EENA Operations Document

Data sharing between Emergency Services

Title:	Data sharing between Emergency Services		
Version:	1.0		
Revision Date:	29/09/2015		
Status of the document:	Draft	For comments	**Approved**

EENA asbl
info@eena.org

Contributors to this document

This document was written by members of the EENA Operations Committee:

Authors	Organisation
Bertrand Casse	Deveryware (Vice-chair EENA Operations Committee)
Iratxe Gomez	Atos (Co-chair EENA Operations Committee)

Contributors	Organisation
Jenny Broman	Ålands Landskapsalarmcentral - Finland
Uberto Delprato	IES Solutions
Mark J. Fletcher	Avaya (vice-chair EENA Technical Committee)
Gunnar Hellström	Omnitor
Cristina Lumbreras	EENA
Thomas Reimann	HAMAT Medical Corporation
Peter Sanders	One2Many (Vice-chair EENA Operations Committee)
Mladen Vratonjić	Vice-chair EENA Advisory Board and Vice-chair of Operations Committee

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.

Table of contents

1 Executive Summary 4
2 Introduction 5
3 Situations where interoperability is essential 6
4 Interoperability and Information sharing 7
4.1 Key elements 8
4.2 Interoperability standards 10
4.3 Sharing mechanisms and agreements 13
4.4 Types of information shared 14
4.5 European examples 16
5 EENA recommendations 17
6 ANNEXES 18
6.1 Annex 1: ESENet Project 18
6.2 Annex 2: Case studies 19
6.2.1 CAP profile of Fire Brigade (Italy) 19
6.2.2 ARIEM 112 (Spain & Portugal) 19
6.2.3 NF399 interoperability standard for PSAPs (France) 21
6.3 Annex 3: Glossary 23

EENA asbl
info@eena.org

1 Executive Summary

Often a call to 112 results in the participation of multiple Public Safety Answering Points and Emergency Response Organisations in the resolution of the emergency situation, often this will include the need for cross-border collaboration. In order to ensure the quick and efficient cooperation during an emergency, response teams need to work under clearly defined rules of engagement, using overall goals that have well defined the type and level of cooperation required.

The level of information sharing and interoperability between Emergency Services organisations (Authority to Authority communications) may greatly vary from country to country, and possibly within the same country, and this could include the need to interact with other non-emergency organisations. Additionally, the type of information to be shared is quite diverse, including simple voice-based information sharing, or more advanced automatic / manual data exchanges - including plain text, mapping info, multimedia data and so on- up to sharing full common operational pictures.

This EENA Operations document describes situations in which interoperability is key, and deals with elements such as standards, sharing mechanisms and agreements, privacy and security, and more, while providing examples of European interoperability implementations.

EENA asbl
info@eena.org

2 Introduction

It is estimated that 320 million[1] emergency calls are made every year in the European Union, enabling emergency services to assist citizens in all sorts of difficult situations. Public Safety Answering Points (PSAPs) are reachable 24 hours a day, all year long. Consequently, PSAPs have to ensure that people who are in life-threatening situations and need urgent assistance can contact Emergency Services (ES). This may mean the difference between life and death for someone in trouble, and also huge losses linked to the environment or infrastructures.

A proper reaction to help requests from citizens often results in a combined intervention by different Emergency Response Organisations (EROs). This implies an efficient sharing of information between PSAPs and ERO Control Rooms, with a specific stress on the importance and complexity of having an understanding of needs and requests in a variety of situations as complete as possible:

- Between different levels of the same PSAP organisation
- Between PSAPs of the same ES within a country or region
- Between PSAPs of different ES within a country or region
- Between PSAPs of different countries with a shared border (cross-border)
- Between PSAPs of different countries of a wider scope (international)
- Between PSAPs and regional or national Public Authorities (PA)
- Between PSAPs and non-emergency services

When describing such interactions and needs, the concept of "interoperability" is often used, which has been defined as '*the ability of two systems to interoperate using the same communication protocol*[2]', '*the ability of equipment from different manufacturers (or different systems) to communicate together in the same infrastructure (same system), or on another while roaming*[3]' and also '*the ability of two or more systems or components to exchange data and use information*[4]'.

The following diagram represents different levels of interoperability:

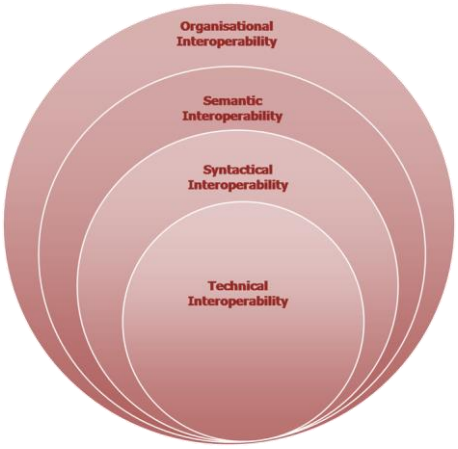

Figure 1 – *Levels of Interoperability*

Organisational interoperability: The ability of organisations to effectively communicate and transfer (meaningful) data (information).

Semantic interoperability: The meaning of content; concerns the human rather than machine interpretation of context.

Syntactical interoperability: Data formats, syntax and encoding.

Technical Interoperability: Machine-to-machine communications; communication protocols and the infrastructure needed for those protocols to operate.

[1] Estimate based on COCOM, EGEA and information provided by EENA emergency services' members

[2] From ETSI Project TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks). The project is now closed but its documents can be accessed from https://portal.etsi.org/tb/closed_tb/tiphon.asp

[3] Definition of interoperability of Next Generation Networks (NGN) from ETS's Technical Committee TISPAN (http://www.etsi.org/tispan/)

[4] In the context of the 3rd Generation Partnership Project (3GPP)

The scope of this document is to:

- Analyse mechanisms and needs for the sharing of information between ES and define the type of data to be exchanged.
- Provide ways to share information in an interoperable manner, with consideration to privacy and security aspects.
- Provide an overview of other types of organisations ES could be interacting with, look into models of cooperation, the impact on cost, and requirements.

The description of practices was obtained from several sources, including research projects and information sent by EENA members. As a conclusion, recommendations and EENA requirements are described.

3 Situations where interoperability is essential

An efficient management of an emergency situation requires different PSAPs to share information and, in general terms, interoperate. This may take the form of data sharing, building of a common operational picture, shared resource management, multimedia data sharing or even handover of situations.

As analysed in the ESENet project[5], different needs and priorities can be identified depending on the geographical extension (we refer to this as "geographical scale" of the incident), severity of the situation (we refer to this as "impact scale" of the incident) and the complexity of the situation (we refer to this as "capacity scale" of the Emergency services).

