whalebone

Shielding Europe

DNS4EU: Pan-European Protective DNS Service for 100 Million Users

Andronikos Kyriakou | Tech Consulting Lead

Co-funded by the European Union

DNS4EU = secure, resilient and private Internet

"...the deployment of a recursive **European DNS resolver service (hereafter DNS4EU)** serving socio-economic drivers, public, corporate and residential internet end-users in the EU, and offering very high reliability and protection against global cybersecurity threats and those **specific to the EU** (e.g. phishing in EU languages).
This is a key policy action announced in the 2020.“

Co-funded by the European Union

DNS4EU Consortium

Consortium Members

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

Associated Partners

- Ministry of Electronic Governance (BG)
- CESNET (CZ)
- F-Secure (FI)
- Centro Nacional de Cibersegurança (PT)

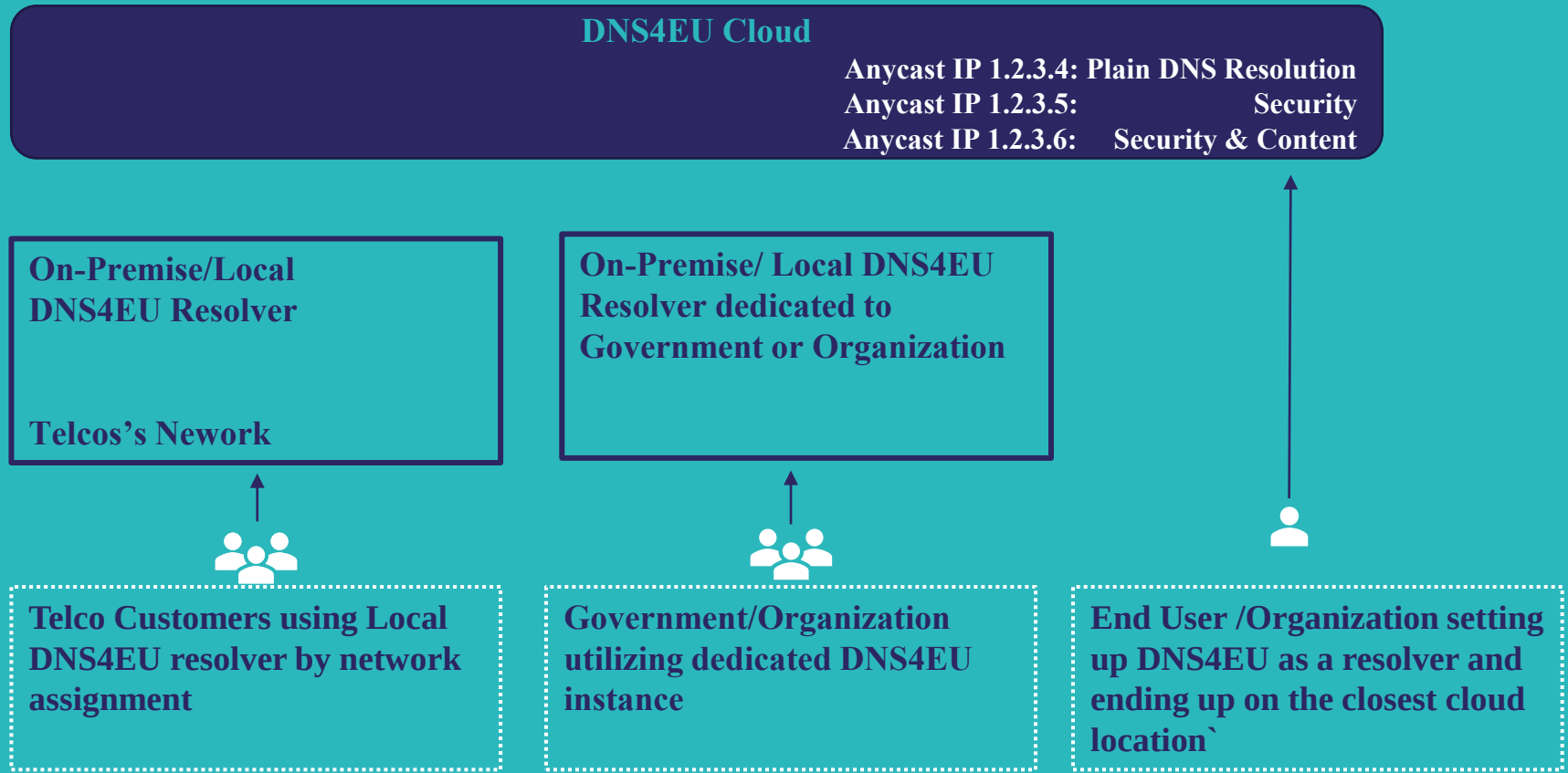
Co-funded by the European Union

Project Requirements and proposed Architecture

Resilience, privacy, and cross-disciplinary collaboration

- Highly-distributed and federated recursive DNS resolver operated within the EU, combining Cloud-based and On-premise instances
- Following EU privacy standards/ GDPR
- Adhering to latest internet security and privacy standards (e.g. DNSSEC, DoH, DoT, full IPv6 compliance)
- Honoring national legislation including lawful filtering
- Offering high reliability and low latency
- Making available protection against cyberthreats and continuously working on threat intelligence research

