Multisigner Support at deSEC

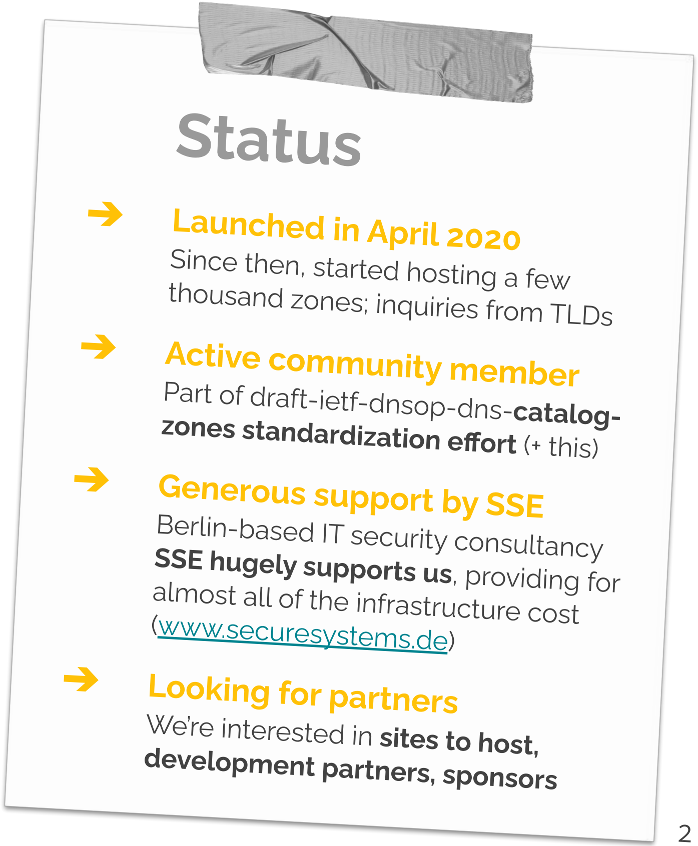
DNSSEC and Security Workshop at ICANN 70

Peter Thomassen (SSE Secure Systems Engineering)
<peter@desec.io>

A free DNS hosting service, designed with security in mind.

We are a **non-profit** doing the same thing as **Let's Encrypt, but for DNSSEC**.

- all **automatic** DNSSEC
- **fancy API** and GUI
- support for modern stuff (SMIMEA, **DANE**/TLSA, long **OPENPGPKEY**, **HTTPS/SVCB**)
- **dynDNS** service (under dedyn.io)



Status

→ **Launched in April 2020**
Since then, started hosting a few thousand zones; inquiries from TLDs

→ **Active community member**
Part of draft-ietf-dnsop-dns-**catalog-zones standardization effort** (+ this)

→ **Generous support by SSE**
Berlin-based IT security consultancy **SSE hugely supports us**, providing for almost all of the infrastructure cost (www.securesystems.de)

→ **Looking for partners**
We're interested in **sites to host, development partners, sponsors**

But why?

- DNSSEC:

😩	🥳
state	appeal

- There’s no other DNSSEC provider out there that’s free (really), feature-complete, and seriously stable.

- We figured it’s time.

