ISITEP
D3.4.1 - PROCEDURES FOR NEW ENTRANTS TO THE ISITEP NETWORK

Document Manager:	Etienne Lezaack	BFP	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	LEONARDO
SP Leader:	DNK

Document ID N°:	ISITEP_D3.4.1_20170126_V1.0	**Version:**	V1.0
Deliverable:	D3.4.1	**Date:**	26/01/2017
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Etienne Lezaack (BFP)
Approved by: (WP Leader)	Etienne Lezaack (BFP)
Approved by: (SP Leader)	Marianne Storrøsten (DNK)
Approved by: (Coordinator)	Paolo Di Michele (LDO)
Security Approval (Advisory Board Coordinator)	Etienne Lezaack (BFP)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Marianne Storrøsten, Jens Petter Johansen, Michel Duits	DNK	Contributor
Kirsten Aabye, Steen Peterson	MOT	Contributor
Jaakko Saijonmaa	ADS FI	Contributor
Etienne Lezaack	BFP	Editor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
All Company Project Managers	All involved companies	Members of the Steering Committee
Elina MANOVA	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V0.1	15/01/2016	All	All	Skeleton draft
V0.2	20/01/2016	All	All	Skeleton draft review
V0.3	13/12/2016	All	All	Draft
V0.5	20/12/2016	All	All	Draft review
V0.5.1	22/12/2016	11, 15,16,17	3, 5	Small adaptations
V0.6	30/12/2016	All	All	Draft review

V0.7	06/01/2017	All	All	Draft review
V0.7.1	09/01/2017	-	2.2.1	A few comments added Suggestion for section 2.2.1 added
V0.8	11/01/2017	-	Appendix	Contributors remarks synthesis
V1.0	26/01/2017	All	All	Final release

Publishable extended abstract

This document summarizes the organisational and technical conditions and activities for new entrants to the ISITEP network (“ISI cloud”) based on a bilateral approach.

The emergence of a TETRA roaming hub is considered in appendix, as a possible next step to simplify the full-mesh lines interconnection topology.

CONTENTS

ABBREVIATIONS

CCA	Critical Communication Application
CCS	Critical Communication Systems
ETSI	European Telecommunications Standard Institute
GSSI	Group Short Subscriber Identity
HW	HardWare
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ISITEP	Inter System Interfaces for TETRA-TETRAPOL Networks
ITSI	Individual TETRA subscriber Identity
I-VDB	Individual subscriber-Visitor DataBase
LTE	Long Term Evolution (= 4G)
MNO	Mobile Network Operator
MS	Mobile Station (= radio terminal)
PC	Personal Computer
PPDR	Public Protection and Disaster Relief
SwMI	Switching and Management Infrastructure
TCCE	TETRA and Critical Communications Evolution
TEA2	TETRA Encryption Algorithm #2
TETRA	TErrestrial Trunked RAdio
TG	Talk Group
TMO	Trunked Mode Operations

1. INTRODUCTION

There are several implementation steps and activities that must be undertaken to allow new entrants to connect to another country's TETRA network. Allowing new entrants to the network involves a comprehensive process of organizational and technical activities that requires participation from organization on different levels in both countries. Thus, connecting a new entrant (country) to an existing ISI cluster of networks (i.e. Norway and Sweden) is not applicable for ad hoc international cooperation where connection is not already completed.

In order to determine the procedures for new entrants to the ISITEP network, the organisational and technical conditions to enable interoperability between two countries are firstly summarized.

Seeing each visited country (SwMI) needs to control which foreign radios (subscribers) are allowed to migrate and with which profile (see D23.2, section 6.2., requirements I-EUR-FUN-4.a and I-EUR-FUN-5.a), we are in a situation where all the connectivity is based on bilateral agreements. This implies that a new entrant has to establish a bilateral interoperability with each member of the "ISITEP network".

Following this principle, activities and procedures for interconnecting new entrants are further summarised.

Relying on bilateral agreements (logical link) and on bilateral lines (physical links) with your neighbouring countries fulfils all the needs for cross-border communications. However, an improved solution might be developed in a next step. Scaling up a bilateral lines approach implies indeed to build up a full-mesh network topology, which could become prohibitive in means when a large number of countries are considered. This issue is addressed in appendix and reflection tracks are proposed to solve it.

This paper is limited to the TETRA technology because interoperability between national networks (which implies terminal migration to a national visited infrastructure) only exists in a TETRA context.

