NG112

Implementation steps

End to End Implementation Guidelines

Discover the key milestones that must be accomplished by stakeholders to achieve an end to end implementation of Next Generation 112.

eena

EUROPEAN EMERGENCY NUMBER ASSOCIATION

NG112 IMPLEMENTATION STEPS

VERSION 1.0

NG112 Implementation steps

Status of the document: Approved

Authors that contributed to this document:

Authors:

Michael Pröstler, GridGears

Contributors:

Luca Bergonzi, Beta80

Iratxe Gomez Susaeta, Atos

Andrew Hutton, Atos

Francisco Nobre, ESRI

Cristina Lumbreras, EENA

Wolfgang Kampichler, Frequentis

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

EXECUTIVE SUMMARY

Living in today's fast-moving world of technology, it is important to understand that future emergency services must be prepared for emergency communications originating from different types of sources. This is especially important when thinking of future use cases related to the innovations made possible by technical progress in areas like 5G, drones or IoT, for example.

The NG112 architecture and its core components provide the solid foundation for emergency services. They are scalable and provide a framework for future use cases and innovation.

Next Generation Emergency Service Standards, such as NG112 and NG9-1-1, specify the core components of an Emergency Services IP Network (ESInet), their interfaces and the communication within the network. While the standards define the processes within the emergency service network, additional actions are necessary to achieve an end to end implementation.

The following milestones need to be accomplished:

- **Milestone 1:** Emergency Services Strategy Plan
- **Milestone 2:** Provision Infrastructure
- **Milestone 3:** Provision Core Services
- **Milestone 4:** PSAP Enablement
- **Milestone 5:** Mobile Network Operators
- **Milestone 6:** Mobile Operating System
- **Milestone 7:** European Interconnection

This document will describe the necessary actions and regulations to enable the full implementation of the Next Generation Emergency Services, focusing on nationwide and Europe-wide implementations within the countries' and Europe's action range.

Next Generation Core Emergency Services are device agnostic and can handle every standard conform IP-based emergency communications, independent of its origin. However, this document focuses on the following currently used originating devices:

- Mobile phones
- Landline connections
- Software applications (Voice over IP clients) via a trusted VoIP provider

On the way to an end to end deployment of Next Generation Emergency Services, multiple milestones must be achieved.

This document describes an inside out approach, where each milestone brings the accessibility of Next Generation Emergency Services closer to the user's end device. The milestones are divided into those needed for a nationwide deployment and those necessary for a Europe-wide deployment of Next Generation Emergency Services.

LIST OF ACRONYMS

BCF	Border Control Function
ECRF	Emergency Call Routing Function
ESInet	Emergency Service IP Network
ESRP	Emergency Service Routing Proxy
IP	Internet Protocol
LIS	Location Information Service
LTE	Long Term Evolution
MNO	Mobile Network Operator
MoI	Ministry of Interior
NG112	Next Generation 112
NG9-1-1	Next Generation 9-1-1
NHI	Non-Human-Initiated
POP	Point-of-Presence
PSAP	Public Safety Answering Point
REG	Regulator
SIP	Session Initiation Protocol
SMS	Short Message Service
UE	User Equipment
VoIP	Voice over IP
ViLTE	Video over LTE
VoLTE	Voice over LTE
VSP	VoIP Service Provider

1 | INTRODUCTION

1.1 CURRENT STATUS

At present, the routing of emergency calls is typically realised via an incumbent Telecommunications Service Provider (TSP). The incumbent TSP ensures that emergency calls are routed to a Public Safety Answering Point (PSAP) based on a static mapping between the address of the subscriber (landline) or the location of the cell tower (mobile) and the responsible PSAP.

Any fixed or mobile provider may, depending on termination contracts, forward emergency calls from their network to a Point-of-Presence (PoP) that serves as a gateway to the emergency network.[1] PSAPs and other TSP typically connect to the incumbent TSP to ensure access to emergency services independent of the caller's TSP.

There are currently multiple limitations of the legacy network. In terms of media, basically, only voice calls are supported and only some areas also support SMS to emergency numbers (112 generally). Sending images, performing a video communication, or transmitting any other additional data is normally not possible.

The static routing reduces the reactivity of the emergency services in exceptional circumstances, e.g. when a PSAP is overloaded or has technical difficulties.

All the components are internals of the TSP and typically not accessible from the outside. This limits the re-use of those components and the corresponding services outside of the context of the TSP. Innovation in terms of additional emergency services relies on the TSP and cannot be achieved independently.

Consequently, it is not possible to reuse the same routing capabilities for services not involving a phone call or SMS, like a chat integration for deaf and hard of hearing citizens, for example.

1.2 NEXT GENERATION EMERGENCY SERVICES

Next Generation Emergency Services enable the digitalisation of today's emergency services. They modernise emergency communications by including video and text capabilities as well as other additional data, such as detailed location information.

