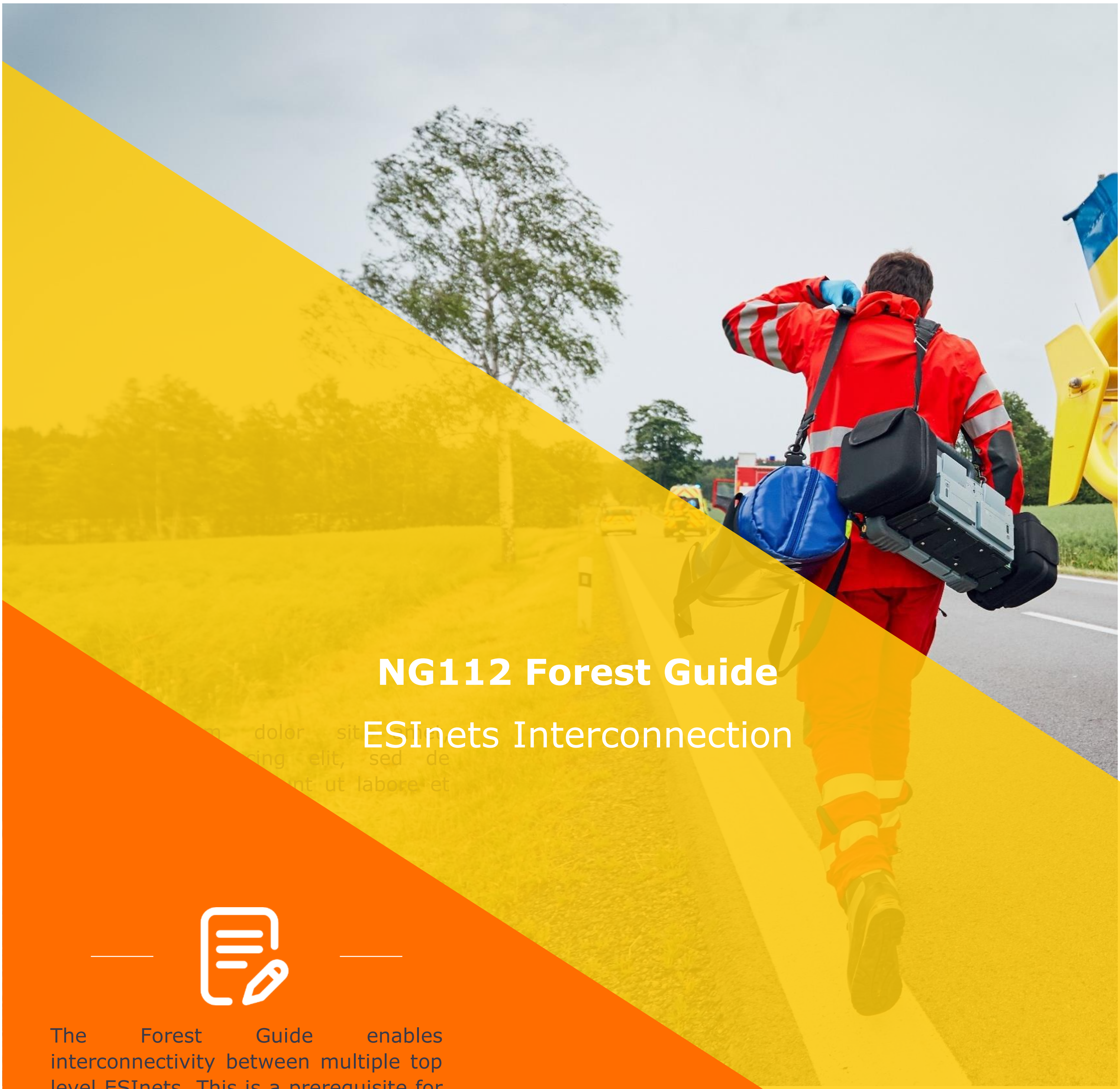


NG112 Forest Guide

ESInets Interconnection

m dolor sit amet,
cing elit, sed de
nt ut labore et

The Forest Guide enables interconnectivity between multiple top level ESInets. This is a prerequisite for interconnecting ESInets across Europe and route emergency communications between different European countries. Technically, it uses established mechanisms from the Domain Name System (DNS), enabling each country to deploy, change and update their own ESInet infrastructure transparently and keep their local autonomy.