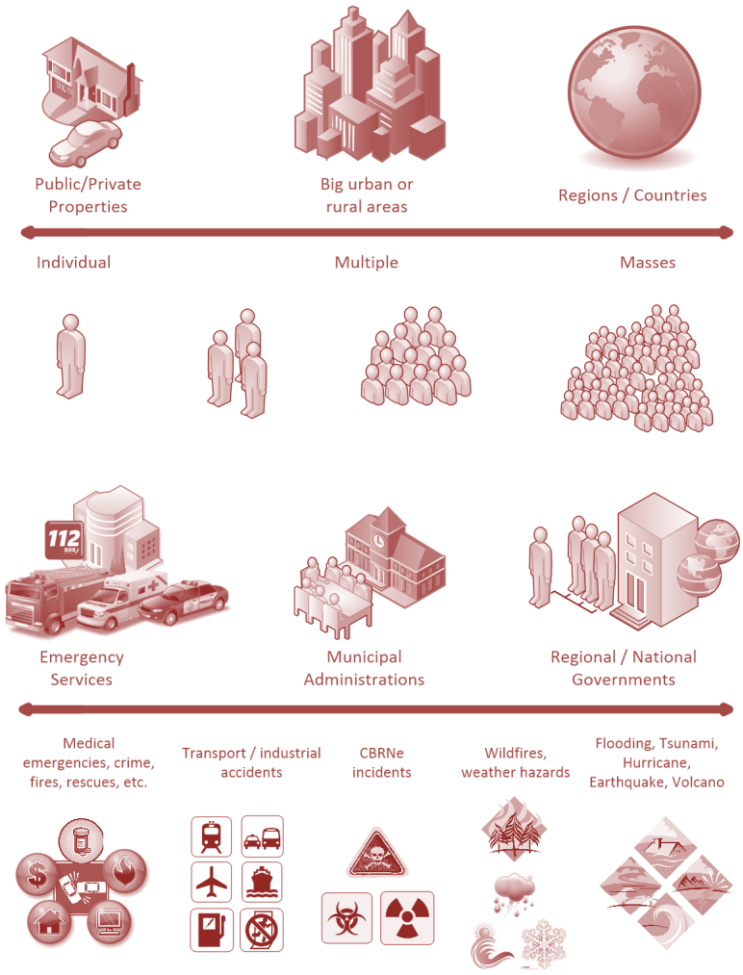

Figure 2 – *Scale of events – a conceptual view*

[5] http://www.esenet.org/

EENA asbl
info@eena.org

For the purposes of this document, we shall refer to the following classification:

- **Geographical scale**: "local scale" or "cross-border scale", where "local" includes all situations happening within the boundaries of a Member States (MS) and "cross-border" describes situations where the incident spans across 1 or more borders between MS (or even borders within a country with regional competences over ES). It should be stressed that "local scale" does not exclude the need for cooperation between different PSAPs operating in different jurisdictions of for different agencies within a MS. On the other hand, situations with the cooperation between MS that do not share a border ("International scale") are not the main focus here.
- **Impact scale**: "limited scale" or "large scale", where "limited scale" refers to situations where the expected evolution is limited and the risks involved are considered low, while "large scale" refers to incidents with the potentiality to escalate in scale or involving medium-high risks for the population.
- **Capacity scale**: "within capacity" or "beyond capacity", where those terms refer to the capacity of the involved ES to cope with the situation with the available resources and capabilities. An example of this could be for instance the result of a Mass Casualty Incident (MCI), or even the management of unavailability of a PSAP.

The possible combinations of the different scales are limited, so considering that all situations "beyond capacity" or at "large scale" require a PSAP to similar level of interaction with another PSAP, 4 different scenarios can be represented:

- Incident at "**local scale**", with "**limited scale impact**" and "**within capacity**", which is the equivalent of "business as usual" for PSAPs.
- Incident at "**local scale**", with "**limited or large scale impact**" and "**beyond capacity**" (multi-agency cooperation and maybe even collaboration with non-emergency services).
- Incident at "**cross-border scale**", with "**limited scale impact**" and "**within capacity**" (international cooperation).
- Incident at "**cross-border scale**", with "**limited or large scale impact**" and "**beyond capacity**" (international cooperation).

4 Interoperability and Information sharing

Whatever the scale of events, there are elements that need to be generally considered when interoperability between ES is required. More interoperable Emergency Services (ES) shall be capable of taking information from several sources (citizens first, but also sensors and web-services) and share them efficiently with other actors, identified by specialisation, jurisdiction, relevance and pre-existing cooperation agreements.

Full data interoperability will require at least:

- An infrastructure connecting computers
- An agreed protocol for having systems "talking to each other"
- An exchange mechanism for having information moved between computers
- A data format for structuring the information to be shared
- A protocol that defines what is to be shared unambiguously and computer-friendly (terminology/taxonomy)
- A user interface for presenting information in a human-friendly way

Interoperability between PSAPs as well as between Responders relies on agreements about both the definition and format of the shared information.

Starting with the establishment of **framework agreements** / **MoU** between all parties potentially involved, including **Quality of Service** aspects, and without forgetting **security aspects**, both in terms of sensitive data handling and infrastructure, and with consideration of the **clearance levels** of the different stakeholders. Facilitating the **mechanisms for interoperability** is of course essential too.

Operational issues need to be taken into consideration when dealing with multi-agency cooperation and/or international cooperation: Procedures (and potential restrictions) for coordination and situation awareness, access to shared information, privacy and security, definition of priorities, responsibilities, liabilities…

And of course **language issues** also become a factor in cross-border collaboration, because when crossing the border information that is shared should be clear and be interpreted in such a way that the meaning of

the data is understood equally by all parties involved. It is extremely important to factor in common languages (taxonomy may be a useful tool for solving this issue) and good training, including simulation/drills.

Last, the **collaboration with non-ES organisations** (which may include traffic management agencies, telemedicine services, organisations dealing with missing persons or suicide prevention, utilities companies, and so on) needs to be considered as well from the interoperability point of view:

- Models of cooperation and procedures
- SLA and impact on cost
- Requirements such as emergency contact numbers, communication channels, privacy and security…

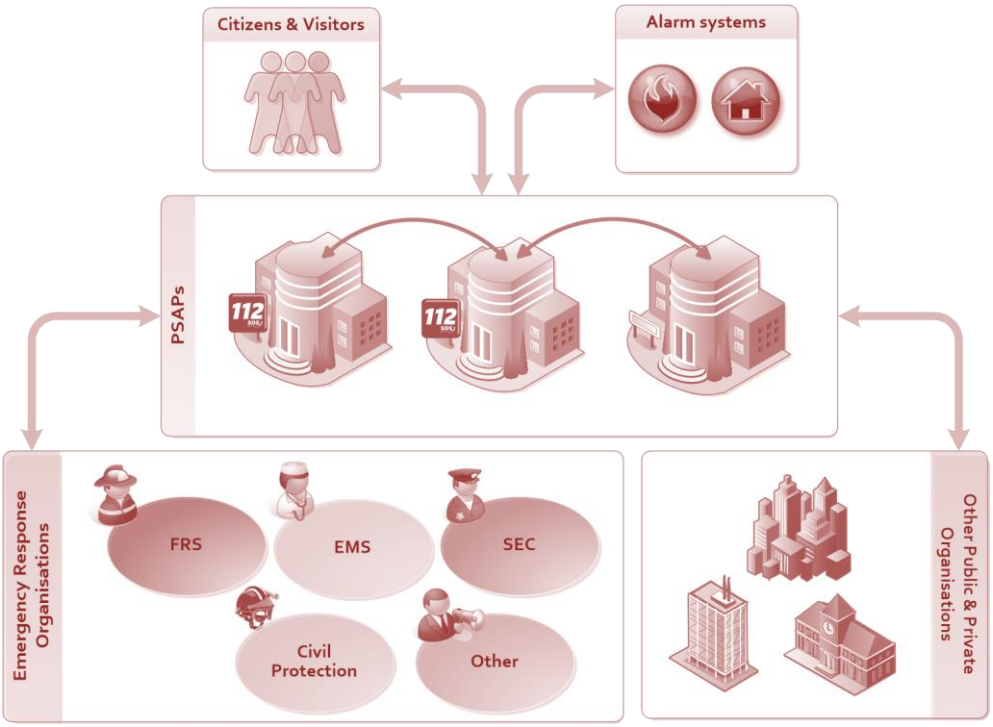

Figure 3 – *Interoperability between ES*

4.1 Key elements

Interoperability is often defined as "a property referring to the ability of diverse systems and organizations to work together (inter-operate)". The term was originally used in a technical systems engineering sense, however it now often used in a broader sense, taking into account social, political, and organizational factors that impact system to system performance.

