ISITEP

D2.2.1 - DRAFT SECURITY REQUIREMENTS

Document Manager:	Ramon Ferrús	UPC	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	Selex ES
SP Leader:	BFP

Document ID N°:	ISITEP_D2.2.1_20150225_V1.1	**Version:**	V1.1
Deliverable:	D2.2.1	**Date:**	25/02/2015
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Ramon Ferrús (UPC)
Approved by (WP Leader):	Ramon Ferrús (UPC)
Approved by (SP Leader):	Etienne Lezaack (BFP)
Approved by (Coordinator)	Claudio Becchetti (SES)
Security Approval (Advisory Board Coordinator)	Etienne Lezaack (BFP) in January 2015

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico.Frosali, Claudia.Olivieri, Andrea Campodonico	SES	Contributor
Etienne Lezaack	BFP	Contributor
Marianne Storrosten, Michel Duits	DNK	Contributor
Anita Galin, Anna Falkdrugge, Peter.Hedman, Robert Danelius, David Arnljots	MSB	Contributor
Jaakko Saijonmaa, Risto Toikkanen	CAS FI	Contributor
Daniele Biondini, Luciana Favia, Ivano Luciani, Giuseppe Pierri, Franco Pangallo, Mario Manzi	ISCOM	Contributor
Cor Verkoelen, Frank Fransen	TNO	Contributor
Ramon Ferrús, Oriol Sallent	UPC	Contributor/Editorial responsibility

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
Federico.Frosali, Claudia.Olivieri, Andrea Campodonico	SES	WP2.2 participant
Etienne Lezaack, Simon Verdegem, Yves Cawet, Marc Vandenbroeck, Marie Carlsson	BFP	WP2.2 participant
Marianne Storrosten, Michel Duits	DNK	WP2.2 participant
Anita Galin, Anna Falkdrugge, Peter.Hedman, Robert Danelius, David Arnljots	MSB	WP2.2 participant

Ronald Van.Der Wal, Herman Van Sprakelaar, Hans Borgonjen	V & J	WP2.2 participant
Jaakko Saijonmaa, Risto Toikkanen	CAS FI	WP2.2 participant
Serge Delmas, Jean-Pierre Quemard, Herve Mokrani, Eric Lorfeuvre, Dominique Eustache	CAS FR	WP2.2 participant
Daniele Biondini, Luciana Favia, Ivano Luciani, Giuseppe Pierri, Franco Pangallo, Mario Manzi	ISCOM	WP2.2 participant
Theodore Tzamos, Michael Spyridakis, Haritou, Dimitris Androutsopoulos	NETTECHN	WP2.2 participant
Cor Verkoelen, Frank Fransen, Bram Verheesen, Marcel Vanderlee	TNO	WP2.2 participant
Ramon Ferrús, Oriol Sallent	UPC	WP2.2 participant/Leader
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	02/10/13	All	All	Initial version
V0.2	28/10/13	All	All	Contributions from partners integrated. Version available for discussion at ISITEP kick-off meeting
V0.3	11/11/13	All	All	First completed draft version. For discussion and review at 12/11/13 PhC.
V0.4	12/11/13	All	All	Reviewed version from 12/11/13 PhC
V1.0	14/11/13	All	All	Contributions from partners integrated. Version delivered to SP2 leader.
V1.1.	25/02/2015	All	All	Added Security Approval field at pag. 1, “General Public” in the distribution list

Publishable extended abstract

Communications security is a central aspect of the ISITEP framework for inter-system interoperability between TETRA and TETRAPOL networks. Ensuring that threats to the interconnected communications systems and terminals are sufficiently and appropriately reduced by technical, procedural and environmental countermeasures is vital to realise the trusted and secure communication system needed for the pursued PPDR transnational cooperation activities.

In this context, ISITEP Work Package 2.2 (WP2.2) "Security Requirements" is aimed at establishing the set of security requirements needed to drive the development of the security architecture and its components. This first deliverable from WP2.2 provides a description of the preliminary framework and methodology defined to carry out the development of the security requirements. The framework includes aspects such as the identification of the ISITEP system components and players that are relevant for the security analysis, and the definition of security objectives.

On this basis, the document also conducts a first assessment to delineate the state-of-the-art of the security features existing in current PPDR technologies and networks, security procedures carried out by PPDR end-users and operators in order to realise the trusted and secure communication system needed in national PPDR networks, and to provide an overview of the regulatory and legislation framework that impacts affects PPDR communication networks. Finally, a preliminary assessment of security threats to ISITEP system is also reported. The assessment is focused on those security threats that are relevant to the new communications capabilities brought by the ISITEP solution in terms of service interworking across multiple national networks and terminal roaming.

CONTENTS

1 INTRODUCTION

Communications security is a central aspect of the ISITEP framework for inter-system interoperability between TETRA and TETRAPOL networks. Ensuring that threats to the interconnected communications systems and terminals are sufficiently and appropriately reduced by technical, procedural and environmental countermeasures is vital to realise the trusted and secure communication system needed for the pursued PPDR transnational cooperation activities. The security architecture of a particular system is often unique and there are threats and security requirements that can be very specific to that system.

In this context, ISITEP Work Package 2.2 (WP2.2) "Security Requirements" is aimed at establishing the set of security requirements needed to drive the development of the security architecture and its components. The resulting security solution must ensure that ISITEP cross border interoperability communications systems will have the required safeguards regarding communications security. Specific objectives of WP2.2 activities include:

- Assessment of existing security measures in national public safety PMR solutions
- Risk and vulnerability analysis
- Security requirement definition of the participating nations/operators

To that end, WP2.2 is split into 3 separate tasks:

- Task 2.2.1 - Security assessment of current PPDR European cooperation (M01 - M06), which focuses on:
    - Assessment on security for communication procedures
    - Assessment of security on current PPDR network
    - Survey of past current and future thread on PPDR network
    - Evaluation of Legislation on national security communication
    - Security procedures survey for national PPDR networks
- Task 2.2.2 - Security risk and vulnerability analysis (M01 - M06), which focuses on:
    - Analysis of breaches on visiting users authentication
    - Assessment of threats on air interface due to roaming terminals
    - Assessment of threats at network interface among national infrastructures
    - Assessment of threats from within national infrastructure to other national infrastructures
    - Risk evaluation on PPDR operational procedures
    - Definition of security gaps addressed by the assessment
    - Assessment of potential security & privacy concerns from a citizens view point
- Task 2.2.3 - Security requirement definition (M03 - M30), which focuses on:
    - Definition of minimal mandatory requirements to interconnect a new PPDR national network to other national networks
    - Suggested modifications or improvements on current legislation
    - Definition of minimal essential requirements on operational PPDR procedures
    - Security requirements for the usage of encryption in cross border operations

Work conducted in the above tasks is to be reported through the following deliverables:

- D2.2.1 "Draft security requirements" (M02)

- D2.2.2 “Candidate security requirements” (M12)
- D2.2.3 “Final security requirements” (M30)

Outcomes from WP2.2 will be used to define the secure network solution to national security infrastructure at PPDR national network (WP2.4, WP4.6), to define procedures for new national network interconnections (WP3.4) and for roaming activation (WP3.5), to guide the security at network interface and gateway level (WP 4.6) and at terminal level (WP 5.3).

2 DOCUMENT SCOPE

This deliverable (D2.2.1) is the first deliverable issued by WP2.2.

It reports on the advances in Tasks 2.2.1 and 2.2.2 until M02. In particular, the following points are covered:

- Section 4: Description of a preliminary framework and methodology to carry out the development of the security requirements. The framework includes aspects such as the identification of the ISITEP system components and players that are relevant for the security analysis, and the definition of security objectives.
- Section 5: First contribution to the security assessment of current PPDR European cooperation.
- Section 6: First contribution to the security risk and vulnerability analysis.

3 DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

This section is intended to capture the definitions of some key terms used in the document for the purpose of increased consistency. Most of the definitions are obtained from official 3GPP and ETSI documents:

Access control: the prevention of unauthorized use of resources, including the use of a resource in an unauthorized manner.

Authentication: the act of positively verifying that the true identity of an entity (network, user) is the same as the claimed identity.

Confidentiality: the property that information may not be available or disclosed to unauthorized individuals, entities or processes.

Data integrity: the property that data has not been altered or destroyed in an unauthorized manner.

Encryption: the conversion of plaintext to ciphertext.

Key: a sequence of symbols that controls the operations of encipherment and decipherment.

Key management: the generation, selection, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

Migration: act of changing to a location area in another network (either with different Mobile Network Code and/or Mobile Country Code) where the user does not have subscription (e.g. ITSI in TETRA) for that network. In this document, migration is used as a synonym of roaming.

Plaintext: information (including data) which is intelligible to all entities.

Profile: the capability of a particular equipment. This is defined separately for individual subscriber terminals and individual infrastructures.

Provision: the act of supplying a given service (Note: A communication system may be capable of supporting a service. However, it may not supply the service to certain subscriber terminals for which the service is not subscribed.)

Repudiation: denial by one of the entities involved in a communication of having participated in all or part of a communication.

