ISITEP
D6.5.2 - PPDR SERVER APPLICATIONS DESIGN DESCRIPTION

Document Manager:	Federica Battisti	RM3	Editor

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

Document ID N°:	ISITEP_D6.5.2_20160215_V1.1	**Version:**	V1.1
Deliverable:	D6.5.2	**Date:**	15/02/2016
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Federica Battisti (RM3)
Approved by (WP Leader):	Claudia Olivieri (FNM)
Approved by (SP Leader):	Dimitris Androutsopoulos (NETFI)
Approved by (Coordinator)	Paolo Di Michele (FNM)
Security Approval (Advisory Board Coordinator)	Etienne Lezaack (BFP)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico Frosali	FNM	Reviewer
Claudia Olivieri	FNM	Contributor
Federica Battisti	RM3	Reviewer
Marco Carli	RM3	Reviewer
George Mitsopoulos	NETFI	Contributor
Alessandro Semproni	EXP	Reviewer

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	02/10/15	All	All	First draft
V0.2	06/10/15	All	All	Manuscript revision
V1.0	07/10/15	All	All	Final release
V1.1	15/02/16	All	All	Updated according to the remarks of the Commission after the 2nd Annual Review

Publishable extended abstract

This deliverable (D6.5.2) is issued within WP6.5.

WP 6.5 is in charge of defining the server side of the PPDR cloud added-value applications, while the design of the client side is provided in WP 6.4.

PPDR cloud added-value applications are:

- Dynamic Functional Numbering (DFN): this function allows to remap the numbers of the operating talkgroups used in a country in the relevant numbers used for the same operating talkgroup in the neighboring country;
- Location Dependent Addressing (LDA): this application provides functional numbers to contact the right PPDR operational center using the GPS position of the terminal instead of the Location Area position;
- Enhanced Message Exchange (EME) application provides the capability to exchange messages between authorized end-users using a different native language exploiting the semantic and syntactic translator capabilities.

CONTENTS

1 INTRODUCTION

The aim of WP 6.5 is the definition of the design of the PPDR cloud added-value applications server-side:

- Dynamic Functional Numbering (DFN): this function allows to remap the numbers of the operating talkgroups used in a country in the relevant numbers used for the same operating talkgroup in the neighboring country
- Location Dependent Addressing (LDA): this application provides functional numbers to contact the right PPDR operational center using the GPS position of the terminal instead of the Location Area position.
- Enhanced Message Exchange (EME): this application provides the capability to exchange messages between authorized end-users using a different native language exploiting the semantic and syntactic translator capabilities.

This WP is developed taking as input the requirements related to the PPDR cloud added-value applications defined in the ISITEP enhanced terminal requirements (WP 5.1). The outcome of this WP is the design of the PPDR cloud added-value application server side.

2 DEFINITIONS AND ABBREVIATIONS

2.1 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:

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

Digest Authentication: challenge-based authentication mechanism based on the use of an MD5 hashing function on a username/password combination. The MD5 algorithm is described in the official document [5] which also provides a sample "C" implementation.

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.

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.

2.2 Abbreviations

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

Acronym	Definition
AuC	Authentication Center
DFN	Dynamic Functional Numbering
EME	Enhanced Message Exchange
GPS	Global Positioning System
HMI	Human Machine Interface
HW	Hardware
IET	ISITEP Enhanced Terminal
IP	Internet Protocol
ISI	Inter System Interface
ITSI	Individual TETRA Subscriber Identity
LAN	Local Area Network
LDA	Location Dependent Addressing
LIP	Location Information Protocol
MS	Mobile Station
PC	Personal Computer
PD	Packet Data
PEI	Peripheral Equipment Interface
PID	Protocol IDentifier
PPDR	Public Protection and Disaster Relief
SDS	Short Data Service
SSI	Short Subscriber Identity
SST	Semantic and Syntactic Translator
SW	Software
SwMI	Switching and Management Infrastructure
VPN	Virtual Private Network

WFM	Workflow manager
WP	Work Package
WSDL	Web Services Description Language

3 SYSTEM OVERVIEW

PPDR cloud added-value applications may be composed by a control room and by a terminal component, referred in the following as server and client side. The server side application is deployed inside an operational unit connected to ISI Cloud Network; on the other hand the client side is deployed inside the ISITEP enhanced terminal (IET).

The ISI Cloud Network is realized interconnecting different PPDR SwiMis from different manufacturers using ISI-GWs. The ISI Cloud Network grants PPDR services to all the mobile stations moving across the ISI Cloud Network.

Both TETRA and TETRAPOL provide narrow band IP packet data connectivity, but ISITEP project scope is the ISI phase 3 features, and Packet Data (PD) functionality is addressed in ISI phase 4. Therefore in the ISITEP project, the data transport offered by the ISI Cloud Network to client-server applications is based on exchanging short data messages.

The operational unit hosting ISITEP server-side applications will be able to connect to any TETRA network using the TETRA air interface.

The operational unit developed in the current WP will be able to provide a data transport bearer not only to the PPDR cloud added-value applications described in this WP, but also to the interoperability enabling applications described in SP5: Work Flow Manager and Semantic & Syntactic Translator.

Concluding, the server applications deployed in the operational unit are:

- Workflow Manager (WFM)
- Semantic & Syntactic Translator (SST)
- Dynamic Functional Numbering (DFN)
- Location Dependent Addressing (LDA)
- Enhanced Message Exchange (EME)

Design Specification of DFN, LDA and EME is addressed inside this work package, the details on the relevant terminal side application are specified in WP 6.4. Design Specification of WFM is addressed inside WP 5.4 and Design Specification of SST in WP 5.5, but the common framework offered to the all the ISITEP applications is described in this document.

In the Figure 1 a general scheme of the system in which the ISITEP applications are deployed, is shown.