When aiming at implementing an efficient cooperation between different organisations in an emergency situation, the concept of interoperability becomes even more complicated. It involves the ability of devices to work together, the possibility of people to understand each other for decision makers to have a common view of what actually is going on and the availability of cooperation frameworks for exchanging resources and information.

To help the understanding of the organisational processes in Emergency situations, the SECRICOM[6] project introduced a useful structure based on "Interoperability Layers", thus giving a synthetic form to all the needed components for realising a full and effective cooperation between EROs. Such a scheme, shown below in *Figure 2*, shows how the crucial challenge of ensuring Interoperability and communication between ES requires the implementation of several levels of Interoperability, ranging from the basic physical interoperability of devices to the agreement of political objectives of the organisations.

[6] SECRICOM - Seamless Communication for Crisis Management - EU funded project – FP7 (http://www.secricom.eu/)

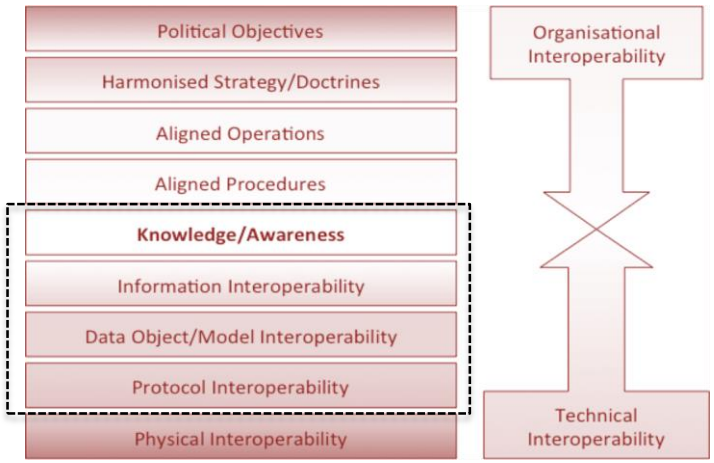

Figure 4 - *Layers of Interoperability (Secricom©)*

In this operations document, we shall focus on the layers from "Protocol Interoperability" up to "Knowledge/Awareness". Some details about them (derived from the ESENet project[7]) are reported in the following.

Protocol Interoperability

Given for granted that physical interoperability is reached (having solved all technical aspects), we still have to be sure that assets and information are used and shared in a harmonized way. We do not refer here only to objects, but also to the way they are used, are maintained, are shared and are exchanged. Again, an example may help in "visualizing" what kind of interoperability we are discussing here.

An emergency call can be originated in many different ways (landline, mobile phone, private network, pre-registered messages, VoIP, alarm systems…). How can we ensure that the heart of the message (somebody in distress) is received and properly handled? Information flow using many communication methods in the end reaches a call-taker; everything that is in between the call originator and the call receiver must be transparent, i.e. there should be no distortions/delays introduced by the communication chain. In other words, all the different possible communication subsystems must operate in a way that a suitable real-time conversational communication can be established, regardless of the devices, the media used, the carriers or the network (to name only some).

This again calls for a number of agreements (i.e. standards) agreed between all stakeholders in the chain.

When it comes to communication between mobile devices, radio systems or computers, things get more complicated but the underlying concept is the same: the users should get their tasks accomplished without taking care of the complexity underneath.

Data Object/Model Interoperability

Stepping up, we have now devices and protocols working well in harmony. How can we ensure that the content of a call or the mechanisms needed to perform a complex task are well harmonised?

Thinking for instance of two organizations willing to share geographical information, the way such information is coded and presented must be compatible. We know well about different unit systems or mapping systems. All information that Emergency Managers want to share must be coded/represented in a way that a computer system can handle and use without ambiguity. This is where standards become useful, as the goal here is to making it easier for an IT system to carry information around without distorting or losing bits in the process. Human understanding is vital to allow for an easy check and use of the data, with IT system simply allowing for a faster and more efficient storage and sharing.

[7] ESENet - "Layers of Interoperability – Introduction and Definitions" (http://www.esenet.org/)

Information Interoperability

We are now dealing with the meaning of information flowing between systems. Even when we correctly receive the data produced by somebody else and even if such data are correctly organized as we like, still we have to understand them and put them in context. There are plenty of examples of this, and we can summarize them with the codification of events or procedures used by an Emergency team. Whatever the complexity or simplicity of this description is, the two sides cannot "interoperate" if their complete meaning is not shared (hence the importance of Taxonomy). The way an emergency is classified, the way a resource is named hiding all the bundled components, all these are examples of what Information Interoperability means.

Knowledge/Awareness

This is the core level of interoperability, where technical and organizational interoperability converge to ensure the widest understanding of the situation and appropriateness of (re)action in an emergency. This is the ultimate goal of any command, control, communication and coordination system that has to count on all technical interoperability layers implemented and operates within a well-organized procedural/political context.

4.2 Interoperability standards

As one can easily guess form the wide range covered, there are many standards regarding interoperability and information exchange. In this table we tried to mention some of the most relevant standards concerning data interoperability and information exchange:

Subject	Standard	Short description
Emergency data	OASIS EDXL Framework[8]	The Emergency Data Exchange Language (EDXL) is a broad initiative by the OASIS Emergency Management TC to create an integrated framework for a wide range of emergency data exchange standards (vendor-neutral and platform agnostic) to support operations, logistics, planning and finance. Some relevant sub-standards include: ▪ Common Alerting Protocol (**EDXL-CAP**) ▪ EDXL Distribution Element (**EDXL-DE**) ▪ EDXL Resource Messaging (**EDXL-RM**) ▪ EDXL Situation Reporting (**EDXL-SitRep**) ▪ EDXL Hospital AVailability Exchange (**EDXL-HAVE**) ▪ EDXL Reference Information Model (**EDXL-RIM**) ▪ EDXL Tracking Emergency Patients (**EDXL-TEP**)
	EDXL-DE[9] (OASIS)	The EDXL Distribution Element (**EDXL-DE**) v2.0 is defined as a standard draft issued by the OASIS Emergency Management TC. It provides a standard message distribution format for data sharing among emergency information systems.
	OASIS-CAP[10] / ITU-T X.1303 bis[11]	Common Alerting Protocol (**EDXL-CAP**), also known as ITU Recommendation X.1303 (the ITU has adopted v1.2 of the CAP protocol and published this as an ITU recommendation), is an XML-based data format for exchanging public warnings and emergencies between alerting technologies and over of kinds of networks (it is sent embedded in an EDXL-DE envelope). CAP implements XML-based standards and specifications as CAP profiles; some interesting examples of CAP profiles include the Italian Civil protection & Fire Brigades (as described in Annex 2), the Australian and Canadian profiles, and IPAWS in the US.
Shared situation	TSO/EMSI (CEN)	Tactical Situation Object/Emergency Management Shared

