NG112 Use Cases

September 2025

NG112 Use Cases

Version: 1.0
Publication date: 23/09/2025
Status of the document: FINAL

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

Author(s):
Michael Pröstler, EENA Tech & Ops Committee Vice-Chair, GridGears

Contributor(s):
Wolfgang Kampichler, EENA Tech & Ops Committee Co-Chair, Frequentis

Cristina Lumbreras, EENA

Annita Elissaiou, EENA

Table of contents

Executive summary

The NG112 architecture consist of multiple core services with standardised interfaces as specified in ETSI TS 103 479. Each core service solves a critical issue when it comes to emergency communications. Leveraging those "First Principle Building Blocks" the NG112 architecture can solve multiple challenges that are present in today's emergency communications. NG112 enables straightforward integration and continuous extensibility by re-using existing standardised interfaces and provides the foundation for modern emergency services.

Purpose of the document

This document explains the NG112 Core Services as "First Principle Building Blocks" and discuss multiple scenarios, challenges and use cases, where those core services and their standardised interfaces can add additional functionality and solve issues in modern emergency communications.

1. Introduction

The NG112 architecture provides a blueprint for modern emergency communications according to the ETSI TS 103 479 standard. Leveraging this architecture and the corresponding core services within an Emergency Services IP Network (ESInet), emergency services can address current and future challenges more efficiently in a standardised way. At the same time, those standards are the corner stone for international interconnectivity and collaboration. In addition, standardised interfaces in combination with "First Principle Building Blocks" enable more efficient integrations with Public Safety Answering Points (PSAPs) and other future services. This document goes beyond the traditional use cases of routing a "simple" phone call and provides examples of more advanced scenarios where the standardised core services provide additional value for the end user, as well as for PSAPs.

2. First Principle Building Blocks

2.2. General

In problem-solving and innovation, First Principle Thinking is a method that breaks down complex problems into their most fundamental truths. Instead of relying on conventional wisdom, past practices, or assumptions, this approach encourages starting from the ground up—analysing a problem at its core and reconstructing solutions based on essential, undeniable principles.

This concept is particularly powerful in software architecture, where complex systems often become fragile due to interdependencies, legacy constraints, and growing technical debt. First Principle Thinking helps us design software from fundamental building blocks, ensuring that each component serves a distinct, well-defined purpose rather than being burdened by unnecessary complexity.

NG112 Core Services within the NG112 architecture follow a similar concept of First Principle Building Blocks. All core services are modular, self-contained software components, each solving exactly one critical issue within the emergency response ecosystem.
The most fundamental issues, which need to be answered during the process of an emergency communication are:

- **Where** is help needed?
- **Who** is responsible?
- **How** can they be reached?

2.3. Location Information Service (LIS)

Accurately determining the caller's location is essential for dispatching emergency responders. The Location Information Service within the NG112 architecture serves exactly that purpose. It

provides a standardised interface to retrieve location information in geodetical (point, circle, etc.) or in civic (address) format.
The Location Information Service can be connected to multiple location sources and even act as an AML Endpoint. Its standardised interface uses the HTTP-Enabled Location Delivery (HELD) protocol to retrieve location information for different types of entities including mobile numbers, fixed line numbers, mobile cell towers, etc.

2.4. Emergency Call Routing Function (ECRF)

Once we know where help is needed, the next critical question, that needs to be answered, is who is responsible. The Emergency Call Routing Function (ECRF) is an essential component that maps a specific location and the required service (ambulance, fire, police, etc.) to the responsible target, e.g. a specific Public Safety Answering Point (PSAP). Its standardised Location-to-Service Translation (LoST) protocol enables entities to retrieve information about coverage, responsibilities and available services. Furthermore, it is a key component when enabling international collaboration as described later in the use cases.

2.5. Emergency Service Routing Proxy (ESRP)

The Emergency Service Routing Proxy (ESRP) is the engine of the NG112 architecture. Based on the location information and service responsibility, the ESRP can route emergency communications to the most appropriate PSAP. Internally, it uses the Policy Routing Function (PRF) to determine what the most appropriate PSAP is, based on various parameters and interacts with the LIS and/or the ECRF. These parameters include location information and required services, but can also consider media types, type of communication (e.g. eCall, NG eCall) and even information about a PSAP's current state (e.g. Overloaded, Out of Service, etc.)

2.6. Border Control Function (BCF)

Although the Border Control Function does not contribute directly to the first principle questions, it is still an important core service. The BCF sits at the edges of an ESInet controlling incoming and outgoing messages. It adds an additional layer of security in addition to network-based security components such as firewalls.

3. NG112 Use Cases

3.1. General Use Case

Probably, the most general use case within an ESInet and the NG112 architecture is routing an emergency communication to the most appropriate PSAP. Since native Real Time Text (RTT) and Video for emergency communication are not yet fully deployed in most countries, we will focus on an emergency communication with audio only. Later we will discuss other use cases and how the ESInet and its core components ease the integration path for multimedia communication including RTT and Video.