NG112 Forest Guide

EENA
European Emergency Number Association
EENA 112
Avenue de la Toison d'Or 79, Brussels, Belgium
T: +32/2.534.97.89
E-mail: info@eena.org

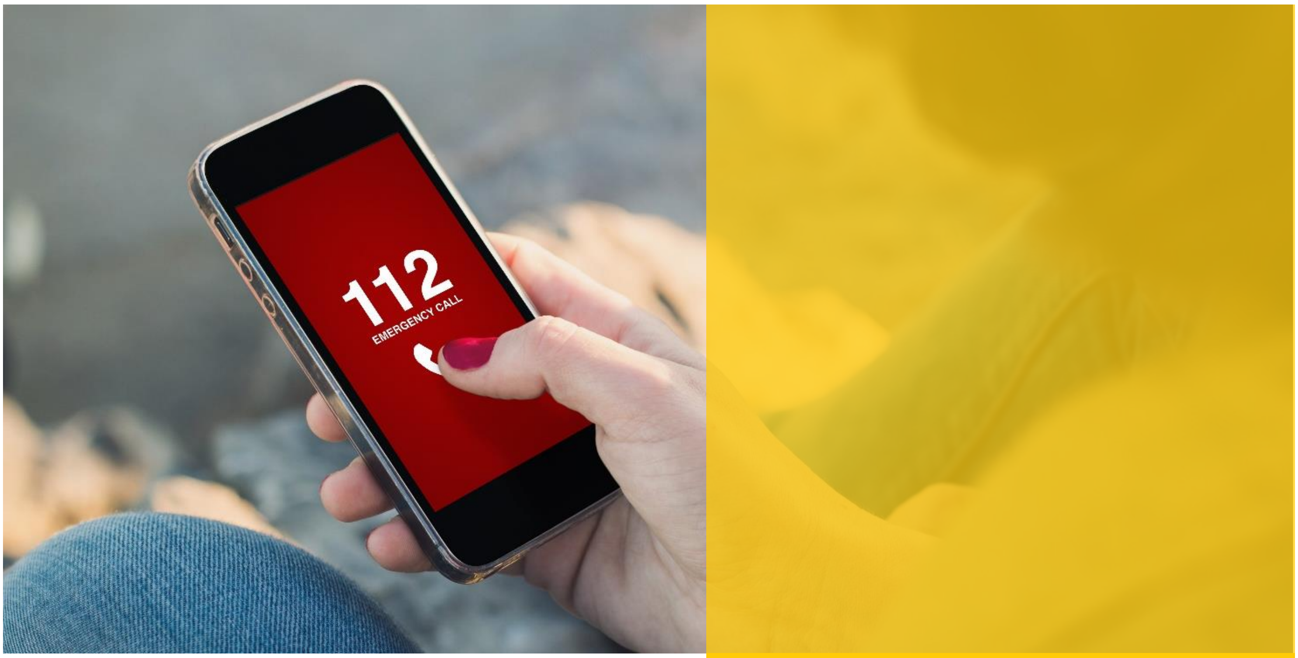
Version: 1.0
Publication date: 11/10/2022
Status of the document: FINAL

Author(s):
Michael Pröstler, GridGears

Contributor(s):
Wolfgang Kampichler, Frequentis
Cristina Lumbreras, EENA

LEGAL DISCLAIMER:
This document is authored by EENA staff members with contributions from individual members of EENA and represents the views of EENA. This document does not represent the views of individual members of EENA, or any other parties.
This document is published for information purposes only and it does not declare to be a statement or interpretation of EU law or the national law of EU Member States. This document is entirely without prejudice to the views of relevant national statutory authorities and their legal functions and powers, whether under EU law or the national law of their Member State. Accordingly, under no circumstances may reliance be placed upon this document by any parties in compliance or otherwise with any applicable laws. Neither may reliance be placed upon this document in relation to the suitability or functionality of any technical specifications, or any other matters discussed in it. Legal advice, technical advice and other advice as relevant, may be sought as necessary.

EXECUTIVE SUMMARY 4
1 | INTRODUCTION 4
Challenges 4
2 | EMERGENCY SERVICES IP NETWORK 5
Border Control Function (BCF) 5
Emergency Services Routing Proxy (ESRP) 5
Emergency Call Routing Function (ECRF) 5
Location Information Service (LIS) 6
European Perspective 6
3 | FOREST GUIDE 6
Purpose and Functionality 6
Basic Concepts 6
Local Autonomy vs. Centralisation 7
4 | TECHNICAL REALISATION 8
Domain Name System (DNS) 8
Next Generation 112 8
5 | SHARED DATA 12
Geographical Data 12
Domain Names 12
Security 12
6 | SUMMARY 13



EXECUTIVE SUMMARY

Interoperability and interconnectivity are the cornerstones of modern emergency services.