[8] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=emergency

[9] http://docs.oasis-open.org/emergency/edxl-de/v2.0/csprd02/edxl-de-v2.0-csprd02.odt

[10] http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.pdf

[11] http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12150&showfl=1

awareness		Information (**TSO/EMSI**). ISO/TR 22351 describes the message structure built in order to facilitate interoperability between existing and new information systems, and contributes to the situational awareness of various parties involved in an emergency or crisis situation. It deals with the message structure and codes for the message structure (semantics) in order to make messages unambiguous, and it is used both for the exchange of messages between human users and as parameters for software programs. The structured message is called EMSI (Emergency Management Shared Information). EMSI follows an XML structure that is compatible for being transported by EDXL-DE. The new ISO/PRF TR 223519 (Societal security – Emergency management - Message structure for exchange of information) is adopting EMSI as message structure for exchanging situational awareness information in emergency scenarios.
	EDXL-SitRep (OASIS)	EDXL Situation Reporting (**EDXL-SitRep**) v1.0 Committee Specification 01[12]. This XML-based specification describes a set of standard reports and elements that can be used for data sharing among emergency information systems, and that provide incident information for situation awareness on which incident command can base decisions.
Geographical Information	OGC[13] and ISO/TC 211[14] family of standards	The scope of the joint collaboration of OGC and ISO/TC 211 is the standardization in the field of digital geographic information. Some relevant examples include: ▪ **GML**[15] (GML 3.2.1 = ISO 19136:2007): The Geography Markup Language (GML) is an XML grammar for expressing geographical features ▪ **WMS**[16] (WMS 1.3 = ISO 19128): The Web Map Service Interface Standard (WMS) provides a simple HTTP interface for requesting geo-registered map images from one or more distributed geospatial databases. Data is provided as web service. ▪ **WFS**[17] (WFS 2.0 = ISO 19142): The Web Feature Service (WFS) Interface Standard offers direct fine-grained access to geographic information at the feature and feature property level. Data is provided as web service.
	CEN/TC 287[18] geographic information standards	The scope of CEN/TC287 Geographic Information is standardization in the field of digital geographic information for Europe. Some relevant examples include: ▪ **CEN ISO/TS 19139:2009** defines Geographic MetaData XML (GMD) encoding, an XML Schema implementation derived from ISO 19115 ▪ **CEN/TR 15449**: It is a report in 5 parts dealing with Spatial data infrastructures.
	ShapeFiles[19] (ESRI)	**Shapefiles** is a widely used de-facto standard format for

[12] http://docs.oasis-open.org/emergency/edxl-sitrep/v1.0/cs01/edxl-sitrep-v1.0-cs01.pdf
[13] http://www.opengeospatial.org/standards
[14] http://www.isotc211.org/
[15] http://portal.opengeospatial.org/files/?artifact_id=20509
[16] http://portal.opengeospatial.org/files/?artifact_id=14416
[17] http://portal.opengeospatial.org/files/?artifact_id=39967
[18] http://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:6268,25&cs=19F6C87410AD7F9F9345287783B7C88C9
[19] http://doc.arcgis.com/en/arcgis-online/reference/shapefiles.htm

EENA asbl
info@eena.org

		vector data. A single shapefile archive (zip) can contain multiple physical files, and depending on the tools used there might be other accompanying files too.
	GeoPackage[20] (OGC)	**GeoPackage** is a universal file format for geodata; it is an open, standards-based, platform-independent, portable, self-describing, compact format for transferring geospatial information. The GeoPackage specification describes a set of conventions for storing data within an SQLite database.
	GeoTIFF	**GeoTIFF** is a public domain raster image format which provides geographical metadata. It is widely used for aerial/ satellite image, but as GeoTiff files tend to be very large, this format is rather used for transmitting small and limited images (using WMS for large images such as satellite or aerial images of a wider area).
	INSPIRE Directive[21]	The **INSPIRE directive** aims to create a European Union (EU) spatial data infrastructure (it uses CEN/TC 287, ISO/TC 211 and Open Geospatial Consortium standards and specifications)
Multimedia	IMS[22] (3GPP)	The IP-Multimedia Subsystem (**IMS**) specification has become the core component within 3G, cable TV and next generation fixed telecoms networks. Session Initiation Protocol (SIP) was selected as the signalling mechanism for IMS, thereby allowing voice, text and multimedia services to traverse all connected networks. 3GPP works closely with experts in the IETF to ensure maximum re-usability of internet standards, preventing fragmentation of IMS standards. Specifically 3GPP TS 22.101[23] and TS 23.167[24] form the base for emergency service access from 3GPP services.
	Total Conversation	The **Total Conversation** (TC) standard was defined in ITU-T recommendation F.703[25] as "an audio-visual conversation service providing bidirectional symmetric real-time transfer of motion video, text and voice between users in two or more locations. The ETSI TS 101 470[26] specification by EMTEL describes conditions for using TC for ES and makes access of emergency services possible to people with disabilities. IMS as well as IETF SIP implementations are covered.
	WebRTC (W3C & IETF)	Web Based Real-Time Communications (**WebRTC**) is a standardization project to enable real-time media transport (Voice, Video and Data) between browsers, with current focus on mobile. Work was initiated by Google in 2010, and is now split between IETF (RTCWEB[27]) and W3C (WebRTC[28]); in late 2015, WebRTC1.0 is hoped to be final in IETF & W3C. However, no emergency service specifications are yet created for WebRTC, although it is generally seen as an important topic because the system may attract many users.
Next Generation	LTD[29] (EENA)	The purpose of EENA's Next Generation 112 Long Term Definition (LTD) standard for emergency services is to define a long-term definition of an European emergency services

[20] http://www.geopackage.org/spec/
[21] http://inspire.ec.europa.eu/
[22] http://www.3gpp.org/technologies/keywords-acronyms/109-ims
[23] http://www.3gpp.org/dynareport/22101.htm
[24] http://www.3gpp.org/dynareport/23167.htm
[25] http://www.itu.int/rec/T-REC-F.703-200011-I/en
[26] http://www.etsi.org/deliver/etsi_ts/101400_101499/101470/01.01.01_60/ts_101470v010101p.pdf
[27] http://datatracker.ietf.org/wg/rtcweb/documents/
[28] http://www.w3.org/TR/webrtc/
[29] http://www.eena.org/uploads/gallery/files/pdf/2013-03-15-eena_ng_longtermdefinitionupdated.pdf

EENA asbl
info@eena.org

		architecture. The document has a profound impact on the operation of 112 services and PSAPs (new data formats, more rigid data structure requirements, new functions, …) The document provides the definition of specific terminology used in the description of the NG112 architecture, a description of elements building the core concept of the NG112 architecture and he description of the state that has been reached after a migration from legacy to all IP-based systems with a corresponding Emergency Services IP network.
	IETF	IETF has specified a framework for IP based emergency service access, forming the base for the regional next generation emergency service specifications. IETF RFC 6881[30] is a best practice document with descriptions of the framework and references to the different detailed documents.

Table 1: Interoperability standards (sample)

Some countries have also defined or are currently defining their own interoperability standards:

- The **UK**, with the Multi Agency Incident Transfer Standard MAIT[31] by British APCO
- **France**, with the new NF399[32] (see annex 6.2.3)

4.3 Sharing mechanisms and agreements

To be able to ensure an efficient sharing of information between ES, a variety of mechanisms and definitions must be agreed upon all stakeholders, covering all aspects of what, why, when and how to be shared.