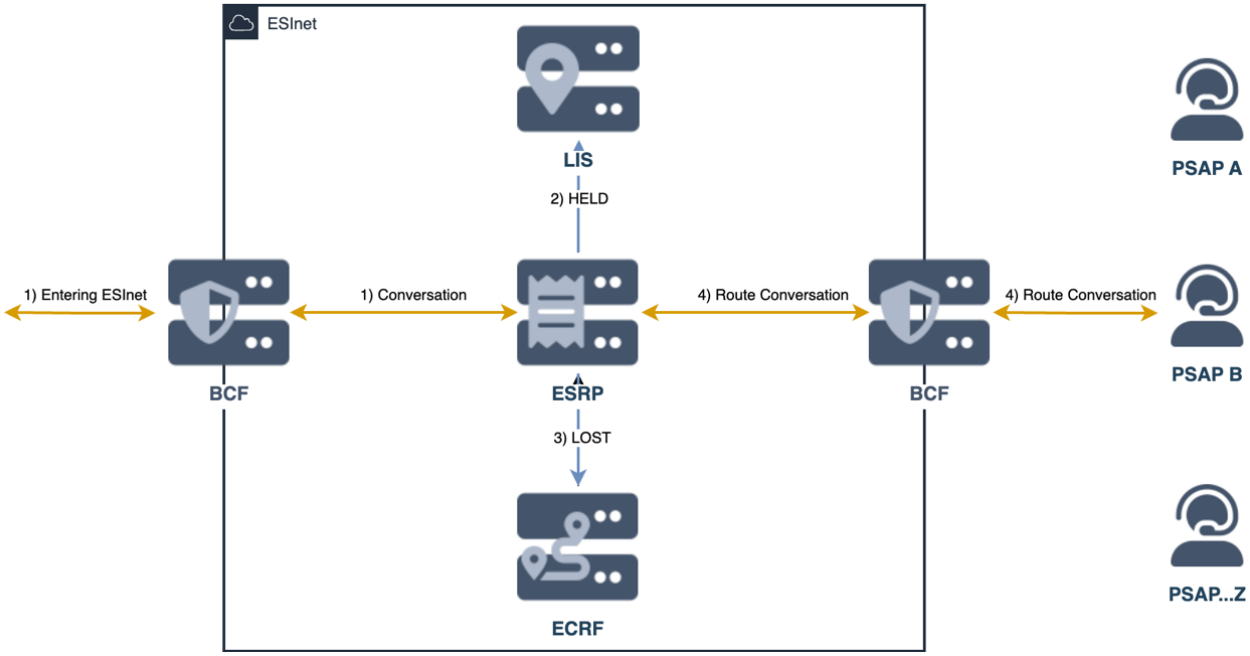

Figure 1: ESInet with NG112 Core Services

Step 1: Entering the ESInet
The ESInet is agnostic of the original communication source and any authorised source may forward communications to the ESInet. The BCF, the security shield around the ESInet, receives the communication and forwards it to the ESRP after successful verification.

Step 2: Determine Location (HELD)
In the next step, the ESRP receives the communication and evaluates its internal Policy Routing Function (PRF) to determine the next target. In this general use case, a location is needed for location-based routing. In case a location is not provided neither by value in the SIP PIDF-LO nor be reference, the ESRP can query a Location Information Services.
In this scenario, let's assume that location is provided by reference. In this case the ESRP dereferences the location using the HELD protocol.

Step 3: Determine Jurisdiction (LOST)
The ESRP can now query the ECRF for the responsible target (in our case a PSAP), which can provide the required services as indicated in the service urn (e.g. urn:sevices:sos.police) at the dereferenced location. The ESRP uses the LoST protocol to interact with the ECRF. In our case the ECRF has an appropriate geodetic mapping for Police at that specific location and provides

the corresponding URL of the responsible PSAP back to the ESRP.

Step 4: Route Communication
If no other policies overwrite the routing decision, the ESRP can now forward the emergency communication through the outgoing BCF to the corresponding PSAP.
Even in this basic use case, we can already identify multiple different sub scenarios.

- How to deal with emergency communications, which do not provide location information, neither by value nor by reference?
- What happens if the location is outside of the ESInet coverage and in a foreign country?
- What happens if only some PSAPs are ready to handle multimedia communications?
- etc.

The following use cases and scenarios address some of the sub scenarios mentioned above.

3.2. Routing based on Media Type / Language Preferences

As technology progresses new routing capabilities are required. Most of the time, when we speak about routing to the most appropriate PSAP, people think of location-based routing, therefore routing to the closest PSAP. This technical limitation is mostly based on the routing capabilities of legacy circuit switched networks. In addition to technology readiness, routing can also take into account the skills of PSAPs, such as trained call-takers for RTT, NG eCall or specific language skills.

Having new data and technologies at hand, routing becomes increasingly more powerful and might even be required for the rollout of new technologies. Let's take Real Time Text (RTT) or NG eCall as examples. In case of legacy routing with neither an NG112 architecture nor an ESRP, there are two options when introducing those technologies. Since not all PSAPs of a country might be able to implement the required features and protocols of the new technology at the same time, you can either choose a dedicated PSAP for NG eCalls or RTT emergency communications, effectively ignoring location-based routing or wait until all PSAPs have implemented those capabilities, which might take a long time.

Leveraging an ESPR and/or ECRF within an ESInet, you can combine location-based routing with the capabilities of routing based on certain features and protocols implemented by the PSAPs. This ensures that calls are directed not just to the closest PSAP, but to the one best equipped to handle the type of communication, whether through specialised staff (e.g., RTT-trained call-takers) or supported protocols.