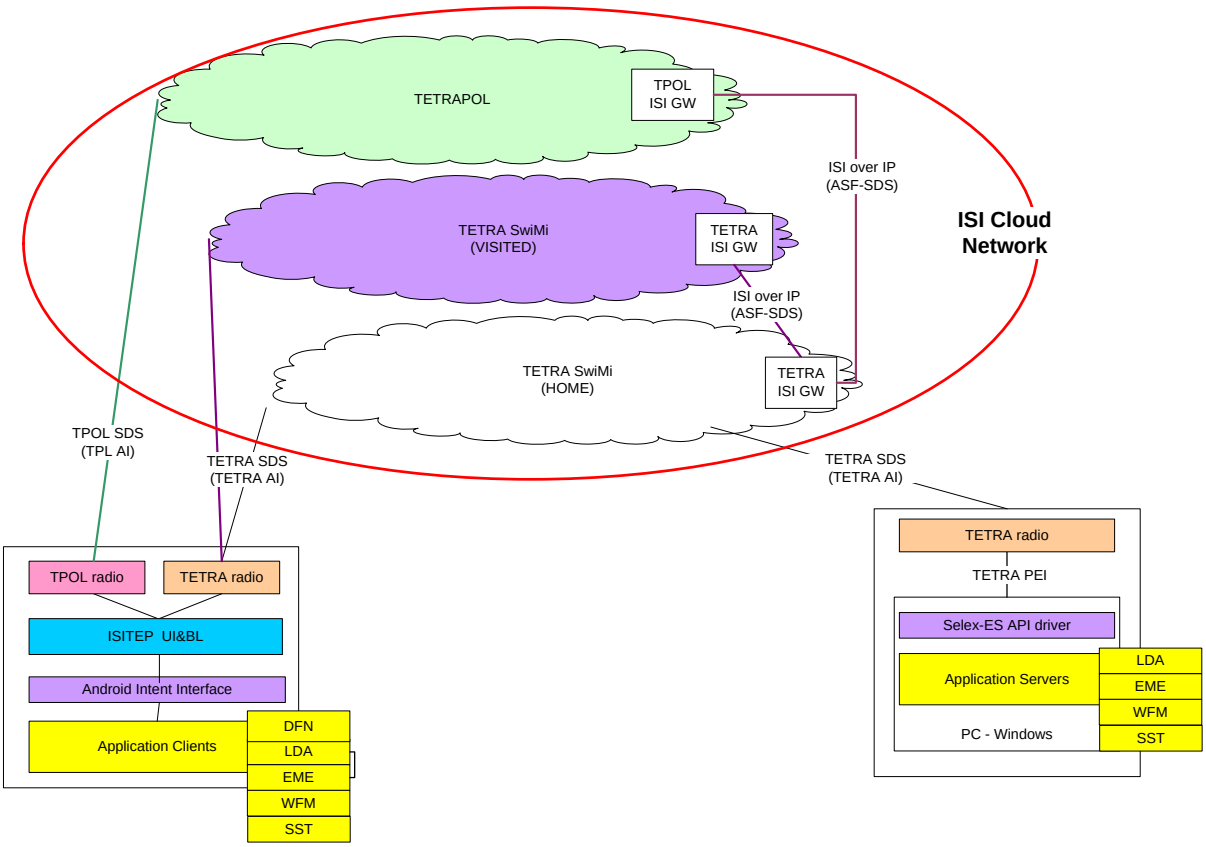

Figure 1: System overall architecture

4 ISITEP SERVER PLATFORM DESIGN DESCRIPTION

4.1 HW Design

The operational unit is a console that is able to connect to any interoperable TETRA Network; therefore, it can be deployed in any control room in which TETRA coverage is available.

The operational unit is composed by a PC and by a TETRA radio unit.

The PC hosts the ISITEP server applications and it is connected with a TETRA radio via LAN interface. A second LAN interface is provided to enable the operation unit console to be connected to an external trusted network.

The PC is a Dell T5600 with O.S. Windows Seven 32 bit.

In Figure 2, the connectivity schema of the operational unit is reported:

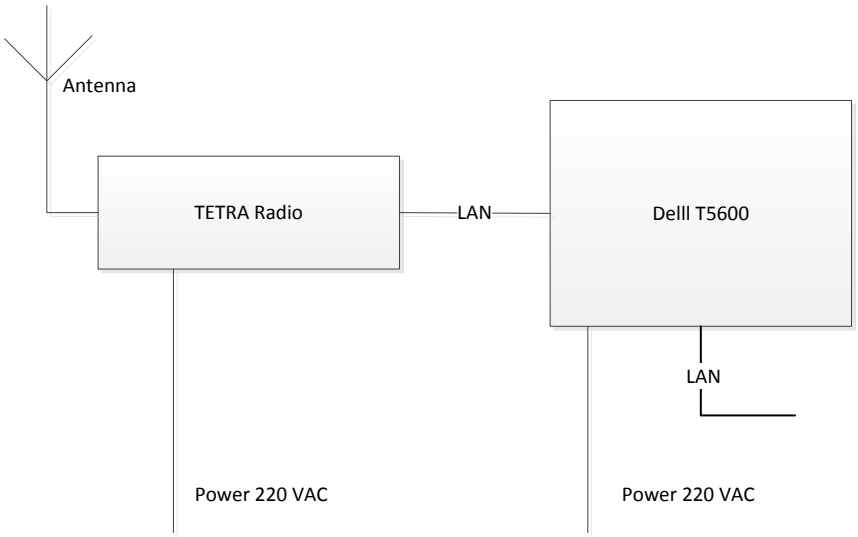

Figure 2: Physical scheme of the operational radio unit

4.2 SW Design

In this paragraph the SW platform of the Window PC that hosts the ISITEP server applications is described. The TETRA radio terminal is a standard TETRA radio that provides TETRA PEI [2] interface over LAN and it will not be described in this document.

Server applications are reachable by their corresponding client applications through the TETRA Identity (ITSI) assigned to the TETRA radio. The Client Application shall send SDS to that specific ITSI in order to reach the Server side application.

Server applications may be deployed in a virtual machine inside the PC or in an external device deployed on the same trusted network. In Figure 3 it has been represented the Sw architecture of the operational unit hosting the ISITEP Server Applications. Four layers are shown, starting from the bottom they are:

- The physical layer realized by a TETRA radio; this layer is in charge to send and receive short data services over the TETRA air interface [3];
- On the top of the physical layer there is the Message Service Layer, that interfaces the radio layer using the TETRA PEI interface [2], the Message Service Layer provides to the upper layers remote and concurrent access to the physical layer;

- On the top of the Message Service Layer there is the Message Web Service Layer that provides to the upper layer a web-based access to the Message service Layer;
- On the top of the Message Web Service Layer, there is the Application layer in which the ISITEP Server applications are developed.

