ISITEP

D8.5.3 – Second detailed Report On Security, Integrity and Availability

Document Manager:	Federico Frosali	SES	Editor

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

Document ID N°:	ISITEP_D8.5.3_20150921_V1.0	**Version:**	V1.0
Deliverable:	D8.5.3	**Date:**	21/08/2015
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Federico Frosali (SES)
Approved by (WP Leader):	Federico Frosali (SES)
Approved by (SP Leader):	Paolo Di Michele (SES)
Approved by (Coordinator)	Paolo Di Michele (SES)
Security Approval (Advisory Board Coordinator)	Etienne Lezaack (BFP)

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
All the partners	All the company	Contributor

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
V1.0	21/09/2015	All	All	First issue

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Terms and acronyms

Abbreviation	Definition
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPR	Intellectual Property Rights
ISITEP	Inter System Interoperability for TETRA_TETRAPOL Networks
PPDR	Public Protection & Disaster Relief
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
IP	Internet Protocol

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Publishable extended abstract

Traditionally, information security focuses on the simply called “C-I-A”:

- **C**onfidentiality: The property that information is not made available to unauthorized individuals or entities.
- **I**ntegrity: The property of safeguarding the information accuracy and completeness.
- **A**vailability: The property of information to be accessible and usable upon demand by an authorized entity.

In ISITEP context, in order to accomplish the necessity of Confidentiality, Integrity and Availability of documents, an appropriate document management system, tracking and storing project documents, characterized by a set of desiderata characteristics, e.g. support to identification, authentication and authorization of users, secure communications, availability, multi language, etc., shall be adopted.

Moreover, the nature of ISITEP project and the presence of several international project-partners, working together to the various tasks, leads to the necessity of a collaborative working tool, for the cooperation and for the work coordination. The use of an effective collaborative tool reduces increases the communication simplicity and efficacy and reduces the needs of time-and-money expensive and international meetings.

To accomplish to these some possible candidates should to be evaluated to choose the most suitable for ISITEP project needs.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

CONTENTS

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

1 INTRODUCTION

The information management is an essential part of good project governance and assumes particular relevance in international project for PPDR networks such as ISITEP.

Traditionally, information security focuses on the simply called “C-I-A”:

- **C**onfidentiality: The property that information is not made available to unauthorized individuals or entities.
- **I**ntegrity: The property of safeguarding the information accuracy and completeness.
- **A**vailability: The property of information to be accessible and usable upon demand by an authorized entity.

.

Figure 1: The three concepts guiding the information security and data management procedures

These three aspects are analysed in the following sections.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

2 DATA CONFIDENTIALITY

Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.
A correct confidentiality management shall assure information accessibility to “the right people” and protect data from the “wrong people”.
Although accurate precautions can be taken to avoid an unauthorized user accessing information, it is extremely difficult to determine if legitimate users are doing something malicious. Therefore, the first layer securing sensitive data is preventing unauthorized individuals from accessing sensitive information, allowing the access on information just to trusted users, really needing it for their work.
Defining and applying policies and processes for who is authorized to access/edit/review/approve specific documents is of paramount importance for the project.
Therefore, there are needed powerful authentication methods, like user-ID and password, uniquely identifying a data system user and supporting control methods that limit each identified user access to the data system resources.
Confidentiality is related as well to the concept of data privacy, as the capacity of limiting access to individual personal information, and to Intellectual Proprerty. Privacy legislation requires that personal information be protected and not accessible from others. Intellectual Property Rights (IPR) express the right of creation and property of mind products. In a research project, they are related to foreground of research activities that can be produced by single or multiple parties in cooperation. Both issues, privacy and IPR, are strictly bounded with ethical and legal norms, arguments of WP85.1.
“Confidential Information” may include all non-public documents, project plans, processes, methods, inventions, studies, know-how, and other information disclosed or developed within the ISITEP framework or in tight connection with the project.
Main mechanisms of protection of confidentiality in information systems are cryptography and access controls, both functions are required for the tools to be used in the framework of ISITEP project (see section 5-6-7).