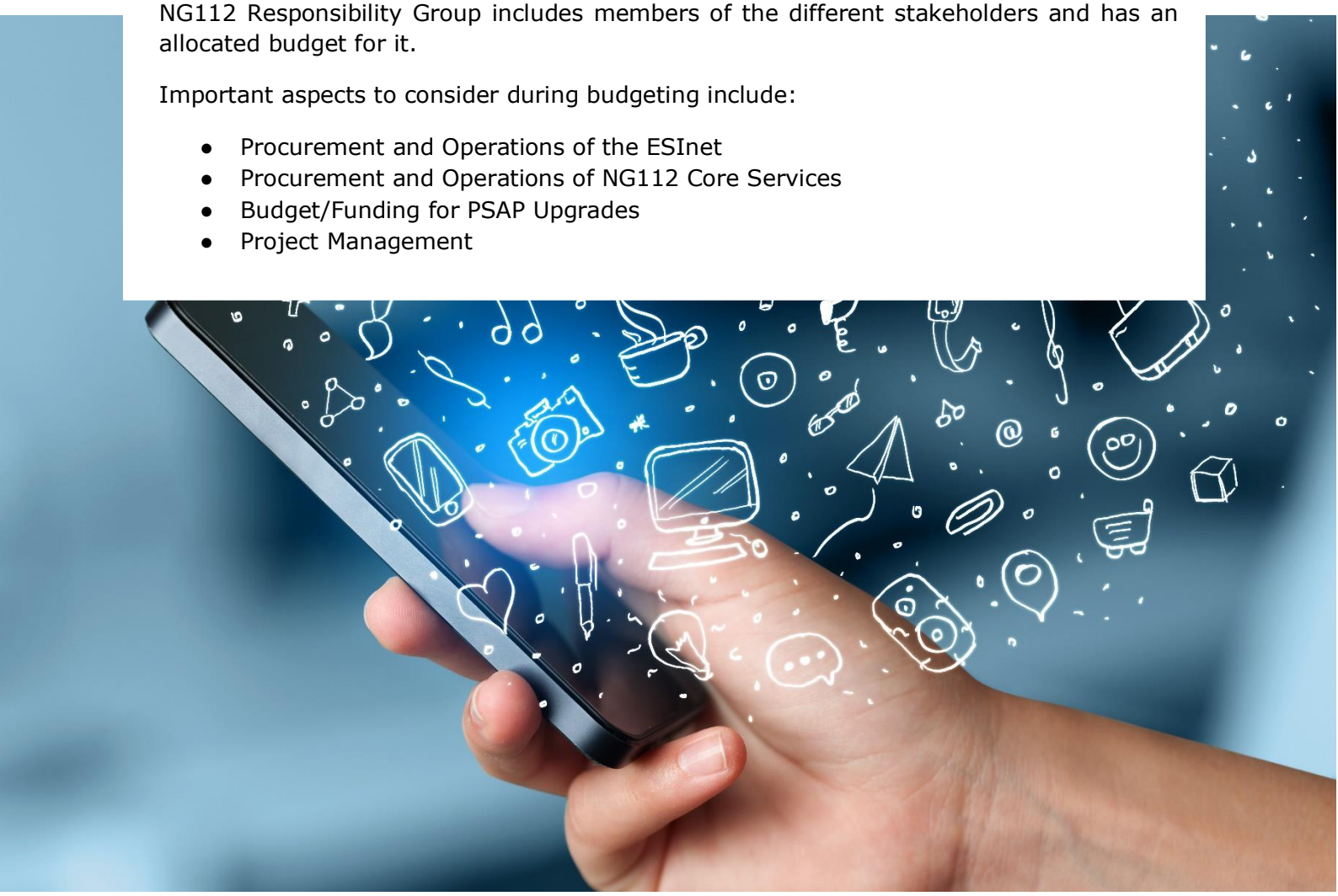
The NG112 standard [ETSI TS 103 479], provides a blueprint architecture for such modernisation. It specifies the necessary components, interfaces, and communications for Next Generation Emergency Services.

1.3 NG112 RESPONSIBILITY GROUP

In order to support the implementation of Next Generation 112, a project management group that is responsible for the NG112 implementation needs to be created. Ideally, this NG112 Responsibility Group includes members of the different stakeholders and has an allocated budget for it.

Important aspects to consider during budgeting include:

- Procurement and Operations of the ESInet
- Procurement and Operations of NG112 Core Services
- Budget/Funding for PSAP Upgrades
- Project Management



2 | MILESTONES

2.1 MILESTONE 1: EMERGENCY SERVICES STRATEGY PLAN

Strategy and planning are the stable foundation on which the implementation of NG112 can be realised. Necessary stakeholders need to be included to plan and decide on the strategy regarding the following topics:

- Emergency Services Model
- Emergency Services Numbers
- Geographic Jurisdiction of PSAPs
- Fallback/Support Level of PSAPs

The emergency services model refers to the different PSAP staging models. Based on the chosen staging model, the supported emergency services (e.g. SOS, Fire, Police, Ambulance, etc.) need to be determined. For all services, the geographic coverage, the PSAP jurisdictions as well as fallback and support scenarios need to be addressed.

Stakeholders	Actions
National Authorities	Lead the NG112 implementation project Establish the migration plan in terms of timeline and funds Specify emergency services model and supported emergency numbers
National/Regional Authorities Regulators	Be actively involved in the NG112 implementation project Establish a digital description of the geographic jurisdiction for each available emergency service and the corresponding PSAP
National/Regional Authorities Regulators Emergency Services and PSAPs	Develop routing rule set including fallback and support scenarios.

2.2 MILESTONE 2: PROVISION INFRASTRUCTURE

The next step towards Next Generation Emergency Services is providing the necessary IP-based infrastructure. This is commonly known as the Emergency Service over IP Network (ESInet). The network has a defined Point of Presence (PoP) that serves as a gateway to the ESInet. Telecommunications Operators can use this PoP to forward emergency communications from their network to the ESInet, while PSAPs provide IP-based endpoints to receive emergency communications.

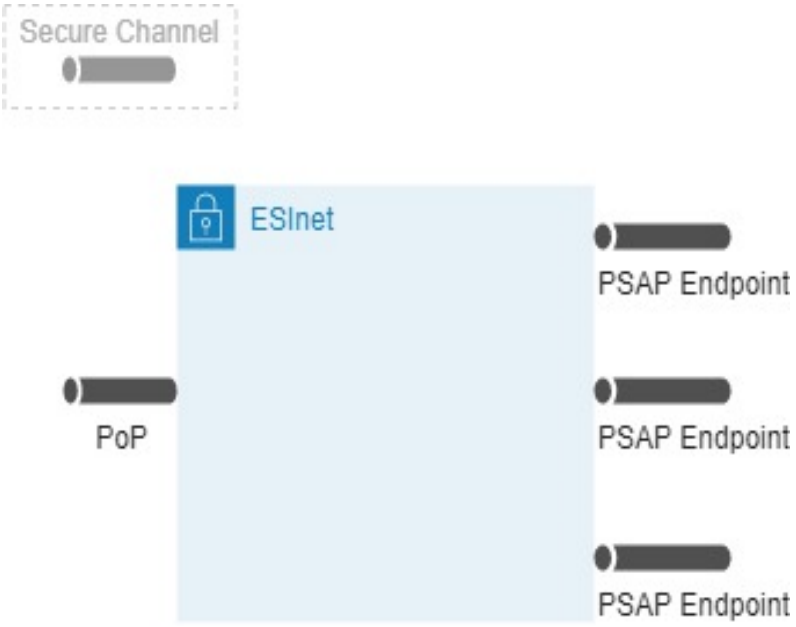


Figure 1: Basic ESInet Infrastructure

Additionally, an authentication authority that is responsible for the connectivity between the internal core services and the connectivity of services linked to the ESInet, like PSAPs and TSPs, needs to be established. Although desirable, there might not be a single ESInet deployment for the whole country. The NG112 standard does support the connection of multiple ESInet deployments (see Forest Guide in [ETSI TS 103 479]).

