



DNS4EU

scope, timeline and challenges

Robert Šefr | CTO



Co-funded by
the European Union

DNS4EU goals

The goal of DNS4EU is to provide EU citizens, companies, and institutions with a secure, privacy compliant, and powerful recursive DNS. The EU desires to make this the officially recommended DNS resolver for public and governmental institutions.



EU's Digital Sovereignty

The European Commission aims to keep user's data in the Union digital space to support its digital independence and sovereignty.



Onboard 100 Million People

The goal of the DNS4EU is to collaborate with various EU stakeholders to significantly improve the Internet in the EU for many citizens.



Privacy

Citizens of the EU should be provided with DNS resolution that adheres to the highest privacy standards, incl all the EU data privacy regulations.



Security

The consortium combines multiple cybersecurity experts from different EU countries that will work together to provide the safest DNS resolution.



Co-funded by
the European Union

DNS4EU Consortium

Consortium Members

- Whalebone, s.r.o. ()
- CZ.NIC ()
- Czech Technical University Prague ()
- Time.lex ()
- deSEC ()
- Sztaki ()
- ABI Lab Centro di Ricerca e Innovazione per la Banca ()
- Naukowa i Akademicka Sieć Komputerowa ()
- Directoratul Național de Securitate Cibernetică ()

Associated Partners

- Ministry of Electronic Governance ()
- CESNET ()
- F-Secure ()
- Centro Nacional de Cibersegurança ()



Co-funded by
the European Union

Whalebone overview

Name and date of incorporation

Whalebone, s.r.o.
Incorporated 05/2016
HQ Czech Republic, Brno

Team size

80 (Q3/2023)

Status

Growth, scaling up

Industry

SaaS Network Security, B2B2C(B), B2B, B2G

Customer Segments

Big telcos (Aura; main use case), ISPs (Peacemaker),
Corporates & Government (Immunity)

Security problem / opportunity

90% of attacks use an internet domain request - Whalebone blocks access to malicious domains on the DNS level.

Users' sensitive data are often stolen and misused, which can be devastating. Whalebone protects users' identity.

Customers want / expect security from their telecoms and are not receiving it (enough).



Co-funded by
the European Union

DNS4EU overview



Threat Intelligence

- Intelligence generated based on the DNS4EU traffic
- Regional intelligence research



DNS for Telcos

- On-premise resolver for Telcos
- DNS4EU Threat Intelligence (DNS4EU shared IP)



DNS for Governments

- Protective DNS for governments
- DNS4EU Threat Intelligence (DNS4EU shared IP)



DNS for Public

- Public DNS service
- DNS4EU Threat Intelligence
- DNS4EU shared IP



Co-funded by
the European Union

Threat Intelligence

Based on DNS4EU traffic

- Actual DNS4EU traffic will be analyzed for new threats and trends
- DNS traffic trends will also be used for false positive mitigation
- Mitigation of global threats
- Tuning the protection accuracy

Regional intelligence exchange

- Setup (or reuse of existing) of platform to exchange the regional Threat Intelligence
- Cooperation with local CERTs/CSIRTs and commercial organizations
- Immediate impact on the DNS4EU resolvers



DNS for Telcos

- Telcos are losing control over the traffic and options for optimizations as some users are switching for public DNS providers
- Some end-users may feel lost in the Telco privacy policy or struggle with standard compliance
- Hosted either on shared IP with public resolvers or own telco IP

Telcos

- On-premise DNS resolvers
- National regulatory compliance
- Telco grade resolver including API, monitoring, logging, troubleshooting, and integration features
- DoH / DoQ out of the box, but still processed within Telco infra

End-users

- Lower latency than public resolvers
- Transparent privacy policy
- Optional protective features