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

3 DATA INTEGRITY

Integrity concerns the trustworthiness, completeness and correctness of information, granted by the prevention of improper or unauthorized modification of information. Integrity in the information security context refers not only to integrity of information itself but also to the origin of the information source.
Integrity ensures that information cannot be modified in unexpected ways, and refers therefore to the trustworthiness of information resources.
Loss of integrity results from a human error, intentional tampering, or unexpected event.
Inaccurate information can become useless or even dangerous, in particular for a project regarding sensible topics as PPDR networks.
A key driver of project success and achievement of its goals is the execution of strategic decisions based on reliable data and the secure storing of activities results.
Every partner involved in project-related activities should be aware of data-integrity importance and should support it responsibly. The complete set of “project data” refers to all information collected, stored, and processed in a systematic manner to meet the objectives of ISITEP project.
The accuracy and consistency of stored data is indicated by an absence of any alteration in data between two updates of a data record - namely, that data have not been changed inappropriately, whether by accident or deliberately malign activity. Data shall therefore be protected from unintended activity, which can include misuse, malicious attacks, inadvertent mistakes, and corruption made by individuals or processes, either authorized or unauthorized.
Integrity is strictly related to how data are disseminated and stored, is therefore need a reliable software/service for data delivery and storing, responding to the security characteristic of ISITEP project. It also includes the concept of "origin" or "source integrity"; this last issue is more bound with data confidentiality and with accounting to storage services, which shall trace the origin of data, where actually came from and the person or entity producing them.

During the project, every version of documents shall be saved, with the possibility of tracking the document lifecycle and restoring/recovery previous versions of a document, if needed.
Integrity protection may be achieved by preventive mechanisms, such as access controls that prevent unauthorized modification of information, and detective mechanisms, which are intended to detect unauthorized modifications when preventive mechanisms have failed. For ISITEP project both mechanisms shall be implemented, giving by the way priority to the preventive ones.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

4 DATA AVAILABILITY

Data and information should be readily accessible to those who need them or those who are given permission to access them. Restricted availability prevents resources from being deleted or becoming inaccessible, e.g. due to attacks against computer systems aimed to disable data access or to steal the data. Limiting access to critical data sources can eliminate accidents and internal mischief; various types and differentiated levels of access needed and as deemed appropriate.
Documentation describing documents changes, versions, or data is critical for ensuring that datasets are useable well into the future. Data longevity is roughly proportional to the comprehensiveness of their documentation. All datasets and project-deliverable should be identified by a unique code (corresponding to the ones related to the working tasks) and documented to facilitate their subsequent identification, management and use, and to avoid the duplication of the same deliverable more than once.
The main goals of activities for data availability are:

- ensuring the longevity of data;
- ensuring that users understand the content, context, and limitations of documents;
- facilitating the research of documents;
- facilitating the interoperability of project-partners in data and deliverables exchange.

A good storage and versioning framework should provide the access to information for both users in their office and for users in mobility, e.g. through a web-based interface.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

5 CONSORTIUM AGREEMENT FOR IPR

Project activities and its outcomes are subject to precise property and dissemination regulations that shall be ratified in a Consortium Agreement, aimed to establish in detail the rules on the internal management of the consortium.
In this document, the partners agree the terms to co-operate in order to execute the ISITEP project according to the Grant Agreement; this agreement shall propose additional rules on dissemination, use and access rights.

5.1 MAIN IPR ISSUES TO BE ADRESSED

Part of the Consortium Agreement have to define publication and usage policies of IPR sensitive materials.
The document shall define guidelines and rules for the use of all the backgrounds provided by project partners for the developing of ISITEP project. These background material means all patents, software copyright, database rights, and any other intellectual property rights (excluding of course the Foreground), owned by any of the project parties, in the field and which are necessary for the exploitation of Foreground IPR.
Also the rights on the Foreground material shall be clearly described. These material means all possible patents, software copyright or any other intellectual property rights arising as a direct result of the ISITEP project.
In particular, within the other wide issue related to other aspects of the project, the Consortium Agreement document should contain:

- Information about foreground and background material provided by each partner for the ISISTEP project;
    - the property of each foreground/background (to partner or group of partners that produced it or whole consortium) and the way to assign it to partners
    - how to proceed for sharing of foreground/background between partners;
    - publication and dissemination guidelines (e.g. if a partner can public foreground of others without permission or if results can be disseminated after the end of the project and under what conditions);
    - access Rights for Use of Foreground owned by another Party
- Information about foreground and background software.
    - agreement about the Source Code Access for carrying out their Workshare within the Project.
    - guidelines about right/prohibition of make foreground/background software available to third parties
- Right aspects about Object Code and Source Code, specified by a traceable agreement specifying and protecting the proprietary rights of the Party or Parties concerned.
- Procedures for dissemination of publications and press releases relating to the Project
- Confidentiality rules for accessing the IPR sensitive material
- Guidelines for the use and/or the integration of Open Source Software
    - production and development of code dependant by other Open Source software
    - guidelines for dissemination of code to be distributed under Open Source licences
    - security responsibilities of partner integrating Open Source Code in the produced Software

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

6 DOCUMENT MANAGEMENT TOOL

In order to accomplish the necessity of Confidentiality, Integrity and Availability of documents, an appropriate document management system, tracking and storing project documents, shall be adopted. Various software and frameworks are available on the market, and a set of desiderata characteristics for the candidate tool have to be identified for choosing the most suitable for ISITEP project.

Following sections resume main functions and technological security measures to be present in the used document management system.

6.1 MANDATORY FUNCTIONS

6.1.1 IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

Protecting resources, data and documents is mainly related with verifying the identity of the person trying to access them.

For a complete access control, an affective document management system shall be able to correctly identify, authenticate and authorize users.

Users ID for project partners and people directly working on documents have to be unique, clearly linkable to people authorized to use it.

The tool to be used in the framework of ISITEP project shall support users access control, e.g. managing them with usernames and passwords or with digital certificates.

After their identification users shall be treated differently, considering their role and the authorization they own for read/modify documents. Once the identity of a user has been verified, the security system needs to control what information the user is allowed to read, write, update, create, and delete.

For some tasks or particular project's documents, it can also be used a role-based access control model: rights and permissions can be assigned to roles instead of individual users. This added layer of abstraction permits easier and more flexible role administration for task where a large set of user are participant and documents edited by several project partners.

6.1.2 SECURE COMMUNICATIONS

If a web-based document management tool will be chosen, TCP/IP will surely be the primary transport protocol used in the client/server dialog, and governing the transmission of data over the Internet.

TCP/IP uses intermediate computers to transport data hop by hop, from sender to recipient. The intermediate computers, especially if exposed on the internet, may introduce weak links to the communication system; there is therefore needed the use of specific security mechanisms, as Encryption, and technologies, as Secure Sockets Layer (SSL), for ensuring the correct treatment to all sensible documents.

The servers of the document management system and web browsers running on users PCs can rely on the SSL protocol to allow users protecting their data by creating a uniquely encrypted channel for private communications over the public Internet during the document transfer toward the document management system. Each SSL Certificate consists of a key pair as well as verified identification information.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Hypertext Transfer Protocol Secure (HTTPS) is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL protocol, adding its security capabilities. The main motivation for HTTPS is to prevent wiretapping and man-in-the-middle attacks.

6.1.3 AVAILABILITY

The document management system, used for the ISITEP project, shall be implemented over secure server or clouds, with redundancy, in order to obtain high availability of data and low probability of malfunctioning.

Documents shall be maintained over servers or clouds, reachable by all partners through network connection.

6.1.4 ACCOUNTABILITY AND LOGGING

The document management system to be use for the ISITEP project should take into account the possibility of tracing actions and events back in time. Also the user that performed actions shall be identifiable by its own unique account, to establish responsibility for actions, modification or deletion.

Main or important actions may be logged in the system.

6.2 ADDITIONAL DESIDERATA

6.2.1 PREVENTIVE AND DETECTIVE CONTROLS

Security efforts to assure confidentiality, integrity and availability can be divided into those oriented to prevention and those focused on detection. The document and information management systems used for ISITEP should employ both. Preventive controls try to prevent security violations and enforce access control. The latter aims to rapidly discover and correct for lapses that could not be, or at least were not, prevented. They come into play when preventive controls have failed or have been bypassed and include cryptographic checksums, file integrity checkers, logs and other mechanisms.

Detective controls may be extended with:

- Corrective check: try to correct the situation after a security violation has occurred
- Recovery procedure: try to recover after a security violations and to restore information to previous version.