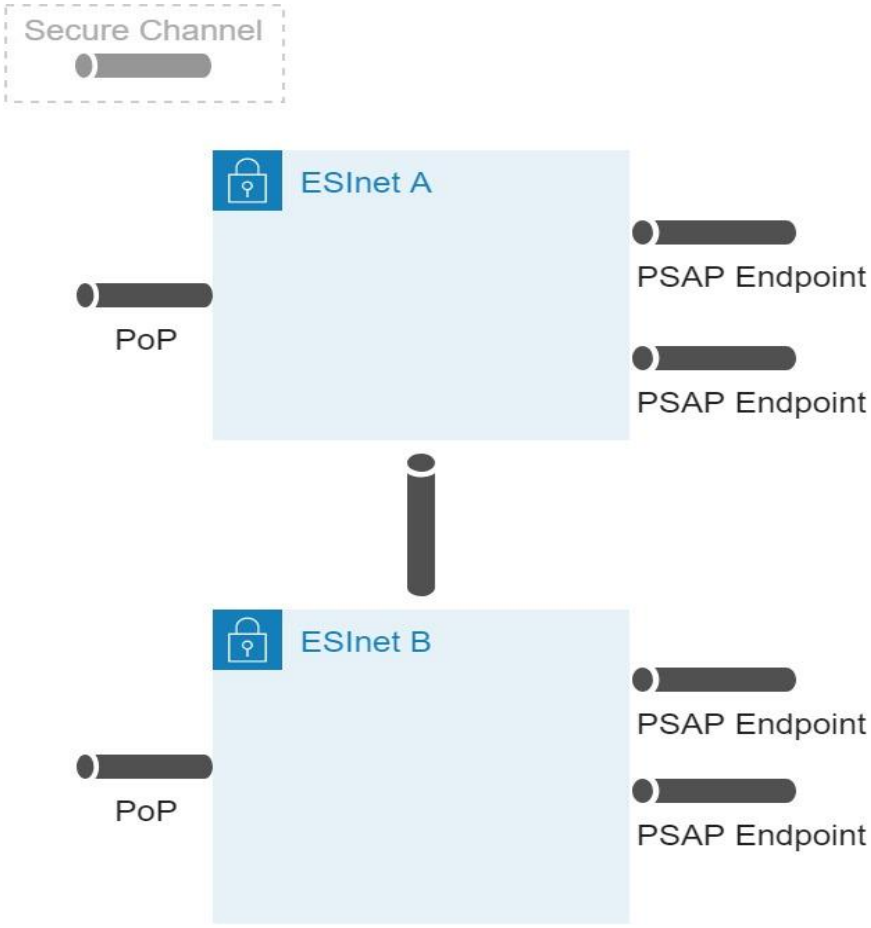
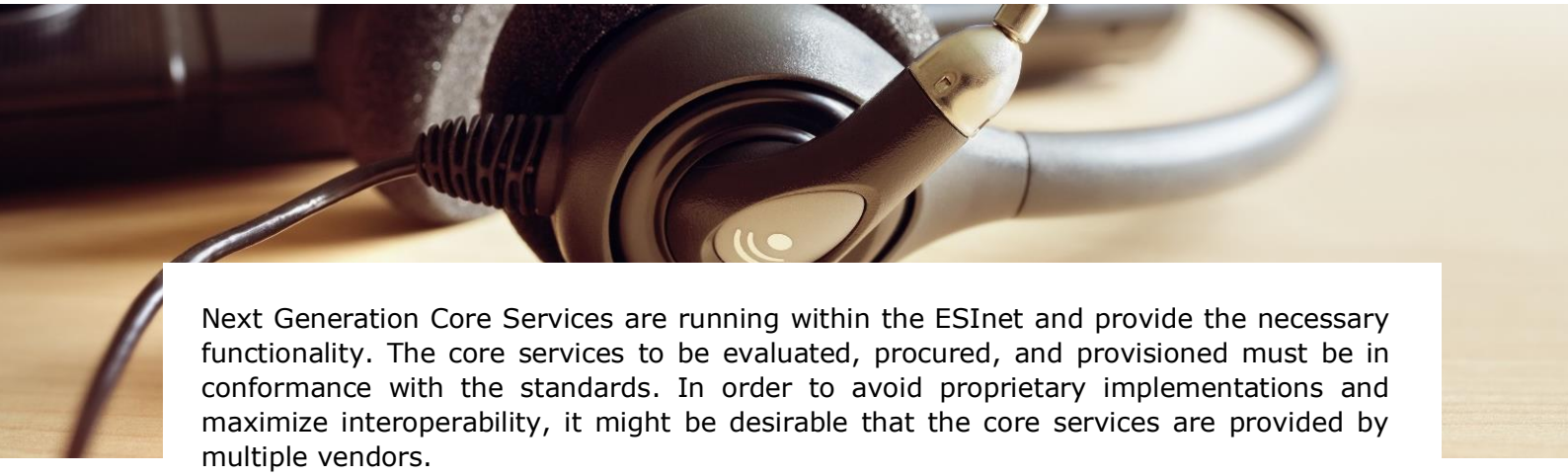


Figure 2: ESInet Interconnection

The authentication authority, however, needs to be established country-wide to allow this interconnectivity between multiple ESInet deployments.