Roaming: utilization of a mobile terminal in a network other than the one where the mobile is subscribed but on which the mobile can still be located and operated by agreement between the respective network operators.

Security domain: a set of entities and parties that are subject to a single security policy and a single security administration. The network security design can consider different domains and sub-domains to surround and delimit the responsibilities in network management and security control.

Security service: a service provided by a layer of communicating open systems which ensures adequate security of the systems or of data transfers.

Security threat: A security threat is defined as a potential violation of security. Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

3.2 Abbreviations

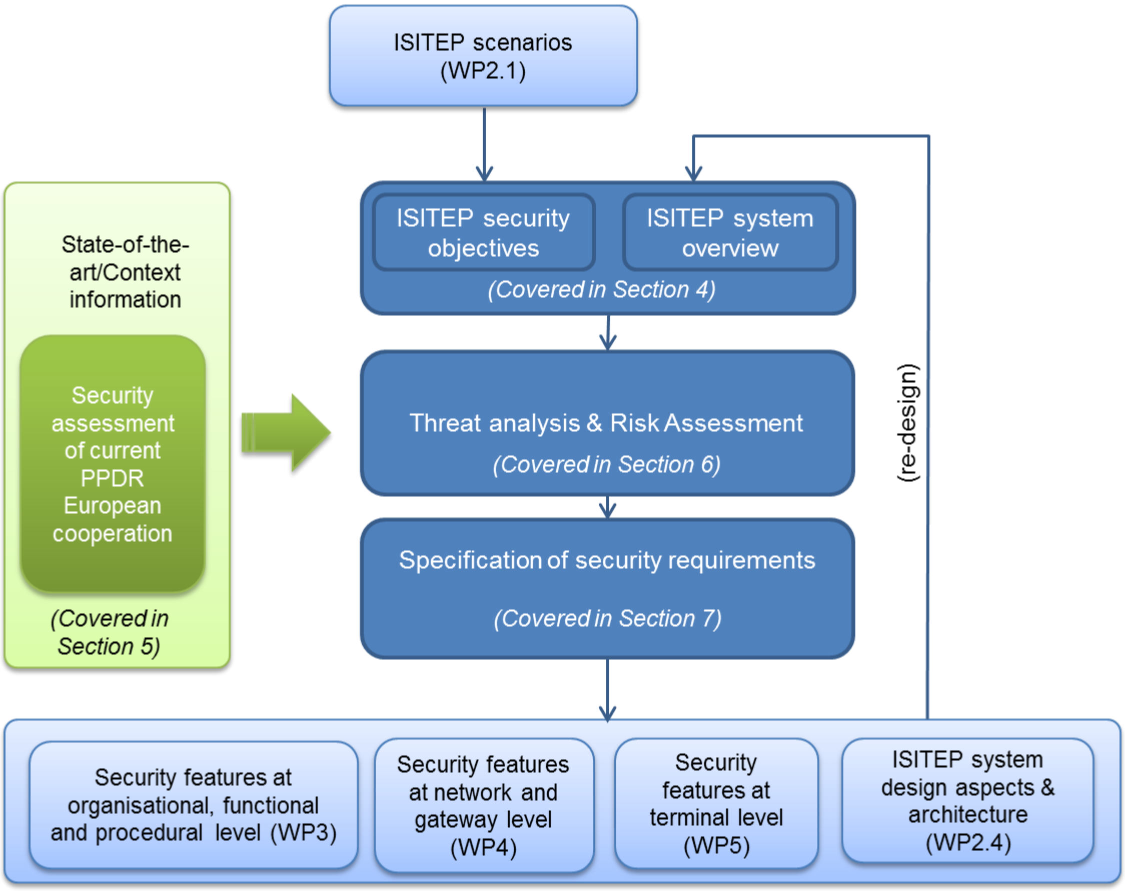
For the purposes of the present document, the following abbreviations apply:

Acronym	Definition
3GPP	3rd Generation Partnership Project
AI	Air Interface
AIE	Air Interface Encryption
AuC	Authentication Center
CCK	Common Cipher Key
DCK	Derived Cipher Key
E2EE	End to End Encryption
ESI	Encrypted Short Identity
GTSI	Group TETRA Subscriber Identity
IOP	Interoperability Profile
IP	Internet Protocol
ISI	Inter System Interface
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
KMC	Key Management Center
KSS	Key Stream Segment
MoU	Memorandum of Understanding
MNI	Mobile Network Identity
MS	Mobile Station
MT	Mobile Terminal
NGN	Next Generation Network
OTAR	Over The Air Rekeying
PC	Professional Computer
PDA	Personal Digital Assistant
PEI	Peripheral Equipment Interface
PMR	Professional/Private Mobile Radio
PPDR	Public Protection and Disaster Relief
PS	Public Safety
PSTN	Public Switched Telecommunications Network
RS	Random Seed
SCK	Static Cipher Key
SDS	Short Data Service
SFPG	Security and Fraud Prevention Group
SIM	Subscriber Identity Module
SwMI	Switching and Management Infrastructure
TAA1	TETRA Authentication and key management Algorithm suite 1
TE	Terminal Equipment
TEAx	TETRA Encryption Algorithm number x
TEDS	TETRA Enhanced Data Services
TEI	Terminal Equipment Identity
TETRA	TErrestrial Trunked RAdio
VoIP	Voice over IP
VPN	Virtual Private Network
WS	Work station

4 SECURITY REQUIREMENTS DEVELOPMENT FRAMEWORK

4.1 Methodology

Different methodologies can be defined for the development of security requirements. One possible methodology is illustrated in Figure 1. This methodology is in line with the main guidelines provided in ETSI Technical Report ETR 332 [1] for security requirements capture.



ISITEP scenarios (WP2.1)

ISITEP security objectives

ISITEP system overview

(Covered in Section 4)

State-of-the-art/Context information

Security assessment of current PPDR European cooperation

(Covered in Section 5)

Threat analysis & Risk Assessment

(Covered in Section 6)

Specification of security requirements

(Covered in Section 7)

(re-design)

Security features at organisational, functional and procedural level (WP3)

Security features at network and gateway level (WP4)

Security features at terminal level (WP5)

ISITEP system design aspects & architecture (WP2.4)

Figure 1. Methodology for security requirements development

As shown in Figure 1, the ISITEP scenarios being developed in WP2.1 are main inputs to the overall security requirements development process. Based on these inputs, a list of basic ISITEP security objectives of general and generic nature is first to be defined. Security objectives represent a high level statement on the aims of the succeeding security investigations. They should give clear guidance and orientation to the following stages of the security requirements development process. Security objectives should consider generic threats and security requirements and obey to internal/external security policies and their priorities, legal issues and data protection requirements. Often the definition of security objectives can be simplified when the system's nature is identified to be similar to another system for which such a definition already exists.

Along with the definition of the objectives, it is also necessary to produce a comprehensive and complete characterisation of the system, its properties, boundaries and relationships to the external world in a way that potential security vulnerabilities become noticeable. This process, referred here to as “system overview”, should provide an abstract model of the ISITEP solution by describing at least the system’s components (e.g., network elements, security management functions, objects to be protected) and the participating entities or subjects that can either be responsible of or affected by potential security breaches (e.g., network operator, end-user, intruder). The model should rather be comprehensive than too much detailed.

Along with the formulation of the objectives and system overview, conducting a security assessment of current PPDR European cooperation is also a cornerstone of the proposed methodology. This assessment is necessary to clearly delineate the state-of-the-art of the security solutions on current PPDR networks, existing security procedures, legislation framework as well as surveying past current and future threads on today PPDR networks. In this respect, ISITEP project can leverage and make extensive use of the collected experiences by the key end-users and manufacturers in the European PPDR sector that form part of the project’s consortium. This state-of-the-art is also to be complemented with the analysis of security requirements specifications of related and similar systems. This helps to simplify the process because security work on systems that have a similar nature may partly or fully be adopted. This state-of-the-art analysis is a valuable input to all the stages of the security requirements development process.

Threat analysis is the next step after the formulation of the objectives and system review. A security threat is defined as a potential violation of security. A pragmatic approach is to define threats with the help of general threat categories which are already known from other investigations and against those already well defined security features exist. A list should be generated from the information gathered during the system's review about all those functions and services of the system that can be accessed by any subjects such as inside (regular) users or operators and outside hackers or intruders. Threats resulting from external requirements (e.g., legal requirements on data protection, regulations for legal interception, national or international trade regulations, and quality requirements) should also be considered. External requirements of a very general nature might have been already defined in the security objectives phase. In this respect, ETSI Technical Report ETR 332 [1] provides some guidelines to the identification of threats related to data protection, inter-network communication, system integrity and due to security policies.

The "threat analysis" phase should come out with a list of system specific threats that have to be categorized to prepare the following "risk assessment". The intention of "risk assessment" is to have some kind of a priority list, which threats are to be considered more severe, more important or more costly than others. Main goals of the risk assessment are the evaluation and comparison of threats; risk assignment to threats; and, identification of major risks.

