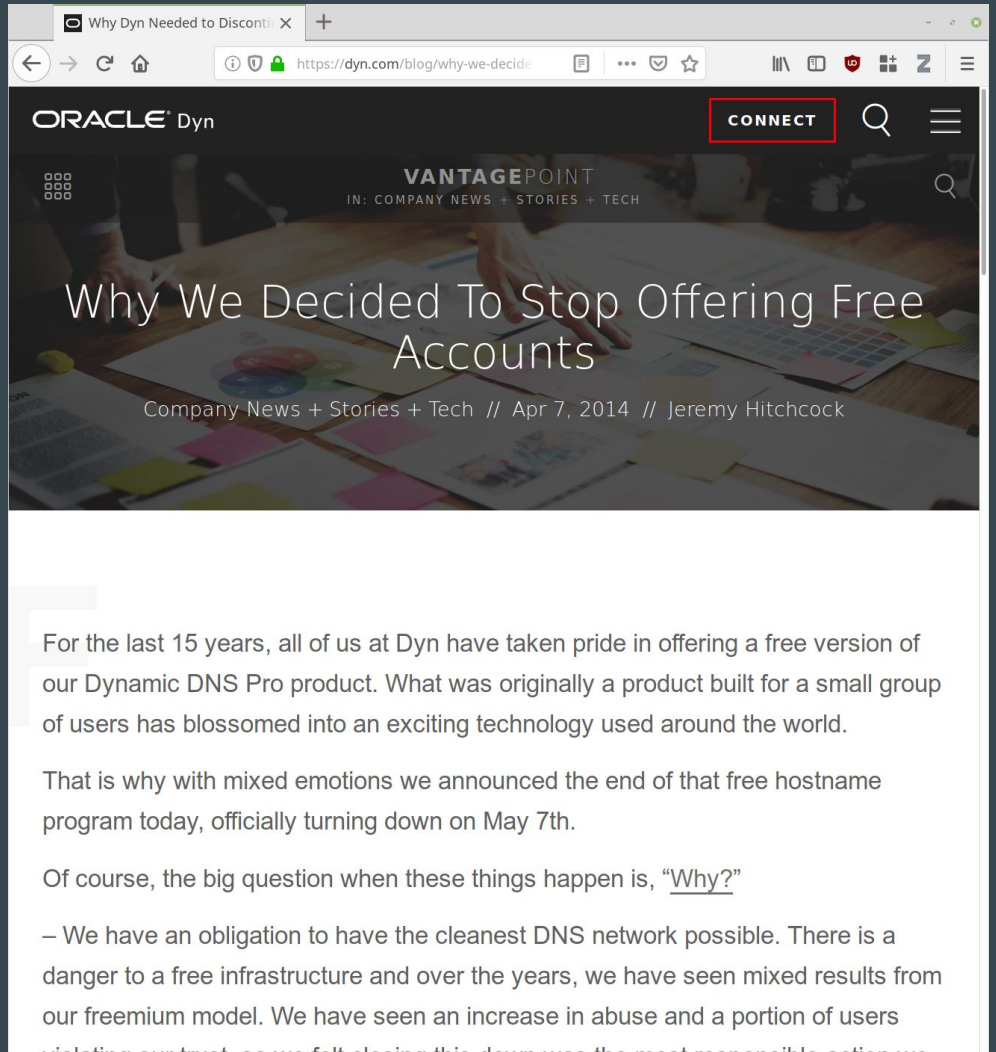
Before a connection to a named Internet host (e. g. *www.fu-berlin.de*) can be established, it is necessary to determine the IP address associated with the host name. This lookup is done using the Domain Name System with a myriad of Internet access providers maintaining their own caches. Thus, the correct 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