Stakeholders	Actions
National Authorities	Establish a country-wide authentication authority
National / Regional Authorities PSAPs and emergency services	Procurement/Provision of the ESInet infrastructure

2.3 MILESTONE 3: PROVISION CORE SERVICES



Next Generation Core Services are running within the ESInet and provide the necessary functionality. The core services to be evaluated, procured, and provisioned must be in conformance with the standards. In order to avoid proprietary implementations and maximize interoperability, it might be desirable that the core services are provided by multiple vendors.

The Next Generation Core Services specified in the standard and their purposes are as follows:

- **ESRP**
  The Emergency Service Routing Proxy (ESRP) is the base routing function for emergency communications. Its basic function is to route a call to the next hop until it reaches the appropriate PSAP.
- **ECRF**
  The basic function of the Emergency Call Routing Function (ECRF) is to provide a query capability to determine which services are available at a given location. The ECRF is used by the ESRP to route emergency communications to the appropriate PSAP based on the location of the caller.
- **LIS**
  The Location Information Service (LIS) provides a location for a specific entity. If Advanced Mobile Location (AML) is enabled, a LIS may implement the capabilities to act as an AML endpoint.
- **PSAP**
  The Public Safety Answering Point (PSAP) terminates emergency communications routed by the ESInet. It may report its internal state and availability back to the ESInet.
- **BCF**
  The Border Control Function (BCF) acts as an additional layer of security and provides technical harmonisation.

A far more detailed description of the interfaces and the communication is available in the technical specification [ETSI TS 103 479].

Stakeholders	Actions
National / Regional Authorities, PSAPs and emergency services	Procurement/Provision of the different Next Generation Core Services

2.4 MILESTONE 4: PSAP ENABLEMENT

The enablement of PSAPs includes the following intermediate steps:

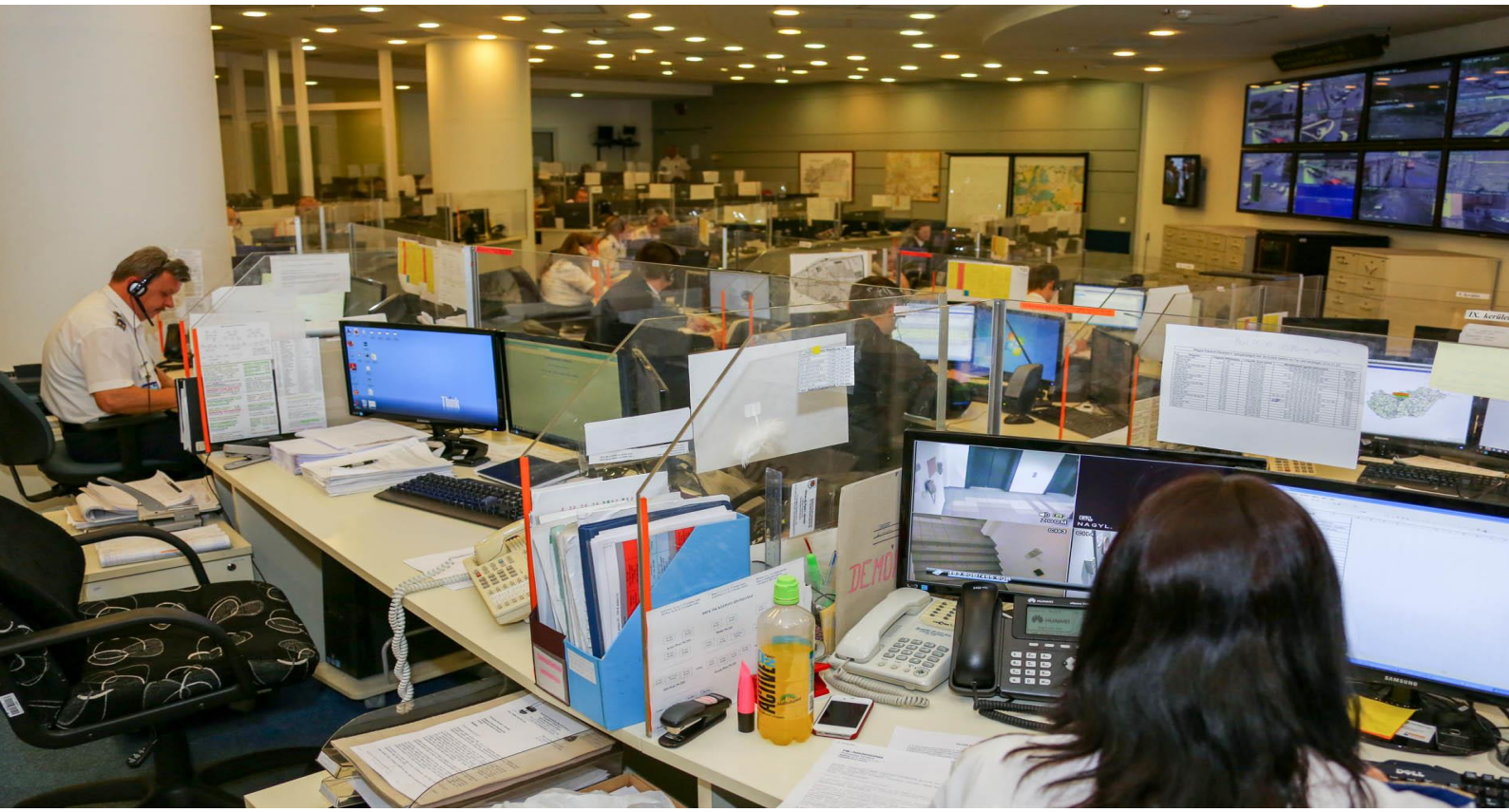
- Technical Ability for NG112
- Operational Training
- Connectivity to the ESInet

Enablement can be achieved by switching and connecting PSAP by PSAP to the ESInet, with no need to change all PSAPs at once.