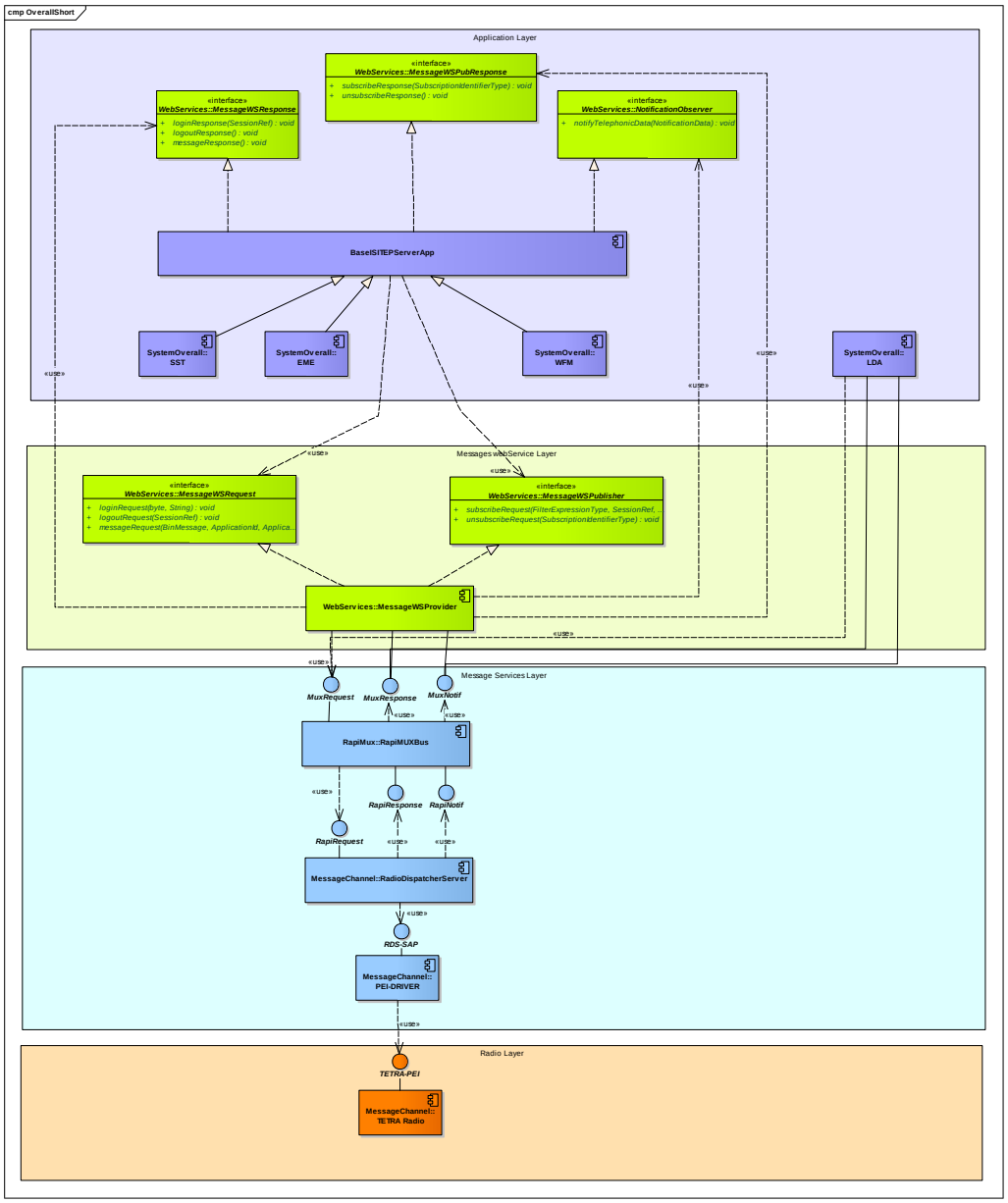

Figure 3: Sw Architecture of the platform used to host ISITEP Server applications

4.3 Web Services Interface

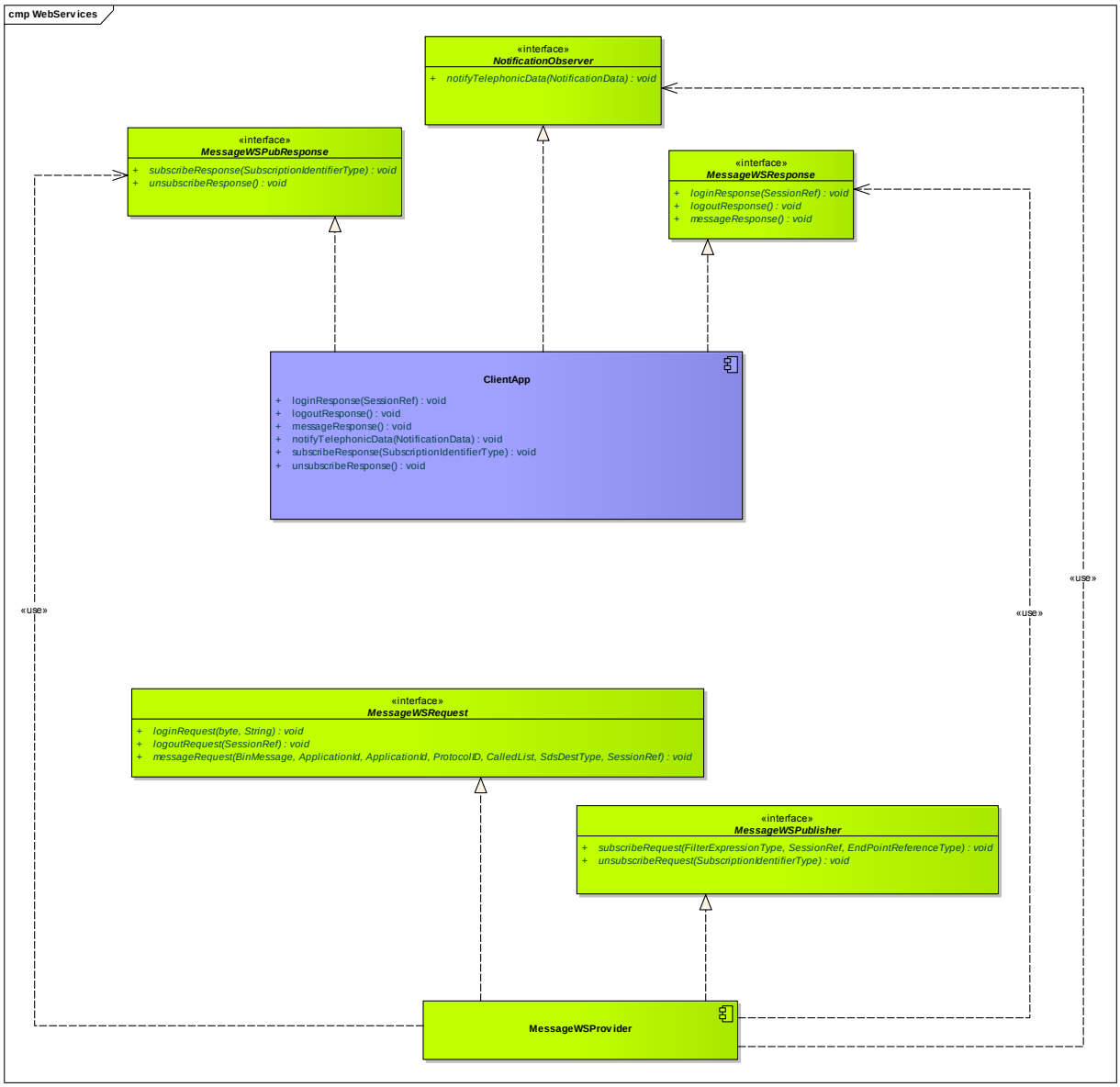

Figure 4: Web Services Interface Diagram

In the following paragraphs the Web services Interface exported by the operational unit toward ISITEP server applications are described. For a formal definition of this interface please refer to the WSDL file (telephonic-nbi-wsdl.jar) delivered with this document.