6.2.2 ALERTS

Important actions and main modification on the documents may be notified to relevant users by e-mails or alerts. The document management system can be used also as dissemination platform, advising all the relevant users about the presence of new or updated documents.

6.2.3 MULTIPLE LANGUAGES SUPPORT

The use of the document management system in an international framework, suggests the choice of tools available in multiple languages. The used language for all communication between partners is

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

English, and the main interface of the document management toll shall be in English, but users may be interested in having a personalized web interface in their mother tongue.

6.2.4 INTEGRATION

In order to make the users' cooperation more effective the chosen document management tool may be integrated with other tools providing additional functions, as mailing lists, shared calendar, alerts, project management tools etc…

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

7 MEETING PLATFORM TOOL

The nature of ISITEP project and the presence of several international project-partners, working together to the various tasks, leads to the necessity of a collaborative working tool, for the cooperation and for the work coordination.

The use of an effective collaborative tool reduces increases the communication simplicity and efficacy and reduces the needs of time-and-money expensive and international meetings.

7.1 COMMUNICATIONS TOOL NEEDED FUNCTIONS

7.1.1 GROUP COMMUNICATIONS AND MESSAGING

An effective meeting platform allow the partners synchronizing their activities in frequent group calls, waiting for the periodic project joint events. The primary use of a digital meeting platform application is to allow partners to discuss together as in a face to face conference. The software shall permit the instauration of single and group calls, with the optional distribution of webcam video, blackboard or group chat, images, files.

7.1.2 USERS IDENTIFICATION

Users participating to a call shall be identified by a unique ID, which can be for example their user name, or the IP addresses of the machine used for the conference.

7.1.3 PC SCREEEN SHARING

Compared with a classic telephonic call-conference, an application or a web browser-based tool has the big advantage of allowing users to share their PC screen with partners.

This functionality can be used for share presentations or jointly use programs and applications.

7.1.4 COMMUNICATION SECURITY

In order to guarantee the communication security, the chosen software shall create SSL certificates for each remote desktop session, used to cryptographically secure the communications between the remote desktop and the accessing computers.

The used software should moreover implement authentication and user identification mechanisms, similarly to the one present in the document management system (see sections 6.1.1 and 6.1.2).

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

8 CHOSEN SOFTWARES

The set of available software for document managing and for realizing a virtual meeting platform is very large.

Considering the needed characteristics and the desiderata for the project, two software have been chosen, responding to most of the required functions: “EMDESK” for the document management and “join.me” as meeting platform. Following sections better describe the two software.

8.1 EMDESK

EMDESK is web-based software for project management conceived to support all the phases of the project, from proposal preparation, drawing up project plan to project implementation, controlling project progress respect to planning. Additional interesting features of this platform deals with communication and collaboration between project partners that is facilitates through tools e.g. mailing lists, shared calendar and a document manager.

8.1.1 DOCUMENT MANAGER

Document manager supply a secure online repository that allows document management and sharing.

All project documents are organized in a folder structure defined by user. Folder can be created, renamed, moved or deleted. Specific permissions can be defined on files, folders or sub-folder on a user or group basis. Sub-folders and documents inherit the access right settings from the parent folder.

The top folder restrictions overrule contained settings. In addition the permissions for sub-folders and documents can be further restricted. Users with Coordinator Right have top-level access to the document manager that implies read/write access to all folders and documents regardless other defined permissions. Upload and removal process can be done on single or multiple file at time, or on entire folders (by users that hold permissions).

A document can be stored in multiple versions. To prevent access collision on a document a Check-Out (lock) /Check-In (unlock) function is available that enables all users to lock editing/updating of certain document versions from other users during an editing process.

Some document properties such as title, folder and description of files that has not been locked can be modified directly from document manager.

Search functionality permits to retrieve files by name, description or keywords related to file name. Filter and Sort act on document view filtering by a tag or sorting by ascending or descending date.

Activities in the document manager as newly uploaded document or version can be notified through emails.

It is possible to share documents stored in EMDESK with no-EMDESK users, through a public link (e.g. inserting it into an email or in a web page). Anyone who has the link can access and download the file just clicking on it without a login. The link points automatically to the latest version of document also if it has been modified after the link creation. The link has to be activated before use and can be deactivated. It points only to the document and no other resources can be reached from it.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

8.1.2 SHARED PROJECT CALENDAR

This functionality permits to share a project calendar between member of consortium to schedule, keep track of project events (e.g. meeting, deadline of milestones or deliverable). New, upcoming or changed events are automatically notified via email.