2.4.1 TECHNICAL ABILITY

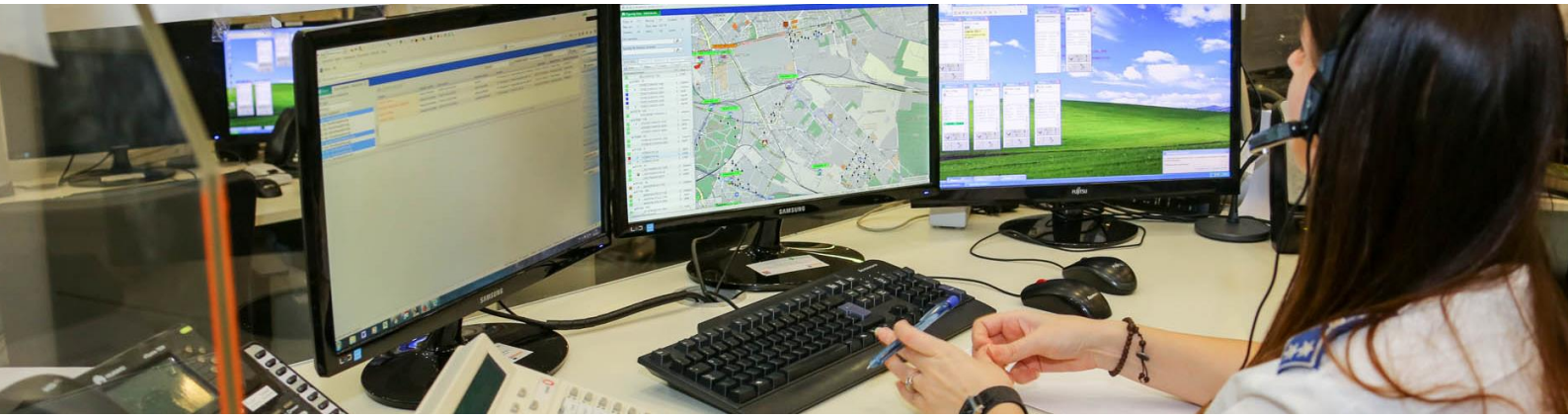
PSAPs need to evaluate their capabilities for technically receiving NG112 Emergency Communications.

Depending on the current status, PSAPs need to upgrade/replace their current technical solution. It is important to understand that this upgrade is also driven by the ongoing transition to IP-based networks in the telecommunications industry, independent of the NG112 Implementation. It is also the foundation for implementing the Next Generation eCall as described in the section "Reflections on NG112 eCall". Nevertheless, this technical upgrade might be subject to governmental funding as calculated in the overall budget.



2.4.2 OPERATIONAL TRAINING

The implementation of NG112 provides additional communication channels, additional data and powerful routing capabilities. This might have an impact on PSAPs' operations, especially for new communication types like text or video.
The flexible routing mechanisms of NG112 support additional backup and overflow scenarios. Although agreements for PSAP collaborations and/or fallbacks are typically already in place, this might require additional operational training as well.



2.4.3 ESInet CONNECTIVITY

Next Generation PSAPs need to be configured and connected with the ESInet. According to the Emergency Services Strategy Plan, the following actions need to be taken for each PSAP:

1. Authentication Authority to provide ESInet access for the PSAP (e.g. issue certificates).
2. Configure ECRF according to the Emergency Services Strategy Plan:
    a. Enable PSAP provided services;
    b. Geographical mapping of jurisdiction for the PSAP.
3. Configure ESRP:
    a. Adapt rules to deliver emergency communications to PSAP.

Stakeholders	Actions
Emergency services and PSAPs	Technical Upgrade & Operational Training
National Authorities	Establish PSAP Access to the ESInet
National/Regional Authorities Regulators	Establish configuration for Next Generation Core Services according to the Emergency Services Strategy Plan

2.5 MILESTONE 5: TELECOMMUNICATIONS OPERATORS & VOIP PROVIDERS

A Telecommunication Operator (MNO) or trusted VoIP Provider enriches the emergency communications with additional data and forwards it to the PoP of the ESInet.

2.5.1 EMERGENCY SERVICE

The routing within the ESInet is based on the ServiceURN provided in the emergency communication setup. When forwarding the communication from the MNO network, the dialled number must be translated into the corresponding ServiceURN. For example, the European emergency number 112 is translated to urn:service:sos and a national emergency number, such as 144 in Austria, is translated to urn:service:sos.ambulance.

If the originating emergency communication already provides a ServiceURN within the communication setup, no additional mapping is required.

2.5.2 LOCATION DATA

The precise location of an emergency communication is highly relevant for PSAPs. While Global Navigation Satellite System (GNSS) based location information is very accurate, it might take some time for the end device to determine its GNNS location. Cell Tower Location is less accurate but always available during the communication setup.
In order to process the emergency communication as quickly as possible, the basic cell tower location might be accurate enough to route the call within the ESInet.

MNOs need to enrich the emergency communication with the location information from the Cell Tower when forwarding it to the PoP.

Stakeholders	Actions
National Authorities	Create the legal frameworks to ensure that TSPs forward emergency communications to the ESInet, following to the NG112 standard.
Mobile Network Operators / VoIP Providers or Core Components Provider	Implement the Emergency Service Number mapping according to the Emergency Services Strategy Plan. Alternatively, this can also be solved at the ESInet level via the core components.
Mobile Network Operators / VoIP Providers	Enrich and forward emergency communications to ESInet

2.6 MILESTONE 6: MOBILE DEVICE OPERATING SYSTEM

To enable video capabilities and additional data over SIP, the user device and mobile network operator must support Voice over LTE (VoLTE) and Video over LTE (ViLTE).

In case of an emergency communication, the mobile device operating system establishes the communication via VoLTE and includes additional data.

The VoLTE emergency communication shall include the precise location if available.