Finally, based on the threat analysis and risks assessment, security requirements can be postulated. A security requirement could be something that helps to satisfy security objectives in the presence of threats. The number of different kinds of security requirements should be kept to a minimum. However, they should be given attributes that allow a detailed specification.

The security requirements derived through this process will feed the development of the security features in the ISITEP system. Security features should be understood as what needs to be provided in order to meet security requirements, e.g. security mechanisms, security management techniques, etc. Particularly, security requirements will drive the development and specification of security features at organisational, functional and procedural level in WP3, at network and gateway level in WP4 and at terminal level in WP5.

Of note is that the overall process for security requirements development is not strictly linear so that feedback coming from the other WPs, especially WP3, 4 and 5, can trigger a revision and refinement of the security requirements. In this regard, a first stable version of the security requirements is planned to be finalised by M12 (reported in D2.2.2 “Candidate security requirements”) and further revisions will be accounted for in the last deliverable to be produced by this WP by M30 (D2.2.3 “Final security requirements”).

The mapping between the processes identified in this methodology and the sections of this deliverable where they are addressed is also indicated in Figure 1 with text in italics.

4.2 General security objectives

Considering that the nature of the ISITEP is that of a telecommunication system where terminals are connected through a radio link and a number of networks may be interconnected to provide roaming and communication services across networks, a set of generic objectives can be derived from the analysis of the security objectives formulated for systems such as TETRA [2][3][4] and 3GPP networks [5][6]. A preliminary set of generic objectives is provided in the following:

- *Verification of identities*: ISITEP interconnected networks should provide capabilities to establish and verify the claimed identity of any actor in the system. This may include users, terminals and networks.

- *Controlled access to resources*: the system should ensure that unauthorized actors are prevented from gaining access to information or resources of the network or devices.

- *Protection of confidentiality and integrity*: the system should provide capabilities to ensure the confidentiality and integrity of stored and communicated data.

- *Availability*: to ensure the availability of the provided services and of related management functions.

- *Accountability*: the system should ensure that an entity cannot deny the responsibility for any of its performed actions. In this context, accountability is used as a synonym of non-repudiation.

- *Compliance to regulatory framework*: the system should be able to guarantee the compliance to the regulations active in the area, where the system operates (e.g. conformity to national security requirements and export controls).

- *Protection of privacy*: to ensure the rights of privacy of the system's users (i.e. PPDR officers, first responders) as well as citizen’s data protected by privacy legislations.

- *Monitoring*: To have the ability to monitor the traffic and the communication in the network. Monitoring is partly in opposition to other security requirements, particularly confidentiality and privacy.

- *Security control of the system management*: the complex security functions within the network call for sophisticated control and management. The management functions are security critical themselves and, therefore, subject to security requirements.

- *Protection of system integrity*: protection of system resources comprises a very large set of requirements, mainly connected to the field of system reliability rather than security.

- *Interoperability*: to ensure that a minimal set of security features are adequately standardised and used by all interconnected networks to ensure proper interoperability and roaming between different serving networks.

- *Backward compatibility:* compatibility of the new required security features with legacy ones in TETRA and TETRAPOL networks and terminals.

4.3 System overview

This section describes the system's components and the participating entities or subjects that are relevant for the definition of the security requirements.

4.3.1 System's components

A schematic of ISITEP system's components is provided in Figure 2.

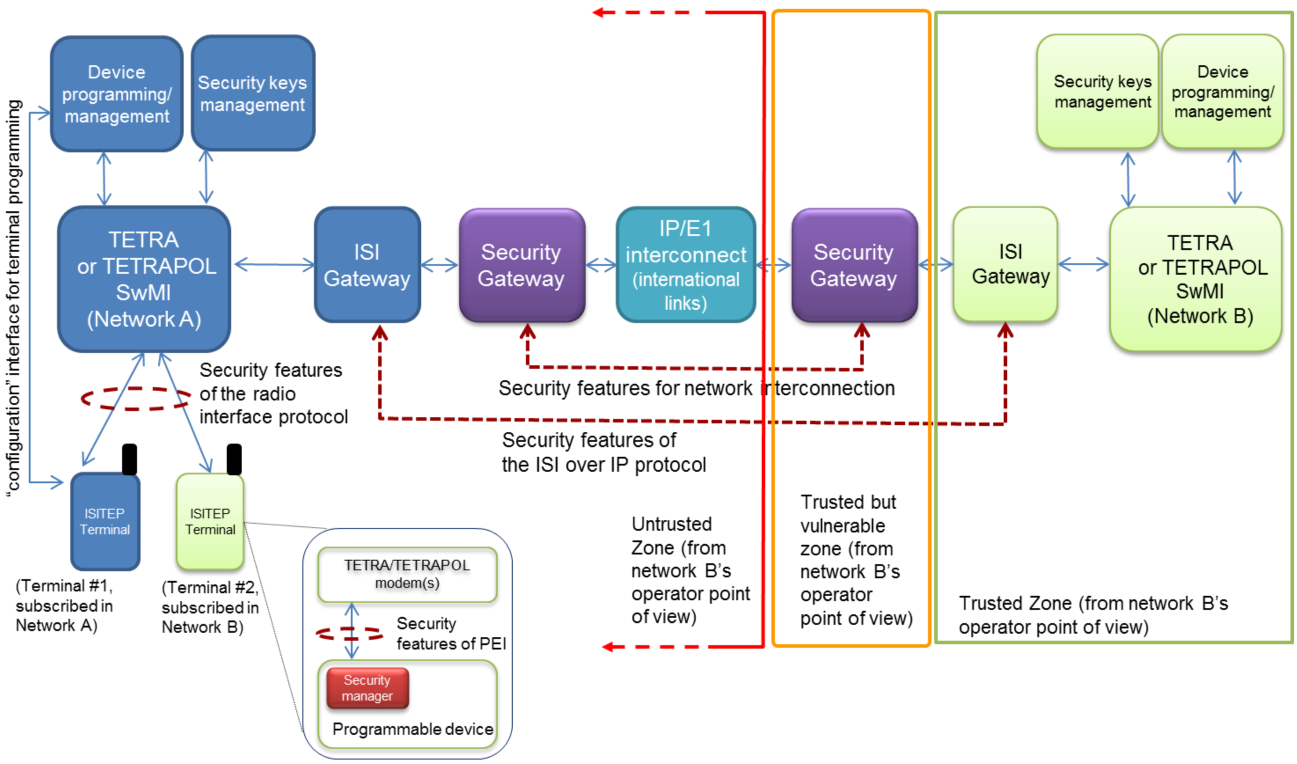

Device programming/ management
Security keys management
TETRA or TETRAPOL SwMI (Network A)
ISI Gateway
Security Gateway
IP/E1 interconnect (international links)
Security Gateway
ISI Gateway
TETRA or TETRAPOL SwMI (Network B)
Security keys management
Device programming/ management
"configuration" interface for terminal programming
Security features of the radio interface protocol
Security features for network interconnection
Security features of the ISI over IP protocol
ISITEP Terminal
ISITEP Terminal
(Terminal #1, subscribed in Network A)
(Terminal #2, subscribed in Network B)
TETRA/TETRAPOL modem(s)
Security features of PEI
Security manager
Programmable device
Untrusted Zone (from network B's operator point of view)
Trusted but vulnerable zone (from network B's operator point of view)
Trusted Zone (from network B's operator point of view)

Figure 2. ISITEP system overview for the development of security requirements

ISITEP system proposes the interconnection of a number of TETRA/TETRAPOL networks by means of Inter System Interface (ISI) gateways (different gateways are to be developed to cover the use of TETRA and TETRAPOL technologies as well as the use of legacy ISI E1 [7] by some networks) and interconnected through international links. A general preliminary assumption is that the interconnected end-points (i.e. TETRA/TETRAPOL networks) are trusted but that the linking network is itself untrusted (when interconnected systems run over trusted networks, for example a trusted network owned by a PS operator that is physically protected, there is little need for additional protection. However, enhanced protection is usually a mandatory requirement if interactions with third-party networks and cross PPDR operator boundaries are requested). Therefore, three separate security zones can be distinguished from a given operator point of view and depending on the operational control of the network operator, the location of the specific network element and their connectivity to other network elements. These tree zones are: a Trusted Zone, where network operator or service provider's elements and systems reside; a Trusted But Vulnerable Zone, where network elements are operated by the network operator or service provider; but are not necessarily fully controlled by that network operator or service provider or might communicate with Un-trusted Zone elements; and the Un-trusted Zone, which is the zone which includes the network elements belonging to other network operators, service provider or end customers. This trust model is consistent with the one proposed by i3 Forum [8] for carriers and service providers involved in international Voice over IP (VoIP) interconnections.

As shown in Figure 2, all the equipment that form part of the TETRA/TETRAPOL switching and management infrastructure (base stations, switching nodes, network management elements, etc.) will be located in the Trusted Zone of a given operator. These elements and systems never communicate directly with external domains such as the networks of interconnected partners. As to the placement of the ISI Gateway, a preliminary assumption is that it will also reside in the Trusted Zone of each operator. It’s worth noting that it should not be assumed that because an element is in the Trusted Zone it is secure: Trusted Zone elements should be also be protected by a combination of various methods. For example elements may be protected by physical security, system hardening, use of authenticated and encrypted signalling or a separated logical network for communication within the Trusted Zone and with network elements in the Trusted But Vulnerable Zone.