4.3.1 MessageWSRequest

The Web Services Provider offers to its client applications (i.e. any ISITEP control room server application) the following services:

- Login
- Logout
- Call

- TextMessage
- Message
- Status

In the ISITEP contest only the login, logout, and Message method shall be managed. In order to access such methods the Web Services Clients shall access to the following URL:

"http:// <serviceLocation>:9092/TelephonicService"

where <serviceLocation> is the IP address in which the Web service provider is located.

4.3.1.1 loginRequest

The loginRequest shall be the first call and it is intended to get a session reference identifier to be used in the subsequent requests.

```
<xs:element name="loginRequest">
	<xs:complexType>
		<xs:sequence>
			<xs:element name="user" type="xs:string"/>
		</xs:sequence>
	</xs:complexType>
</xs:element>
```

This message is sent from the ISITEP Server Application to the Web Services Component to create a user session.

- user: identity of the user (user-Name) configured in the Web Services
- password: password associated to the user-Name

4.3.1.2 logoutRequest

```
<xs:element name="logoutRequest">
	<xs:complexType>
		<xs:sequence>
			<xs:element name="session"  type="tns:SessionRef"/>
		</xs:sequence>
	</xs:complexType>
</xs:element>
```

This method is used by ISITEP Server Application in order to close an open user session, the session reference identifier is provided in the message.

- sessionRef: identity of the user session

4.3.1.3 messageRequest

```
	<xs:element name="messageRequest">
		<xs:complexType>
			<xs:sequence>
			    <xs:element name="session"      type="tns:SessionRef"/>
				<xs:element name="type"         type="tns:SdsDestType"/>
				<xs:element name="called"       type="tns:CalledList"/>
				<xs:element name="pid"          type="tns:ProtocolId"/>
				<xs:element name="srcApplId"    type="tns:ApplicationId"/>
				<xs:element name="destApplId"   type="tns:ApplicationId"/>
				<xs:element name="userData"     type="tns:BinMessage"/>
```

```
                    </xs:sequence>
                </xs:complexType>
        </xs:element>
```

This method is used by the ISITEP Server Application in order to send a text message to the ISITEP client Application deployed inside the IET.

The following parameters shall be evaluated:

- session: identity of the user session;
- type: used to identify the SDS type individual or group;
- called: string that contains the phone number of the enhanced terminal that hosts the ISITEP client application;
- PID: non negative integer that is used to identify the protocol transported over TETRA short data service with Transport Layer Cfr. [3] Chap. 29. TETRA network infrastructures guarantee delivery of PID value between the two end-points of the message channel. PID shall have a value inside the [192 – 254] range. **A specific PID will be chosen in the proper range in order to support ISITEP application demultiplexing on the message channel. In order to avoid conflict with PID values already adopted by different vendors the PID value will be configurable both in the client and in the server applications;**
- srcAppId: byte that contains the identify of the ISITEP Server application that is sending the message;
- destAppId: byte that contains the identity of the ISITEP Client application that shall receive the message;
- userData: binary user data, in this field the end to end signaling exchanged between the ISITEP applications server-side and client side is transported.

4.3.2 MessageWSPublisher

4.3.2.1 subscribeRequest

This method is called by the ISITEP Server Application in order to subscribe to the asynchronous notification mechanism.

The ISITEP Server Application shall subscribe to the system notification-publisher using the following URL :

"http:// <serviceLocation>:9092/TelephonyNotificationPublisher

<serviceLocation> is the IP address in which the Web service provider is located.

```
<xsd:element name="subscribeRequest">
        <xsd:complexType>
                <xsd:sequence>
                        <xsd:element name="consumerUri" type="tns:EndPointReferenceType"/>
                        <xsd:element name="session" type="tls:SessionRef"/>
                </xsd:sequence>
        </xsd:complexType>
 </xsd:element>
```

The following parameters shall be evaluated:

- consumerUri: the URL exported by the Telephony Web Services client application (i.d. any ISITEP control room server application) that will consume the asynchronous notifications.
- session: identity of the user session received during login procedure.

4.3.2.2 unsubscribeRequest

This method is called by the ISITEP Server Application in order to unsubscribe from the notification mechanism and stop receiving text messages from the ISITEP client application.

```
<xsd:element name="unsubscribeRequest">
	<xsd:complexType>
		<xsd:sequence>
			<xsd:element name="subscriptionID" type="tns:SubscriptionIdentifierType"/>
		 </xsd:sequence>
	</xsd:complexType>
 </xsd:element>
```

The following parameters shall be evaluated:

- subscriptionID: string that identifies the subscription request, this is returned in the subscribeResponse.

4.3.3 MessageWSPubResponse

4.3.3.1 subscribeResponse

This is the response to the subscribe method provided by the Web services interface towards the ISITEP Server Application.

```
<xsd:element name="subscribeResponse">
	<xsd:complexType>
		<xsd:sequence>
			<xsd:element name="subscriptionID" type="tns:SubscriptionIdentifierType" minOccurs="0"/>
		</xsd:sequence>
	 </xsd:complexType>
 </xsd:element>
```

The following parameters will be evaluated:

- subscriptionID: string that identifies the subscription request and that shall be used when the ISITEP Server Application shall unsubscribeRequest.

4.3.3.2 unsubscribeResponse

This is the response to the unsubscribe method provided by the Web services interface towards the ISITEP Server Application.

```
<xsd:element name="unsubscribeResponse">
	<xsd:complexType>
		<xsd:sequence/>
	</xsd:complexType>
 </xsd:element>
```

The unsubscribeResponse method is empty because no data shall be provided with this method by the system to the ISITEP Server application.

4.3.4 NotificationObserver

4.3.4.1 notifyTelephonicData

The notifyTelephonicData is a generic method that is used to transport asynchronous information addressed toward the ISITEP Server Applications.

The ISITEP Server Application will receive notifyTelephonicData only after subscribing to the notification service.

```
<xs:complexType name="NotificationData">
              <xs:sequence>
                <xs:element name="callStatus"  type="tns:callStatusNotification"   minOccurs="0" />
                <xs:element name="textMessage" type="tns:textMessageNotification"  minOccurs="0" />
                <xs:element name="message"     type="tns:messageNotification"      minOccurs="0" />
                <xs:element name="status"      type="tns:statusNotification"       minOccurs="0" />
                <xs:element name="heartbeat"   type="tns:Heartbeat"                minOccurs="0" />
       </xs:sequence>
</xs:complexType>
```

The notifyTelephonicData provides a set a different type of asynchronous notifications, in the ISITEP contest only the messageNotification and the Heartbeat shall be managed.