The deliverable D35.1 "Procedure for roaming activation" describes more in details why the interoperability is so difficult in the TETRAPOL case and proposes solutions for ad hoc international cooperation.

2. TECHNICAL AND ORGANISATIONAL CONDITIONS TO ENABLE INTEROPERABILITY BETWEEN TWO COUNTRIES

2.1 Summary of the organisational conditions developed in the WP's 3.1 till 3.3

The organisational conditions listed below are based on the Norway-Sweden collaboration of connecting Nødnett and Rakel and is a shortlist of necessary main activities and agreements to allow new entrants (countries) to enter the network.

Please, confer to the following ISITEP papers: D31.1 "Framework Model", D32.1 "Functional Model" and D33.1 "Handbook of PPDR Procedures" for more detailed insights into organisational conditions and areas of collaboration among participants in cross-border cooperation. Confer to D31.2 "Norway-Sweden Agreement" for areas of regulation between owners/operators of national emergency communication networks.

2.1.1 Legal agreements

Bilateral agreements on different levels as well as within the country must be in place before allowing interoperability between 2 countries. This includes political agreements between the authorities that ensure the intention and general process of connecting the networks, end-user agreements regulating the rules and mandates for operating in the other country and agreements between network operators to allow the actual connection.

More specifically, agreements must cover several aspects and organizations to allow the interoperability:

- Political agreement
- End-user agreements
- Owner/operator agreement
    - Transmission
    - Network (visitors register and talkgroup-linking provisioning)
    - Operations
    - Control room
    - Radio terminal

As an example, figure 1 illustrates the complexity of the agreements that must be in place at Norway's side in order to establish an ISI connection between Nødnett (No) and Rakel (Se). Red lines indicate bilateral business agreements, purple lines indicate user support and green lines indicate operator support. xDOs are the emergency agencies operation and maintenance centres.

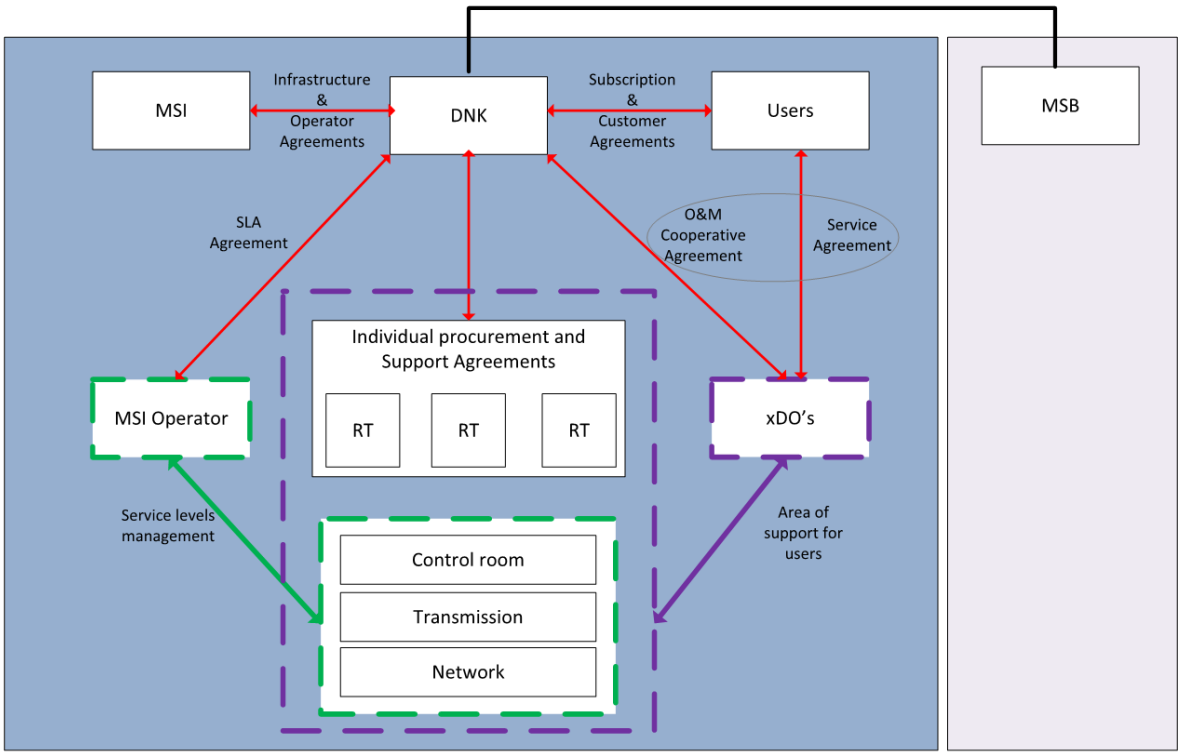

Figure 1: Agreements that must be in place from Norway's side to establish interoperability with Sweden