In addition to the challenge of establishing an Emergency Service IP Network (ESInet) and hosting the NG112 core components, it is yet another one to interconnect with other ESInets from different authorities.

The NG112 architecture not only provides a blueprint for the core components within an ESInet, but also defines the Forest Guide as the element to establish interconnectivity between multiple ESInets. The Forest Guide enables local autonomy and leverages well known principles to allow multiple independent Forest Guide installations while keeping the local ESInet’s autonomy.

This document intends to provide a blueprint for the core components within an ESInet, and also defines the Forest Guide as the element to establish interconnectivity between multiple ESInets.

1 | INTRODUCTION

Challenges

In the past, without mobiles, where only landlines were available, it was quite easy to route a call based on the correlating address of the landline. Fast forward a couple of decades ahead, we now live in an interconnected world, using mobile devices for voice, video and text in our communication, sending pictures and sharing our location or any other data with our friends and family.

In emergency situations, this additional data provides better situational awareness and enables access to emergency services for everybody. We can now start emergency communications via websites, mobile applications and even automatically in the case of a car accident. Due to the limitless access to emergency services, we find ourselves in situations where an emergency communication is received in country A while the actual person is in a different country B. This can be due to VPNs, Cell Towers covering an area of a different country (especially close to borders) or even Third Party eCalls. In all those situations, the emergency communication and/or additional data needs to be routed to the appropriate PSAP, which might be in a different country.

The Forest Guide is the key component within the NG112 Architecture to interconnect ESInets in those situations and enable routing between them.

2 | EMERGENCY SERVICES IP NETWORK

The Emergency Service IP Network (ESInet) hosts multiple core components specified by the NG112 architecture, including:

- Border Control Function (BCF)
- Emergency Services Routing Proxy (ESRP)
- Emergency Call Routing Function (ECRF)
- Location Information Service (LIS)

Border Control Function (BCF)

The BCF is the entry point (point-of-interconnect) to an ESInet. It can be seen as a firewall and additional security layer protecting the core elements. Once an emergency communication is received at the BCF, it is forwarded to a well known Emergency Service Routing Proxy (ESRP).

Emergency Services Routing Proxy (ESRP)

The ESRP with its corresponding Policy Routing Function (PRF) provides the powerful and dynamic routing capabilities of the NG112 architecture. Multiple rules are evaluated in order to determine the most appropriate PSAP or next hop to forward the emergency communication to.

Emergency Call Routing Function (ECRF)

The ECRF is queried by the ESRP to provide information about which service (e.g PSAP) is responsible for a specific service type (e.g. urn:service:sos, urn:service:sos.police, etc.) at a specific location. This query is performed using the LoST protocol, more specifically, using the findService request.

Location Information Service (LIS)

The LIS can be seen as an additional service that can provide location information for a specific entity (e.g. a mobile phone) via the HTTP-enabled Location Discovery (HELD) protocol, which uses PIDF-LO to represent location information.

European Perspective

ESInets can be deployed in a hierarchical structure based on the responsible authorities and the underlying structure of responsibilities. From an European perspective, the Forest Guide only interconnects the ESInets of countries. The internal hierarchical structure is the responsibility of each country and not considered by the Forest Guide.

One of the most important aspects, besides the concept of Local Autonomy, which is explained in detail in section Local Autonomy vs. Centralisation, is that the Forest Guide is not a centralized concept, but that there can and should be multiple Forest Guide providers.

3 | FOREST GUIDE

Purpose and Functionality

The main purpose of the Forest Guide in Europe is to interconnect the ESInets of the individual countries. It can be seen as a map-based dictionary where you can look up the responsible ESInet for a certain location. Instead of providing the technical information about an ESInet directly, the Forest Guide provides a pointer, where additional information about the responsible ESInet can be found. This pointer can then be used to retrieve the technical endpoints for different services within the ESInet.

Usually, a Forest Guide is contacted when an ESInet receives an emergency communication with a location outside of its jurisdiction. More precisely, if the Emergency Call Routing Function within the ESInet has no knowledge / mapping for a certain location, it can query the Forest Guide, which will then return the responsible domain name. The ECRF can resolve the ESInet's routing service for the returned domain, which can then provide the necessary routing information. The term "Forest Guide" is derived from the fact that ECRFs can be deployed in an hierarchical structure (tree-like) and the Forest Guide is the element to interconnect / navigate between those trees, which form the forest.

Basic Concepts

The mechanisms used by the Forest Guide are similar and actually re-use concepts of the well known Domain Name System (DNS), which we all use on a daily basis when using the internet.