- **Why**: Consideration of geographical scale (eg. different jurisdictions), impact scale (eg. different ES) and/or capacity scale, overflow of emergency calls, management of calls routed to a wrong PSAP….
- **What**: Basic incident data (type, location, victims, damages), requests for support, information on resources dispatched, command structures, acknowledgements and updates, incident handover …
- **How**: With a clear strategy which includes the use of standard data formats, exchange mechanisms and tools (which should be regularly tested), providing access to shared information repositories, feeding a common operational picture available to all involved parties, with strong consideration of privacy and security aspects, with verification and validation mechanisms, and planning for contingency.
- **When**: Real-time information is essential, and delays due to technical or operational issues should be minimized.

Some of these general aspects are described next.

- **Strategy**: Clear guidelines and roadmaps need to be defined by each of the stakeholders involved in data sharing. Items like **common/shared databases** should be part of an overall strategy between ES, and furthermore, a **transnational database** (a pan-European fully secure database where each country can nominate one PSAP to be the "lead PSAP" and to handle such interoperability issues as they arise) should be established in Europe to allow MS to transfer emergency calls between their lead PSAPs if and when it is needed (although as each MS is based on its own legislation, this may not be always possible). **Overflow of calls** one of the key factors affecting the response by ES to citizens, so there needs to be a common approach for dealing with call overflow in order to have adequate and consistent actions taken, and legislation on both the EC and MS level is required. The strategy should also cover management of unavailability and business continuity, together with **regular testing** of interoperability and call overflow response plans with drills and simulations (as disparate technologies could be involved).
- **Framework agreements**: This refers to the framework for ES (and other stakeholders) which shall govern how information is shared in day-to-day operations as well as in major incidents. The amount

[30] https://tools.ietf.org/html/rfc6881

[31] UK MAIT standard (http://mait.org.uk/)

[32] French standard NF399 (http://www.nfsecuritecivile.fr/)

of data that can be shared is enormous and it is important to address the risk of "over" information of decision makers. It is worth highlighting the importance of neighbouring jurisdictions defining frameworks in how to use data to combine forces in preparation, response and recovery activities. As an example, an inter-agency policy Memorandum of Understanding may prioritize intra-country activities, with a secondary focus on inter-country activities. Of course any agreement will have to cater for legislation (e.g. liabilities) and administration (e.g. reimbursement of costs) aspects too.

- **Security:** Two main areas need to be considered at least: **Infrastructure security and sensitive data sharing** among different agencies. When responding to incidents different Services have different **responsibilities** and needs for information. Police Agencies might depend on sensitive information to carry out their assignment, a sensitivity that might require a higher **security clearance** than most have. So clear **boundaries** in sharing information is paramount to ensure operational and national/international security. **Verification and validation** of data needs to be factored in, with consideration of aspects such as what sources do we trust, should we integrate Social Media communications to get "live" feeds from disaster struck areas or not, and more.
- **Contingency and business continuity:** Procedures would have to establish when and how PSAPs have to cooperate with others in case of unavailability. This collaboration could be made between PSAPs from the same country or from different countries. Using **cloud-based solutions** in Emergency Operations may be seen as a high risk solution, but at the same time, it may be the best way to share large amount of data quickly (e.g. GIS data). PSAPs and EROs would have to carefully construct SOPs that cater for use of off- and online data.

4.4 Types of information shared

As we have seen in previous chapters, the level of information sharing in A2A communications during emergency and crisis situations may vary a lot from country to country, and even within the same country; on top of that, often there is also a need to interact with non-emergency services.

This document will not be dealing with aspects such as available communication lines, contact points and directories, conferencing capabilities, automation of information exchange, sharing mechanisms, or even cloud-based solutions vs. databases vs. structured messages.

Instead, this section analyses different types of information that may potentially be shared between ES, from communications-related aspects to operational data sharing.

Managing communications

The following examples present situations in which communications interoperability is needed:

- **Handling calls routed to the wrong PSAP**: Either because a PSAP has received a call not corresponding to their jurisdiction, or because a PSAP in country A needs to seamlessly connect a citizen to a PSAP in country B (e.g. because an incident has happened to their family member/friend who lives there). The distributed geographical databases and services used for routing of calls to the most appropriate PSAP need to use interoperable methods and consistent data, and the management of this data need to have procedures for maintaining its consistency through changes in borders and technologies.
- **Handling of calls with need of assisting services for language or modality translation:** There are sometimes needs to involve external services to translate between communications forms managed by the user and managed by the PSAP at the emergency site. The translations can be between different spoken languages as well as between sign language and spoken language, or even between text and spoken language for cases when the local PSAP does not handle text communication. In some cases the translation is handled by relay services, in other by interpreter agencies or special ES internal resources.
- **Overflow of calls**: When demand capacity exceeds supply (call overflow), PSAPs could have the facility in place to re-route emergency calls on congestion and to re-direct the excess calls to a "buddy" PSAP room in a controlled, pre-arranged and efficient manner.
- **Mission critical communications**: Sharing of information through various radio systems infrastructures to deliver information between A to B, with clear rules for communication.
- **Contingency management**: Due to a temporary or permanent unavailability of a PSAP, a PSAP from a different jurisdiction or even country may need to take over operations.

Shared information repositories

- **Mutual collaboration agreements**: Harmonised strategy, administrative details (contact details, reimbursement of costs, etc.), legislation aspects (data protection, liabilities, boundaries, etc.), responsibilities, privacy aspects, etc.
- **Agreed protocols and procedures**: Details about basic resource needs, rules of engagement, escalation, command structure, glossaries, taxonomies, communication aspects (and maybe even specific media strategy), etc.
- **Resource description**: Details about assets that may potentially be used in multi-agency, multi-regional or multi-national cooperation.

Operational data sharing

The following examples present information that may potentially be shared between ES during emergency or crisis operations.

- **Alerts and updates**: Requests for help (and acknowledgements), incident details, location, EROs involved and so on. PSAPs may also consider the need to sharing enhanced data obtained from eCalls or through emergency Apps, for instance.
- **Resource management**: Description of needs, access to available resource data, tracking information, etc.
- **Incident command structure**: Definition of joint command structure and ERO-specific command structure, public communication needs, nominated spoke-person, etc.
- **Multimedia data**: Sharing of relevant images (still or video) in support of operations, relevant data such as blueprints of buildings or electricity/gas/water lines, guides on hazardous materials involved in the incident, and so on.
- **Shared situation awareness**: With agreed mapping, iconing and coding for presenting information, Common Operational Picture and so on.
- **Incident handover:** De-escalation and de-activation of resources, reports, etc.

Of course all technical and operational aspects related with information sharing needs to be tested and trained extensively, and it is important to carry out exercises involving all stakeholders, especially for international situations in which on top of everything, language may also be a barrier.