*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*






*This is how a popular dynamic DNS service closed in 2014*

# Things That are Desperately Missing

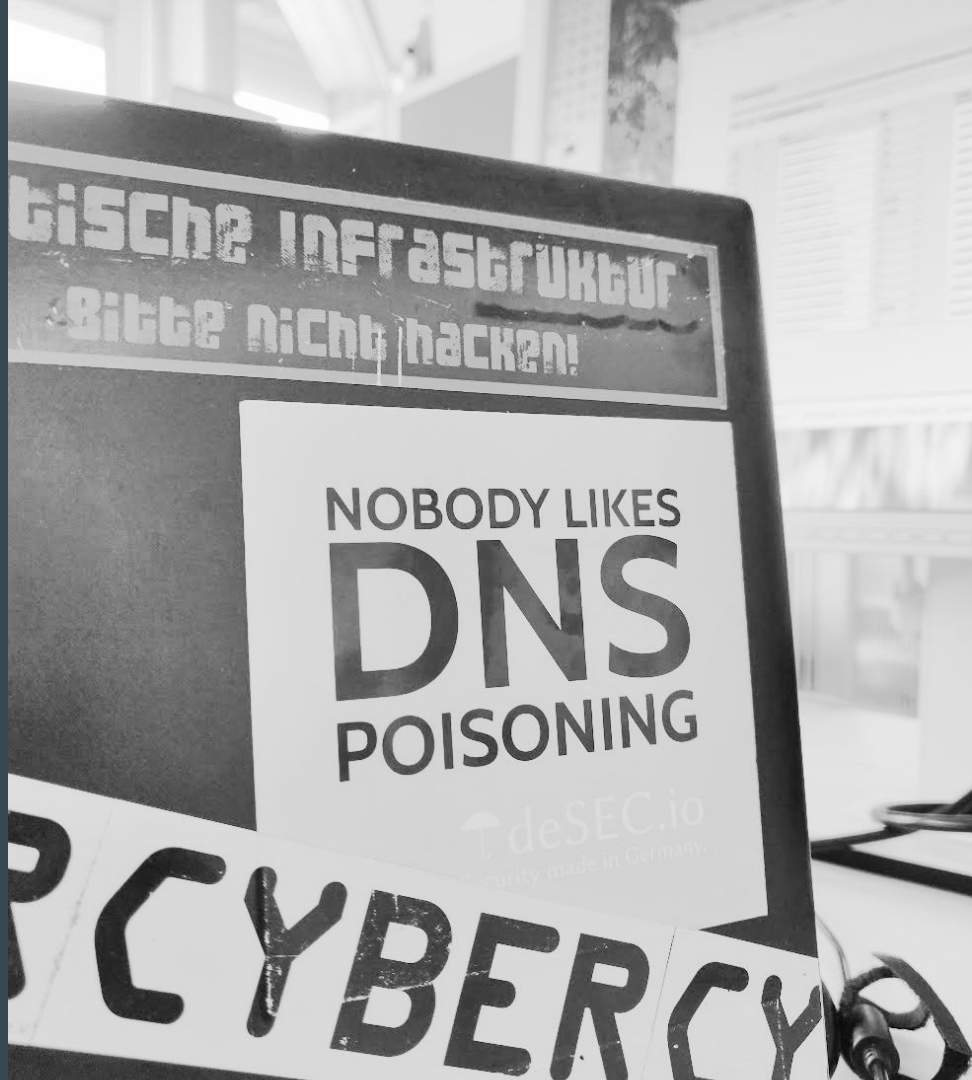
- **Usability**
  - API access
  - Convenience features like search and replace
  - Flexibility in record types and TTLs