2.1.2 Functional model

An international fleetmap and operational procedures must be defined and implemented before allowance of new entrants. International talk groups between the participants must be defined and programmed in the radio terminals and implemented in the core networks. A functional model must be accepted by the end-user community as well as implemented by the network operators.

Depending on the national repartition of the mandates, the functional model shall be developed under the lead of the network owners or directly by the user organisations. In any case, the user organisations in both countries will be involved in the definition process.

2.1.3 Guidelines, terms of use and training.

Operational guidelines for communication between emergency agencies in the two countries are necessary and must be in place before allowing interoperability. The emergency systems differ between countries as well as communication guidelines. Guidelines that regulate methodology, procedures, overview of differences in emergency systems, core terminology and rules of operation must be in place.

Education and training in these guidelines are also necessary for both countries. These are products that must be well grounded within and between the end-user organizations as well as the network operators.

2.2 Generic description of the supplementary functional modules and provisioning to ensure the migration between two countries

2.2.1 Functional modules to ensure the communication interoperability

- ISI gateway

  An ISI gateway has to be implemented at both sides. It includes:

  - A capability to configure permissions and capabilities for visitors. This concerns among others the allowed TG for visitors.
  - The Individual subscriber-Visitor DataBase (I-VDB)

    This is the database of the current location of all the visiting individual subscribers. When the visiting MS is authorized, then it is inserted in the I-VDB. Not necessary before: the necessity or not for pre-provisioning visiting MS in a visited SwMI is vendor specific.

- Transmission lines

- Upgraded software for TETRA radio terminals as in use in both countries.

- Modified software for control rooms to incorporate addressing and communication with the visiting TETRA terminals as used by the visitors.

2.2.2 Provisioning to ensure the logical interoperability

- ISI communication path
  - Own and peer SwMI address (to be used by the transport layer)
  - Jitter buffer (ensure that the outbound jitter does not exceed the maximum allowed value)
  - In case of E1 links, the Traffic channel selection mode must be agreed between the operators to avoid unnecessary call collisions.

  The requirements to the physical communication path is described in section 2.4

- Allowed visitors
  - A visiting MS is authenticated in a visited SwMI based on authentication information items received from the Home SwMI.
  - The MS is configured and licensed for Air Interface Migration into the foreign SwMI
  - A visiting MS will have an agreed profile defining the usage of services in the visited network.

These three bullets make up the space to define user rights for migrations (in Norway and Sweden).

- Profiles for visiting radios

  Independent of vendor, owner or operator specific features and functions on the Air Interface of any given TETRA system, the provisioned MS on a specific SwMI will have a profile defining which talkgroups can be used, if telephony calls can be made, if it is allowed to scan et cetera. These access rights are referred to as user rights or profile (stating the access or capabilities assigned to an ISSI in a SwMI) per system in this document.

  Per system (that is Home and Visiting system), the provisioned mobile subscribers that are actually allowed to migrate into the other network have to be known in the generic user databases with its ITSI. Equal as any radio user has user rights to access functions in the home network, these rights are for the visiting or foreign network too.

  Per group of users from the foreign network the following rights can be assigned in a profile to allow or deny the following services after successful authentication in the visited system:

  - Access to defined talkgroups (depending on cooperation with agencies)
  - Access to multi agency talkgroups
  - Allow scanning
  - Allow private call half or full duplex
  - Allow access to the PSTN
  - Allow a geographical profile where the MS is allowed to use talk groups

  Note : This list is vendor dependent : there might be more or less restrictions in the profiles.

- Talk Group-linking

  A linked group is defined from creating a controlling talkgroup in a network on which other groups (participating groups) from other networks are linked.

  To ensure the full control of the set of linked talkgroups, the length of the ‘hang-time’ must be coordinated. The ‘hang-time’ configured for the controlling talkgroup must have a higher value than the ‘hang-time of any of the participating talkgroups.