In this way, new technologies such as RTT or NG eCall can be enabled as soon as the first PSAP is able to process those technologies. Subsequently, as more and more PSAPs are ready, routing based on RTT or NG eCall can be dynamically adapted without any necessary change to the ESInet, enabling a smooth and gradually rollout of new technologies. Ultimately, this ensures that emergency communications are routed not only to the nearest PSAP but to the best-skilled one.

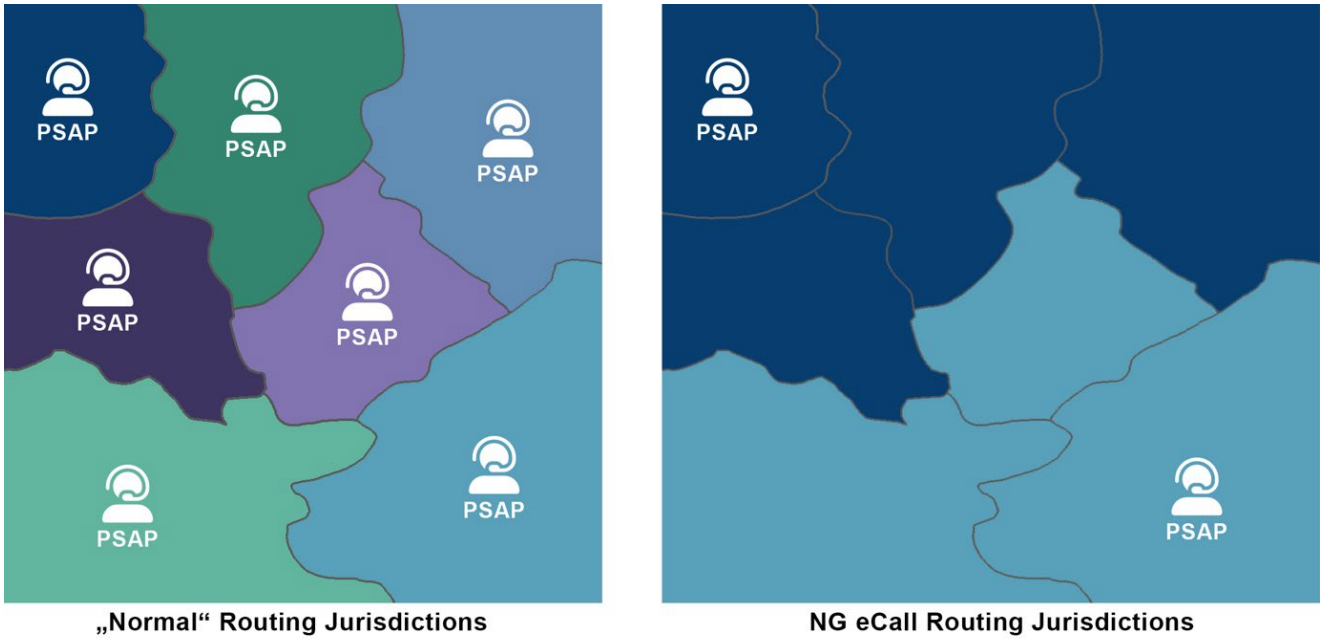

Figure 2: Media-based Routing Jurisdictions

3.3. International Collaboration

International collaboration, data exchange and interconnectivity are a corner stone of modern emergency services. Emergency communications might be misrouted due to various reasons. After crossing the border to another country, you might be still connected with the other country's cell tower. Network topologies, especially in the case of Voice over Wi-Fi (VoWiFi) or your company's internal telephone system might lead to communications ending up in a different country. Those scenarios are extended by use cases leveraging other technologies, such as messenger services, VoIP providers or IoT.

International collaboration is also required, if the general purpose of an emergency conversation, is to provide information about an emergency abroad. People may contact emergency services because they were made aware that friend, family or colleague has an emergency in another country. In this case, the emergency conversation is correctly routed, but it cannot be handled, since the emergency is in another country. This might also be the case, where people are on vacation in another country and detect a burglary through their private security system.

Those real-world use cases provide a reference for the necessity of international collaboration. One current solution is PSAP Directory hosted by ECO, European Communications Office (https://eena.org/our-work/eena-special-focus/psap-directory/), which provides the required information on how to contact a PSAP in another country directly. This approach however requires each PSAP to integrate the data provided by hand, or to perform a manual lookup during an emergency.
An ECRF provides the same information as EENA's PSAP Directory, but with standardised interfaces and protocols. This is even independent of a country's ESInet deployment and can be directly integrated into existing PSAPs. Updates to the directory are then immediately available to all participating countries / PSAPs without any additional integration.