In ISITEP it is proposed to develop a Security Gateway to provide enhanced protection to traffic and signalling information running on the interfaces that cross PPDR network operator boundaries. The security gateway will be located at Trusted But Vulnerable Zone. The main role of this element is to protect the elements in the Trusted Zone from the security attacks originated in the Un-trusted Zone. In particular, ISITEP security framework grounded on security gateways shall solve two main issues: provide confidentiality and integrity of traffic exchanged among networks; and, prevention of intrusions into the national networks. Hence, essential requirements are needed to interconnect national networks within the interoperability cloud and from them adopt the proper security features for network interconnection. In the context of VoIP interconnections, the elements equivalents to the Security Gateway are referred to as Network Border Elements or Border Function elements [8]. In case of ISI E1 connected networks the Security Gateway may take the form a line encryption device.

ISITEP system will allow for the roaming of terminals across networks. Therefore, as an example, terminal #2 whose home network is Network B in Figure 2, will be able to get access to communication services through Network A, which will be serve as a visited network. This might demand the utilisation and/or development of new security features in the radio interface as well as in the ISI over IP protocol to be developed between the networks. The security, the privacy and the integrity of the existing systems will be maintained while sharing the needed data for interoperability.

Roaming terminals shall interoperate securely using Over the Air TETRA encryption algorithms, which are a standard for European public safety (i.e. TEA 2) and TETRAPOL security. In TETRA, security is mainly provided through Air Interface Encryption (AIE) or through End to End encryption (E2EE). The first mechanism is interoperable across Europe while E2EE does not allow complete interoperability cross countries. Since E2EE is often classified or national specific such theme can hardly be faced in a FP7 project. ISITEP will possibly use E2EE without entering into classified aspects of encryption. On the other hand, according to end users AIE is suitable for all joint operations apart from Special Forces, which require extra security measures such as E2EE. TETRAPOL has a similar national specific approach but there is no way to manage security configuration from outside the TETRAPOL terminal for security reasons.

ISITEP terminals are expected to rely on a terminal control interface (e.g. PEI for TETRA and PEI-equivalent for TETRAPOL) in order to interconnect the TETRA/TETRAPOL communication modem(s) with the programmable device that host the applications. As such, security features may also be required to protect such a control interface. ISITEP terminals will also embed a Security Manager to configure existing security parameters according to counterparts and the associated security capability. This Security Manager software will facilitate a secure roaming functionality, allowing terminal configuration with respect to the specific end-to-end encryption mechanism, which is network specific. The Security Manager shall also adapt the authentication mechanisms implemented in TETRA networks, allowing interoperability. For TETRAPOL networks a limited control on these functionalities is allowed.

Additional elements of the TETRA/TETRAPOL systems that are relevant for the security analysis are the elements used to manage the network security keys and the elements used to configure/program terminals.

4.3.2 System's players

ISITEP players are those already present in PPDR TETRA and TETRAPOL systems, plus the ones resulting from the specifics of cross-border, multinational PPDR operations and the use of international connectivity services across nation PPDR networks. A draft, preliminary list of the players and roles to be considered in the drafting of security requirements are given in the following:

- **Network operator**: the person or company that runs the TETRA/TETRAPOL network and who has people or organisations as customers.
- **Organization manager**: the person who runs the organization of his users within his organization. The organization manager can be the same as the network operator in the case of a PMR.
- **Operational dispatcher**: the person who manages the groups and users. There can be different levels within the operational dispatchers like a supervisor who manages several dispatchers.
- **Subscriber**: this is the organization or person identified in the PPDR network by his subscription. Billing if applied will relate to the subscriber.
- **User**: the user is the person who belongs to the organization and who uses a mobile or line connected terminal for his calls or data transfers. The user can be the same as the subscriber. The user identity will be defined in the future TETRA standard.
- **Mobile owner**: a mobile can be used by different users within the organization or belonging to different organizations. The terminal can belong to a different person from the user or subscriber. The terminal owner can be the same as the user or subscriber.
- **Manufacturer**: this is the mobile manufacturer or the infrastructure manufacturer.
- **Maintenance personnel**: these are the personnel which maintain either the mobiles or the infrastructure.
- **Home network operator**: the role that has overall responsibility for the provision of a service or set of services to users associated with a subscription because of the association with a subscriber.
- **Serving network operator** (or visited network operator): the role that provides radio resources, mobility management and fixed capabilities to switch, route and handle the services offered to the users. Serving network capabilities are provided on behalf of home environments, with which the serving network has an appropriate agreement, for the benefit of the users associated with those home environments.
- **Transport or transit services carrier**: an intermediate entity that provides interconnection in different levels (Service, Transport).

In addition, off-line players to consider are:

- **Regulators:** the role of anybody which is authorised to set laws or guidelines governing the provision or use of communication services, or terminal or networking equipment. Examples of regulators are national governments and their agencies, including law enforcement agencies, national security agencies, export control authorities, etc. The security features and mechanisms must be such that they do not inhibit the legitimate activities of such organisations.

Finally, to refer to persons or systems that do not belong to previous categories and that intentionally or accidentally might compromise system's security, the following actor is considered:

- **Intruders:** the role of a party who attempts to breach the confidentiality, integrity or availability of the communication services, or who otherwise attempts to abuse the system in order to compromise services or defraud users, home environments, serving networks or any other party.

An intruder may, for example, attempt to eavesdrop on user traffic, signalling data and/or control data, or attempt to masquerade as a legitimate party in the use, provision or management of communication services.

5 SECURITY ASSESSMENT OF CURRENT PPDR EUROPEAN COOPERATION

This section reports on the initial outcomes of Task 2.2.1 “Security assessment of current PPDR European cooperation”.

5.1 Regulatory and legal framework on national security communication

Operators of PMR networks, and manufacturers of PMR equipment, have to ensure compliance with the legislative framework of the region in which they operate.

In Sweden, the Swedish Government has decided that the Swedish Civil Contingencies Agency (“MSB”) shall build, maintain and develop a telecommunications system for co-operation, commanding and control within the area of public protection and disaster relief. The task is given MSB in the form of a governmental regulation, i.e by law, dated in 2003. In order to fulfill its obligation, MSB has from 2005 until 2010 built and deployed a nationwide TETRA based system called “Rakel”. To a large extent, MSB has used, and currently uses, subcontractors for the construction, operation and development of Rakel. Rakel services are provided to municipalities, counties, national agencies and even commercial entities, emergency services and others in the fields of civil protection, public safety and security, emergency medical services and healthcare. The Rakel services have replaced the majority of old time analogue systems; however some are still in use. Thus, MSB has, by law, the overall responsibility to expand, develop and support the Rakel system. The following regulations impact on the national security communication services provided by Rakel system:

Rakel’s communications services. Rakel is a telecommunications network and the 2003 Swedish Electronic Communications Act is applicable to the provision of Rakel services. However, since Rakel is not a publicly available telecommunications network, many of the provisions in the Act are not applicable to Rakel.

Spectrum. The Swedish telecommunications regulator (the Swedish Post and Telecom Authority) has by a number of decisions given MSB the right to use certain frequencies for the provision of Rakel services. The frequencies are 380-385 and 390-395 MHz and are exclusively allocated to MSB and Rakel. The right to use such spectrum is combined with a very important limitation. MSB received the license to use the spectrum without charge and without having to participate in any auction or “beauty” contest. Therefore MSB may only provide Rakel services to entities providing services for public order, public security or health care activities. The user group for Rakel is thus limited. The limitation is given by the 2003 Swedish Electronic Communications Regulation 20a §, i.e. by law.

Ciphering. ETSI has defined a number of TETRA Encryption Algorithms and the TETRA Encryption Algorithm 2 (“TEA2”) is restricted to the use by European Union Public Safety organizations and PPDR networks. MSB is granted a right to use TEA2 by ETSI and MSB has implemented TEA2 as the encryption of the air-interface in Rakel. Thus, TEA2 must be installed in all devices for use within Rakel and the end-user must have a TEA2 license from MSB before they can become a user in the Rakel system and before they can purchase TEA2 equipped devices from hardware suppliers. Therefore, an entity wishing to become a Rakel user, must apply to MSB for a ”Rakel license”, i.e. a right to use the TEA2 cipher in Sweden. As described above, MSB may only provide Rakel services to entities providing services for public order, public security or health care activities. In case the applicant belongs to the allowed user group, MSB will grant a Rakel license to the applicant. They may then start the work to define how they will communicate within the network and what equipment to use.

Swedish Confidentiality obligation. The information which the users transmit through Rakel is normally information that shall be kept confidential under the Swedish Public Access to Information and Secrecy Act. Rakel provides a secure way of communication and therefore the users’ need for secrecy is fulfilled. However, it is each user’s obligation to maintain its own secrecy according to law.