As an example, let's take the domain *eena.org* which is owned by the "*European Emergency Number Association"*. We can use this domain name in several ways by using different services, which are configured and provided by the "*European Emergency Number Association".* We can use the *https* service of the domain by typing it into our browser and visiting the website. Alternatively we could use the *mail* service of the domain and write a mail to *info@eena.org*. Although we use the same domain name in both scenarios, the technical infrastructure (e.g. web and mail server) can be completely separated and could even be running on different providers. The actual technical endpoint is only the result of the domain name resolution for a specific service.

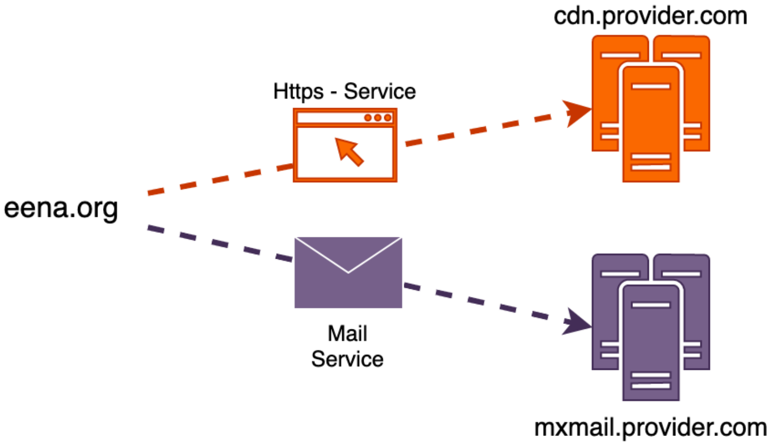


Figure: Domain / Service Resolution

The Forest Guide uses the same concepts. We can query the Forest Guide to retrieve the responsible ESInet for a certain location. The ESInet itself is represented by a domain name, owned by the responsible operator of the corresponding ESInet.

From an European perspective, the Forest Guide is configured with the geographic borders of the European countries and their ESInets' domain names. For example, it could resolve locations to government owned domain names, such as esinet.belgium.gov.be. However, those domain names can be freely chosen, but it is important that the owner of the domain name is also responsible for the ESInet in order to leverage local autonomy.

Local Autonomy vs. Centralisation

Using the previous example, the European Emergency Number Association owns the domain name eena.org and can autonomously manage the underlying services. The organization can freely add and remove services, resolve to other technical endpoints, change providers etc. The organization owning the domain name is in full control and can do everything without having to notify anyone or change the domain eena.org itself. This is referred to as Local Autonomy.

Accordingly, all the necessary information about the services within a country's ESInet can be resolved by the corresponding domain name. This is in direct contrast to centralized services, where all the configuration is within that centralized services. In this way, the Forest Guide only acts like a search engine without any direct knowledge about countries' ESInets.

In order to realize this search engine, the following two European datasets need to be available:

- Geographical borders
- Domain Names

Details regarding those datasets are explained in section Shared Data. At this point, it is important to understand that this data as such is no secret and can be well known to the public, similar to today's emergency number information.

Although it might seem that there would only be one single Forest Guide, this concept actually enables multiple implementations of European Forest Guides, since the underlying data is well known and the configuration is decentralized and leverages local autonomy. This takes away the massive burden of deciding who will provide and operate a Forest Guide on an European level. Multiple Forest Guides can co-exist, thus enabling great redundancy, flexibility and preventing dependency on a single provider or implementation.

4 | TECHNICAL REALISATION

Domain Name System (DNS)

As explained in the previous sections, a Forest Guide uses domain names in order to leverage local autonomy and decentralization using concepts based on the Domain Name System (DNS).

Considering the eena.org domain name for example. Besides the "normal" resolution of the domain name to a web server, additional data for that domain is stored in the DNS in the form of so-called Records. The Mail Exchange (MX) records specify the Fully Qualified Domain Name (FQDN) of the corresponding mail server for that domain. Again, this is public information and it can be easily retrieved by using any DNS tool, such as "nslookup".

Example:

```
% nslookup
> set type=mx
> eena.org

Non-authoritative answer:
eena.org       mail exchanger = 20 alt2.aspmx.l.google.com.
eena.org       mail exchanger = 30 alt3.aspmx.l.google.com.
eena.org       mail exchanger = 10 aspmx.l.google.com.
eena.org       mail exchanger = 30 alt4.aspmx.l.google.com.
eena.org       mail exchanger = 20 alt1.aspmx.l.google.com.
```

Next Generation 112

In the context of NG112, so-called Naming Authority Pointer (NAPTR) Resource Records are used to resolve a specific service of a specific domain. The following illustrates and describes the technical details.