High Level Architecture



DNS4EU overview

Threat Intelligence

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

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 end-users

- 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
- Refining the effectiveness of protection

Regional intelligence exchange

- Establishing (or leveraging existing) threat intelligence sharing platforms
- Cooperation with local CERTs/CSIRTs and commercial entities
- Immediate use on DNS4EU resolvers

Co-funded by the European Union

DNS for Telcos

- Operators lose control over traffic and thus options for optimization possibilities, as some users switch publicly available DNS resolvers
- Some end users are not familiar with the privacy settings of operators or are not comfortable with the standard settings

Operators

- On-premise DNS resolvers
- Compliance with national regulations
- Support for DNS standards
- Telco-grade resolver including API, monitoring, logging, troubleshooting and integrations features

End Users

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

Co-funded by the European Union

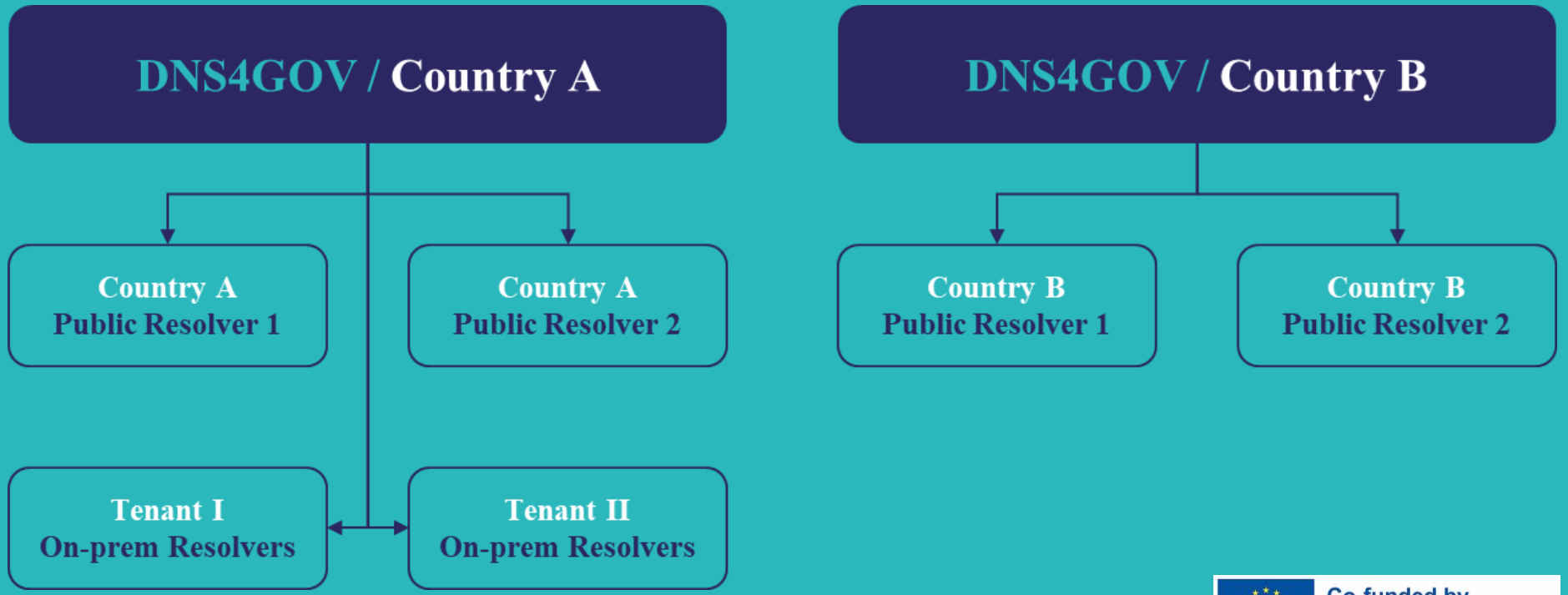
DNS for Governments

- 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** 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

- **Telcos are an ideal partner for B2G sales**

Co-funded by the European Union

DNS for Governments Architecture



Co-funded by
the European Union

DNS for end-users

- 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)

Co-funded by the European Union

DNS4EU/High level timeline

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

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

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

- Continuous improvements

Co-funded by the European Union

DNS4EU in a nutshell

The goal of DNS4EU is to provide EU citizens, companies, and institutions with a secure, privacy compliant, and powerful recursive DNS.

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

Thank you!
Questions?

Connect with me on LinkedIn

Andronikos Kyriakou
Tech Consulting Lead
andronikos.kyriakou@whalebone.io

Co-funded by the European Union