4.3.4.1.1 messageNotification

In case a messageNotification is received the following fields will be evaluated:

- sourceIdentity: identity (ITSI) of the IET where is deployed the ISITEP client application that is sending the message to the ISITEP server application;
- PID: non negative integer that is used to identify the protocol transported over TETRA short data service with Transport Layer Cfr. [3] Chap. 29. TETRA network infrastructures guarantee delivery of PID value between the two end-points of the message channel. PID shall have a value inside the [192 – 254] range. **A specific PID will be chosen in the proper range in order to support ISITEP application demultiplexing on the message channel. In order to avoid conflict with PID values already adopted by different vendors the PID value will be configurable both in the client and in the server applications;**
- srcAppId: a byte that contains the identifier of the ISITEP Client application that is sending the message;
- destAppId: a byte that contains the identifier of the ISITEP Server application that shall receive the message;
- userData: binary user data, in this field the end to end signaling exchanged between the ISITEP applications server-side and client side is transported.

4.3.4.1.2 Heartbeat

The Heartbeat message is periodically received by those clients that have been logged and subscribed into the system. This message is used by the system in order to check that the session with the ISITEP server applications is alive. The same message can be used by the ISITEP Server application to check if the system is hanged (it does not send periodic heartbeat anymore).

In case a Heartbeat notification is received, the date and time of the heartbeat will be evaluated.

4.3.5 MessageWSResponse

4.3.5.1 loginResponse

This is the response to the loginRequest method provided by the Web services interface toward the ISITEP Server Application.

```
<xs:element name="loginResponse">
	<xs:complexType>
		<xs:sequence>
			<xs:element name="loginResponse" type="tns:SessionRef"/>
		</xs:sequence>
	</xs:complexType>
</xs:element>
```

The loginResponse contains the Session Reference (SessionRef) to be used in the following method requests. In case of error it is generated an exception (loginException)

4.3.5.2 logoutResponse

This is the response to the logoutRequest method provided by the Web services interface toward the ISITEP Server Application.

```
<xs:element name="logoutResponse">
	<xs:complexType>
		<xs:sequence>
		</xs:sequence>
	</xs:complexType>
</xs:element>
```

The logoutResponse method is empty because no data shall be provided by the system to the ISITEP Server application.

In case of error an exception is generated (logoutException).

4.3.5.3 messageResponse

messageResponse is the response to the messageRequest method provided by the Web services interface towards the ISITEP Server Application in order to notify that the relevant messageRequest has been accepted and taken in charge by the Web Service Provider (this is not an acknowledge from the ISITEP control client application deployed inside the IET).

```
<xs:element name="messageResponse">
		<xs:complexType>
			<xs:sequence>
			</xs:sequence>
		</xs:complexType>
</xs:element>
```

The messageResponse method is empty because no data shall be provided by the system to the ISITEP Server application.

In case of error, an exception is generated (messageException).

4.3.6 Message Sequence

4.3.6.1 Login and subscription

In the Figure 5 the message sequence exchanged during the login and subscription procedure executed by an ISITEP Server Application toward the Web Service interface offered by the system (WS system in the figure) is presented.

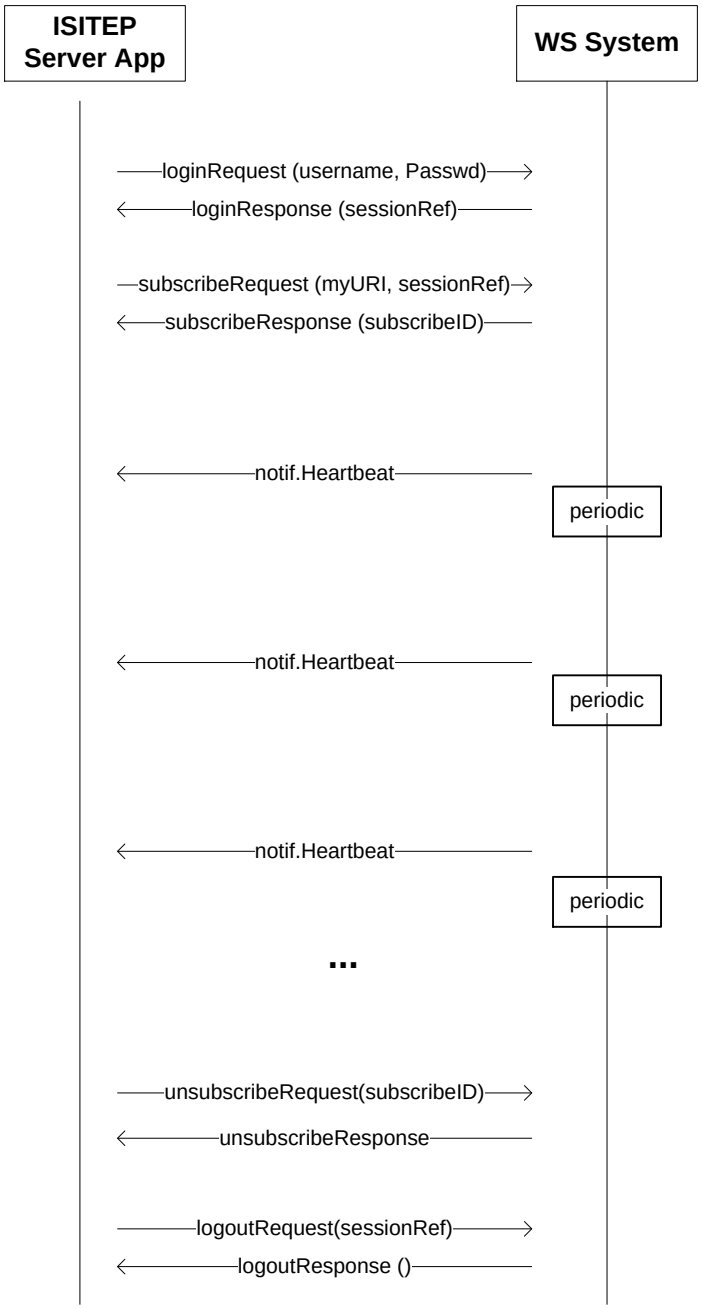

Figure 5: Login and subscription message sequence

4.3.6.2 Incoming Message

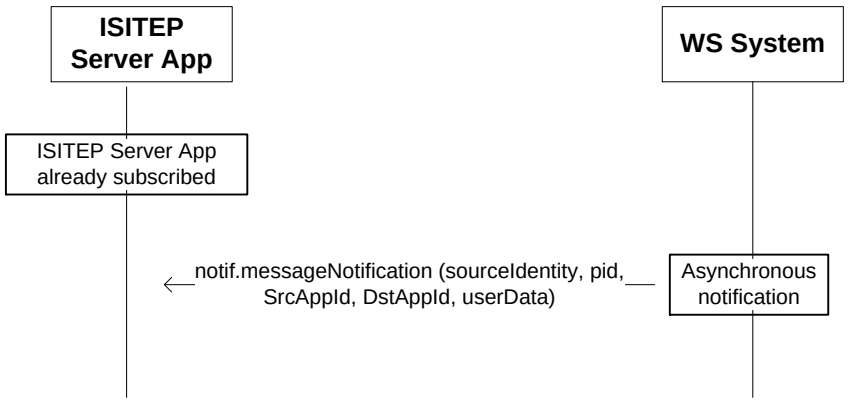

Figure 6: Message from ISITEP Client App is received from ISITEP Server App.