- **Security**
  - DNSSEC

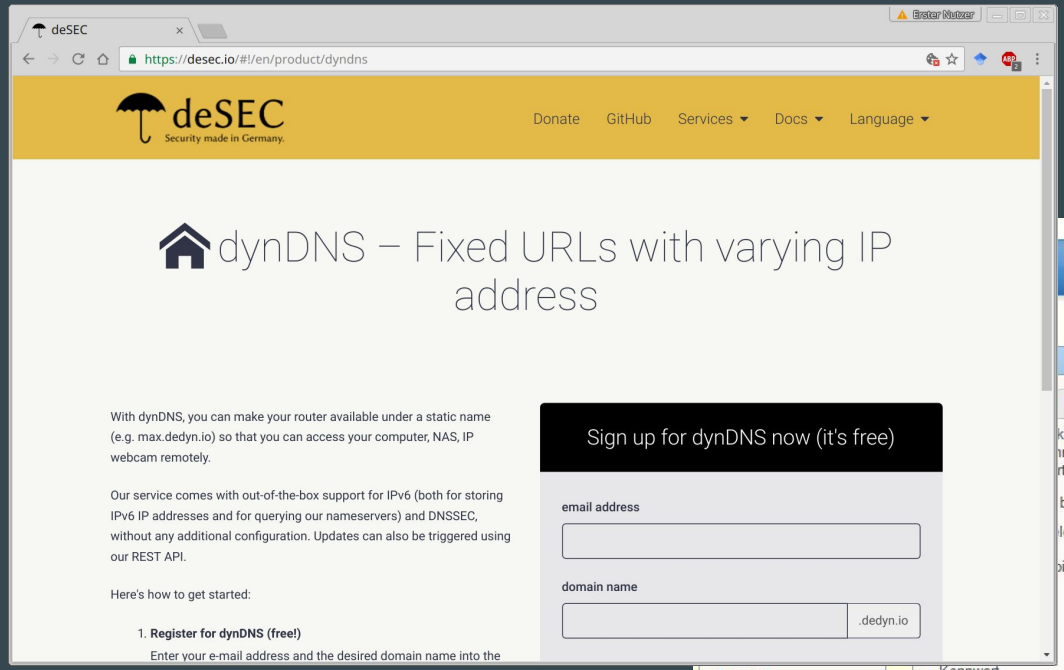
- **Organization**
  - Data protection
  - European laws
  - Free open-source software
  - Low cost hosting