EENA asbl
info@eena.org

4.5 European examples

In the next table, some relevant European interoperability experiences are presented:

Scope	Region	Concept / Participant PSAPs	Details
Use of standards	Italy	CAP profile of Italian Fire Brigade	The *Corpo Nazionale dei Vigili del Fuoco* (Italian FRS) have adopted EDXL-CAP for full messages exchange with any other ERO. See case study in Annex 2 for further details
	France	NF 399 implementation for ES interoperability	NF399: *NF Logiciel Sécurité Civile* is the French interoperability standard for PSAPs. It contains ISO/IEC 25051:2014 (Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing). See case study in Annex 6.2.3 for further details
Cross-border & scale	Spain & Portugal	ARIEM 112 project	The aim of the ARIEM112 (112 Galicia, 112 Castilla y Leon, and CCDRN from Northern Portugal) project is the "Cross-border reciprocal Assistance in Emergency Matters" through the implementation of the collaboration agreements and interoperability tools. See case study in Annex 6.2.2 for further details
	Europe	ERCC	The European Emergency Response Coordination Centre (ERCC[33]), is participated by the 28 EU Member States, the former Yugoslav Republic of Macedonia, Iceland, Montenegro, Norway and Serbia (Turkey has recently signed the agreements to join the EU Civil Protection Mechanism too). The participating states pool resources that can be made available to disaster-hit countries and share best practices in disaster management.
Multi PSAP/ERO	Austria	144 Lower Austria	*Notruf Niederösterreich*[34] (Lower Austria) ▪ Single organisation providing services from 4 distributed PSAPs (Zwettl, Tulln, St. Pölten, Mödling); ▪ Exchange of data with several integrated EROs (EMS, POL, FRS, CP…)
	Bulgaria	112 Bulgaria	112 Bulgaria[35] ▪ 6 distributed stage 1 PSAPs (Sofia, Montana, Ruse, Varna, Burgas, Kardshali); ▪ Data exchange with all ERO-specific stage 2 PSAPs;
	Finland	112 Finland	ERCA 112 Finland[36] ▪ In mainland Finland there are 6 distributed stage 1 & 2 PSAPs (ERCs in Oulu, Kuopio, Pori, Kerava, Turku, Vaasa), with POL, FRS and EMS integrated. There is one more PSAP in the autonomous region of Åland Island, which is not part of the Finnish *Nödcentralverket* with no data interaction with the PSAPs on mainland Finland. ▪ The ERC IT system is a source of data not only for the "traditional" security authorities and their field command system, but also - when needed - share different data to other systems and organisations as well.

Table 2: European interoperability examples

[33] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[34] www.144.at
[35] www.112.mvr.bg/
[36] www.112.fi/

5 EENA recommendations

As a summary of this document EENA would like to make recommendations about how to improve interoperability and information exchange between ES and with other stakeholders. It is not intended that all measures are to be taken in all cases.

Stakeholders	Actions
European Authorities	• Define legal provisions about data organization and sharing; define a legal framework to become a reference to agreements between governments at any level (from national to local); • Mandate the definition of a common European standard and mechanism for data exchange; • Launch dedicated research and development projects; • Launch implementation and monitoring programs, and facilitate pan-European training programs.
National / Regional Authorities	• Regulate the adoption of standards. • Start multi-lateral legal agreements for defining the political and administrative interfaces between states, regions and ES. • Monitor the implementation of such agreements, and the achievement of operational alignment of procedures and formats. • Define and monitor the implementation of training and exercise.
National telecommunication regulator	• Monitor the adoption of standards; • Regulate and monitor the implementation of mechanisms for data sharing between states, regions and ES; • Involve TNOs if and when needed
Emergency services	• Upgrade their technology to NG112 and be interconnected; • Implement standards and mechanisms for data sharing between states, regions and ES; • Establish Framework Agreements with all relevant stakeholders, defining all interoperability aspects (why, what, how, when) aimed at achieving operational alignment of procedures and formats.
Other stakeholders	• Establish agreements for data sharing with all relevant ES, defining all interoperability aspects.

Table 3: EENA recommendations

EENA asbl
info@eena.org

6 ANNEXES

6.1 Annex 1: ESENet Project

ESENet[37] - Emergency Services Europe Network, is a project that ran for two years (2013-2014), having received funding from the European Union's Seventh Framework Programme. Its partners were EENA, ERUPSI and IES Solutions (coordinator).

This Coordination Action aimed at establishing a network of stakeholders in the Emergency Management domain that would identify, discuss and agree on needs, requirements, new technologies and best practices in responding to everyday as well as to major emergencies.

Knowledge gained from the results of the SECRICOM[38] project, the objectives of ESENet was:

- The identification of gaps in the emergency service provision chain and the collection of user requirements.
- The selection of available and/or promising technologies for tackling the identified challenges, also identifying areas where further research was needed.
- The analysis of organizational gaps, with suggestions and best practices at EU level about procedures, framework agreements and reorganizing suggested tasks.
- The identification of available standards or areas where standards would be needed.

A total of five face-to-face workshops (including the final workshop) and up to eight web meetings were held in total. The ESENet project final workshop took place on 14-16 October 2014 in Brussels. It served as an opportunity for summarising the results of several cycles of discussion and revising the list of recommendations identified by the experts and included in the final report. During the three day workshop, participants from around Europe discussed topics related to emergency services including caller information, transnational calls, methods of interaction with emergency services, next generation techniques and services, and much more.

The three cycles of discussions between decision makers, users (i.e. PSAPs and EROs), and industries, focused on:

1. Citizen to Authority communications (C2A)
2. Authority to Authority communications (A2A)
3. Authority to Citizen communications (A2C)

Specifically in the cycle of discussions on A2A communication, three main aspects were considered:

- **Contingency Management**: Redundancy of control rooms and business continuity can be seen from the following angles: Individual PSAPs' perspective (each PSAP has to take their own measures of redundancy of their own infrastructure) and collaboration between PSAPs, for which procedures need to be established for when and how PSAPs shall cooperate with others in case of unavailability; this collaboration could be made between PSAPs from the same country or from different countries.
- **Interoperability between Control Rooms:** In the workshops, different scenarios were considered (local scale vs. cross-border and within control room vs. beyond control room capacity), and the following issues were discussed: Mutual aid agreements, sharing data, handing over the incident, taxonomy, mission critical communication, mapping, fleet management and incident command system.
- **Interoperability with and between Responders**: In the workshops, different scenarios were considered.

The detailed results of the workshops in the cycle of discussions on A2A communications can be browsed in the following link: http://www.esenet.org/results/results-from-the-workshops/

[37] http://www.esenet.org/

[38] SECRICOM - Seamless Communication for Crisis Management - EU funded project – FP7 (http://www.secricom.eu/)

6.2 Annex 2: Case studies

This section presents three case studies of European data sharing practices, covering cross-border cooperation, the use of international standards and the implementation of a national standard.

6.2.1 CAP profile of Fire Brigade (Italy)

With the Italian Decree dated 23 May 2011[39], the Italian Ministry of the Interior - Department of Fire (*Corpo Nazionale dei Vigili del Fuoco*) - established the full adoption of the EDXL-CAP Protocol as '*Profilo CAP Vigili del Fuoco*' (CAP Profile Fire Brigade), together with models and mechanisms for a full messages exchange with any other organization.

The guidelines and requirements of the FRS CAP Profile comply with the requirements of the CAP standard v1.2. The National FRS generates and sends messages in accordance with "Profilo CAP Vigili del Fuoco" and ensures the reception and handling of all alert messages compliant with CAP, even if they are not in accordance with the FRS CAP Profile (but such messages might not be optimally viewed by FRS PSAP operators and this could lead to some delays in the interventions).