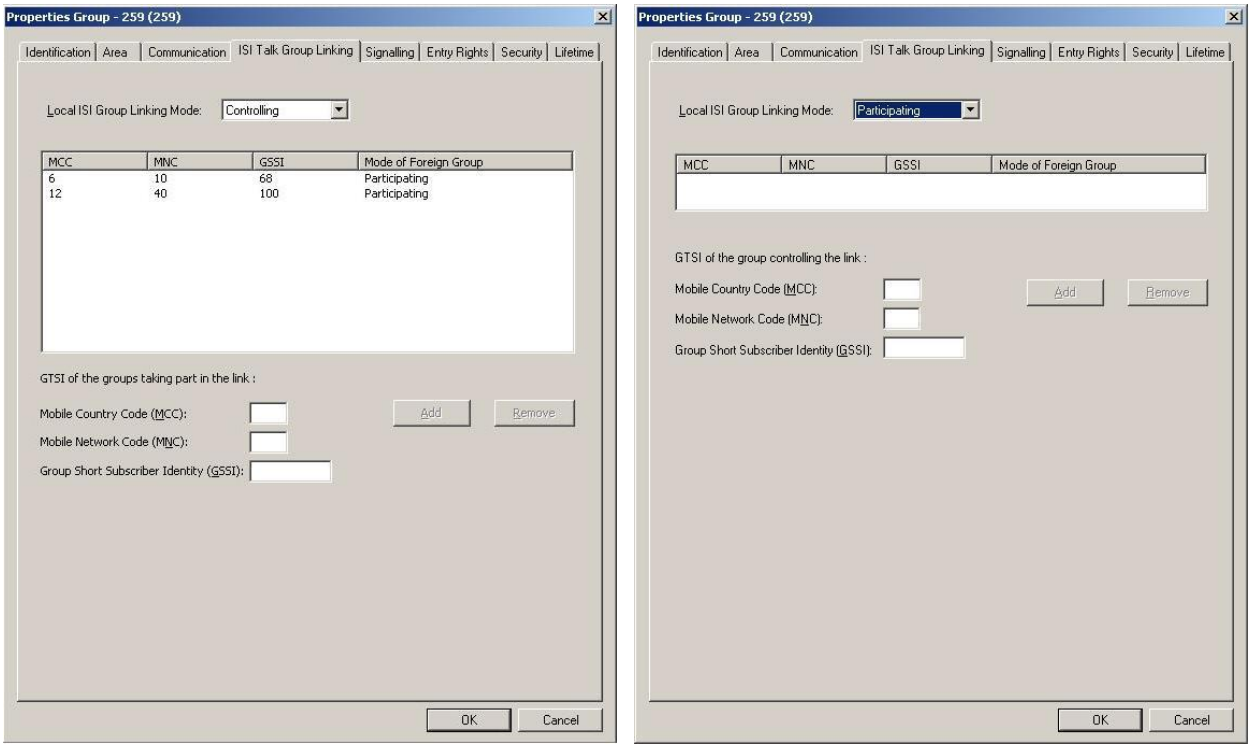

Figure 2: Dialogue boxes used for defining a controlling and a participating group (Airbus)

2.3 Synthesis of the technical and organizational conditions to enable interoperability between two countries

	Country A	Country B
Legal aspects	International treaties	
	Bilateral treaties	
Operational agreements	Agreements between the end user organisations Missions descriptions/Operational procedures	
Communication agreements	Agreement between networks owners/operators Security/capacity/resilience/maintenance/financial model	
	Agreements between the end user organisations Mono- and multi-agencies radio functional models	
Radio functional model, procedures and training	International Fleetmap	
	International radio features	
	Cross-border Radio procedures	
	Cross-border Education materials	
Technical aspects	Core network ISI ready	Core network B ISI ready
	Control rooms ISI ready	Control rooms B ISI ready
	Terminals A ISI ready	Terminals B ISI ready
	ISI gateway A	ISI gateway B

For more background on implementation and organisational conditions with examples from the Norway-Sweden collaboration, see:

- D31.1 “Standard Framework Model”.
- D32.1 “Functional Model for more background on these issues”.

2.4 Technical Requirements and Considerations for Inter-System Connections

New entrants connecting to existing members of the ISITEP network must ensure a secure and stable connection to the system.