Swedish Integrity obligations. Since personal data of subscribers and others will be handled by MSB the Swedish Data Protection Act will also impose obligations on MSB. Such obligations are general and similar throughout the EU, and it is not necessary to expand on them here. Personal data may be transferred within the EU without any particular consent, provided that such personal data is not of a sensitive nature.

In Norway, the delivery of the national PPDR network is under the supervision of the Directorate for Emergency Communication (established 01.04.2007). The assignment is to develop, build and maintain the nationwide TETRA Network called Nødnett. In addition DNK is responsible for procurement of the radio terminals and control rooms to be used by PPDR organisations within Nødnett. The nationwide rollout, including the ISI with Rakel and deployment of TEDS, is scheduled to be completed in 2015.

Nødnett services are provided to PPDR organisations and other organisations (including voluntary organisations) in the field of civil service and protection. The Nødnett network will replace all existing analogue networks currently in use by the aforementioned user groups.

The Norwegian Post & Telecommunications Authority has assigned the 380/385-390/395 MHz frequency band to Nødnett and a spectrum for microwave (23Ghz). The condition is that these frequencies are to be used for the PPDR network to provide the Nødnett services for the allocated user groups in public safety, order, security and health services.

The assigned classification by the National Security Authority for the Nødnett network implies that all information on the infrastructure objects is classified under the security act. A security clearance on the individual person is needed to work with(in) Nødnett. This is including all affiliated organizations and companies, governmental or commercial. A security policy as in use applies to all physical locations, systems and applications where access is granted on assigned roles, user profiles or user and access rights. Security as applied on the Nødnett is to be divided in physical security (access control and object control), system security OSS (O&M services) and Provisioning and Crypto management (Authentication / ETSI TEA2). In the operational model for the Nødnett radio network, the Security as in Authentication and key management for the infrastructure and radio terminals is done by DNK. E2EE provisioning is done by the user agency using this additional security. The enable/disable functionality is available from the default OSS for user organisations. Security procedures are in place in case a radio is missing or stolen.

Concerning data privacy issues, the Norwegian Authority for Data handling (Datatilsynet) released regulations for handling of information regarding private persons. DNK can store the Charging Data Records (CDRs) produced by the network for a period of 6 months, or longer if made anonymous. In this case it means removing the data that can refer back to an ISSI and the actions performed in the network.

5.2 Security features on current PPDR technologies and networks

The technologies currently used in Europe to build PPDR networks infrastructure are TETRA and TETRAPOL, in the following sub paragraphs the security assets available in each technology are detailed.

5.2.1 TETRA technology security features

In order to provide verification of identities, protection of confidentiality and integrity and ensuring that users are protected against lost or stolen terminals, the TETRA standard provides the following security features:

- Authentication
- Air Interface Encryption (AIE)

- Enable and Disable
- End to End Encryption (E2EE)

5.2.1.1 Authentication

Authentication service allows the MS and the SwMI to prove each other's real identity, by proving to both parties the knowledge of a shared secret key (i.e. the authentication key K), unique for each MS and only available in the MS and in the authentication centre (AuC) of the home SwMI. The MS is considered, for the purposes of authentication, to represent the user as defined by the ITSI.

The authentication process describes a confirmed two pass challenge-response protocol in which the actors are the MS and the SwMI. Authentication relies on the verification that the MS and the AuC share the same authentication key K. The authentication key K is never exchanged between the MS and the AuC. Indeed, the authentication key K of the MS is never visible outside the AuC. Temporary encryption keys, called session authentication keys (KS), are actually used to prove the party identity. Session authentication keys are derived from the authentication key K and from a Random Seed (RS) internally by MS and AuC. Session authentication keys (KS) are delivered by the AuC to the authentication entity within the SwMI (e.g. a base station) that is in charge to carry out the authentication protocol on behalf of the AuC. The authentication entity in SwMI generates a random number as a challenge RAND1 and send it to the MS together with the RS. The session authentication key (KS) is never exchanged over the radio interface. After the reception of RAND1 and RS, the MS computes a response, RES1. In a similar way, the authentication entity in SwMI also computes the expected response, XRES1. The computation of both RES1 and XRES1 depends on the same inputs (session authentication key KS, that is obtained from K and RS in the MS, and RAND1) and algorithms. The authentication entity in SwMI on receipt of RES1 from the MS shall only compare it with XRES1 to decide on the authentication result.

TETRA specifies mechanisms for authentication of an MS, authentication of the infrastructure and mutual authentication.

5.2.1.2 Air Interface Encryption

Air interface encryption (AIE) service allows encrypting the 'air interface', signalling and voice, between an MS and the SwMI. There are two types of AIE: dynamic and static.

Static AIE is provided when the TETRA system is in security class 2 or in Fallback. A Static Ciphering Key (SCK) is used to encrypt signalling and voice on the air interface, the SCK is the same in the entire TETRA system all the MSs use the same SCK. Each MS shall be able to store at least 32 SCK for each MNI.

Dynamic AIE is provided when the TETRA system is in security class 3. Signalling and voice are encrypted using different encryption keys, from the authentication session key is derived one different ciphering key for each MS the derived ciphering key (DCK), DCK is used to cipher all the individual signalling and voice communications. Group communications can be ciphered using the Common Ciphering Key (CCK) or the Group Ciphering Key (GCK). A different CCK may be used in each location area of the system, all the MS located under the same location area share the same CCK, CCK shall be generated by the SwMI and it shall be distributed to the MSs. GCK is a ciphering key used to cipher group signaling and voice addressed to a specific Group TETRA Subscriber Identity (GTSI), GCK shall be known by the SwMI and it shall be distributed to the MSs.

5.2.1.3 Enable and Disable

Enable and Disable service provides a mechanism by which an MS can be denied or allowed access to a TETRA system, in ETSI EN 300 392-7 [4] are defined two levels of disables for an MS: 'temporary' or 'permanent'. A temporarily disabled MS will be barred from using the majority of TETRA system facilities. A permanently disabled MS is unable to access any TETRA system facility.

A temporarily disabled MS may be re-enabled by the TETRA system over the air interface. A permanently disabled MS cannot be re-enabled over the air interface.

Within the MS, the user subscription (ITSI), the equipment (TEI) or both may be disabled (and enabled as applicable) over the air interface.

For temporary disabling of the TEI, the MS equipment remains disabled even if a different ITSI is field-programmed in the user subscription memory area of the equipment. Another MS equipment, field-programmed with the same ITSI as a disabled equipment, still operates.

A typical use of this facility could be to bar a lost or stolen MS from full access to the system, whilst still allowing registrations, which identify the cell location of the MS.

If an MS is lost or stolen it is desirable to retrieve the MS. However, it would not be desirable to allow an unauthorized user, to access the TETRA network and possibly compromise the network integrity and/or security. Preventing a user from registering denies access to the system; however this does not assist in tracking the location of the mobile terminal. When a mobile terminal is temporarily disabled, it continues to register as defined by the network configuration and it continues to broadcast SDS messages containing location information.

5.2.1.4 End To End Encryption

End-to-end encryption (E2EE) service has not been standardized by ETSI yet; this service is specified in the Recommendation 02 by SFPG.

E2EE allows two parties to communicate in secure mode by ciphering the whole communication data at terminal level. The data is ciphered and deciphered by each terminal during the speech, with the use of a Terminal Encryption Key (TEK) and a strong ciphering algorithm (i.e. IDEA). The data travels ciphered through both the air interface and the network; it is only deciphered at addressee’s end, ensuring the maximum degree of security of communication protection and integrity. In order to achieve the desired degree of security, a proper key management policy has to be implemented by the network’s manager.

Over The Air Key Management (OTAK) service allows to manage (add and delete) TEK keys over the air interface simplifying the management of crypto-groups and increasing the degree of security.

5.2.1.5 System capabilities not covered by existing TETRA security measures

TETRA standard covers only security of TETRA air interface, security of authentication/encryption keys and support for end-to-end encryption. Internal implementation of TETRA network security is not covered by the TETRA standard. Security of network elements, control room, dispatching, network management, subscriber and service management as well as API/gateway interfaces are neither covered by TETRA standard. Thus securing of an operative TETRA network and the ICT environment, where TETRA network and its peripherals operate, are on the responsibility of the TETRA operator.

In addition to the air interface, the TETRA standard specifies two interfaces relevant to ISITEP that are not yet covered by existing TETRA security measures:

- Peripheral Equipment Interface (PEI). PEI is the interface used to split the TETRA terminal in two separate devices: the terminal equipment (TE) and the mobile termination (MT). The primary assumption in PEI is that the connection is between two trusted equipment (TE and MT) and that the connection is wired using a short non-radiating cable.
- Inter System Interface (ISI). ISI is the interface specified to allow the interconnection between two TETRA Networks that have an agreement to communicate. When two TETRA networks are interconnected with ISI link, an MS is able to migrate (i.e. roam) from one TETRA network, its Home Network, to another TETRA network, the Visited Network. ISI connection is foreseen over

E1 and over IP, no application level security has been specified over ISI, a general consideration is that the two interconnecting end-points are trusted but the linking network is un-trusted.