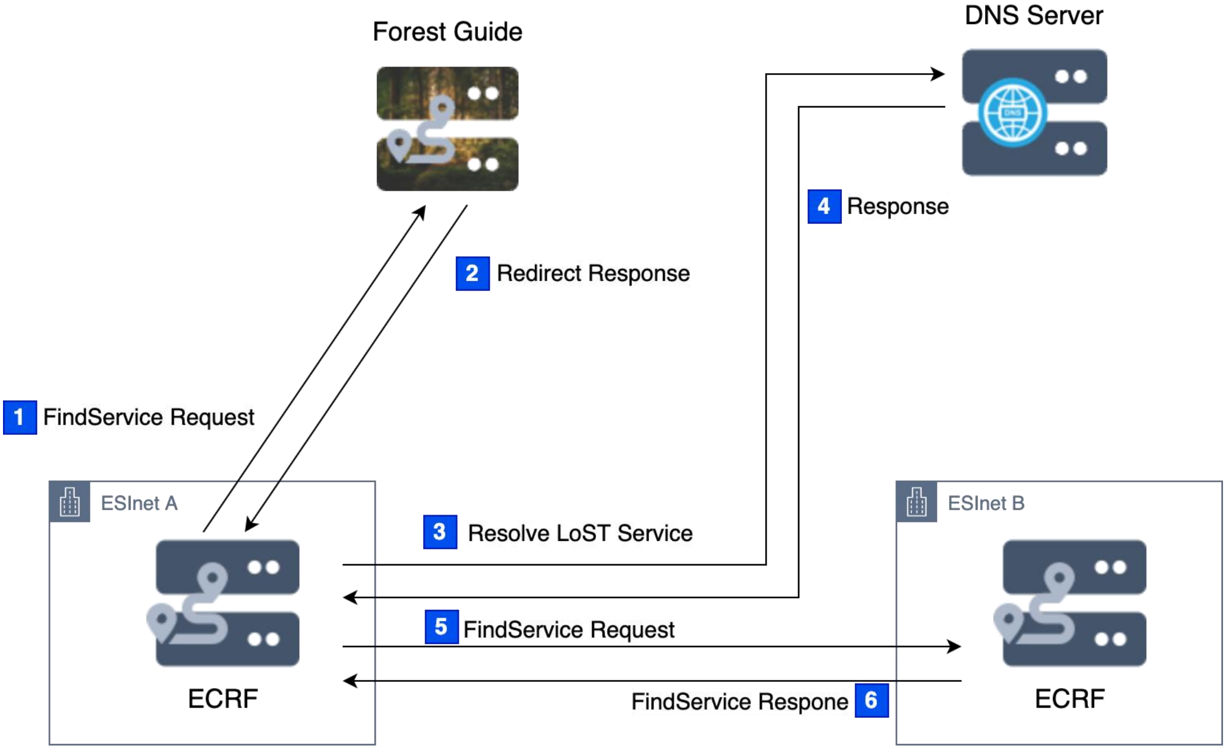
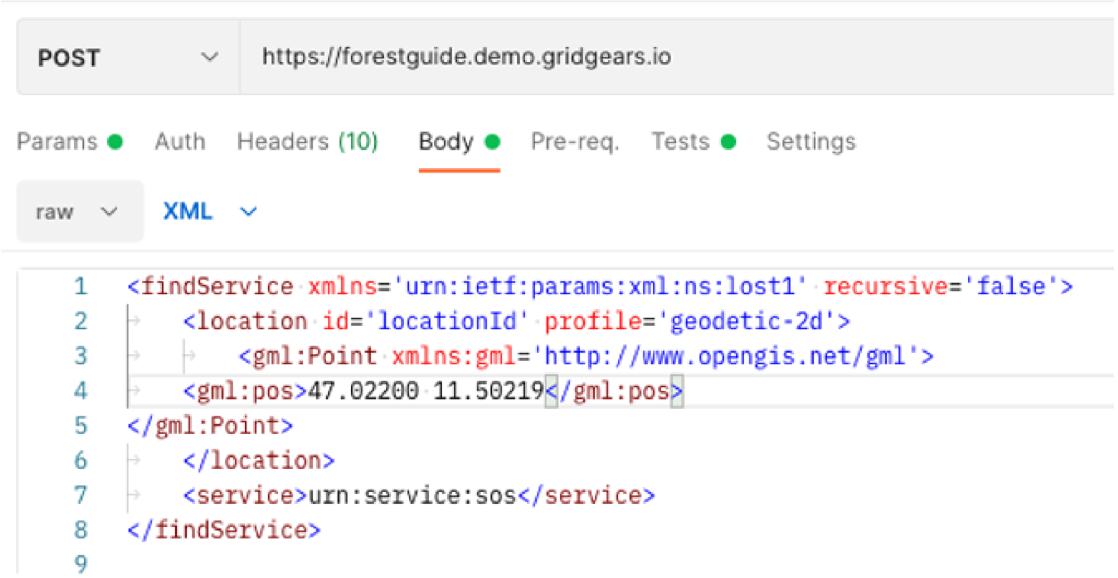


Figure: Sequence Overview

1. FindService Request

As described, when an ECRF wants to resolve the next destination for an emergency communication for a location outside its jurisdiction, it queries a Forest Guide. The figure below shows a findService request to the Forest Guide.