4.3.6.3 Outgoing Message

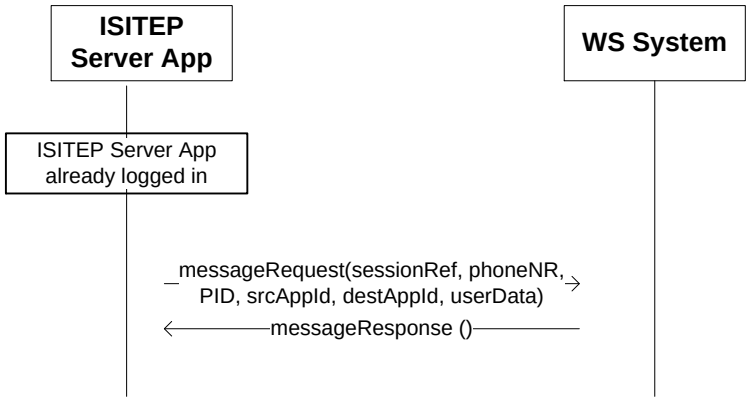

Figure 7: Message sent from the ISITEP Server App toward the ISITEP Client App deployed on the enhanced terminal

4.3.6.4 Client – Server End to End message delivery

In Figure 8, a message sequence in which more client applications are able to exchange messages with the corresponding server applications is depicted; over the air, the exchanged messages use the same source and destination identities (i.e. Control Room phoneNR and IET phoneNR), but the framework realized on the control room server and on the IET provides the capability of demultiplexing the received messages towards the different apps (i.e. clientApp_1, clientApp_2, userWSApp_1 and userWSApp_2).

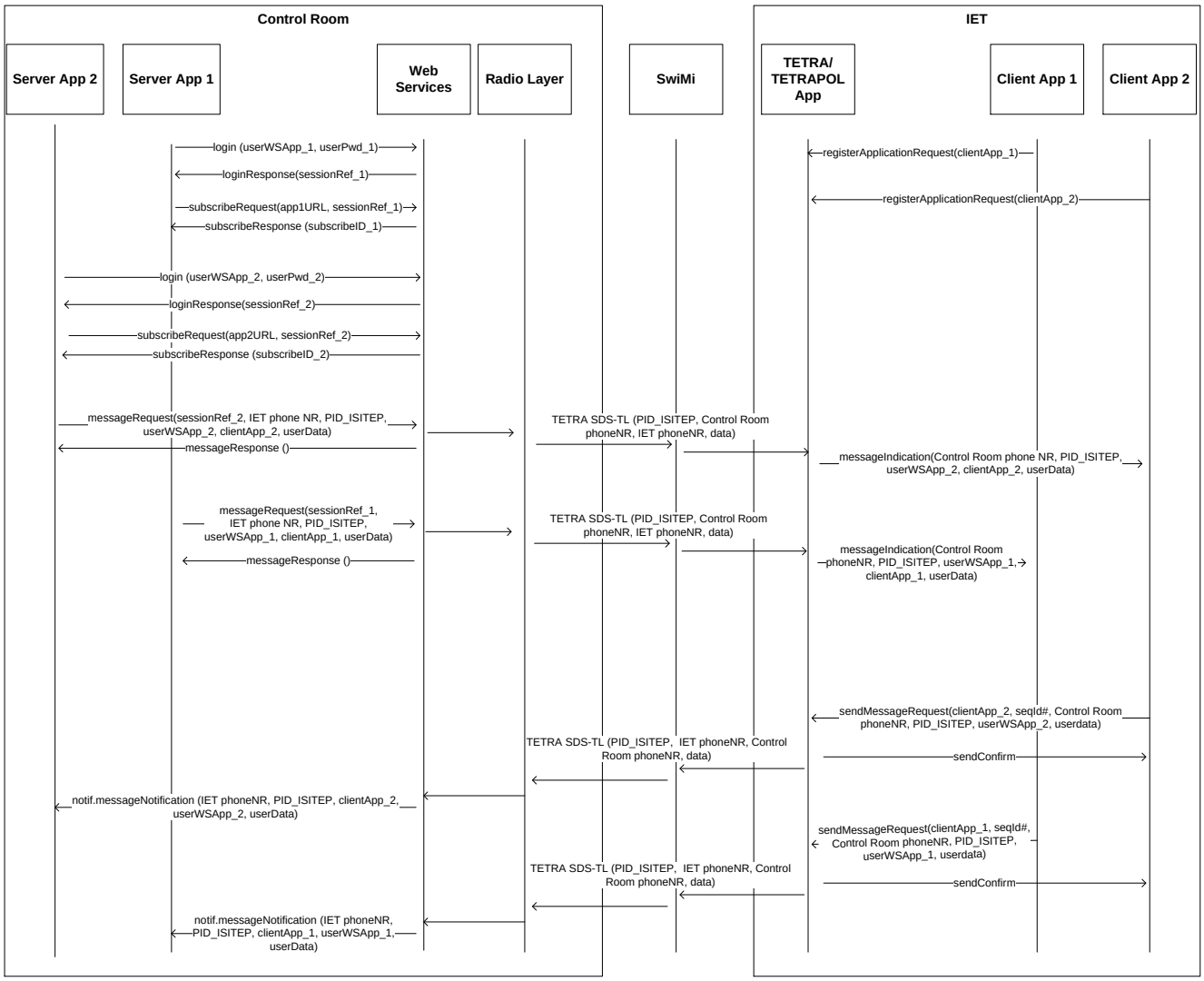

Figure 8: Client-Server End-to-End message delivery

5 ISITEP PPDR CLOUD ADDED-VALUE APPLICATIONS DESIGN DESCRIPTION

In this chapter, the SW architecture of the ISITEP PPDR cloud added-value applications server-side and the corresponding client-server end to end application protocols is described.