There have been considerations about using the European TESTA-ng network as network provider for the transport of ISI related information (signalling and audio), but up till now this network is not able to provide the required bandwidth, priority and maximum delay which is required for PPDR communication.

2.4.1 Security

The security considerations have be elaborated in a number of deliverables as part of the ISITEP program. The following deliverables describe the security requirements for new entrants before they can connect to existing members of the ISITEP network and some implementation proposals. This includes the definition of VPN, IPSec tunnels, encryption level etc. The security requirements will not be elaborated further.

D22.3 – "Final Security Requirements" lists the security requirements which new entrants must fulfil in order to connect to other members of the ISITEP network. This includes system internal and external security measures.

D46.2 – "Security Architecture to Support Demonstration Cases" describes the security components which shall be in place before connection towards other members of the ISITEP network can start.

D46.3 – "Security Solutions" evaluates off-the-shelf security components and suggests the configuration of those components.

2.4.2 Stability

The network stability is a product of a number of parameters:

- Network Architecture
- Service Availability
- Bandwidth
- Priority
- Quality of Service (QoS)
    - Jitter
    - Latency
    - Packet Loss
    - Out of order delivery

D24.4 – "Network Architecture Final Release" elaborates about the Quality of Service (QoS), Service Level Agreements (SLA) and Service Level Specification (SLS).

Network Architecture

Dependent on the level of availability which is wanted one or two security gateways must be deployed towards the intermediate carrier network.

Service Availability (Service Level Agreement)

The service availability is important for a mission critical system. The service availability for the intermediate carrier network must be as close to 100% as possible. In case of a break down the service restoration time is utmost important.

Bandwidth

The required bandwidth is dependent on the technology used for the transport of call control signalling and audio and the number of simultaneous calls. The bandwidth requirements are symmetric (same bandwidth requirements in uplink and downlink toward the intermediate carrier network).

If IP links are used between the systems the required bandwidth is 20 Kbit/s per call.

If E1 over IP is used between the systems the required bandwidth is 10 Mbit/s per E1 link (32 timeslots).

Priority

To obtain the necessary stability of the audio stream it is important that the audio has the highest priority in the security gateway and in the intermediate carrier network. If the inter-system connection is an E1 connection emulated over IP it is important that all communication has high priority (due to the nature of the E1 related transport protocols).

Jitter

Jitter impacts the audio quality and must be kept as low as possible. The current specifications for the ISI Generic Speech Format [x][(1)] states that the jitter in the originating end shall be less than +/-5 ms. As no jitter is expected on an E1 link (for which the specification is written). In order not to degrade the audio quality too much the requirement towards the intermediate carrier network shall be that the jitter in this network is less than +/-10 ms which in total gives a calculated jitter of +/-11,2 ms (within 99,7% confidence) at the receiving point which should be manageable in all systems.

Latency

The latency between two ISI GWs shall not exceed 200 ms[(2)]. This includes any buffering (jitter buffer) in a MUX in case of E1 over IP. Higher latency will cause an audible delay in the audio transmission where users will notice the silence between speech items. Especially when more than two systems are involved in a call a high latency will affect the audio delay and audio quality.

Packet Loss

Packet loss in the audio stream causes metallic sound. To have a decent audio quality the packet loss must be as low as possible. A packet loss of maximum 0,1% is recommended.

Out of Order Delivery

Out of order delivery will have the same effect as packet loss. Out of order delivery is generally avoided by establishing a VPN tunnel between the ISI GWs.

[1] TTR 003-05-3 V1.1.0 (5 Oct 2016); TETRA + Critical Communications Association (TCCA); TETRA Interoperability Profile (TIP); ISI Part 05-3: Generic Speech Format Implementation (ISFG)

[2] During WP7.2 were the public Internet was used, the latency between Copenhagen and Genoa was measured to 35 ms and between Copenhagen and Helsinki to 100 ms (including a jitter buffer of 60 ms in the MUX).

3. CONDITIONS FOR INTERCONNECTING NEW ENTRANTS

To obtain a full interoperability inside an initial cluster of countries, what WP 3.4 names the “ISITEP network”, each of them must have a bilateral interoperability with each of the others (fully meshed scheme). So, when you defined the conditions for a bilateral interoperability (see section 2), the extension to several countries is straightforward.

This was also the only way for interconnecting the MNO’s in the GSM technology before the introduction of the “multi IMSI roaming” and the “open connectivity roaming hub” service concepts.