8.1.3 GROUP, MESSAGING AND CONTACT ADMINISTRATION

Group administration feature enables the organization of the project members in groups in order to facilitate communication and cooperation. A group can be composed of an unlimited number of member chosen between project users or external members. Groups can be used to define permissions or specific roles in the project regardless the users that cover theme. Together with groups also mailing list can be created to facilitate communications using an unique email address for multiple users. In EMDESK an internal messaging tool is available that enables user-to-user and user-to-group messaging and discussions. Message composition, replying, single and group contact managing, document attaching actions are performed directly from EMDESK interface. The framework provides an address book to keep all contacts organized, to brows groups members shoving users and contacts, to export contacts via vCard file format.

In addition a forum tool can be used in alternative to emails to facilitate the discussion about topics that can interest several users.

8.1.4 EMDESK SECURITY

Data security is guaranteed since all data are stored on a secure servers with daily automatic backups and 99% declared uptime. Data can be recovered for up to 7 days back. Data storage is performed in multiple location so that they can be retrieved even in case of multiple server disruptions or disasters. This guarantees data availability. Moreover, since no applications have to be installed on PCs, but the access is performed via web through an application regularly updated, complete compatibility with operating systems, fully availability and robustness are guaranteed.

Information exchange between local PCs and servers are performed only via a secure SSL connection with a 256-bit encryption. The access to project is possible only on explicit invitation. To the sake of maintain confidentiality the access to the project data, authentication procedure has to be performed with unique user names and strong password, moreover a procedure of automatic logout is foreseen for users that are idle for more than 60 minutes. More information can be found in [1].

8.1.5 DESIDERATA ACCOMPLISHMENT

Following table resumes how the EMDESK software respond to desiderata characteristics for the document management tool in the framework of ISITEP project.

Characteristic	Yes/No	Note
Identification, Authentication, Authorization	Yes	Access through login, permission and group management
Secure Communications	Yes	SSL connection and data

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

		encryption
Availability	Yes	Redundant data storage, daily backup
Accountability and logging	Yes	
Preventive and detective controls	Yes	
Multiple languages support	Yes	
Integration	Yes	
Alerts	Yes	Messaging tool

Table 1: accomplishment of desiderata for the document management tool

8.2 JOIN.ME

join.me is an online meeting and screen sharing service. In professional version, here described, the access to join.me services are subordinated to a registration. This tool permits to a user to start a meeting and share his screen (or a specific windows). A scheduler tool permits to set up single or recurrent meetings and send invitations compatible with iCal and Outlook. The maximum number of participant to a meeting is 250, no limits are fixed for duration and number of meetings.

The meeting can be performed via a browser or via a desktop application that permits to start the communication in an easy and quick manner, also an app for mobile devices is available that permits to join the meeting but not to share the screen, only version for iPad allows to present files.

The meeting joining can be performed through a direct link that can be reached from a browser or a multi-digit code to be typed in join.me desktop or mobile applications, both created at the meeting scheduling and shared by the presenter.

During the presentation, participants can send files to other participant or to presenter. It is possible to perform audio conferences through a phone line (using both local and international numbers) or via internet-based VoIP technology inserting the meeting link in the mobile or desktop application. The meeting (or a portion of it) can be recorded in an audio or video file and the presenter can allow a participant to take the control of his PC. join.me includes a chat tool to send messages to one person at a time or all participants simultaneously. In addition, the application permits to automatically generate reports of the meeting containing the follow information:

- Presenter name: the name of the presenter in your pro account who organized the meeting.
- Presenter email: the email address of the meeting organizer in your pro account.
- Host IP: the IP address of the organizer's computer.
- Meeting subject: the subject of an invitation to a scheduled meeting. Only available for one-time code meetings. Not available when you use your personal link.
- Meeting code: the 9-digit meeting code that participants use to join the meeting.
- Start time: the time when the organizer started the meeting.
- Duration: duration of the meeting from the time when the organizer started the meeting to the time when he ended it.
- Number of participants: the number of participants, including the presenter, who joined the meeting.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

- Features used: a list of features used during the meeting: remote control, file transfer, chat, laser pointer, annotation, presenter swap, audio, or window share.