How it works

Backend

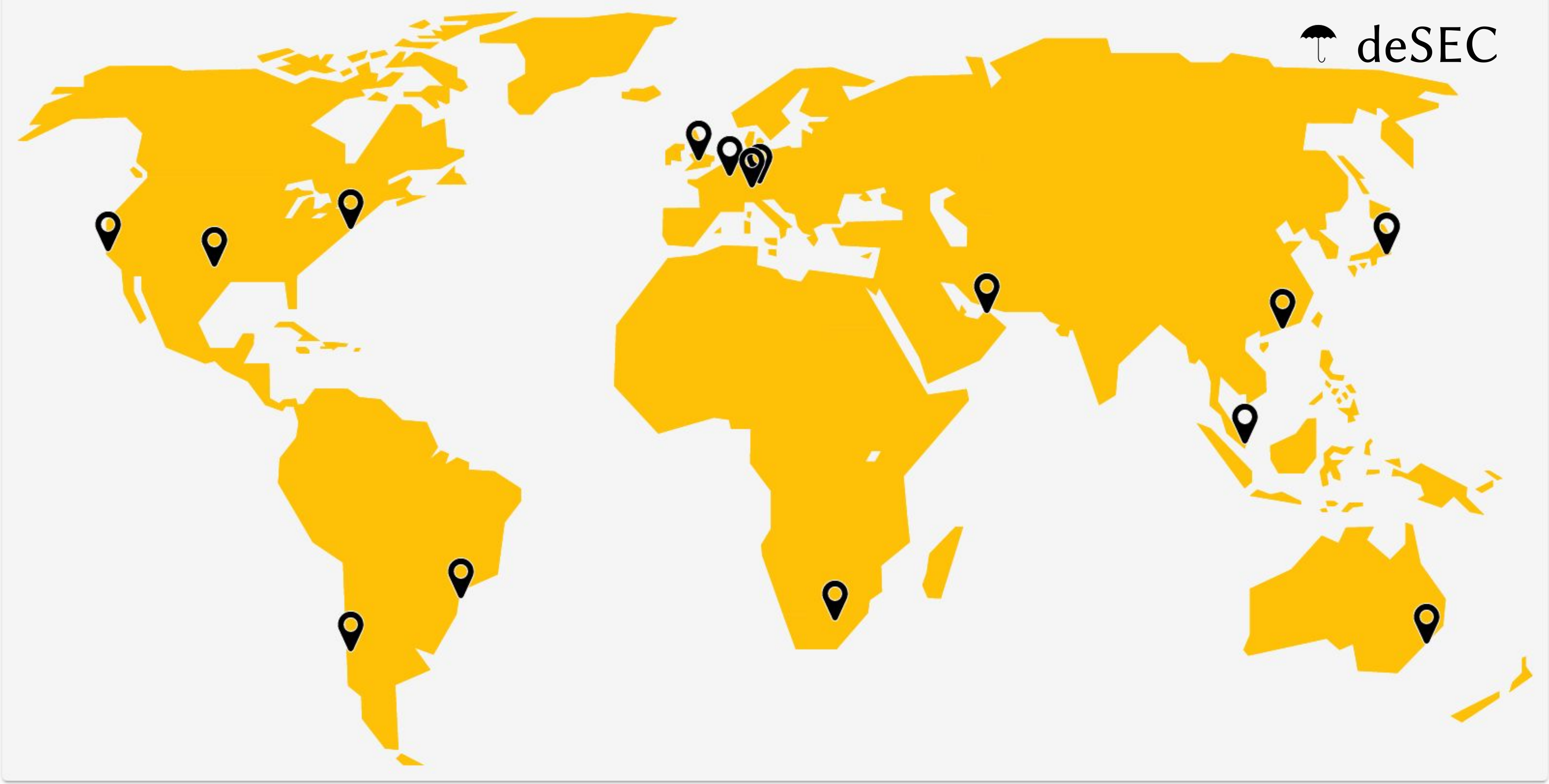
- Tech stack:
  - **PowerDNS** engine
  - **Django** for the API
  - **Postgres** database
  - **RabbitMQ** for queues
  - **Memcached** for caches
  - **Prometheus** for monitoring
  - **OpsGenie** alerting
- **signing happens in Germany**

DNS Frontend

- **2 anycast networks** under **independent TLDs**
  - **15 POPs** worldwide
  - capable of serving **~1M zones**
- **instantaneous replication**
  - both via catalog zones / AXFR, and via git
- Tech stack
  - **dnsdist** gateway
  - **diverse auth** vendors