A new entrant has to establish a bilateral interoperability with each member of the “ISITEP network”; nothing more, but also nothing less.

Each existing linked group being controlled by one of the countries of the ISITEP network, if the new entrant has also to join this international talkgroup, it is the ISI between the new entrant and this controlling country that will be used to ensure the communication path. Linked groups topology always keeps a star configuration.

4. ACTIVITIES AND PROCEDURE FOR INTERCONNECTING NEW ENTRANTS

Activities for interconnecting new entrants are mentioned in the following bullet list. This is based on the section 2 describing the technical and organizational conditions to enable interoperability between two countries and on the section 3 describing how to scale up to connect a new entrant to an initial cluster of countries.

4.1. Prerequisites:

- Costs/benefits study for interconnecting your network to another one(s)
  - The cost study has to be led by the involved operators/network owners, in negotiation with the industry suppliers.
  - The benefits study has to be led by the end-user organisations, showing that cooperation between the first responders on the field and/or the possibility to intervene beyond the borders are saving forces, time and lives, while ensuring better results
- Political decision from the concerned networks authorities

4.2. Common discussion between each couple of operators/network owners and the related end user organisations

- Defining the scope
  - Interconnecting radio network only or interconnecting control rooms too
  - If control room interconnected, defining which applications are concerned (automatic location…)
- Defining the radio functionalities that will be available for the first responders
  - Migration & Authentication
  - Individual Calls
  - Telephony Calls
  - Group Calls
  - Group Patching
  - Emergency Calls
  - Exchange Short Data and Status messages
  - …
- Defining the amount of terminals concerned by the roaming, their chance to be simultaneously abroad and the maximal number of simultaneous common communications over the ISI.
- Defining the degree of security of the communications
  - Air Interface Encryption

- End to End Encryption
- Lines encryption

- Defining the financial principles related to the roaming for the end-user organisations

4.3. Operators and end users streams progressing in parallel

4.3.1. Activities and procedures between each couple of operators/network owners

The industry suppliers are tightly involved when the discussions concern the technical design and the maintenance. They are the key actors during the implementation and testing phase.

- Designing the ISI gateways and the communication links (redundancy, resiliency, capacity and security)
- Interconnection/testing of both reference networks
- Terminals compliancy testing sessions
- Rollout of the upgrades for implementing the releases “ISI ready” on the operative networks
- Connection of the operational networks
- Preparing the communication agreement:
  - The Parties
  - Purpose and background
  - Definitions and interpretations
  - Prerequisites for becoming an ISI user
  - ISI Services delivered
  - Cost allocation, payment and payment terms
  - Rights and obligations, cooperation
  - Confidentiality
  - Term of the Agreement
  - Cancellation
  - Changes and amendments to the Agreement and Appendices
  - Counterparts and Date of execution

4.3.2. Activities and procedures between the related organization users

Different international working groups have to been established, at similar agencies level and at multidisciplinary level.

- Talk Group structure and usage
- Crisis management
- Functionalities and technical prerequisites

- Technology and methodology
- Education, training and scenarios
- Legal aspects
- Terminology and status messages
- Preparing the handbook with the guidelines and procedures for cross-border communication

Note: some working groups will involve user organisations from more than two countries, e.g. talkgroups definition for three country border regions or for areas encompassing more than two countries, defining the communications related to international events, operations, escorts, phenomenon's covering large regions or crossing multiple countries etc.

For more detail on the development of a functional model, see D32.1 Functional Model.

4.4. Operational trial

- Operational trial
- Approbation period before the definitive bringing into service

APPENDIX: TOWARDS A GLOBAL INTERCONNECTION APPROACH

An ISITEP network of N countries is a full-mesh network topology containing N (N-1) / 2 ISI's. If a full interoperability has to be ensured between this ISITEP network and a new entrant, this latter has to establish N new bilateral ISI (VPN) links.