A discussion on the threats associated to the use of these interfaces is covered in Section 6.

5.3 Security procedures survey for national PPDR networks

Security procedures are those carried out by PPDR end-users and operators in order to realise the trusted and secure communication system needed in national PPDR networks. Security procedures deal with multiple and diverse aspects such as the provisioning/distribution of secret keys within networks, the configuration of security settings on terminals, the use of security features such as authentication, AIE, OTAR, E2EE, Enable-Disable, the approval of network equipment and applications, etc.

A description of some relevant procedures carried out by PPDR operators are given in the following for the case of the Rakel system:

Approval of equipment and applications. All equipment and applications that interconnects to Rakel systems must be approved by MSB. This is done to ensure that the applications will not be any risks for the security, availability, capacity or operations in the Rakel network. It is the end-user or the supplier who is responsible to apply for approval. Only users in Rakel can apply to get a product or application approved. Suppliers and dealers can not apply for approval if it is not done at a customer's explicit mission. Already approved applications needs only to be registered. MSB has a specification of what is required to get an application approved. An application containing a description of the product and how and where it will be used should be sent to MSB. MSB reviews the submitted documents and decides whether the product is acceptable or should be rejected or if additional information is required and / or if practical tests has to be done before a decision can be made. Information about MSB requirements for products and applications are available on the MBS/Rakel website.

Licensing procedure by MSB to use TEA2 cipher. As described in section 5.1, MSB may only provide Rakel services to entities providing services for public order, public security or health care activities. In case the applicant belongs to the allowed user group, MSB will grant a Rakel license to the applicant. They may then start the work to define how they will communicate within the network and what equipment to use.

Use of E2EE. In the Rakel network the E2EE encryption is already available. E2EE also demands support in radio terminals workstations as well as distribution of keys. Today there is support of E2EE in some of the radio terminals approved for the Rakel network, but the solution for the workstation is delayed. Security class and destination of the OTAC server is yet to be decided. The solution is based on smart cards and supplier independent.

Authorized to order subscription/services and Authorized to report faults. All end-users must have authorized personnel to place orders of subscriptions and services as well as report fault in the Rakel network. After the end-user got an Rakel license the have to report to MSB, via a form, which personnel in their organisation who will have rights to be in contact with Rakel Customer Support. If an end-user is not approved Rakel Customer Support cannot process their request.

Activation/deactivation of terminals. All radio terminals are temporarily deactivated during transport from/to supplier and end-users. After receiving the radio terminals the end-users must contact Rakel Customer Support to have them activated. This can only be done by the personnel who is authorized to be in contact with Rakel Customer Support.

Secured facilities. A company that holds a classified contract is cleared and a Facility Security Clearance (FSC) is issued according to Swedish laws and regulations. The security requirements for handling, storing and distribution of project related information is dependent of the Security

Classification Guide (SCG). As to site access, every visit is requested in advance and visits are monitored and/or accompanied depending on the type of facility to be visited.

5.4 Survey of security compromises on current national TETRA/TETRAPOL PPDR networks

ISITEP consortium includes all the manufacturers of national European networks and some of the main PPDR stakeholders.

As so expressed by manufacturers, no major stakes have been encountered in delivered PPDR networks. TETRA security features are required especially by those customers belonging to law enforcement. Until today TETRA security features: authentication, Air Interface Encryption, End to End Encryption and Enable and Disable covers all security objects required by the most demanding customers. It is to be noted that there are still a big number of analog (a non-secured digital) PPDR networks in use, were anybody can rather easily listen to the voice communication and also interfere it. Evidently the users know the case and avoid sensitive talk in such radiotelephone.

On the operators/end-users side, to handle threats on the PPDR network MSB has developed a process for security incident management. A report with information about what happened, when and where, and if known, what is the cause and effects of the incident. The report is sent to the security manager who, if necessary, contacts Cassidian. So far the process hasn’t been used.

6 SECURITY RISK AND VULNERABILITY ANALYSIS

This section reports on the initial outcomes of Task 2.2.2 “Security risk and vulnerability analysis”. Current analysis is primarily addressed to identify the potential security threats. An assessment of potential security & privacy concerns from a citizens view point is also reported. Risk analysis is left for next deliverable.

6.1 Threats on visiting users authentication

Security of authentication and air interface session keys inside TETRA networks is not defined by TETRA standard. To verify security of session keys within TETRA networks, security assessment of the TETRA system and its certified TETRA terminals is to be in place, including key generation and management servers.

Hence there may be risk of compromise of session keys within a TETRA network if the implementation does not ensure adequate measures. There are no international agreements for this in place, but each national operator ensures the overall security of public safety TETRA networks and terminals at national level.

Compromise of session keys may open some possibilities for spoofed terminals and base stations, which may not be detected immediately and thus may have as a consequence, possibility to listen TETRA communication within a spoof base station or in role of a spoofed TETRA terminal. Deployment of this method for malicious attempt is complex and requires special TETRA skills, so more real issue of this kind of vulnerability is not spoofed, but stolen terminals. A stolen/lost terminal may be used to get access or disturb the services. To our knowledge, no public info of any session key breaches has been reported in public safety TETRA networks.

When two TETRA networks are connected, the risk of session key compromise is in addition to the two interconnected TETRA networks also over the ISI interconnection of the networks.

In order to provide authentication service cross two TETRA systems, the visited network shall be able to get the RS and KS keys from the home network so that it can be verified that the migrating MS has the right K key. In the ETSI EN 300-392-7 [4] it is specified how the session keys for the authentication are transported across the ISI connection: session keys are requested by the Visited Network at the first time the migrating MS shall authenticate to the Visited Network and they can be re-used for subsequent authentications during the migration period. Of note is that in TETRA specifications there is no application-level security protecting session keys in transit over the ISI link.

In case the visited network is less trustable than the home network, the threat that session keys are intercepted and then compromised is greater in the Visited Network than within the Home Network. Currently there is no mechanism enforced in TETRA Standard to change the session keys before their expiration, except change the authentication key K.

Once an intruder has the session keys of a migrated MS two different attacks can be successfully completed:

- Using spoofed MS it is possible to decipher the TETRA signalling addressed to the attacked MS and detect the CCK.
- Using a spoofed BS it is possible to provide denial of service for those terminals for which the spoofed BS has got the valid session keys.

TETRA standard supports two versions of session key management over ISI interface. One uses the session keys of home network, enabling migrating TETRA terminals to use authentication in a visited network in same way as at home. The other version defines modified session keys for each visited network (i.e. are obtained using the MNI as an input), thus limiting to risk to the specific visited network, but requiring the modified procedures to be implemented in TETRA infrastructure and terminal in addition to the first (this to be defined in TETRA IOP). In both cases there are shown some possibility to use compromised keys for spoofing of terminal or base station. This issue has been widely analysed in SFPG, and TCCE WG6 contributions [9][10].

In order to be able to withdraw compromised session keys in the Visited Network in ETSI 300 392-7 [4] without modifying the authentication key K, it has been specified that the session keys depends not only from the MNI of the visited network but also from a designated session key modifier GCK0, in this way when the Home SwMI change the GCK0 the spoofed terminal with older GCK0 do not pass the authentication in the Visited Network.

It is recommended to encrypt the ISI connection between TETRA networks in cases that there is a significant risk of being able to capture the session keys, sent over ISI connection. This issue may be relevant especially in case of IP based ISI connection, where the keys are sent over IP networks, typically target for malicious cyber-activities. As for the case of TETRA services transport over IP between two TETRA networks, an IP VPN should be used, securing also session keys over ISI. Therefore, a counter measure to avoid the session keys get compromised is that the ISI link shall be encrypted. Also, re-use of session keys in the visited network shall be deprecated.

6.2 Threats on air interface due to roaming terminals

Security threats due to roaming terminals may arise from several sources. A visiting terminal may compromise the security of the home network if the terminal is not security certified to the national requirements of the visited network. In the same way, a terminal migrated in a foreign network may be posed to security risks that exist in the visited TETRA infrastructure but not in own infrastructure. A discussion on terminal security certification and a description of potential security threats in TETRA migration scenarios are covered in the following.

6.2.1 Terminal security certification

A TETRA terminal may pose security risks in hardware, operation system, memory encryption, key security etc. Commercial cellular intelligent terminals, connected to IP networks and to the Internet are increasingly posing security risks by viruses, malware, trojans, etc. Information of the terminal may be deleted or stolen, terminal may be made un-operative, taken to malicious control by malware, etc. This risk is increasing also in TETRA terminals as their richness of services and features grow and connections to Intranets (and also Internet) are becoming available.

Roaming PMR terminals are usually security certified to the requirement of home country, but not security certified to the requirements of the country, where the terminal may roam to. Most countries adapt some kind of security assurance process to ensure security of PMR terminals. The processes are national and may be rather demanding and heavy in certain countries. An example is CESG security requirements for TETRA terminals in UK (Airwave). Also in Germany (BOSNET) there are Germany specific BSI security requirements, not applied in other TETRA countries. It is obviously difficult to certify terminals of other countries to the national specific certification of own country, almost impossible for roaming capable terminals that are already in operative use.