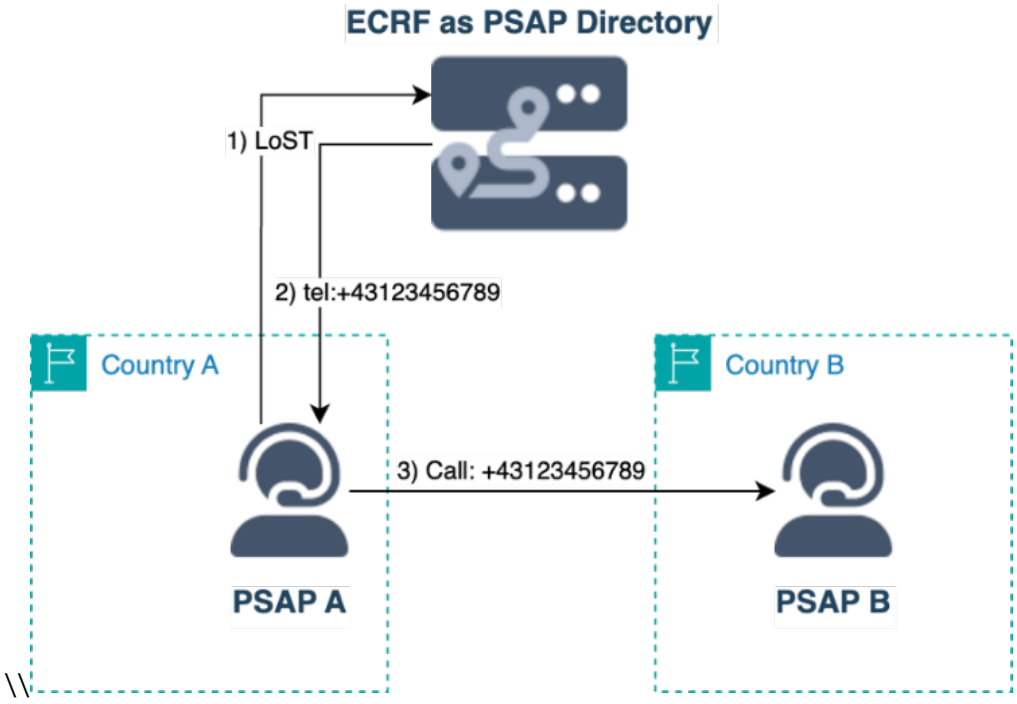

Figure 3: ECRF as PSAP Directory

The Forest Guide (FG) within the NG112 architecture can be seen like the PSAP Directory, but instead of PSAPs it provides technical lookup capabilities of the ESInets in different countries. Instead of having to manually coordinate and relay emergency communications from one country to another, the Forest Guide enables the automatic routing of a communication to the appropriate ESInet without any manual intervention.