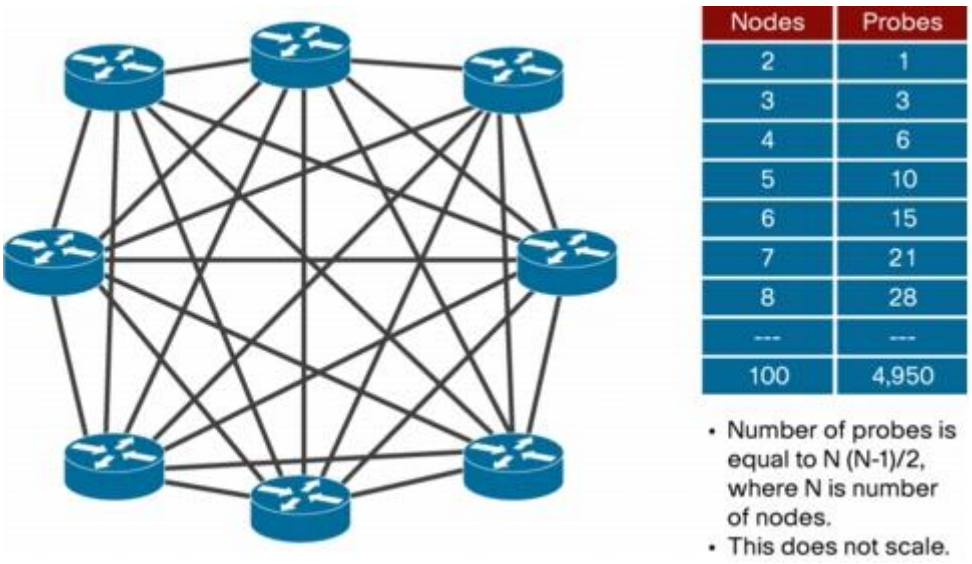

Figure 1: Full-mesh network topology

Seeing the cost and the complexity of maintaining one full-mesh ISITEP network, we can imagine that countries will limit ISI implementation to their neighbours. Therefore, a simpler solution has to be developed, if we really want full interoperability to face *international visit missions* or *full international missions*, where first responders from several countries are converging to the same location or where first responders are sent far away from their home country.

Referring to D24.2, § 4.1, a hubbing mode interconnection model is highly preferable. In this case indeed you don't need any more to establish bilateral lines with all the networks with which you want to interwork, you have only to connect yourself to the roaming hub.

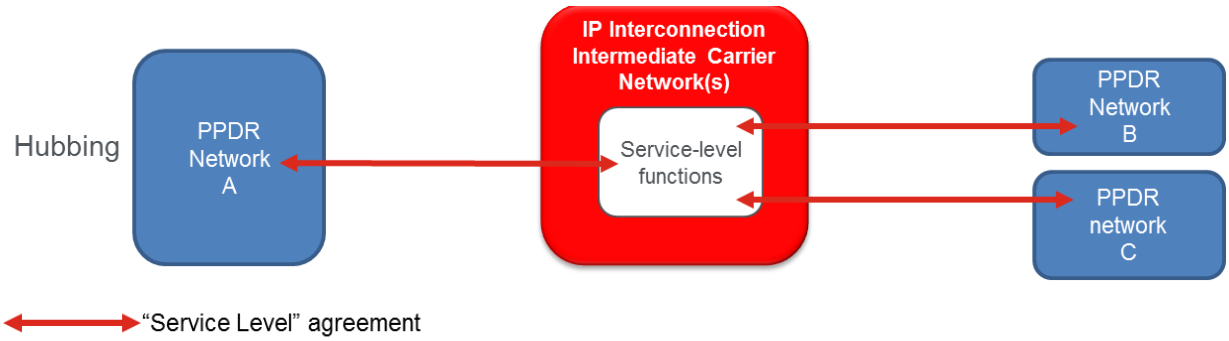

Figure 2: Indirect IP interconnection hubbing mode

Since the end of the first decade of the twenty first century, GSM/2G/3G/LTE operators are looking to such an interconnection solution, like dedicated IPX intranet networks, to save costs and resources (see D24.4, § 4.2).

Existing Bilateral Agreements can be retained while roaming service coverage is extended to new areas via Hubs.

Legacy TDM networks (GSM/2G/3G) use Signalling System #7 (SS7), whilst LTE uses SIP and Diameter signalling. IPX LTE/3G roaming hubs allow interconnection between the two signalling types.