8.2.1 SECURITY IN JOIN.ME

How security, confidentiality and reliability is addressed in join.me application is described in [2] and [3].

join.me application is basically a web application, whose hardware and software main components are the presenter software that constitutes the interface for the presenter. It connects to an application server that establish a session interacting with a database where all information are stored. Information about the session are then relayed to viewer application. When the session establishment is completed, application server acts as intermediate to data communication (e.g. images, messages, voice) between presenter and viewers, interface between user browser and application core is managed through a web server.

To ensure the service reliability and availability, the server architecture is characterized by an high level of redundancy. In particular it is composed of four datacentres; one of theme hosts the active database that is the core of application. A passive database is instead hosted in another datacentre and acts backup in case of active database failure. All datacentres are interconnected each other's with a VPN mesh and host the applications servers and webserver. The choice of application server to be used is performed on the basis of availability, geographical proximity and load. Viewers are connected to the same application server of the presenter that maintains session state information. If the an application server or a datacentre goes offline or becomes unreachable the session is migrated to another within seconds without service interruptions.

Security of communication is obtained through:

- Authentication of parties
- Confidential exchange of messages
- Detection of compromised messages

Join.me communication are secured via SSL. Key exchange is performed via RSA protocol and encryption is AES256. Data exchanged between presenter and viewer such as images, files, etc. are not stored on servers except if the recording feature is enabled.

Session code is used to identify session and users that connect to it. It is a 9 digit code that is reused after the session is expired. A static code (i.e. static link) can be chosen from a user to all its meeting. It is longer that session code (up to 127) to minimize the possibility of to be guessed. If static code is used for a session each viewer has to be approved from presenter.

Characteristic	Yes/No	Note
Group communication and messaging	Yes	
User identification	Yes	Direct link or multi-digit code
PC screen sharing	Yes	
Communication Security	Yes	Datacenters redundancy, SSL communication and RSA

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

		encryption protocol

Table 2: accomplishment of desiderata for the digital meeting platform

9 USE OF CHOSEN TOOLS AT M24

This section describe how the two chosen software, “EMDESK” for the document management and “join.me” as meeting platform, have been used in first 24 month of the project: what of the previous described functionalities have been used and how project guidelines have been accomplished.

9.1 EMDESK

ISITEP project is identified on EMDESK platform with Project ID 312484(v3). Currently (July 2015) 70 users from 18 Contractors are active, under the coordination of Selex ES.

Users are identified by a unique user-name and accesses are verified though a personalized password.

It is possible to access EMDESK repository of ISITEP project in general EMDESK webpage (https://emdesk.eu) or directly through the form on the right of ISITEP website (http://isitep.eu/).