The elements of a message are contained in three main blocks: Alert, Info and Resource, and in all those blocks there may be compulsory, conditional and optional data. All incoming alert messages need to be validated, and the preferential mode of transmission of messages uses standard-compliant Atom Feed (as specified by RFC 4287[40]).

The following example, extracted from a document by Vigili del Fuoco[41], shows a standard message exchange between three regional PSAPs: PSAP 1 (FRS), PSAP 2 (EMS), PSAP 3 (POL) following a relevant incident. The message flow can be summarized as follows:

1. An emergency call is received by PSAP 1, informing of a severe incident linked with railway transport of dangerous good.
2. An alert message is issued from PSAP 1 to PSAP 2 & PSAP 3 providing initial incident details.
3. An update message is issued by PSAP 1 to all other PSAPs involved (providing additional incident details).
4. A second update message is issued by PSAP 1 to all other PSAPs involved (providing additional incident details).
5. An acknowledge message is issued from PSAP 2 to PSAP 1.
6. An alert message is issued from PSAP 2 to PSAP 1, confirming that they've received calls about the incident and are responding to it.
7. An update message is issued from PSAP 2 to PSAP 1 (informing of resources dispatched).
8. An alert message is issued from PSAP 3 to PSAP 1 confirming that they've received calls about the incident and are also responding to it; also informing of resources dispatched.
9. An update message is issued from PSAP 3 to PSAP 1 (informing of estimated arrival time of resources).
10. A second update message is issued from PSAP 3 to PSAP 1 (confirming the location and situation).
11. An acknowledge message is issued from PSAP 1 to PSAP 3.
12. An alert message is issued from PSAP 1 to PSAP 3, confirming FRS resources are on-site.

6.2.2 ARIEM 112 (Spain & Portugal)

ARIEM-112[42] is a project in the framework of the Spain-Portugal cross-border cooperation programme, with the title "**Cross-border reciprocal Assistance in Emergency Matters**". The project has been funded by the EU and the regions; it run initially between 2011-2014, with an extension running until 2015.

[39] http://www.vigilfuoco.it/aspx/Page.aspx?IdPage=4554
[40] http://tools.ietf.org/html/rfc4287
[41] http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=4857
[42] Source *Axencia Galega de Emerxencias* (Galicia, Spain): http://www.ariem112.eu/Contenido/PRESENTACI%C3%93N-Comite%20de%20Rexi%C3%B3ns-Novembro%202013%20(Ingl%C3%A9s).pdf

The three partners of the project are the *Xunta de Galicia – Axencia Galega de Emerxencias* (Galician regional government emergency agency, Spain), *Junta de Castilla y León – Agencia de Protección Civil* (Castilla y León regional government civil protection agency, Spain) and *CCDR-N Commissâo de Coordenaçâo e Desenvolvimento Regional do Norte* (Northern Portugal regional coordination and development commission).

The Mutual Aid Agreements and Joint Action Protocols of ARIEM-112, signed in Porto (Portugal) in October 2013, set the legal framework for cooperation and mutual assistance and determine the activation mode to be used, together with communication mechanisms and resources on both sides of the northern Spanish-Portuguese border.

The scope of the cross-border cooperation spans through an area of 17.000 Km^2 and 109 municipalities from both sides of the border (87 in Spain and 22 in Portugal), with a total population of ~572.000; this is the ARIEM area.

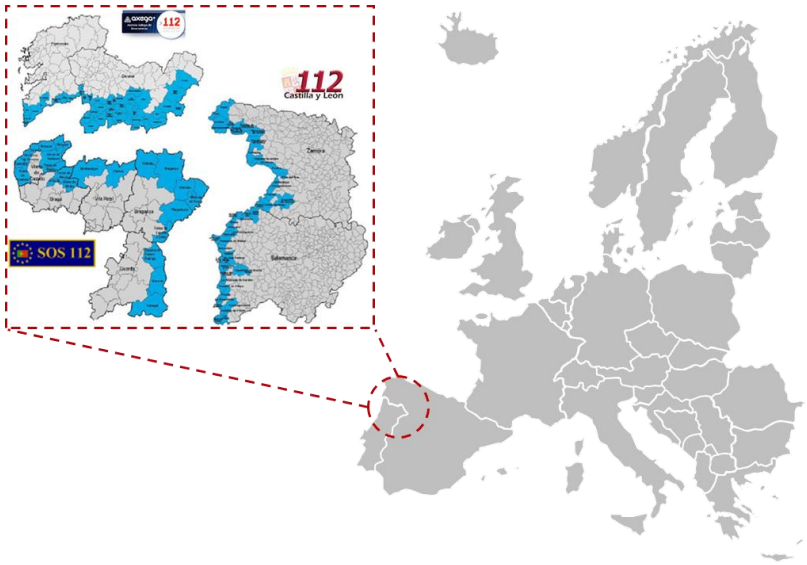

Figure 5 – ARIEM 112 area and participating PSAPs

The regional PSAPs participating in the project are **112 Galicia** (in Santiago de Compostela) and **112 Castilla y León** (in Valladolid) in Spain, and several EROs (in Viana do Castelo, Braga, Vila Real, Bragança & Guarda) in Northern Portugal. Between all the organisations participating in the project, the accumulated ES resources include some 1196 FRS staff, 73 squads, 263 FRS vehicles, 8 EMS helicopters, 4 rescue helicopters, 121 teams for specialized emergencies and 211 healthcare institutions.

The main objective of ARIEM 112 being the establishment of a mechanism for collaboration between the emergency management and mobilization of resources from the areas of Galicia, Castilla y León and the North of Portugal, the work was focused on creating a common space for the management of emergencies where everyone helps everyone, rationalizing the use of existing resources while reducing response times, and increasing the efficiency and quality of services provided.

The project faced some initial constraints, which can be summarised as legal and administrative issues, lack of any institutionalized interoperability between PSAPs of different regions/countries and a whole new context of cross-border cooperation. The Project started off in 2011 with a diagnostic study that identified a number of challenges for improvement and the development of:

- **Creation of a legal framework** by developing Mutual Aid Agreements and Joint Action Protocols between the participating regions in the ARIEM area, which were signed in Porto on 25/10/2013 (the detail of the SOP and mutual assistance agreements is subject to confidentiality). Among other things, they determine the activation mode and communication mechanisms to use, and draw out a common typology for joint interventions and establish the protocols for resource mobilization and Joint Action Procedures on both sides of the border.

- **Deployment of tools** to automate the coordination of resource mobilization in the ARIEM area, with real time communications and information exchange. The technical tools for requesting / offering help and resources included phone and video conferencing capabilities, and the Remote Manager Terminal System ARIEM-112, which allows any of the participating agencies to request / offer support in emergency situations happening in the ARIEM area, and to exchange real-time information with all participants in the incident; it also provides a catalogue of media and resources integrated with a GIS module containing all the basic mapping coverage. The system has been deployed in all participating PSAPs (including the mobile command vehicle of 112 Galicia) and also in EROs in the ARIEM area, upon request.
- **Training program and joint drills** to enable pooling of efforts, experience and knowledge, while establishing a networking that will support the formal and informal communications, strengthening the cohesion and collaboration. Some specific types of incidents covered in training included traffic accidents (urban and rural), fire intervention techniques in tunnels, police related emergencies and flooding-related situations. And also 4 international drills has been carried out so far:
    - Flooding due to a dam breakdown (2012): Activation of the INUNCyL emergency plan in the Nuestra Señora de Agavanzal dam in Castilla y León.
    - Fire in a railway tunnel (2013): Fire and MCI in a train inside the O Corno railway tunnel in Galicia.
    - Rescue in the Miño/Minho river (2014): A leisure vessel capsizes in international river waters between Galicia and Portugal.
    - Traffic accident with victims in difficult rescue area (2014): A car with multiple occupants tumbles off a 120m cliff in Galicia.