Stakeholders	Actions
European Authorities	Create the necessary legal instruments to mandate VoLTE / ViLTE for emergency communications to enable SIP-based communications
Mobile Network Operators / VoIP Providers	Enable VoLTE/ViLTE for SIP-based emergency communications
Mobile Operating System Vendors	Integrate additional data according to the NG112 standard in the VoLTE/ViLTE

2.7 MILESTONE 7: EUROPEAN INTERCONNECTION

In some cases, the jurisdiction of the precise location of a caller is different from the jurisdiction of the cell tower where the mobile device is connected. This is especially the case in the vicinity of jurisdiction borders. As a result, emergency communications will not be routed to the PSAP that is responsible for the area where the caller actually is, but to the PSAP that is responsible for the area where the connected cell tower is located.

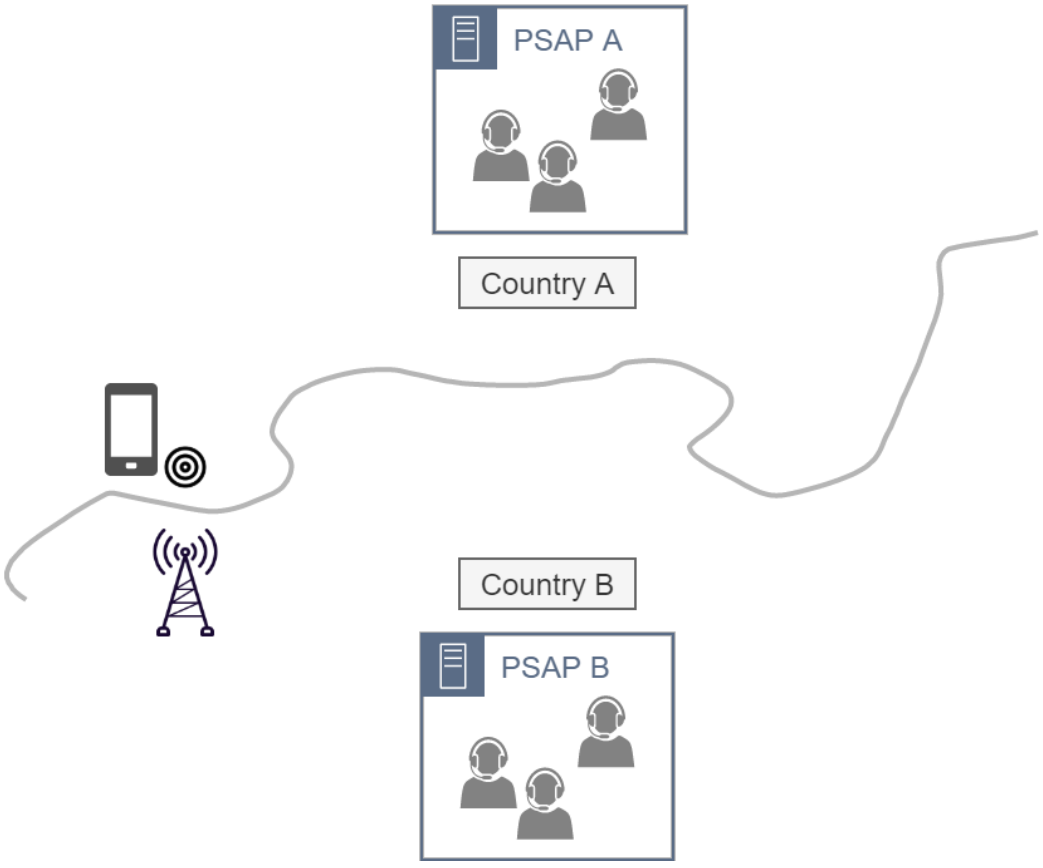


Figure 3: ESInet Interconnectivity

The NG112 architecture foresees a technical component, the so-called Forest Guide (FG) that enables interconnectivity between multiple independent ESInets. The FG provides a mapping from a given location to the responsible ESInet. In the given example, if the caller provides their precise location with the call setup, the ESInet in country B would recognise that the precise location of the caller is outside its jurisdiction. Using the FG, the ESInet in country B will automatically determine the correct ESInet to forward the call to. The emergency communication would then be terminated at PSAP A.

To establish the interconnection between ESInets, each country needs to provide its access point. In addition, the corresponding geographical data for each country needs to be provided.

Stakeholders	Actions
European Authorities	Create the necessary legal instruments to ensure that Member States provide the access points of their ESInet to other Member States.
European Authorities	Define the operation data set for the Forest Guide (geographic jurisdiction of each connected country)
National Authorities	Provide their access point to ESInet to other Member States / European authorities
Mobile Network Operators / VoIP Providers	Implement the access to the ESInet out of the home network

2.7.1 REFLECTIONS ON ADVANCED MOBILE LOCATION

Advanced Mobile Location (AML) fits well into the NG112 architecture and can be integrated into the NG112 core services. The most suitable core component to integrate AML is the Location Information Service (LIS). The LIS acts as an AML endpoint and receives the mobile location via SMS or HTTPS. The corresponding LIS interfaces to retrieve the location from the LIS are specified in the NG112 standard (TS 103 479). This enables all ESInet components, including PSAPs, to retrieve the location in a standardised way as shown in following figure.