As generic rule, the roaming terminal user rights (access to services) of those foreign roaming terminals should be restricted to the minimal necessary to limit the consequences of potential breaches. In this respect terminal/organisation specific access rights management in TETRA networks is essential.

6.2.2 Air interface encryption

Air interface encryption (AIE) service allows encrypting the ‘air interface’, signalling and voice, between an MS and the SwMI, it is highly unlikely to be able to carry out a successful attack when all the signalling is encrypted. Anyway, the first time the MS accesses to a TETRA system the exchanged signalling is not ciphered, so that in these few seconds the system is more vulnerable to attacks because an intruder could identify the MSs to attack. In order to reduce as much as possible the exposure time to these attacks, TETRA specifications contain encrypted cell reselection procedures, in this way just the first time the MS is switched on the signalling exchanged with the SwMI is not ciphered. In the specific case of two interconnected TETRA system, when an MS moves from its home network to a visited network the authentication procedure is not ciphered because the visited network does not know yet the migrating MS.

Even if authentication signalling is not ciphered it is highly improbable to complete successfully an attack if intruder has not gained the relevant session keys; but once an intruder has gained the session keys of an authenticating MS, using an air interface analyser it would be able of detecting the DCK of the attacked MS and the CCK for the location area where the MS is located, in this way the following attacks can be successfully completed:

- Eavesdropping of all group conversations ciphered with the detected CCK.
- Eavesdropping of all individual conversations ciphered with the detected DCK.

If the same CCK is used in all the location areas of the system the intruder would be free to move in all the TETRA systems listening for group conversation ciphered using CCK, a counter measure to this is to use a different CCK in each location area.

Practically all European public safety TETRA networks enforce AIE to be in use. European TETRA networks and terminals deploy TEA2 security algorithm in line with TETRA standard. In case of terminal roaming from outside Europe with a lower AIE security level, the network should support also that algorithm for roaming terminals. This is a compromise, if not significant, of the AIE security level of the country using TEA2. Again, roaming terminal user rights should be minimised to limit the risk consequence.

6.2.3 Enable and disable

A disable feature is supported in TETRA to cover, inter alia, the case of a trusted terminal that has been stolen and may allow the intruder to access directly to the TETRA system. TETRA defines two levels of disable for an MS: ‘temporary’ and ‘permanent’. A permanently disabled MS cannot be re-enabled over the air interface.

Disable facility is invoked by Home Network, in the specific case of a migrating MS the disable command shall cross the ISI link to reach Visited Network and then the migrated MS. In order to be able to face this threat the Enable / Disable feature shall be provided cross ISI link.

It is possible that an intruder, using a spoofed BS, attempts disabling a MS, in order to avoid this threat the MS shall always require the SwMI authentication before accepting a D-Disable.

6.2.4 End-to-end encryption

End-to-End Encryption (E2EE) service does not require direct interaction between the SwMI and the MS because encryption algorithm and encryption keys are deployed inside the MSs that interact directly, the SwMI is just in charged to transport the encrypted voice as it does for the clear voice. In the same way the E2EE key management mechanism is realized directly between the Key Management Centre (KMC) and the MS, however for the key distribution over the air the SwMI is used as transport.

Two MSs are able to communicate successfully using E2EE if they share the same encryption key and the same algorithm; in the specific case of two interconnected TETRA Systems it would be possible to create a mixed crypto group where MSs belonging to both networks share the same encryption keys.

If static encryption key management is used, there is no technical issue to create mixed crypto group. On the other hand, if dynamic management of encryption keys (OTAK) is used, some architectural issues arise. The KMC belonging to the Home Network is able to update the keys only on the MSs belonging to the Home Network, while the KMC belonging to the Visited Network is able to update the keys only on the MSs belonging to the Visited Network. For the TETRA End to End Encryption (E2EE) the standardisation process is still in progress, and the communication between two KMCs has not been addressed then the KMC belonging to the Home Network is not able to communicate with the KMC of the Visited Network, so encryption key for mixed crypto group should be exchanged using manual and out of band procedures (i.e. using REC01 file).

The use of OTAK and the manual alignment between two KMCs open the ISI system to synchronisation problems in encryption key management, indeed it is possible that MSs belonging to the two networks are updated in different moments causing communication problems between migrating MSs and Visited Network MSs. In order to avoid synchronisation problems on encryption keys management, it is suggested to avoid using OTAK for inter TETRA Systems E2EE communications.

In principle the use of static E2EE allows the creation of mixed crypto group where migrating users are able to have E2EE communications with the visited country users. But the current specification for the TETRA E2EE is open to any encryption algorithm and when two TETRA systems belonging to two different countries are interconnected, it is possible that the encryption algorithms used in one country are not legal in the next one. So E2EE communications between roaming MS and visited country users could not be available, while in the Visited Network migrating MSs could be able to make E2EE communications with other migrating MSs. This consideration arise a legal issue on the migrating MSs that are able to make E2EE without any control by the Visited Network. Another issue that the use of E2EE could arise regards lawful interception policies of the country where the visited network is deployed, because recording system would not be able to play back encrypted speech calls between visiting MSs.

There is a big variance of the use of E2EE in national TETRA networks. Many countries use E2EE only for high security users, while normal users deploy only AIE. Contrary to this, BOSNET uses BSI specified E2EE in all terminals in all voice communications. It is possible to roam BOSNET terminal to another country and still use E2EE to communicate to home, but joint communication (joint groups with visited country users) must avoid use of German E2EE as visited network terminals cannot decrypt/encrypt that traffic. This poses a lower than normal security level to those, using E2EE terminals. When other countries TETRA user migrates to Germany, all joint communications should not use E2EE. This poses challenge for BOSNET terminal to work in the best way of making and accepting calls and groups with two type of communication: E2EE and non-E2EE.

In order to solve the security and legal issues described above the use of E2EE communications shall be regulated by international and legal agreements between the involved countries.

6.3 Threats at network interface among national infrastructures

In case of deploying existing TETRA standard ISI interface (based on E1/leased lines), the interface is a dedicated point-to-point link, difficult to attack from outside and from remote. Intrusion to the lease line network management (commercial operator) could manipulate the configurations of the lines to route those connections to another termination point but that is typically immediately detected and it would be difficult to eavesdrop to any traffic of relevance. Using encrypted lines the risk can be removed.

In case of deploying a new IP based ISI interface, the threats are more diverse and resemble the cyber-threats of any mission critical IP and Intranets, much discussed, analysed and also mitigated today.

IP connected elements are vulnerable to IP threats. IP networks are exposed to various threats, known and unknown. The most advanced and complex, presumable new currently unknown attacks will be targeted specifically against the networks and services of national security and mission critical communication networks.

Most used security threats today are denial of service (DoS) attacks. A successful attack could block the use of ISI connection for some (short) time, so the obvious scenario would be such attack to take place just during some international police operation. The IP ISI connection should be isolated from any common IP address space and redundant connections should be in place to work around rapidly.

6.4 Threats from within national infrastructure to other national infrastructures

National PMR networks are certified to the security requirement of each nation and these are variable. When the security level of the other country is less than own, there is risk that a security breach in the other country has effects also to home country network and services. Examples of potential security threats are the following:

- Non- traceable actions of malicious WS users/ laptop users in one country may block use of the ISI interconnection and also harm communications in the other country.
- Malicious insiders. A user with a valid subscription may try to misuse or disturb the services.
- Denial of service attack to one network or its elements, not security hardened, has effects to the connected other network.

Hence there has to be an evaluation of the risks, posed by connecting TETRA networks together in relation to the risks, residing in the national home network. Risk can never be fully avoided and it is the evaluation of benefits compared to the risk. The risk level and its consequence need to be assessed to define feasible risk mitigations, due to the interconnection.

As there are variable national security rules of internal TETRA communications as well as variable rules to the personal data of TETRA using authorities and first responders, those communications and those individuals should be isolated in the national PMR network from access by foreign migrating users and from access via ISI interconnection. The guideline is to provide to the ISI interconnection and to visiting users access only to those communications and identity to those officers, needed to comply with the use case. This means that limited access rights to resources and users in the visited network are provisioned to the visiting users. Also visiting terminals should be pre-configured and pre-programmed to this limited use in each visited network, where the terminal may roam.

6.5 Threats within ISITEP terminals

As described in previous section 4.3, ISITEP terminals are expected to rely on a terminal control interface (e.g. PEI for TETRA and PEI-equivalent for TETRAPOL) in order to interconnect the TETRA/TETRAPOL communication modem(s) with the programmable device that hosts the applications.

In TETRA, the Peripheral Equipment Interface (PEI) is the interface used to split the TETRA terminal in two separate devices: the terminal equipment (TE) and the mobile termination (MT).

The equipment may be a PC or a PDA while the mobile termination acts like a modem between the IP protocol stack and the TETRA air interface.