POST https://forestguide.demo.gridgears.io

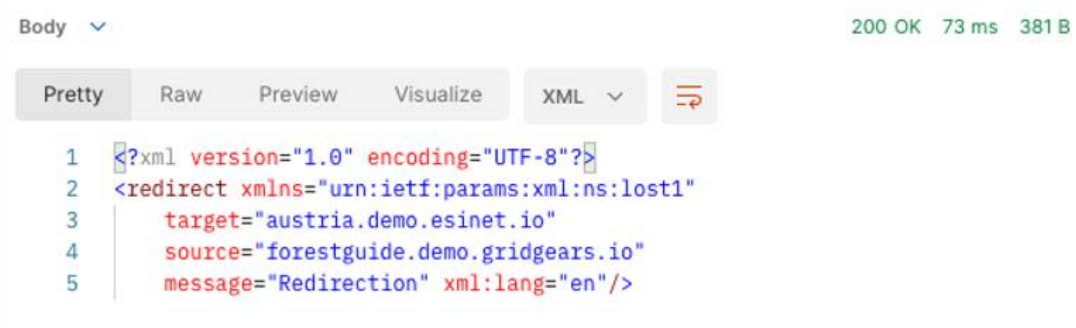
raw XML

```xml
<findService xmlns='urn:ietf:params:xml:ns:lost1' recursive='false'>
    <location id='locationId' profile='geodetic-2d'>
        <gml:Point xmlns:gml='http://www.opengis.net/gml'>
    <gml:pos>47.02200 11.50219</gml:pos>
</gml:Point>
    </location>
    <service>urn:service:sos</service>
</findService>
```

Figure: Example FindService Request to Forest Guide

2. Redirect Response

The Forest Guide returns a redirect response, including the domain name responsible for this specific location as shown in the figure below:



```
<?xml version="1.0" encoding="UTF-8"?>
<redirect xmlns="urn:ietf:params:xml:ns:lost1"
    target="austria.demo.esinet.io"
    source="forestguide.demo.gridgears.io"
    message="Redirection" xml:lang="en"/>
```

Figure: Example Redirect Response

In this example, the Forest Guide redirects the ECRF from ESInet A to the domain *austria.demo.esinet.io*.

3. Resolve LoST Service

In the next step, the ECRF needs to resolve the Fully Qualified Domain Name (FQDN) of the ECRF in ESInet B. To achieve this, it uses DNS resolution to resolve the NAPTR record provided by the domain name.
For demonstration purposes, we can use the command line tool "dig" to fetch this information as shown in the following:

```
% dig -t naptr austria.demo.esinet.io
```

4. Response

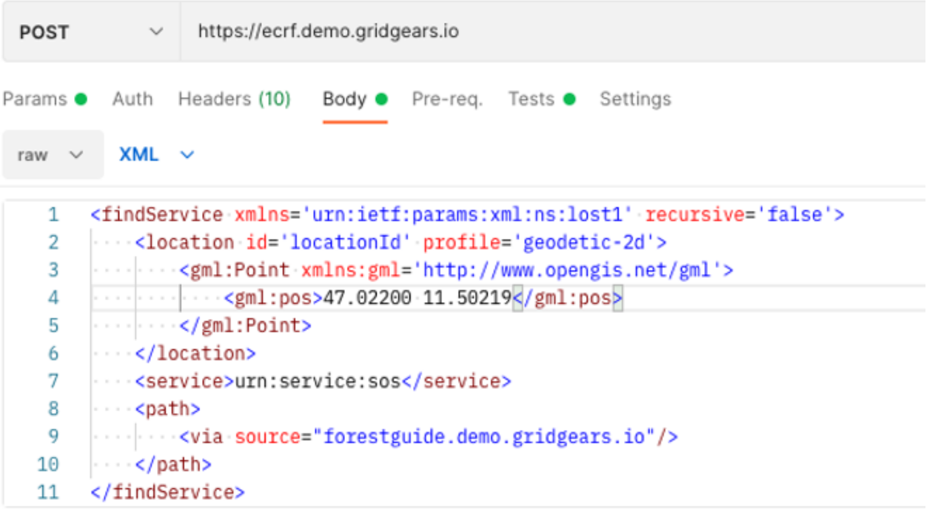
When receiving the response of NAPTR records from the DNS, the ECRF can extract the FQDN of the ECRF in ESInet B.

```
; <<>> DiG 9.10.6 <<>> -t naptr austria.demo.esinet.io
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38763
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;austria.demo.esinet.io.             IN      NAPTR

;; ANSWER SECTION:
austria.demo.esinet.io.       300     IN      NAPTR   100         50          "U"          "LoST:https"
"!^.*$!https://ecrf.demo.gridgears.io!" .

;; Query time: 41 msec
;; WHEN: Mon Jul 25 17:37:28 CEST 2022
;; MSG SIZE  rcvd: 119
```