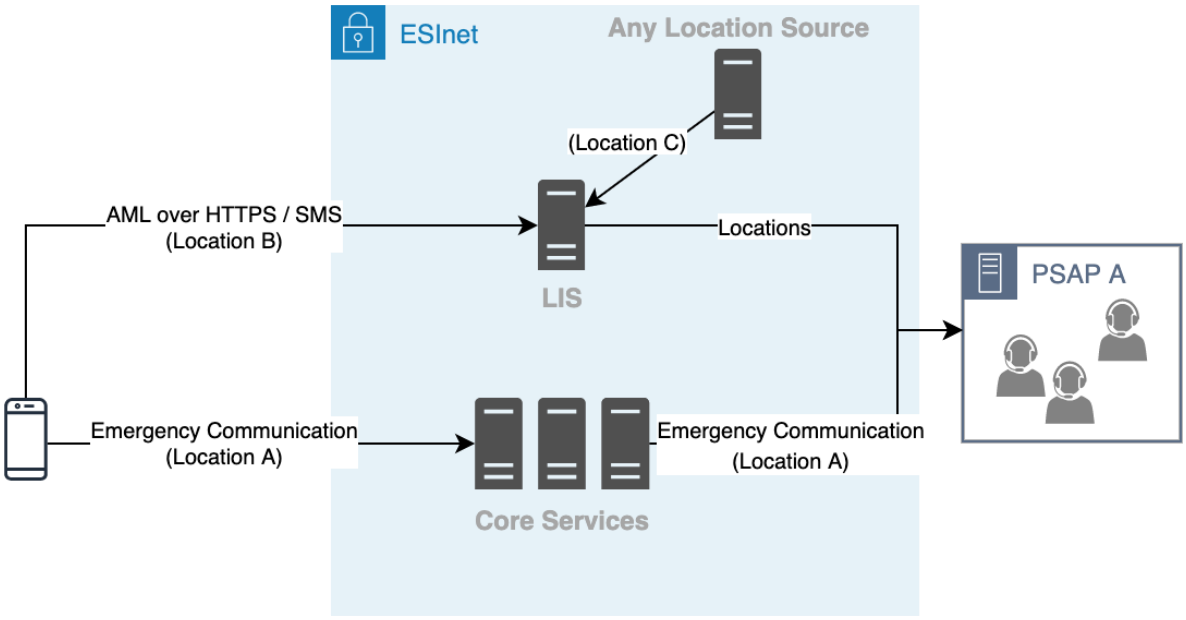


Figure 4: AML

The integration of AML into the NG112 core components shows the flexibility and scalability of the NG112 architecture. The LIS can integrate different localisation technologies while

keeping the same interface. This allows core components to be extended by adding different location sources in the future, without any impact on the PSAPs.

2.7.2 REFLECTIONS ON MOBILE APP INTEGRATION

Once the Mobile Operating System enables Voice over LTE (VoLTE) for emergency communications, Mobile Applications can trigger an emergency communication and provide additional data that is transmitted during the communication setup. Similar to triggering a normal phone call, the Mobile Application uses the built-in functionality of the Mobile Operating System and does not need to be aware of the NG112 protocols, as shown in the following figure. This enables a highly effective integration of NG112 emergency communications into Mobile Applications.

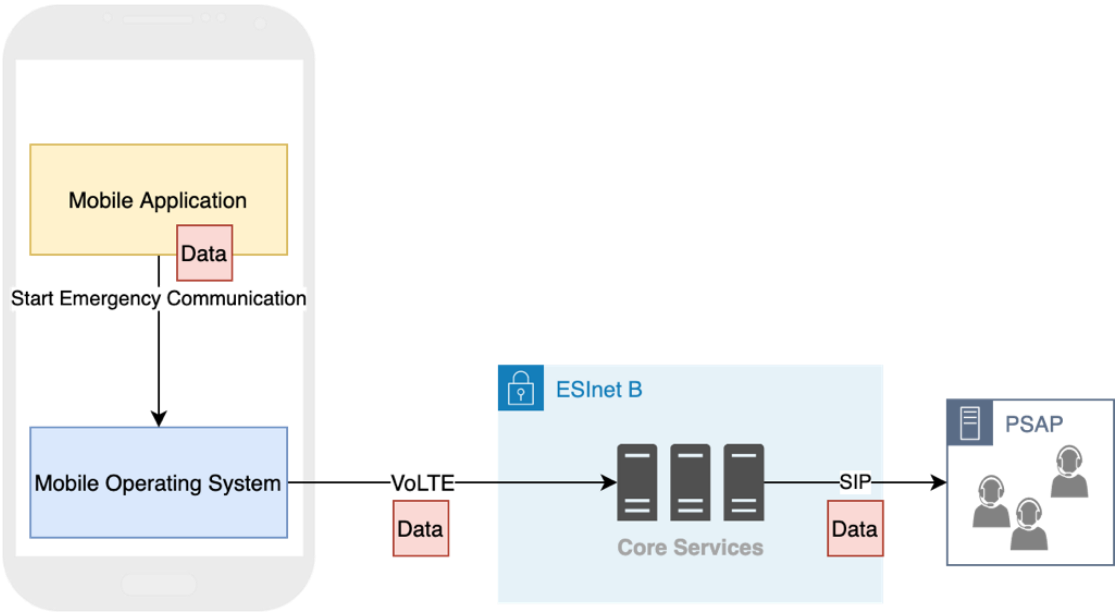


Figure 5: Mobile App Integration

In addition, independent of VoLTE, Mobile Applications might send data via a Trusted Provider into the ESInet for later usage. A Mobile Application could, at the request of the user, continuously transmit the current location, without establishing an emergency communication for a specific amount of time (TrackMe Feature).

2.7.3 REFLECTIONS ON NG112 ECALL

The continuous shutdown of 2G and 3G networks drives the demand for Next Generation eCall. The Next Generation eCall will improve the users' experience by providing faster data transfer and new sensors. It uses the same technical foundation and therefore can easily be integrated into the NG112 architecture.

In case of an accident, the Minimum Set of Data (MSD) is transmitted during the communication setup. The ESInet is agnostic of the data sent so that the NG112 eCall can benefit from all the routing capabilities of the NG112 core components.