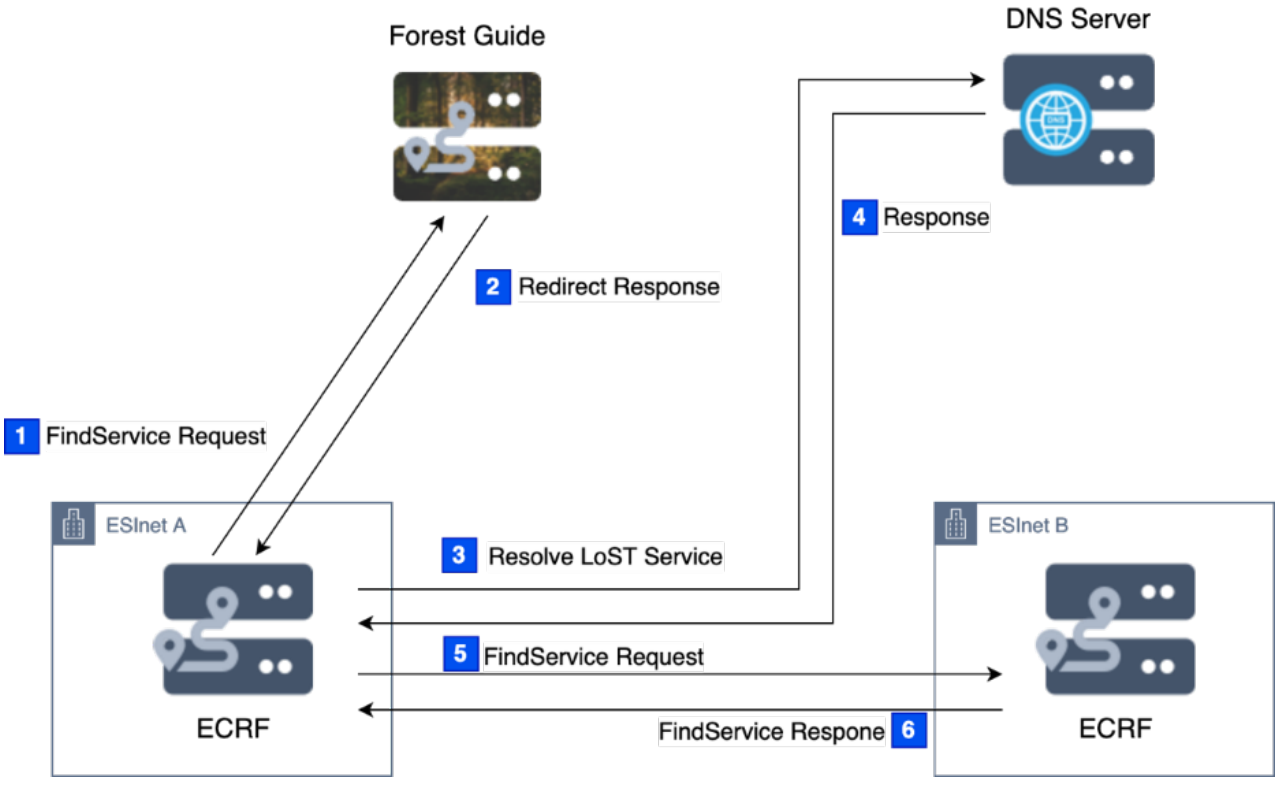

Figure 4: Forest Guide Interaction

Let’s look at the example, where the caller’s actual location is not within the boundaries of the connected country due to cross border cell coverage. Within the NG112 architecture, when the ESRP queries the ECRF for the next target based on the configured jurisdictions, the ECRF will detect that the provided location is not covered. It can then reach out to the Forest Guide, which then provides the correct country’s ESInet as the routing target for the ESRP. This ESInet can then apply all standard mechanisms to route the communication . Additionally, it could have special rules and routing decisions for those communications, originating in other countries’ ESInet.

3.4. Adhoc Routing (Events, Attacks, etc.)

Other advantages gained by the NG112 architecture in comparison to legacy routing arise from the ability to change routing and jurisdictions independently of the mobile network. In case of special events such as concerts, sport events or even for terrorist attacks, the ESInet, more precisely the ECRF, provides the capabilities to quickly re-route emergency communications from a particular area to a special (mobile) control room independently of the mobile network.

In case of mass leisure events, which may require a mobile control room close to the event to provide better situational awareness, the corresponding area can be pre-configured for the time of the event to route emergency communications to the corresponding control room. During terrorist attacks, it might be useful to route emergency communications to a dedicated (mobile) control room.

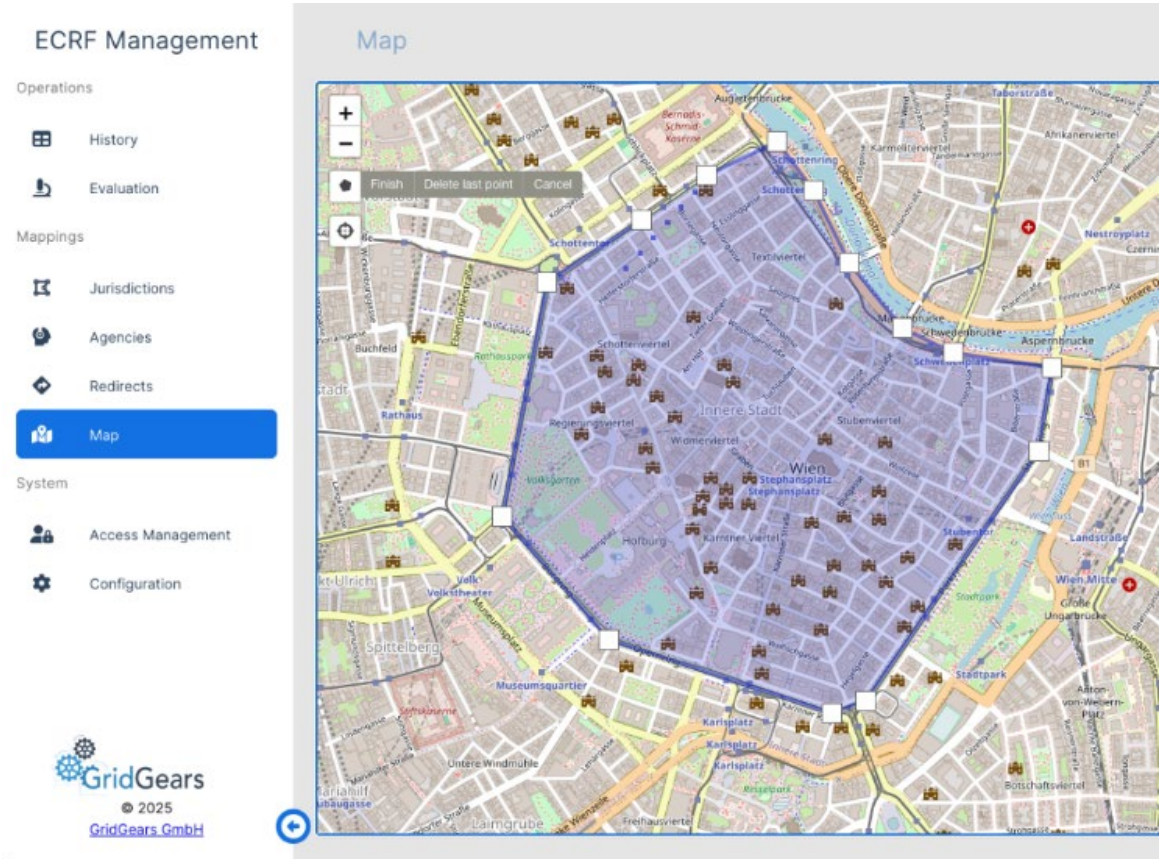

Figure 5: Example - Creating an Adhoc Routing Area for Vienna’s City Center

3.5. Third Party Service Providers

The efficient integration of Third Party Service Providers (TPSPs) is crucial for modern emergency services. TPSPs play an essential role in delivering assistance to groups of customers, organisations, or individuals when conventional access to emergency services is not possible or appropriate. This includes Security Systems Service Providers, Health Monitoring Services or Relay Services where TPSPs contact emergency services on behalf of another party. In addition, TPSPs can provide filtering services by blocking/redirecting non-emergencies and only passing real emergencies to emergency services, which is an approach some countries took for the eCall implementation.
One challenge all those use cases for TPSPs have in common, is that they need to decide how to initiate and route an emergency conversation to the most appropriate PSAP. Without a centralised routing logic in place, each TPSP needs to maintain and manage its own routing logic, often by maintaining an internal PSAP lookup directory. In addition, each TPSP needs connectivity to each PSAP.