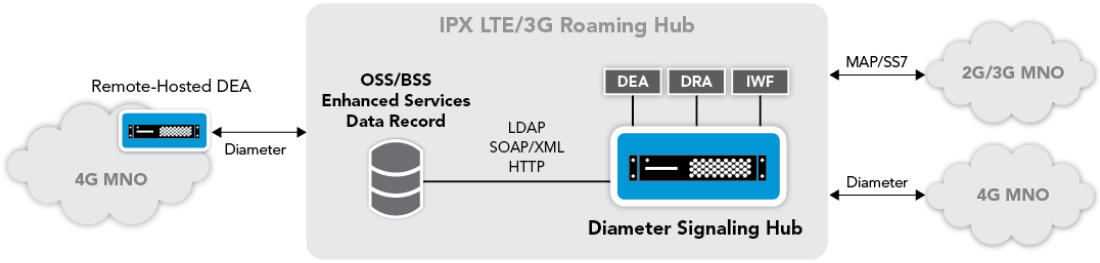

Figure 3: 3G, 4G roaming services

As we see, the cellular commercial networks offer connectivity options on transport/network layer. These options are however not transposable to transport the ISI protocol (application layer), since the TETRA ISI is a point-to-point application.

When it comes to interconnection of group calls of several networks, adding the more complex structures of TETRA group linking / combining / priorities / emergency etc., the issue gets much more complicated: we should create a kind of dynamic (i.e. at need) multiparty group routing that does not exist today. Transparent extension of home groups over ISI to visited network (group migration) already turned out too complex (operationally and technically) in TCCA to get it to work in reality.

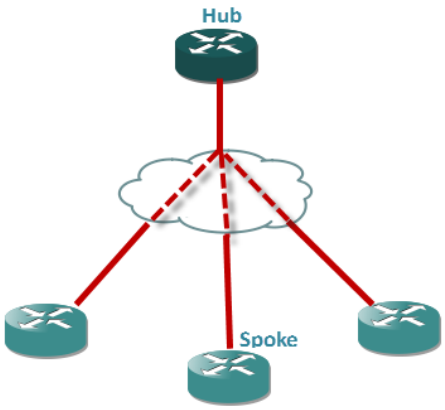

Figure 4: Hub and spoke Topology

If we keep the current TETRA group linking model, which is highly satisfying except when you need a group migration[3], we could establish a central neutral TETRA network, without any subscriber and TBS, that would be exclusively used as roaming hub. This hub network would contain the controlling group of all the international talkgroups defined from the considered spoke networks. The “hub manager”, mandated and trusted by the network owners/operators, would create a controlling talkgroup and, following a predefined agreed international fleetmap, the concerned countries would link a participating talkgroup to the hub controlling group. To realise this, new developments should be yet necessary

[3] Group migration is only relevant when you cross the border without having to cooperate with other agencies or forces from the visited country.

seeing a participating SwMI has less control over some functionalities

Moreover, adopting such a star ISITEP network should require a new solution for the visitors' authentication. The simplest way to proceed seems to extend the TETRA hub functionalities for routing authentication information, the authentication being still ensured by the visitor home network. Eventually, the international visitor database of each spoke network should take into account the ITSI from the other spoke networks, defining their profiles.

Especially if there is a European drive for implementing TETRA ISI at EU level, ETSI/TCCE should be able to extend the ISI standard in this direction.

Developing a TETRA roaming hub while some countries, like Norway, Sweden Finland, are already bilaterally interconnected would offer them the advantage to extend rapidly their roaming capabilities by establishing one connection to the hub. It must then be decided if the existing bilateral ISI is maintained or if the link migrates to the hub connection.

The solution outlined supra, which could be named the "ISITEP 2.0" solution, could be a fully grounded intermediate one, waiting for the broadband solution described in D24.3, §4.3.

As a matter of fact, there is currently an arising consensus among the PPDR community to gradually and surely migrate from TETRA/TETRAPOL networks to broadband and interoperable LTE Critical Communication Systems (CCS). Even with broadband CCS, the operational issues of security/ authentication/rights, sharing of talk groups and procedures for cross-border operations must be solved.

However, it can be observed in the same time that most of the European countries are massively investing in their TETRA or TETRAPOL national network, implementing it (e.g. Italy), having just implemented it (e.g. Norway, Germany), totally renewing it from inside (e.g. France, Spain, Belgium, Denmark) or even swapping it (the Netherland). All these countries will probably not abandon their legacy networks before their live cycle (~15 years). This tends to proof that, if we except Great Britain that decided to migrate from TETRA to (pre-)Mission Critical LTE in a period of 27 months (Oct 2017 – Dec 2019), the migration to mature Mission Critical LTE, enabling inter Critical Communication Application (CCA) interfaces (8) (see D24.3, page 35), will be progressive, and justifies meanwhile to invest in TETRA roaming hub(s).