In the answer section, we see a NAPTR record for the "LoST:https" protocol and the corresponding FQDN "https://ecrf.demo.gridgears.io".

5. FindService Request

The ECRF can now send a findService request to the ECRF in ESInet B.

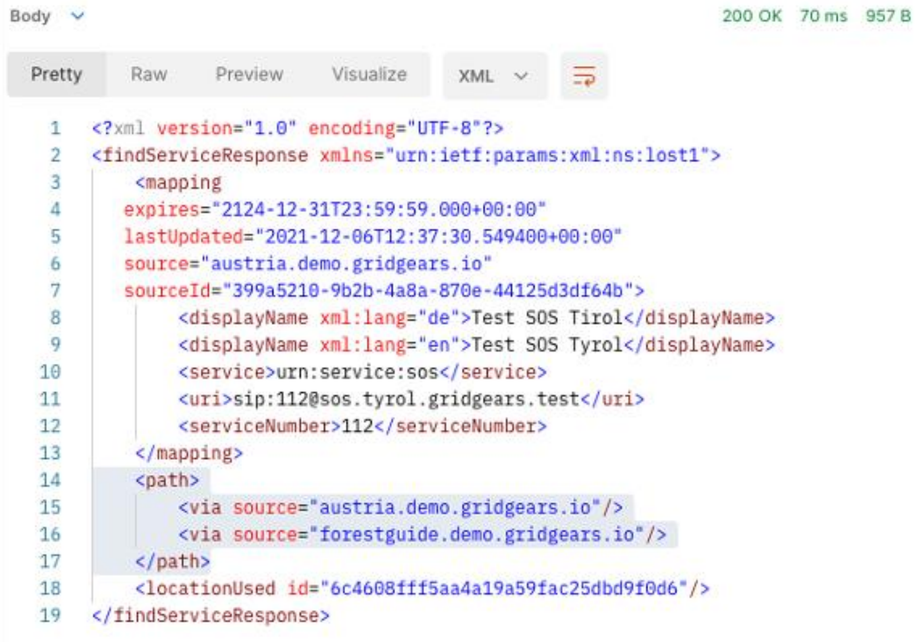


```xml
<findService xmlns='urn:ietf:params:xml:ns:lost1' recursive='false'>
    <location id='locationId' profile='geodetic-2d'>
        <gml:Point xmlns:gml='http://www.opengis.net/gml'>
            <gml:pos>47.02200 11.50219</gml:pos>
        </gml:Point>
    </location>
    <service>urn:service:sos</service>
    <path>
        <via source="forestguide.demo.gridgears.io"/>
    </path>
</findService>
```

Figure: Example FindService Request to ECRF

6. FindService Response

Since the provided location is in the jurisdiction of ESInet B, the corresponding ECRF has a mapping for the location and can respond with the correct next hop. In this example, the PSAP in Tyrol.



```xml
<?xml version="1.0" encoding="UTF-8"?>
<findServiceResponse xmlns="urn:ietf:params:xml:ns:lost1">
    <mapping
  expires="2124-12-31T23:59:59.000+00:00"
  lastUpdated="2021-12-06T12:37:30.549400+00:00"
  source="austria.demo.gridgears.io"
  sourceId="399a5210-9b2b-4a8a-870e-44125d3df64b">
        <displayName xml:lang="de">Test SOS Tirol</displayName>
        <displayName xml:lang="en">Test SOS Tyrol</displayName>
        <service>urn:service:sos</service>
        <uri>sip:112@sos.tyrol.gridgears.test</uri>
        <serviceNumber>112</serviceNumber>
    </mapping>
    <path>
        <via source="austria.demo.gridgears.io"/>
        <via source="forestguide.demo.gridgears.io"/>
    </path>
    <locationUsed id="6c4608fff5aa4a19a59fac25dbd9f0d6"/>
</findServiceResponse>
```

Figure: Example findService Response

5 | SHARED DATA

Geographical Data

As stated, the geographical data describing each country's boundary is required. This data should be standardized and be provided by a general entity. A common geographical dataset is necessary in order to avoid overlaps or gaps, which might occur, if each country provided its own geographical data.