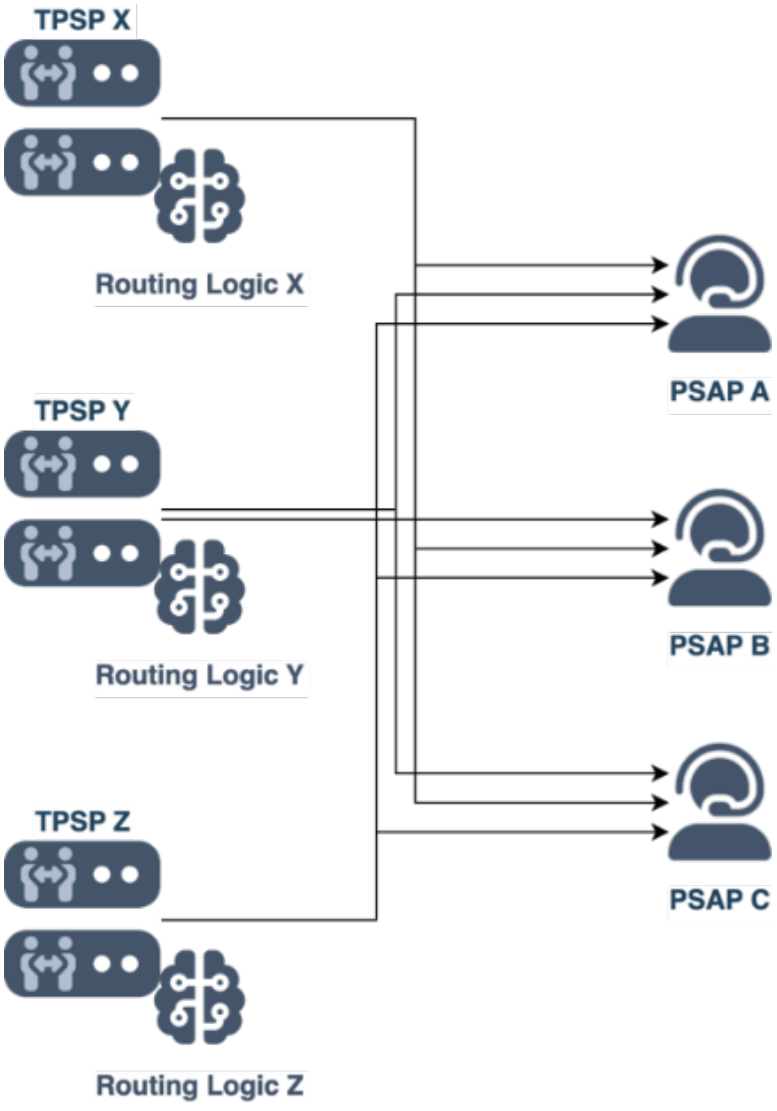

Figure 6: TPSP Routing Logic and PSAP Connectivity

Within an ESInet the ESRP and ECRF provide all necessary capabilities to route emergency conversations to the most appropriate PSAP. TPSPs, after receiving an accreditation for connecting to the ESInet, can simply forward emergency conversations to the ESInet. The ESInet then routes based on multiple properties of the conversation. This approach leverages a centralised routing logic instead of relying on each TPSP's internal logic and can be dynamically adapted, depending on PSAP states and capabilities.