The TETRA PEI has been designed to provide access to the full set of the mobile termination functionalities, for speech call the PEI provide control only for the call signalling, therefore voice packets are never sent over the PEI.

There are three components in TETRA PEI:

- AT command: Mobility Management, Speech Call Control, Short Data Services, Circuit Mode Data and Radio Status & Configuration
- Packet Data: IP v4, IP v6

- TNP1: Mobility Management, Speech Call Control, Short Data Services, Circuit Mode Data, Radio Status & Configuration and Supplementary Services. TNP1 commands can be sent in parallel with on-going packet data services while AT commands can only be sent in the command line.

The Primary assumption in PEI is that the connection is between two trusted equipment and there is no authentication and authorization. It is further assumed that the connection is wired using a short non-radiating cable clause 5 of ETSI EN 300-392-5 [4].

Currently there are a number of standard physical interfaces offered by PCs and PDAs both wireless and wired. Where the physical connection does not satisfy the clause 5 of ETSI EN 300-392-5 and a wireless connection is used between the TE and the MT all the capabilities open to TNP1 and the AT command set can be exposed to attack.

To counter this threat, security model arrangements for the proper physical connection adopted shall be used.

6.6 Potential security & privacy concerns from a citizens view point

Before discussing privacy within a PPDR communication system it is necessary to distinguish between privacy of the end-users (i.e. first responders) and privacy of citizens who may be the subject of the communication over the PPDR communication system. It is, however, relevant to mention that when end-users are roaming the usage of the PPDR communication system in the visiting country will be logged in that country. Although this usage is part of the performance of the end-users work, a record is created that could be linked to an end-user terminal (which ultimately may be linked to an individual). Within this section we further focus on the privacy aspects of citizens.

When roaming with PPDR terminals cross network operator boundaries, it is possible that personal data from citizens of the home country are accessed over the visited SwMI or shared with PPDR organisations of the visited country. For instance, in the police hot pursuit use case a car is chased across borders. When crossing the border police will share the license plate number, and possibly other personal data that can be retrieved from national information systems based on the license plate number of the chased vehicle (e.g. address/name of the registered owner), with the local authorities using the roaming PPDR terminal. Since the personal data is shared across jurisdictions it is important to ensure that there are legal frameworks and privacy protection procedures and mechanisms in place to protect the privacy of the citizens. In this section, an assessment of potential security & privacy concerns from a citizens view point is presented.

For this assessment we use the definition for personal data from the EU Data Protection Directive (Directive 95/46/EC [11]).

> ***'personal data'*** shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

Aspects that will influence the possible privacy concerns, and for which a good understanding is necessary, are:

- the *technical capability* that is enabled by ISITEP. For instance,
    - What are the communication options of a user of a roaming terminal with users or the control room (dispatcher) of the visiting network? Voice, data, and image communication?

  - Which information services are accessible from a roaming terminal. National information services over the visiting SwMI and/or information services within the visiting SwMI.

- the *usage scenario's* in which personal data is accessed or shared over the visiting network. These scenarios should address issues like:
  - the *type of personal data* which is accessed or shared (e.g. identity information, criminal record, medical data);
  - the *type of PPDR organisations* (i.e. police, fire and ambulance services) or Non-Governmental Organisation (NGO) (e.g. the Red Cross) which is accessing the information or with whom the personal data is shared;
  - the *purpose* for which the personal data is shared (the principle of *purpose limitation* is important to limit to the collection and further processing of the personal data);
  - the *scale* of personal data that is accessed or shared (e.g. there is only information shared regarding one individual vs. there is information shared regarding a large group of people).
- the *privacy regulations* of citizen in the all countries involved, since they vary between countries.
- the relevant national, bilateral and international *legal frameworks* to enable and safeguard cross border sharing of personal data. The Prüm Convention for instance enables the participating countries to exchange data regarding DNA, fingerprints and vehicle registration of concerned persons in combating terrorism and cross-border crime.

It is relevant to note that the security & privacy concerns of citizens can differ per country. Results of an assessment from a citizens view point would thus differ per country.

The assessment of the potential privacy concerns from a citizens point of view used the following approach:

1. Collect and investigate different usage scenario's in which personal data is accessed over a visiting network or shared with a PPDR organisation of the visited countries;
2. Determine security & privacy aspects.

As part of an initial assessment, based on the different use cases (police hot pursuit; airplane disaster; joint police surveillance; VIP protection) identified for ISITEP, different several aspects that may influence the privacy impact within ISITEP are examined and some early generic conclusions can be drawn.

Technical capability

The property of ISITEP with the most impact regarding possible privacy aspects, seen from a technical point of view, is the property that communication channels within ISITEP is mainly based on voice communication channels. Within ISITEP this is referred to as 'Mission Critical Voice'. Besides this voice communication channel, only the exchange of (manually constructed) short data messages is supported.

From this property it may be concluded that (roaming) terminals will not have an (automated) information exchange with information services within the visited and/or home SwMI. Possible leakage of personal data within this information services through ISITEP is thereby eliminated. However, in case it is possible to access an information system containing personal data, the authentication and authorization necessary for these information systems should not be based on the TETRA network authentication/authorization. A separate application level authentication should be required in each country. Based on the identity of the visiting user, the authorisation of access to personal data should be restricted in such way not to violate the privacy regulations: this restriction may overrule the need for availability of such data to a visiting user even when the use case would require access.

The fact remains that personal data can still be communicated between ISITEP (roaming) terminals. However, this requires a human-in-the-loop to obtain this data (out-of-band) from the information services and consciously exchange this information by voice. To prevent any leakage of personal data the end-users of the (roaming) terminals should be aware of the information that may and may not be exchanged in the different use cases. A non-technical measure to implement is to establish proper procedures. These procedures should also reflect the applicable regulations for the exchange of information, e.g. the Prüm convention.

Usage scenarios

Within the identified use cases different types of information may be exchanged. E.g. within the police hot pursuit it will probably be vehicle information, within the airplane disaster use case the information that may be exchanged may also include medical information. This difference in type of information that may be exchanged will most likely influence the opinions regarding the impact of a privacy breach. Another difference within the use cases that will most likely influence the perceived privacy impact is the amount of information that will be exchanged. The VIP protection use case will only exchange the (sensitive) information regarding a single person.

However due to the fact that the information across ISITEP is only communicated by using voice communication channels the protection measures for all use cases (independent of the type of data; type of organisations; purpose of the exchange; scale of information exchanged) should be realized by the implementation of applicable procedures.

Based on the assessment above ISITEP may enable exchange of personal data via the mission critical voice information across borders. Since the possible exchange of personal data is done by end-users of the (roaming) terminals, we propose to ensure that the end-users are made aware of the fact that personal information that may or may not be exchanged under different circumstances. This should be done by means of proper procedures that reflect the applicable regulations for the exchange of personal data under the particular circumstance.

7 CONCLUSIONS

A framework and methodology defined to carry out the development of the security requirements has been specified. The framework includes aspects such as the identification of the ISITEP system components and players that are relevant for the security analysis, and the definition of security objectives.

On this basis, a first assessment has been addressed in Section 5 to delineate the state-of-the-art of the security features existing in current PPDR technologies and networks, security procedures carried out by PPDR end-users and operators in order to realise the trusted and secure communication system needed in national PPDR networks, and to provide an overview of the regulatory and legislation framework that impacts affects PPDR communication networks. As so expressed by some manufacturers and operators involved in ISITEP, no major security stakes have been encountered in delivered PPDR networks.

Finally, a preliminary assessment of security threats to ISITEP system is also reported. The assessment is focused on those security threats that are relevant to the new communications capabilities brought by the ISITEP solution in terms of service interworking across multiple national networks and terminal roaming. In this regards, the following categories of threats have been covered: threats on visiting users authentication; threats on air interface due to roaming terminals; threats at network interface among national infrastructures; threats from within national infrastructure to other national infrastructures; threats within ISITEP terminals; and potential security & privacy concerns from a citizens view point.

8 REFERENCES

[1] ETSI ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture", November 1996

[2] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects", January 1994

[3] ETSI TR 102 512 V1.1.1, “Security requirements analysis for modulation enhancements to TETRA”, August 2006

[4] ETSI EN 300 392-7 V3.3.1 (2012-07), “Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security”

[5] 3GPP TS 21.133, “3G Security; Security Threats and Requirements”, December 2011

[6] 3GPP TR 22.893, “Study into identification of advanced requirements for IP interconnection of services; (Release 10)”

[7] ETSI EN 300 392-3-1 V1.3.1 (2010-08), “Terrestrial Trunked Radio (TETRA);Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 1: General design”

[8] i3 Forum, “Security for IP Interconnections (Release 1.0)”, May 2011

[9] ETSI/TETRA(13)000023r1, TETRA#41, 11th - 13th March 2013, Title: ISI authentication, Source: Cassidian, BDBOS, MSB, ERVE, RIKS

[10] SFPG 12/26r2,”Security consideration in TETRA ISI authentication r2”, 10th September 2012

[11] European Parliament and European Council. Directive 1995/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995