As an example, it could be agreed that Forest Guides should use the geographical data at a certain scale provided by Eurostat - Geographical Information and Maps (GISCO).

Domain Names

Since the Forest Guide leverages local autonomy, the domain names need to be provided by each country. Countries then also need to configure their NAPTR records behind those domain names according to their ESInet infrastructure. Although those domain names can be freely chosen, it might make sense to suggest a certain schema that countries can follow, e.g. esinet.<country>.gov.<country code>

Security

The NG112 Architecture uses certificates for mutual authentication. Since the Forest Guide itself does not contain any secret information, it can choose the level of security it wants to enforce on the clients in order to protect itself. It could enforce mutual authentication via a certificate, traceable to a trusted root certificate, or be open to the public. Even more dynamic security models can be implemented, e.g. limiting the throughput of public requests while always ensuring that requests with mutual authentication are being processed.

When the Forest Guide redirects to a different ESInet, it is the responsibility of the targeted ESInet to apply appropriate security mechanisms.

Usually the ECRF of ESInet B will not directly provide the most appropriate PSAP back to ESInet A. Instead it will provide its BCF as an entry point as shown in the figure below:

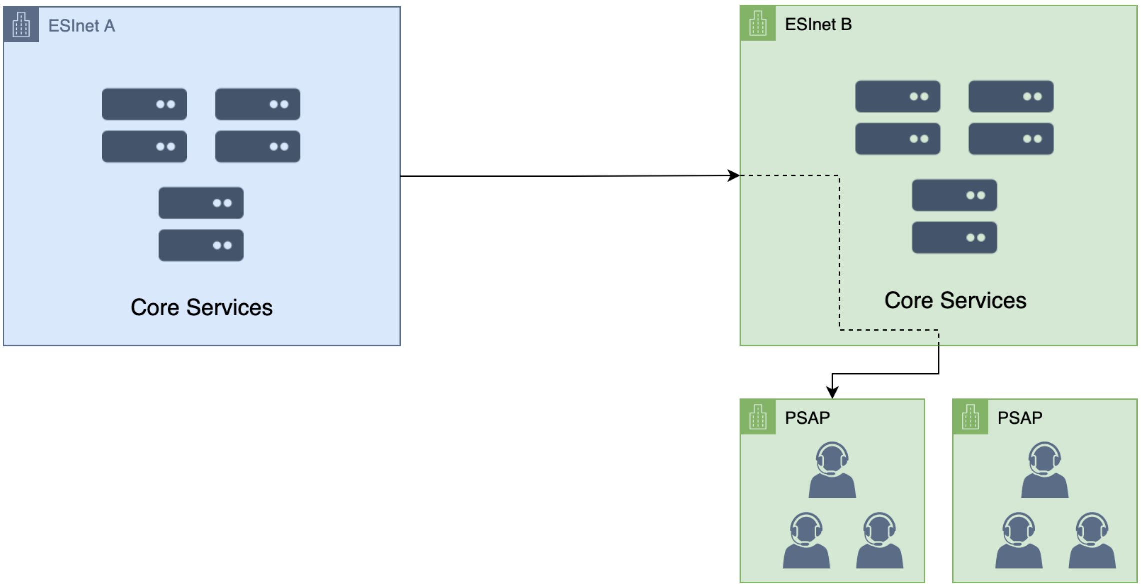


Figure: Example of Isolated Security Model

This has the advantage that only ESInet B is able to provide emergency communications to its PSAPs. Additionally, multiple security mechanisms can be implemented at the BCF of ESInet B, such as rate limiting and additional filtering. This is probably the most feasible solution, when connecting top level ESInets from different countries.

6 | SUMMARY

The Forest Guide enables interconnectivity between multiple top level ESInets. This is a prerequisite for interconnecting ESInets across Europe and route emergency communications between different European countries. Technically, it uses established mechanisms from the Domain Name System (DNS), enabling each country to deploy, change and update their own ESInet infrastructure transparently and keep their local autonomy.

Multiple Forest Guides can co-exist, using domain names provided by each country and publicly available information about each country's geographical boundary. The Forest Guide is the key element when interconnecting Europe’s ESInets and enables the routing of emergency conversions without borders.