The descriptions of SW architecture of ISITEP interoperability enabling applications, Workflow Manager (WFM) and of Semantic Syntactic Translator (SST) are reported respectively in D5.4.2 [8] and in D5.5.3 [9].

5.1 Dynamic Functional Numbering

Dynamic Functional Numbering is a service that allows identify the number used by PPDR resources in charge of a mission in a specific area. When a terminal moves from one country to a neighboring country in order to perform an international PPDR operation the Dynamic Functional numbering automatically updates the address book containing the international talk groups used in the visited country.

The DFN application is entirely realized on the terminal side, please refer to D 6.4.2 [10] for details.

5.2 Location Dependent Addressing

In each country, for each PPDR force there are many operational centers, typically each one is responsible for a certain geographical area. It would be very difficult for an end-user to address its call to the right center using a different telephone number for each area in which he may move. Usually PPDR networks provide the network capability to address properly this kind of calls providing special numbers (functional number) mapped to the different operational center using the Location Area where the calling party is registered. This solution is limited by the relative imprecision bounded with the use of Location Areas; therefore we propose the use of GPS.

The goal of the ISITEP Location Assisted Numbering application is to provide functional numbers to contact the proper PPDR operational center using the GPS position of the terminal instead of the Location Area position.

Scope of LDA application is providing a mechanism to map functional numbers to geographical areas based on the GPS position of the end-user.

5.2.1 LDA Server Application

The LDA Server Application provides the capability to assign a number of an operational center to a certain geographical area.

The cartography used is based on geospatial vector data. In particular the adopted cartographic approach is based on the use of GeoSets that are datasets composed by standard maps of the same geographic region that convey different type of information. In more details, each map can be personalized based on four basic types of features:

- Regions: closed objects that cover a given area (i.e. country boundaries);
- Point objects: represent single locations of data (i.e. user location);
- Line objects: open objects that cover a given distance (i.e. streets);
- Text objects: text that describes a map or another object, such as labels and titles.

In this context the cartography management system is mainly a standalone solution that allows users to explore spatial data within a dataset, symbolize features, and create maps, but is open for integration with external data sources.

The main interface (shown in Figure 9) is composed of a cartography on which the cartographic levels representing the various entities managed by the system are arranged (positions of the vehicles, polygonal lines, etc.). There are also two toolbars, an upper one and a left-hand one, for accessing the main software functions.

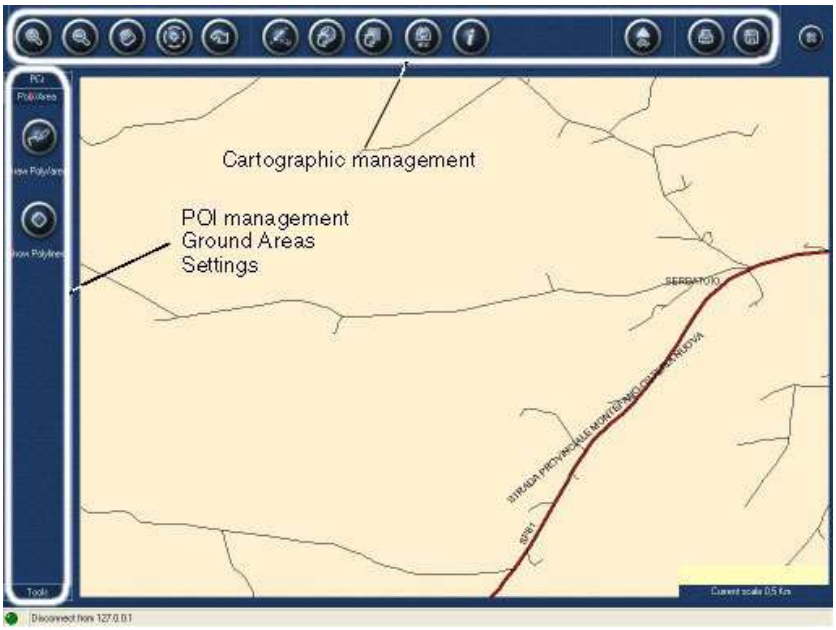

Figure 9: LDA Server Application Interface

The macro functions of the program are the following:

- Settings;
- Cartographic management;
- Polylines and guard areas management.

All the cartographic functions are accessible on the upper toolbar, while program settings are accessible on the left-hand toolbar.

The LDA Server Application receives the GPS position by the IET and tracks on the map its position, on the other hand it is possible to manage polygonal lines and the areas displayed in cartographic layers; it is foreseen that the LDA Server application sends an SDS to a certain IET upon the entry or exit of the IET from a polygonal area. The SDS will transport using the LDA-protocol the telephone number of the operational center related to the area where the IET is entered.

As a proof of concept there will be only one geographical subdivision of the territory and only one telephone number will be assigned to each geographical area, but the concept in the future could be extended assigning to each geographical area more than one telephone number, or also providing more different geographical subdivisions of the territory.

As a pre-requisite, the IET shall use the LDA Application server as localization system in order to send to the LDA Application server its GPS position using the LIP protocol.

5.2.2 LDA protocol

The LDA Server periodically receives the position of the MS through the TETRA LIP position messages, Cfr. [3] clauses 29.4.3.9 and 29.5.12 and Cfr. [4]. When the LDA Server detects that the MS has moved into a new operational the LDA Server sends to the LDA client a TETRA SDS containing the reference group SSI for the current operational area.

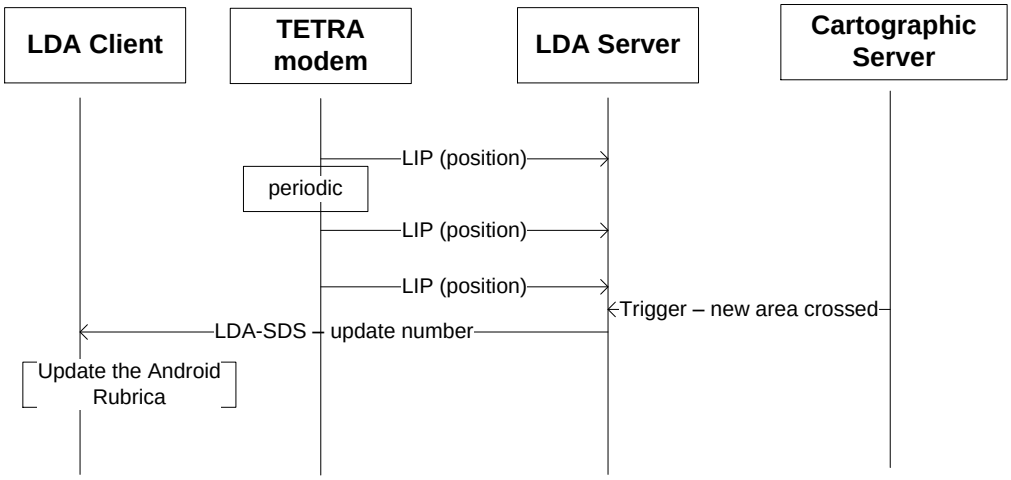

Figure 10 LDA Message Sequence

5.2.3 Message Content

The LDA-SDS update number is the LDA message transported over TETRA SDS that provides the telephone number for the operational centre responsible for the geographical area where the MS is located.