There have also been real activations of the ARIEM 112 Plan, the first one in August 2014 due to an industrial fire in Porriño (Galicia), in which both the local ES and Portuguese FRS participated in the incident response. And as of mid-August 2015 there had been 3 more activations in Galicia alone: The search for a missing fisherman in Entrimo in April, the search for a missing person in the Miño/Minho river in Tomiño in June and a wildfire in Calvos de Randín in August.

The project was presented at the Committee of Regions in Brussels in November 2013 as a successful example of best practice, with special emphasis and focus on a common channel of communications for emergency management, standardization of materials and equipment, promoting the use of ICT in emergencies, consolidation of training and joint practice programs and also the dissemination of 112.

ARIEM 112 has served to raise the pillars of a common space for emergency management together with mobilization of emergency resources in the border area. The challenge now is to consolidate the Project in the coming years, continuing with the legal and educational framework developed up to this point.

6.2.3 NF399 interoperability standard for PSAPs (France)

The French regional FRS (SDIS) and EMS (SAMU) and the rest of stakeholders that intervene in emergency situations use for their operations software products that usually cover their needs concerning call management, operations follow-up, data transmission, resource dispatching, reporting, communications and so on, but with the interoperability requirement set by the public safety modernisation law (Law 2004-811 from the 13th August 2004), a deep analysis of the standardization of solutions in terms of ways of communicating was forced. At that time there was a clear lack of technical specifications concerning security, compatibility, interoperability, etc. to support the operations of the regional EMS and FRS.

The ANTARES network (*Adaptation Nationale des Transmissions Aux Risques Et aux Secours)* offers natively functionalities that cater for a full interoperability of ES nationwide (unique terminal identifier, transmission of status and short messages, transmission of the call to stage 2 PSAPs and resources, other data transmission, call and vehicle location). As the years went by, and with new regulations, additional transversal interoperability domains had to be considered too, such as the link between EMS & FRS, or even eCall.

In order to use such functionalities fully, they needed to be implemented in existing or future solutions through a formal technical framework, so the French Emergency Services and Public Authorities, together with

expert members and solution providers created the GT399[43] working group to define the interoperability requirements (data, functionality, features, relationships…) of emergency management systems deployed in PSAPs.

Every year they release a new version of the certification rules called NF *Logiciel sécurité civile* (NF 399), a French norm for public safety software. The NF 399 standard for incident management interoperability is widely used in France, as it contains specific French values (unfortunately this also makes it more difficult to replicate in other countries).

The GT399 work is aimed at identifying product categories, agreeing specific functionalities and defining interoperability requirements. It is formed by +200 members, including:

- End users representing PA, Police, FRS and EMS (French Ministry of Interior, *Bataillon de Marins Pompiers de Marseille, Brigade de Sapeurs-Pompiers de Paris, FNSPF, Préfecture de Police de Paris, SAMU de France, SDIS).*
- Expert members from the Ministry of Interior (DGSCGC and DSIC), ASIP SANTE, AIRBUS D&S, AFNOR Certification and INFOCERT.
- Solution providers

The *NF Logiciel Sécurité Civile* (NF399[44]) brand defines the requirements that all public safety solutions producing, managing or exchanging data through national public safety networks need to comply with. These solutions are certified by INFOCERT according to the certification rules of NF399, to guarantee data and operational management function interoperability.

The NF399 provides both native and additional functionality defined by GT399, and convers data exchange and management aspects, operational exchange aspects and data exchange and treatment between operational management systems from the different ES PSAPs and also in the field, with consideration to escalation requirements too. It also ensures the compliance with quality, QoS and specific public safety requirements. The main idea behind NF399 is that interoperability between different national or regional systems allows deploying homogeneous applications all across the country, and ensures total interoperability with other regional, national or European reinforcements.
The GT399 has also released a normative document which defines the nature and format of flows between third-party services dealing with eCalls and PSAPs.

The certificates[45] of the products that have already been certified specify that "The indicated product is certified in accordance with the certification rules *NF Logiciel Sécurité Civile* and the ISO/IEC 25051[46] standard" (Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing).

[43] http://www.nfsecuritecivile.fr/index.php?option=com_content&view=article&id=69&Itemid=538

[44] http://www.nfsecuritecivile.fr/index.php?option=com_content&view=article&id=67&Itemid=535

[45] Certificate for NICE Recording (issued to Nice Systems UK Ltd): https://services.infocert.org/certificats/CERTIF-13-35-R1.pdf

[46] http://www.iso.org/iso/catalogue_detail.htm?csnumber=61579

6.3 Annex 3: Glossary

All definitions of terms and acronyms related to 112 are available in the 112 Terminology EENA Operations Document[47]. For convenience, the ones used in this document are also listed below:

Acronym	Description
3GPP	3rd Generation Partnership Project
A2A	Authority to Authority
A2C	Authority to Citizen
BAPCO	British Association of Public Safety Communications Officials
C2A	Citizen to Authority
CAP	Common Alerting Protocol (Oasis)
CBRNe	Chemical, biological, radiological, nuclear or enhanced explosives
CEN CWA	European Committee for Standardization (CEN) CEN Workshop Agreement (CWA)
CEN/TC 287	Technical Committee on standardisation in the field of digital geographic information for Europe
CP	Civil Protection
ECHO	European Commission's Humanitarian Aid and Civil Protection department
EDXL	Emergency Data Exchange Language (Oasis)
EMS	Emergency Medical Services
ERC	Emergency Response Centre
ERCC	Emergency Response Coordination Centre (EU)
ERO	Emergency Response Organization
ES	Emergency Services
ETSI	European Telecommunications Standards Institute
EU	European Union
FRS	Fire & Rescue Services
GIS	Geographic Information System
GML	Geography Markup Language
GT399	Working Group on the "*NF Logiciel Sécurité Civile*" (NF399), the French Interoperability Standard for PSAPs and EROs
IETF	Internet Engineering Task Force
IMS	IP-Multimedia Subsystem
ISO	International Organization for Standardization
ISO/TC 211	Organisation responsible for standardization in the field of digital geographic information / Geomatics (the ISO geographic information series of standards)
ITU	International Telecommunications Union
MCI	Mass Casualty Incident
MoU	Memorandum of Understanding
MS	Member States (European Union)
NG112	Next Generation 112
NGN	Next Generation Network
LTD	Long-Term Definition (EENA's NG112 LTD standard for emergency services)
OGC	Open Geospatial Consortium
PA	Public Authorities
POL	Police
PSAP	Public Safety Answering Point
SLA	Service Level Agreements
SOP	Standard Operating Procedures
TC	Total Conversation
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TNO	Telecom Network Operators
TSO	Tactical Situation object
W3C	World Wide Web Consortium
WMS	Web Map Service (OGC)
WFS	Web Feature Service (OGC)
XML	Extensible Markup Language

Table 4: Glossary

[47] http://www.eena.org/uploads/gallery/files/operations_documents/2012_10_16_112terminology.pdf