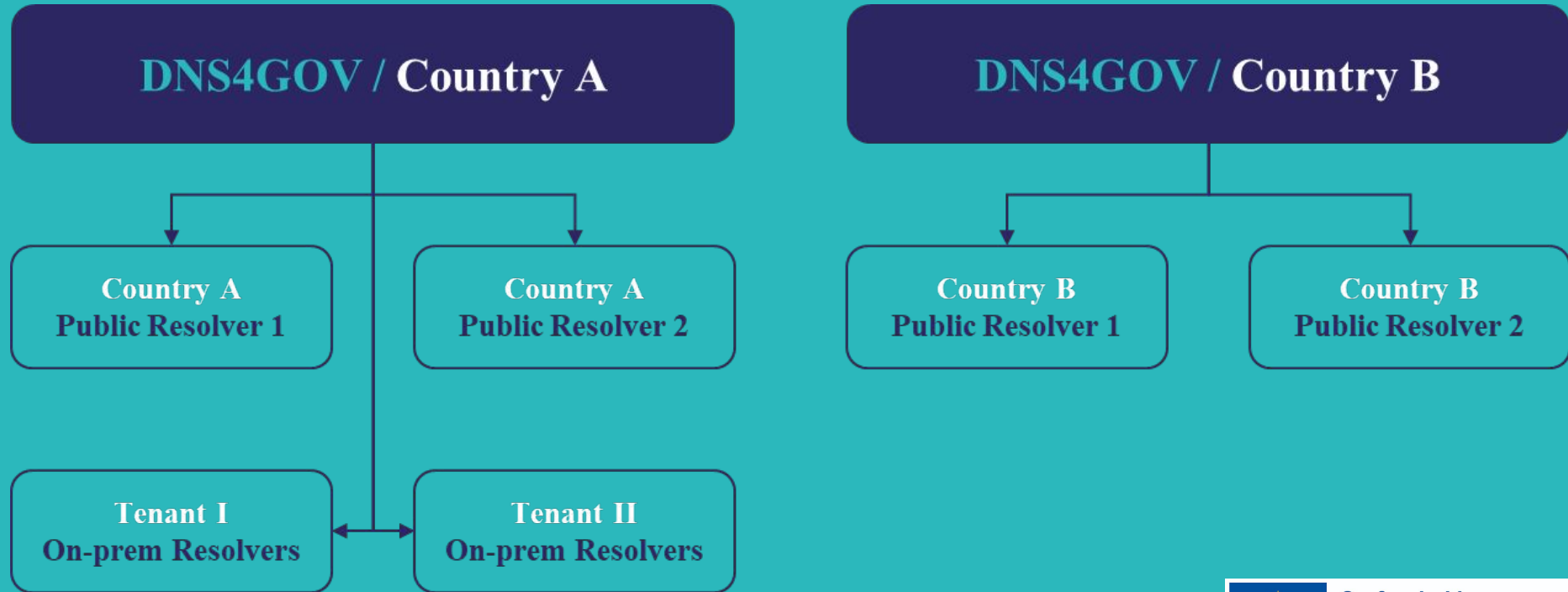


DNS for Governments

- There are many underprotected public organizations (offices, hospitals, schools)
- To fix the issue, governments around the world have started implementing Protective DNS on a countrywide level
- **UK, Australia, Canada, US** have been running DNS country-wide services for public already for some time, built as turnkey projects
- Rather than a turnkey project, DNS4EU will offer a ready-made product to be deployed (and/or customized) for any region/country



DNS for Governments Architecture



DNS for Public

- Public and distributed DNS resolvers managed by the consortium members
- Multiple anycast IP addresses / hostnames for different flavours
 - Plain DNS
 - Protective DNS
 - Protective DNS + Adult content blocking
 - ...
- Shared IP / hostname with the “DNS for Telcos” if the Telco chooses to do so
- Support for IPv4/IPv6, DNSSEC, DNS over TLS, DNS over HTTPS, (DNS over QUIC)



Content filtering aspects

Public

- Any filtering opt-in only
- Option for pure DNS resolution
- No regulatory / legal blacklists applied

Governments

- Only for governmental institutions
- Set by the respective administrator as a protective measure

Telcos

- DNS4EU will provide compliance with local law
- Net Neutrality still applies



Privacy aspects

Public

- Fully anonymous
- Premium service may need some identifier

Governments

- IPs are logged for investigation purposes
- Security service rather than just infrastructure

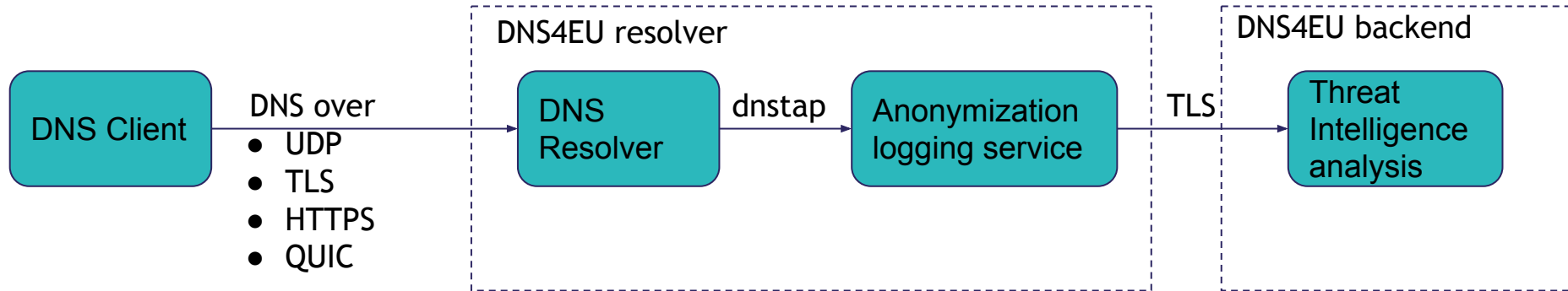
Telcos

- Shared IP -> Follows the DNS for Public policy
- Own IP -> Privacy policy defined by Telco



DNS for Public / Anonymization

- Following RFC 8932 (Recommendations for DNS Privacy Service Operators)
- No client IP address will be logged or stored in any other way
 - Source ASNs may be logged
 - Source IP will only appear in memory to process the query



Knot Resolver change candidates

- (D)DoS protection
 - Configurable reflection and amplification attacks protection
- Fallback on unavailable Authoritative Servers
 - Avoid impact on a single resolver being unable to properly communicate
- Cache prediction improvements
 - Improve chances to keep the proper cache records warm
- DNS over QUIC protocol support



Co-funded by
the European Union

DNS4EU/High level timeline

2023

**Preparations
and kick-offs**

- Technology, Security and standards compliance designs
- Backend deployment
- Research kick-offs
- Attracting Telcos and Governments

2024

**Telco and Gov
deployments**

- Regional Threat Intelligence exchange setup
- Legislation and Security requirements compliance achieved

2025

**Attracting
end-users**

- Discoverability
- Attracting end-users
- Scaling the deployments as needed

2026+

**DNS4EU
post-project
continuation**

- Continuous improvements



Co-funded by
the European Union

Connect me on LinkedIn



Thank you



Robert Šefr

Whalebone CTO

robert.sefr@whalebone.io



Co-funded by
the European Union