Name	Value	Note
AppProt	1	LDA
MessID	1	Update Number
Service	String	Talkgroup Name
MCC	<0 … 999>	Destination MCC [6]
MNC	<0 … 9999>	Destination MNC [6]
SSI	<0 … 16777215>	Destination SSI [6]

Table 1: LDA message content

5.3 Enhanced Message Exchange

During PPDR operations, unexpected emergency scenarios shall be faced by resources belonging to different PPDR organizations. Unexpected emergency scenarios may require PPDR joint action outside the pre-established patterns of a standard workflow. Often in this kind of emergency situations, it is not clear how the emergency should be faced and the solution may be clear to some skilled persons but not to the entire PPDR organization. In this context, it would be very helpful if the useful information could be disseminated quickly and efficiently to the involved PPDR forces.

In an international context, the language barrier is an issue for fast and efficient communication. In this context, one of the ISITEP project goals is to reduce language barriers in PPDR operations by deploying an Enhanced Message Exchange application.

The Enhanced Message Exchange application shall be used to provide written communications (i.e. orders or information) to the PPDR resources, which shall be translated into the proper language of the end-user. This application would help in overcoming the language barriers in international PPDR operations, where intervention teams may be composed by PPDR forces that speak different languages. Moreover, it has been verified that, often in the PPDR operations, there is high background noise that prevents from speech understanding. Therefore, written communications also in this case could help in improving understanding.

Written communications shall be "real-time" translated by a server application after the source and destination language have been detected.

Enhanced Message Exchange application exploits the translation services exported by the Semantic and Syntactic Translator (SST).

For security reasons, only authorized end-users in charge for providing communications to a specific PPDR forces shall be allowed to send written communications using the Enhanced Message Exchange application to the relevant PPDR group.

5.3.1 EME Server Application

The EME application is composed by an authentication center deployed on the server side and by an EME client deployed inside the IET.

Only those user authenticated to the EME authentication center are enabled to send EME messages while all users are able to receive translated messages using the EME application.

In this paragraph it will be described the EME authentication center (AuC), while for the EME client application design description refer to D 6.4.2 [10].

The EME Server application provides AuC capability with digest authentication based on a pre-shared secret and MD5 algorithm. For each user the EME AuC stores the username and the relevant pre-shared secret, during the authentication phase the EME AuC generate an unpredictable value used to prevent replay attacks (nonce). The EME AuC calculates the digest value of the nonce and at last check it with the response received from the EME Client.

EME authentication is transported over short data messages exchanged between the EME Client and the EME Authenticator.

5.3.2 EME Protocol

As described in the previous paragraphs, in order to be able to send messages, the EME client deployed in the IET shall be authenticated to the EME Server. In Figure 11 the authentication message sequence has been represented.

The authentication is based on a pre-shared secret stored both in the EME client and in the EME Server. When the EME Server receives the authentication request, it sends to the client the nonce and both client and server calculate the digest of the exchanged nonce. The client sends in the response the calculated digest and the Server compares the digest calculated by the client with the digest calculated internally; if they correspond, the authentication succeeds, otherwise the authentication fails.

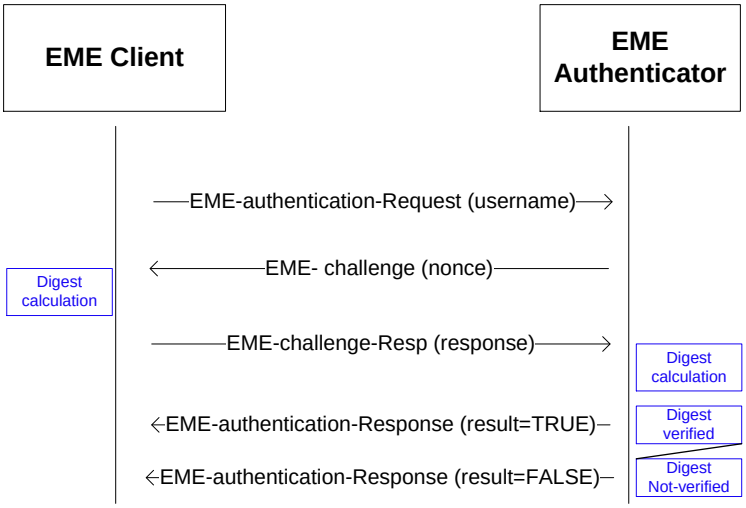

Figure 11: EME authentication

5.3.3 EME Message Content

In Table 2-5 the composition of the messages exchanged between the EME client and the EME Server during the authentication procedure described in the previous paragraph is reported.

Name	Value	Note
AppProt	2	EME
MessID	1	Authentication Request
UserName	String	UserName

Table 2: EME Authentication Request

Name	Value	Note
AppProt	2	EME
MessID	2	EME-Challenge
nonce		An unpredictable value used to prevent replay attacks.

Table 3: EME Challenge

Name	Value	Note
AppProt	2	EME
MessID	3	EME-challenge-Response
response		The calculated checksum expressed as a string of 32 hex digits.

Table 4: EME Challenge Response

Name	Value	Note
AppProt	2	EME
MessID	4	Authentication Response
Result	TRUE/ FALSE	Boolean if true the EME Client authentication succeeded

Table 5: EME Authentication Response

6 REFERENCES

[1] D5.1.1 Enhanced Terminal Requirements
[2] ETSI-TS 300 392-5 V2.2.1 - TETRA – Voice Plus Data (V+D) and Direct Mode Operation (DMO) – Part 5: Peripheral Equipment Interface (PEI).
[3] ETSI EN 300 392-2 V3.4.1 - TETRA – Voice Plus Data (V+D) – Part 2: Air Interface.
[4] TS 100 392-18-1 - TETRA – Voice Plus Data (V+D) and Direct Mode Operation (DMO) – Part 18 air interface optimized applications – Sub-part 1 Location Information Protocol (LIP)
[5] RFC 1321 - The MD5 Message-Digest Algorithm
[6] ITU-T Recommendation E.218 - Management of the allocation of terrestrial trunk radio Mobile Country Codes
[7] BCP-47 – Tags for identifying language
[8] D5.4.2 Workflow manager design description
[9] D5.5.3 Semantic/syntactic translator engine design description
[10] D6.4.2 PPDR Client Applications Design Description