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

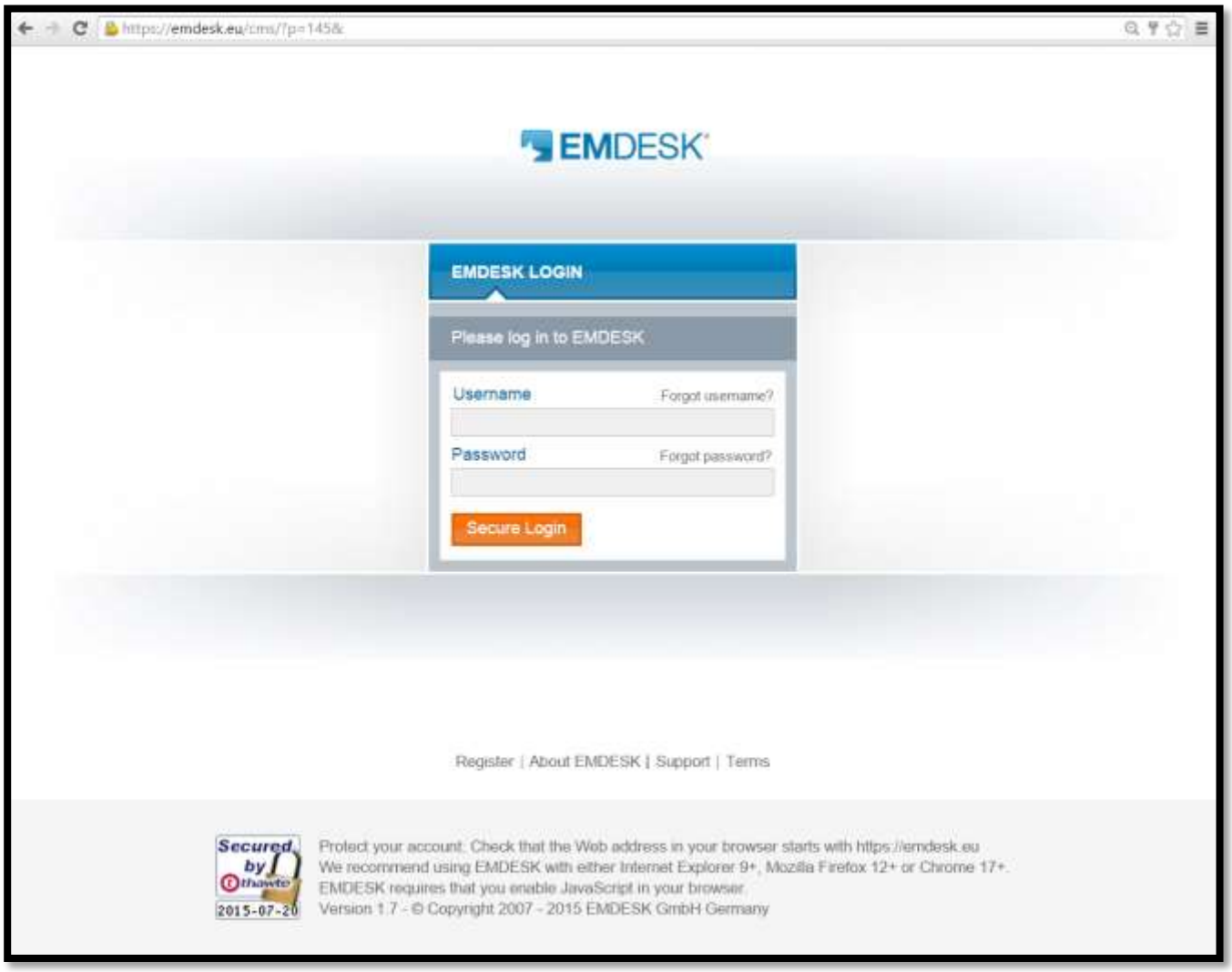

Figure 2: The EMDESK access page; the login data are sent through HTTPS protected connection