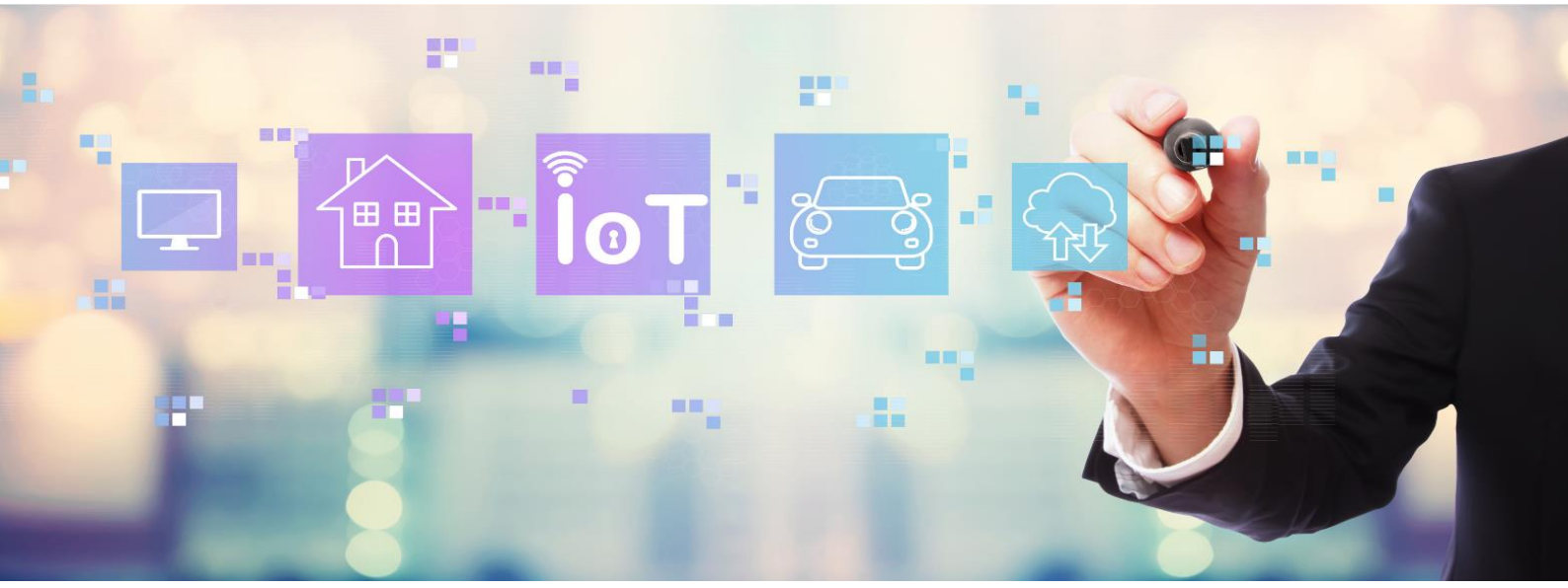
2.7.4 REFLECTIONS ON "NON-HUMAN-INITIATED" EMERGENCY COMMUNICATIONS

The NG112 eCall is just one example of a "non-human-initiated" emergency communication. Although the eCall also allows the transmission of voice and video, the initial trigger, the Airbag sensor, is purely data driven.

Due to technical progress in various areas, it is safe to assume that data driven emergency communications will increase. This requires emergency services that are independent of the originating device. The NG112 architecture and its core components do not make any assumptions nor rely on any originating device. It is important to understand that emergency communications may be triggered by different devices and are not limited to mobiles or mobile applications.

Considering the latest technical progress in the areas of Artificial Intelligence (AI), 5G, IoT, and drones, it is easy to imagine that emergency communications may be triggered by IoT sensors or AI-based analysis of drone footage.

The NG112 architecture and its core components provide the solid foundation for such future use cases and innovations.



3 I SUMMARY MATRIX

The following table provides a summary of the milestones and the corresponding actions of the stakeholders. Actions in *italic* format might be taken by different stakeholders depending on the emergency services model and division within a country.

Stakeholders / Milestones	MS1: Strategy Plan	MS2: Infrastructure	MS3: Core Services	MS4: PSAP Enablement
National Authorities	Lead the NG112 implementation project Be actively involved in the NG112 implementation project Develop routing rule set including fallback and support scenarios Establish the migration plan in terms of timeline and funds Specify emergency services model and supported emergency numbers *Establish a digital description of the geographic jurisdiction for each available emergency service and the corresponding PSAP*	Establish a country-wide authentication authority. *Procurement/Provision of the ESInet infrastructure*	*Procurement/Provision of the different Next Generation Core Services.*	Establish PSAP Access to the ESInet *Establish configuration for Next Generation Core Services according to the Emergency Services Strategy Plan*
Regional Authorities (depending on the county)	Be actively involved in the NG112 implementation project Develop routing rule set including fallback and support scenarios *Establish a digital description of the geographic jurisdiction for each available emergency service and the corresponding PSAP*	*Procurement/Provision of the ESInet infrastructure*	*Procurement/Provision of the different Next Generation Core Services.*	*Establish configuration for Next Generation Core Services according to the Emergency Services Strategy Plan*
Regulators	Be actively involved in the NG112 implementation project Develop routing rule set including fallback and support scenarios *Establish a digital description of the geographic jurisdiction for each available emergency service and the corresponding PSAP*			*Establish configuration for Next Generation Core Services according to the Emergency Services Strategy Plan*
Emergency services PSAPs	Develop routing rule set including fallback and support scenarios.	*Procurement/Provision of the ESInet infrastructure*	*Procurement/Provision of the different Next Generation Core Services.*	Technical Upgrade & Operational Training

Stakeholders / Milestones	MS5: Operators	MS 6: Mobile	MS 7: Interconnectivity
National Authorities	Create the legal frameworks to ensure that TSPs forward emergency communications to the ESInet, following to the NG112 standard.		Provide their access point to ESInet to other Member States / European Authorities.
Mobile Network / VoIP Providers	Enrich and forward emergency communications to ESInet *Implement the Emergency Service Number mapping according to the Emergency Services Strategy Plan. Alternatively, this can also be solved at the ESInet level via the core components.*	Enable VoLTE/ViLTE for SIP-based emergency communications	Implement the access to the ESInet out of the home network
Core Components Provider	Implement the Emergency Service Number mapping according to the Emergency Services Strategy Plan. Alternatively, this can also be solved at the ESInet level via the core components.		
European Authorities		Create the necessary legal instruments to mandate VoLTE / ViLTE for emergency communications to enable SIP-based communications	Create the necessary legal instruments to ensure that Member States provide their access points to their ESInet to other Member States. Define the operation data set for the Forest Guide (geographic jurisdiction of each connected country)
Mobile Operating System Vendors		Integrate additional data according to the NG112 standard in the VoLTE/ViLTE	