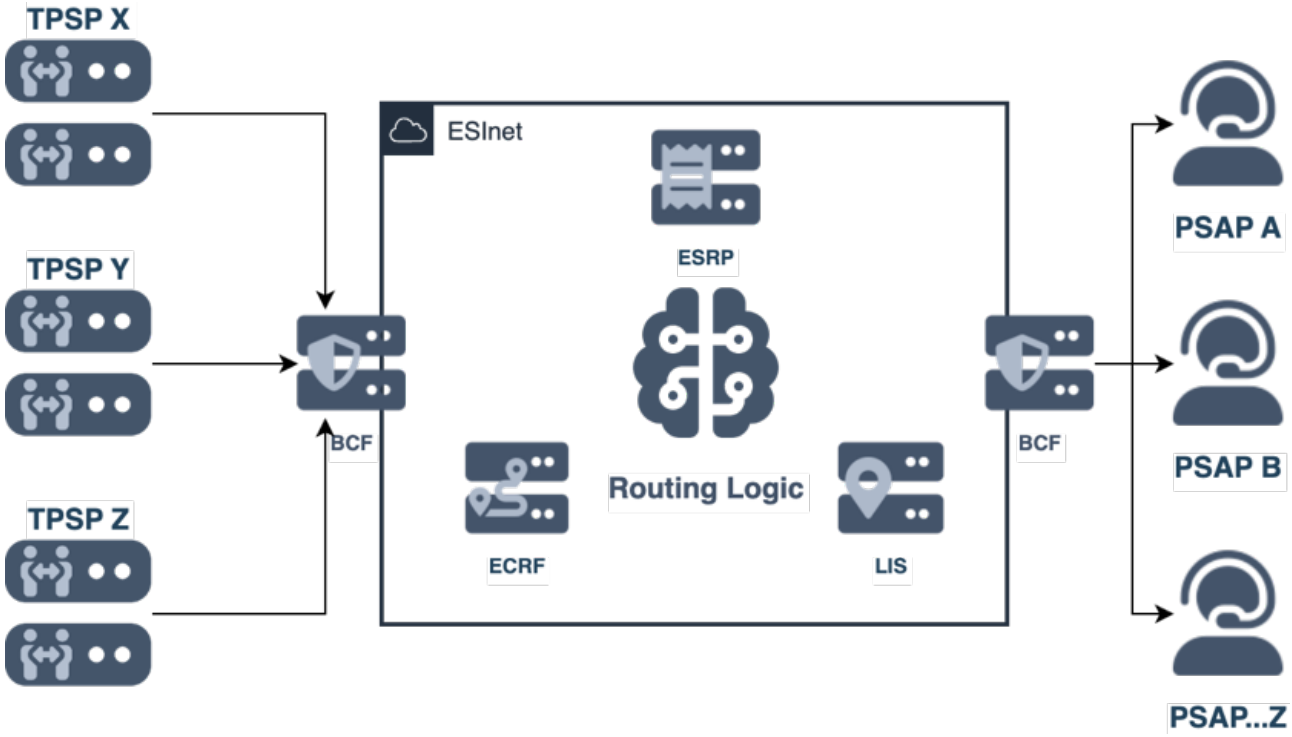

Figure 7: TPSP & PSAP ESInet Routing & Connectivity

3.6. Localisation by Mobile Network Operator

In general, emergency communications must follow a certain standard when entering an ESInet. This includes the availability of location information and the presence of a service URN. Mobile Network Operators (MNO) may provide location by reference and a corresponding Location Information Service/HELD protocol to retrieve location information. Such requests are normally subject to judicial or law enforcement authorisation, not initiated by the PSAP alone. However, there are use cases and scenarios where localisation of a third person, independent of the emergency communication initiator is required. This includes incidents such as a missing person, hijacking etc., where PSAPs and/or dispatched resources need to localise a person without a correlated emergency communication. To trigger this localisation, which is usually performed by the MNOs, a certain interface and protocol needs to be implemented between the PSAP and the MNOs.

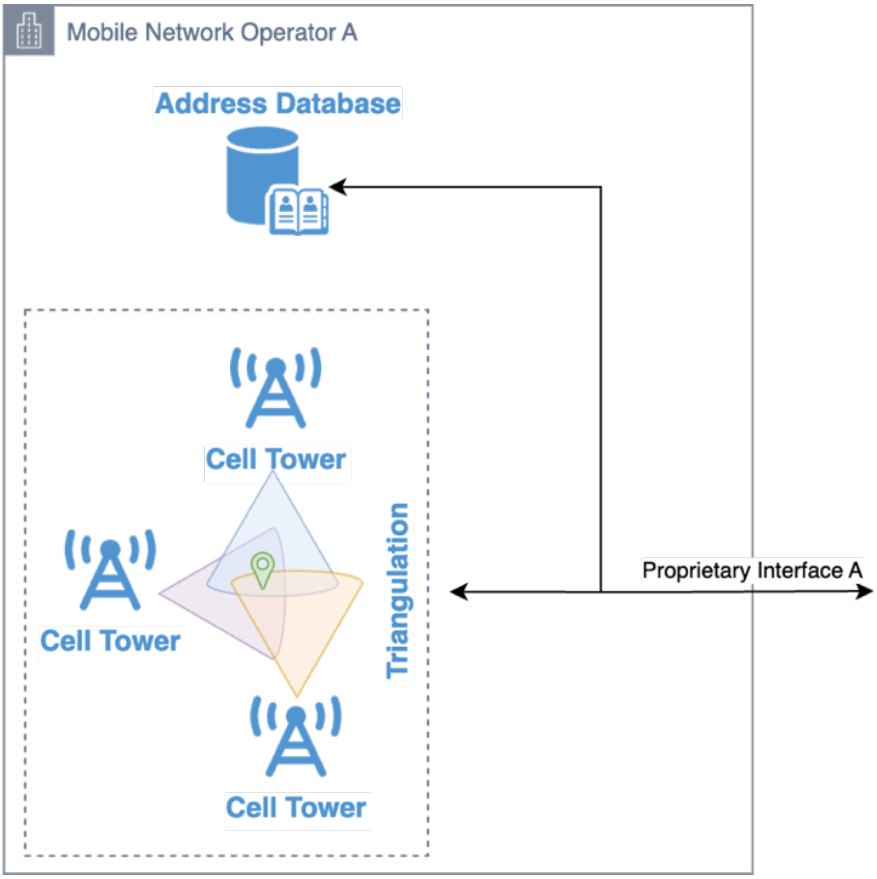

Figure 8: Mobile Network Operator: Proprietary Interface

Unfortunately, the chosen protocols (which might be subject to countries' regulators) are often proprietary and might even be different depending on the MNO within a country, adding additional complexity and increase integration efforts.
As MNOs need to provide a Location Information Service and therefore implement the HELD protocol when sending location by reference, it makes a lot of sense to re-use the same protocol for emergency communication independent localisation. Leveraging the same protocols, PSAPs can easily integrate with MNOs, which might perform cell triangulation or master data lookups to provide location information.