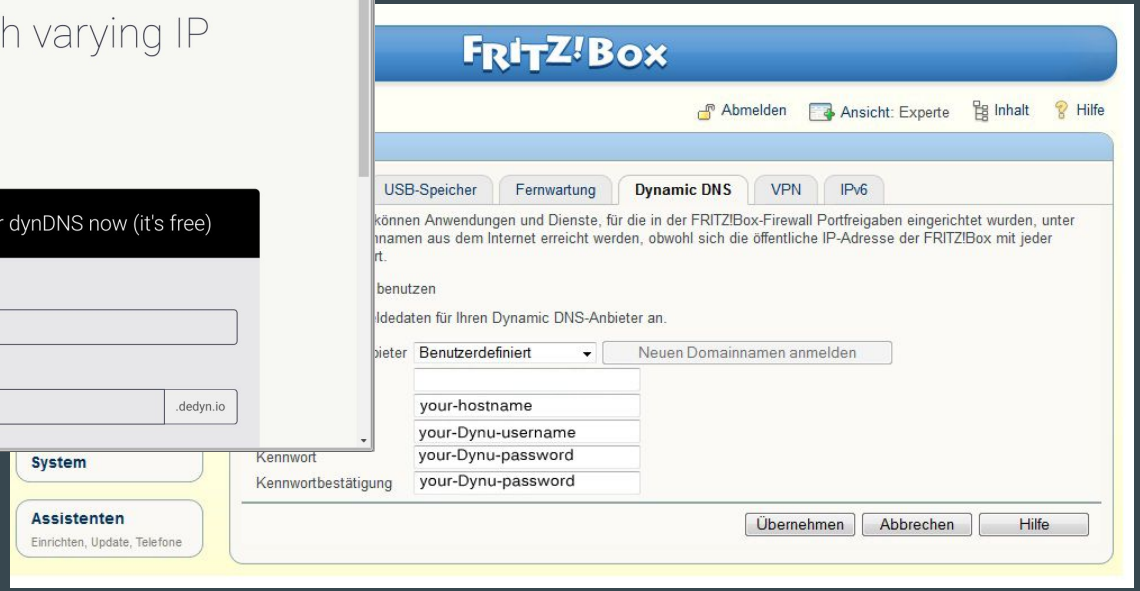
Section 3

# deSEC: DNS Hosting for Everyone

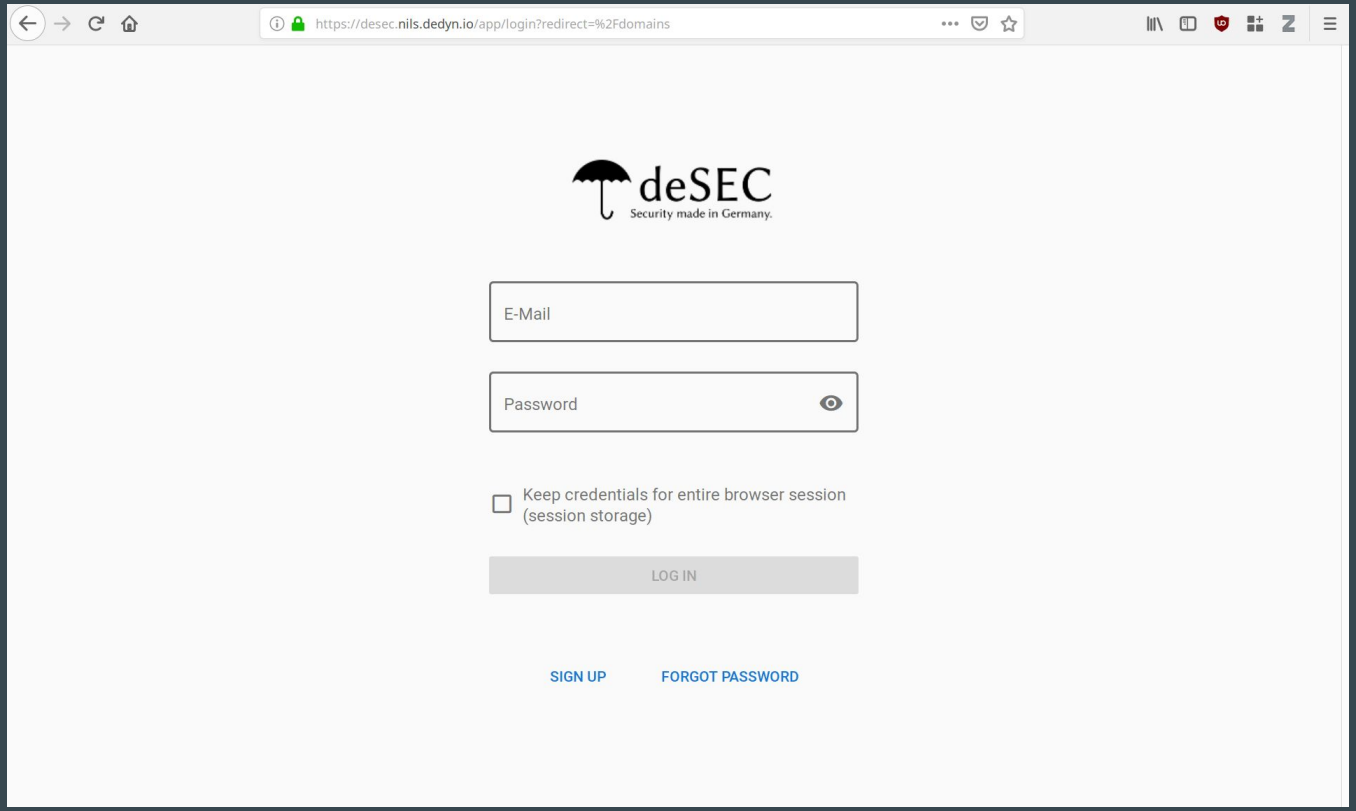


# Home Use: Permanently Free Dynamic DNS



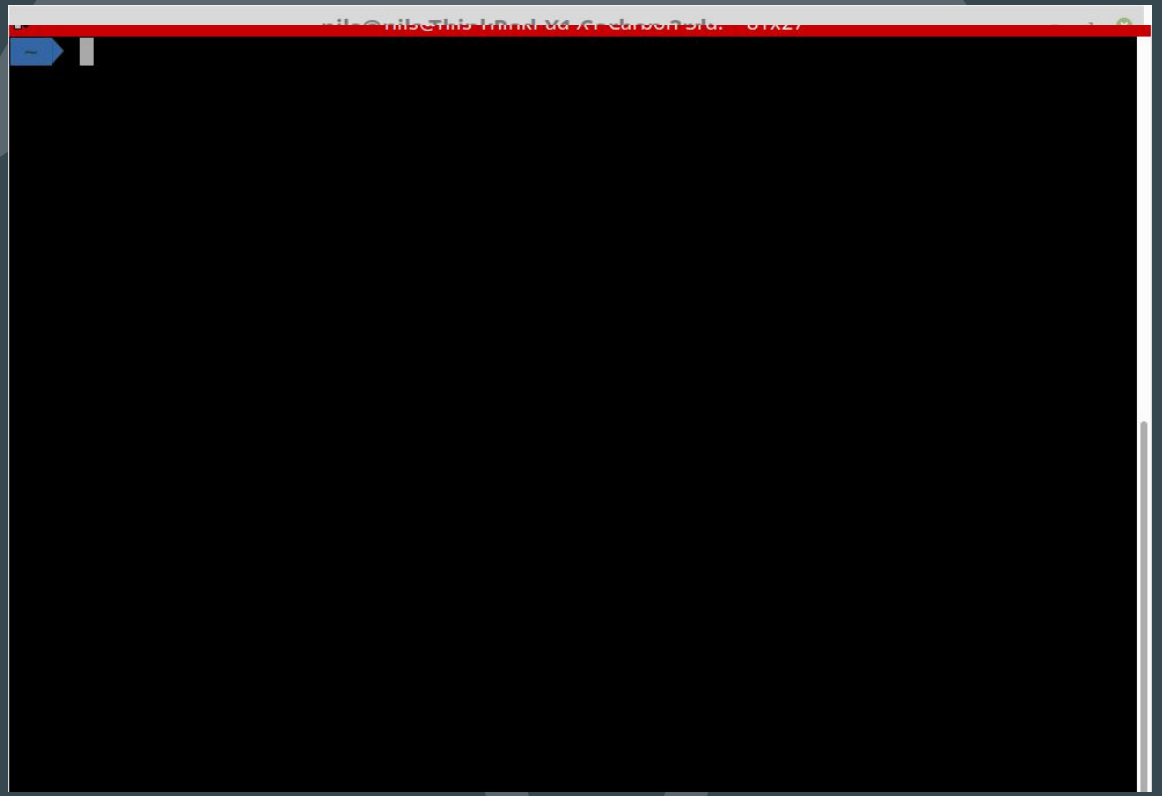



# Professional Use: Good-Looking Web Management App



# 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 ✔

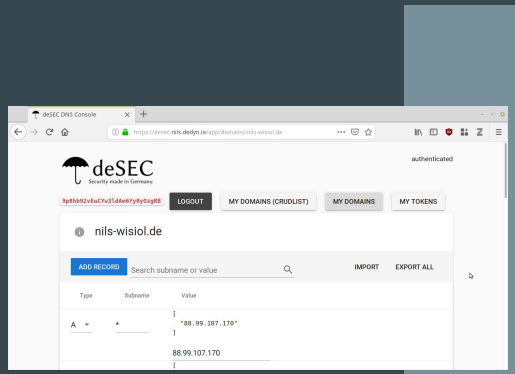