User Frontend

- **Vue.js GUI**
- **REST API**
  - transactional bulk ops
- **integration** (dnscontrol, Traefik, Terraform, various ACME clients / routers)
- **libraries** (Ansible, Go, Python, PHP, JavaScript)



deSEC

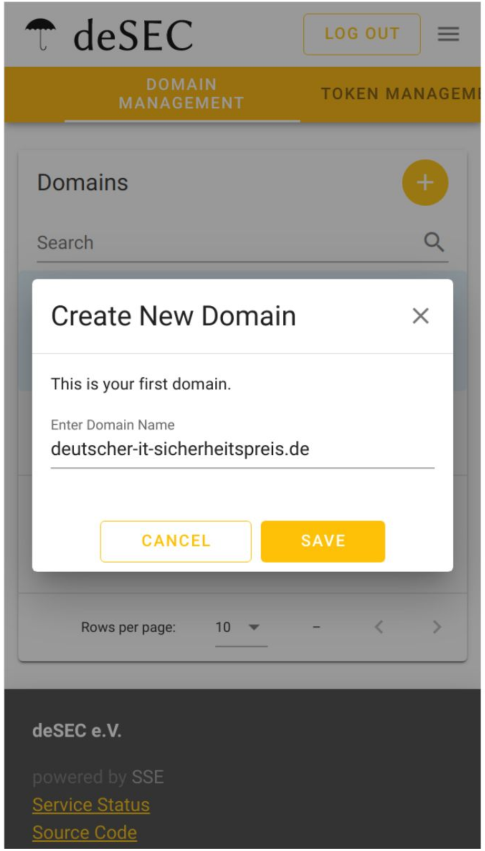
Using deSEC 101

GUI

- Straightforward
- Reactive
- Field-level validation
- Mobile-friendly
- Zero external resources

REST API

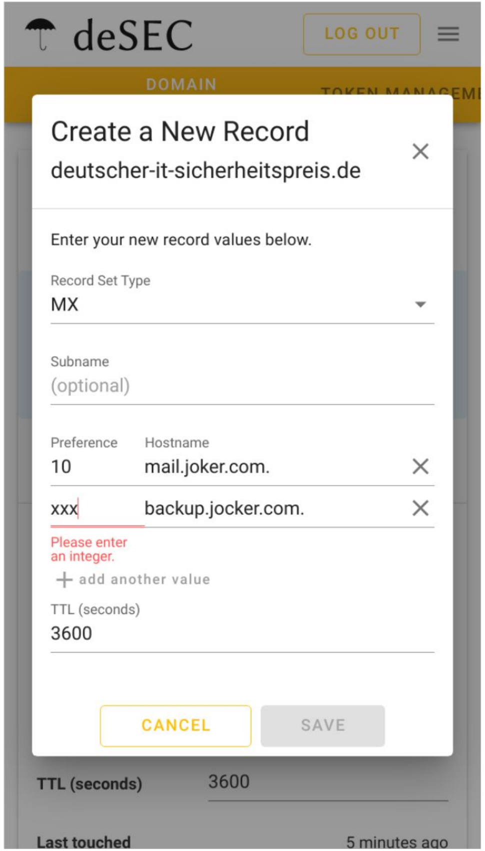
- Transactional bulk actions
- Helpful validation
- Paging
- API token scoping
- docs: https://desec.rtfd.io/



Create New Domain

This is your first domain.

Enter Domain Name
deutscher-it-sicherheitspreis.de



Create a New Record
deutscher-it-sicherheitspreis.de

Enter your new record values below.

Record Set Type
MX

Subname
(optional)

Preference: 10 — Hostname: mail.joker.com.

xxx — backup.jocker.com.

Please enter an integer.

TTL (seconds)
3600

TTL (seconds) 3600

Last touched 5 minutes ago

Demo time!

https://youtu.be/m6KZx8c_wig

Enabling Multi-Signer DNSSEC Models (RFC 8901)

- Multi-signer scenarios require all signing parties to **publish the other parties' public keys**
  - achieved by adding their keys to the DNSKEY record set (RFC 8078)
- deSEC **automatically publishes its own DNSSEC records**
  - e.g. DNSKEY/CDS/CDNSKEY (using the CSK key model)
- deSEC now **supports provisioning extra DNSKEY records**
  - Queries are answered with a merged RRset (automatic + manual values)
  - The same applies for CDS/CDNSKEY
- For fully automatic migration of NS RRsets, **CSYNC is needed**
  - not yet supported (PowerDNS dependency)