The same mechanism can of course be used by an ESRP in case that no location information is provided for emergency communications entering an ESInet.

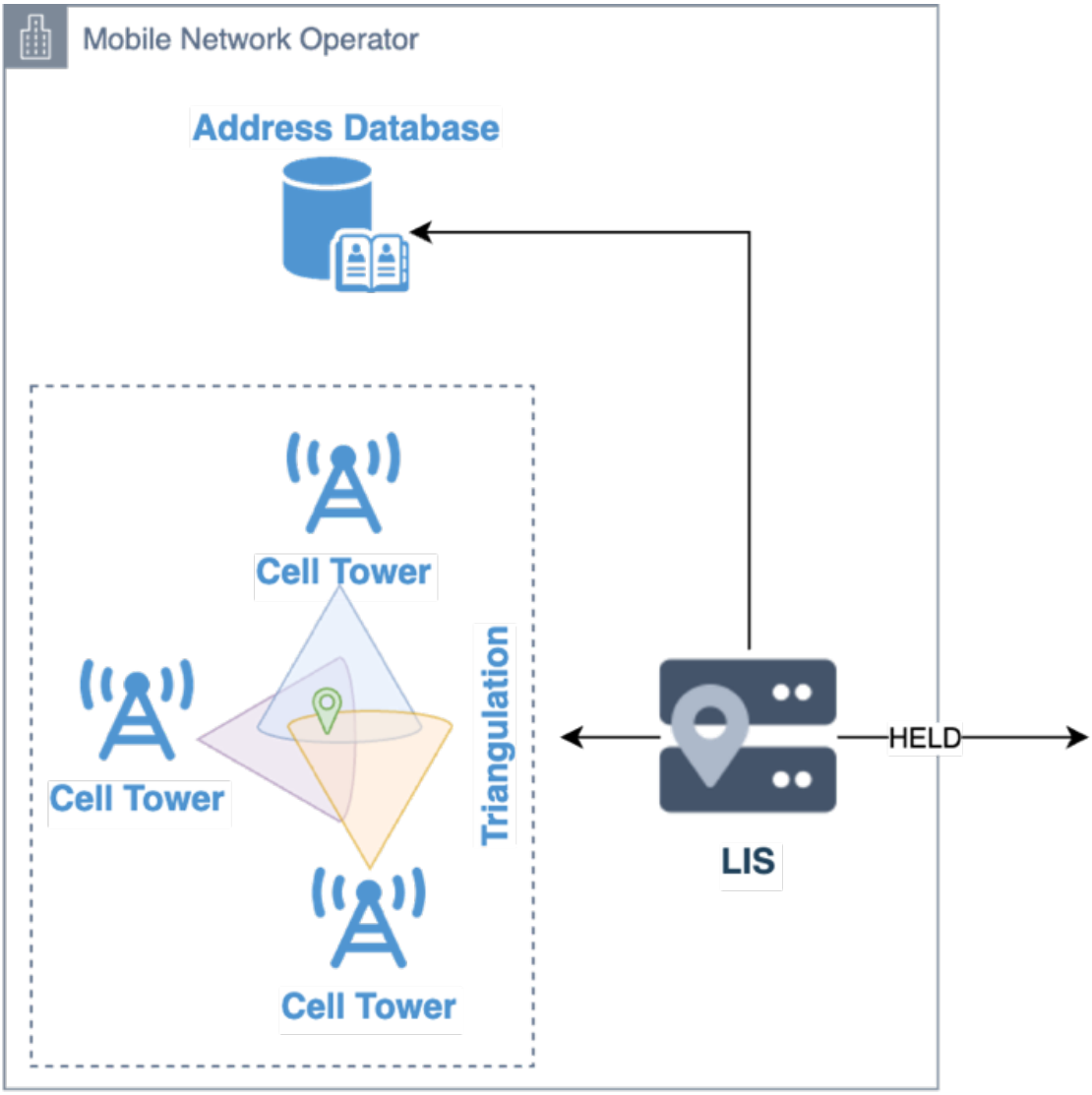

Figure 9: Mobile Network Operator: Standardised Interface

This approach eases integration and reduces complexity by leveraging existing standards, protocols and interfaces as specified in ETSI TS 103 479 to retrieve location information.

4. Conclusion

As shown in this document, the NG112 architecture, the ESInet and its corresponding core services, according to ETSI Standard TS 103 479, provide a technical solution to first principle challenges in emergency services. Furthermore, additional use cases and demands can be seamlessly integrated and fulfilled by leveraging those standardised interfaces and protocols, while easing integration efforts and even enabling international connectivity and collaboration. It is clear, that those standardised interfaces and services cover way more use cases and scenarios then the examples mentioned in this document. In addition, by following first principles, it should be clear that it is not a question of "if you need those services", but rather "if you want them to be implemented in a standardised way" to enable extensibility and as such provide the foundation not only for modern emergency services but also for future innovations.