- **Security**
  - DNSSEC ✔

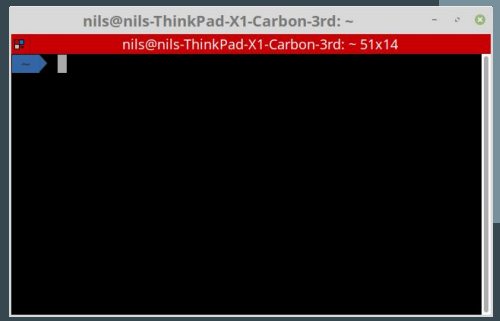
- **Organization**
  - Data protection ✔
  - European laws ✔
  - Free open-source software ✔
  - Low cost hosting ✔

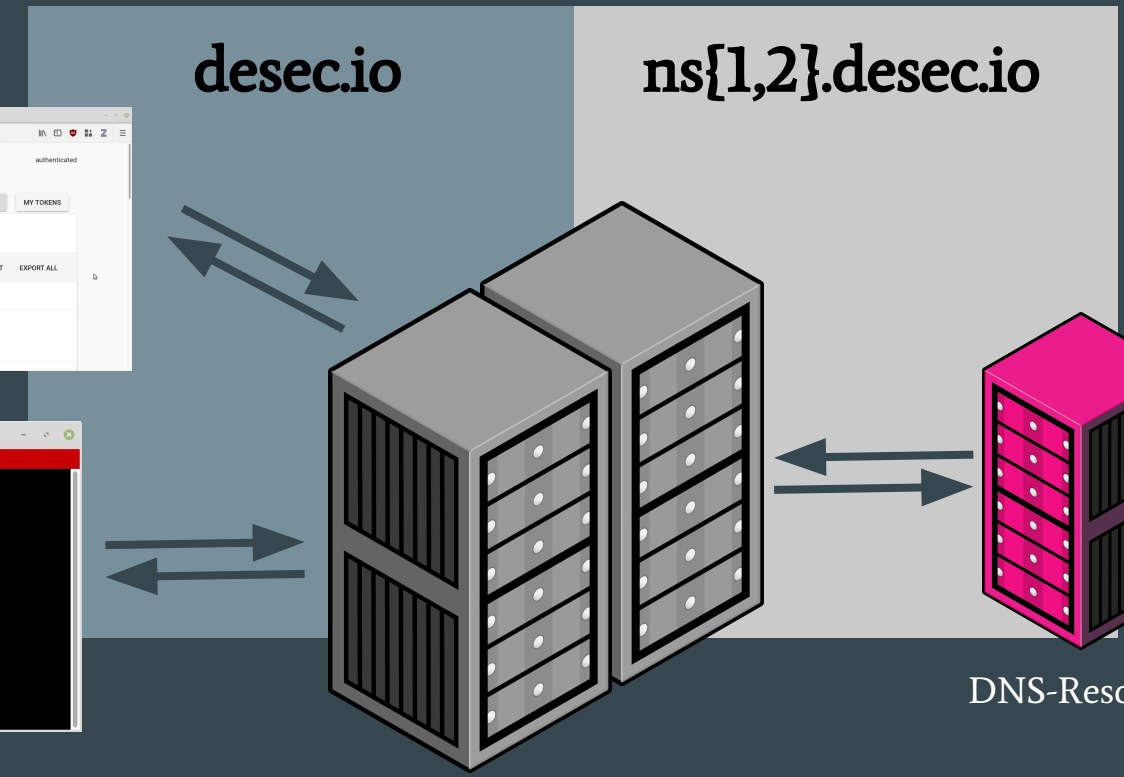
Section 4

# Technical Solution

# Public Interfaces: HTTP, DNS



# Internal Structure

HTTP

## desec.io

Frontend HTTP/TLS Server

Static Web Content

API

API Database

Signing Server

Private DNS Database

Master DNS Server

Public DNS Database

## 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!

12.02.2019 · Datengarten/97 · CCC Berlin

deSEC
Dr. Peter Thomassen
Nils Wisiol

Donations kindly accepted: we take money and code