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

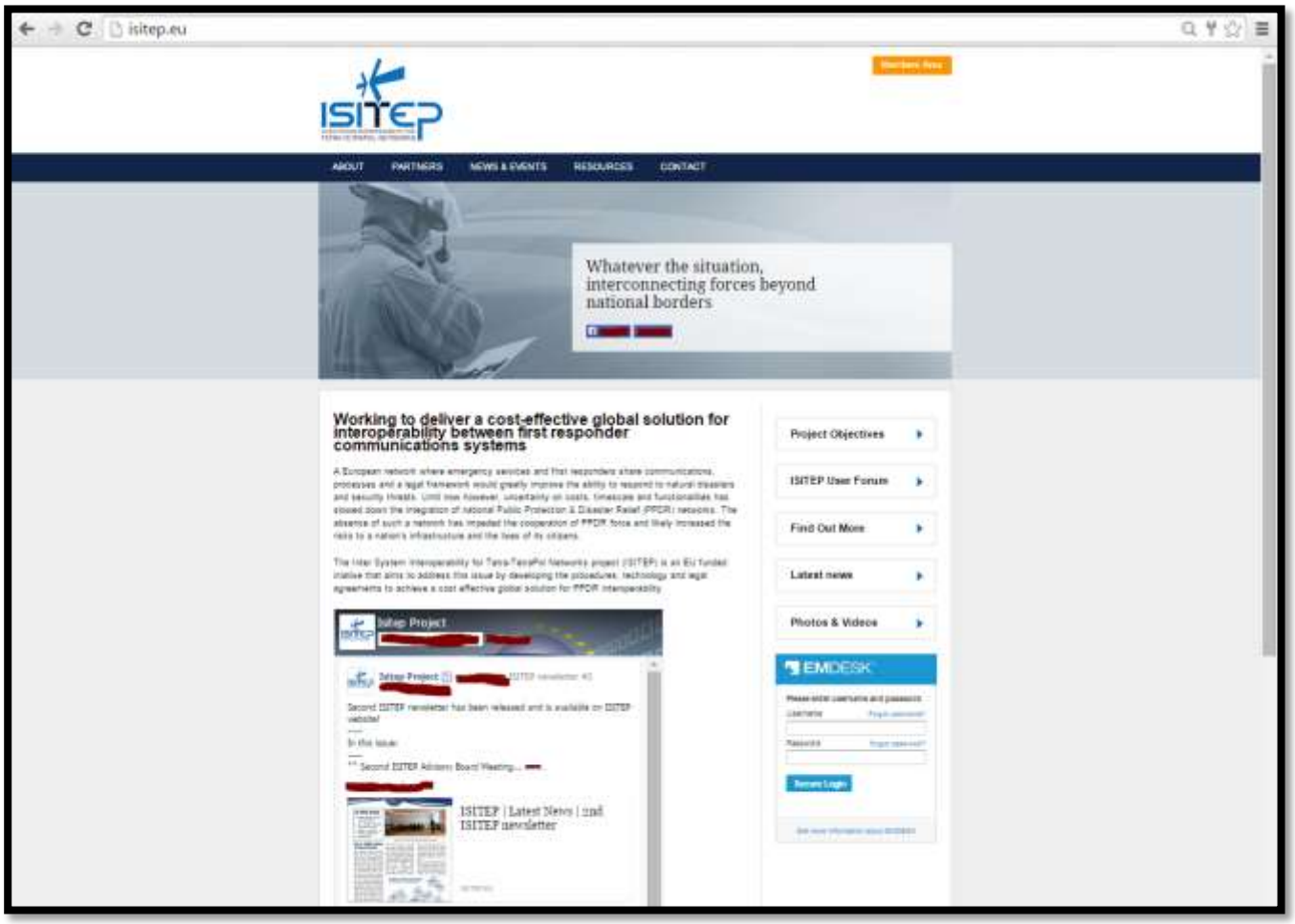

Figure 3: The EMDESK access form direct from ISITEP web page

Users access is protected through the use of HyperText Transfer Protocol over Secure Socket Layer (HTTPS); information exchanged between the computers and EMDESK servers are securely managed with SSL (Secure Sockets Layer) connection (256-bit encryption).

Inside the EMDESK homepage of the project it is possible to monitor the users currently online, last access of offline users. This helps to control the access on EMDESK and identify possible misuse.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Figure 4: EMDESK users list shows how is online and last access of all users.

When users finish their activities on EMDESK it is recommended to log-out.
For security reason EMDESK sessions last anyway for a limited period. After less than 60 minutes of inactivity, sessions are automatically closed and user have to re-enter its credentials to access EMDESK again. A countdown on the right-bottom of the webpage shows to the user the time left before the automatic logout.

Figure 5: The bottom bar of EMDESK webpage show a countdown for log inactive users off.

EMDESK web based software have been chosen since its accomplishment to eight main characteristics/functionalities requested by the project.
Following table reports if and how these characteristics have been actually used in first two years of the project.

Characteristic	Used	Note
Identification, Authentication, Authorization	Yes	Access through login, role and permissions related to the username, users identification and action logging.
Secure Communications	Yes	SSL connection and data encryption. EMDESK website access only admitted trough HyperText Transfer Protocol over Secure Socket Layer (HTTPS).

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Availability	Yes	EMDESK redundant data storage. No issue identified so far.
Accountability and logging	Yes	Each user is identified with an account. Accounts are distributed and managed by ISITEP project coordinator. Users' actions (documents upload, change, update) are logged by EMDESK software.
Preventive and detective controls	Yes	Only registered user are allowed to access EMDESK and their credentials are sent through the internet using https protocol. This prevent the unwanted access to EMDESK platform. Users' activities and accesses are logged; in case of misuse, the responsible user can be identified. No security issues occur so far.
Multiple languages support	No	English has been chosen as common language for the project. Single users are free to set different languages for EMDESK interface, but at project level English is the only used language.
Integration	Yes	EMDESK login has been embed in ISITEP website, for a quick access to internal document database and project information.
Alerts	Yes	EMDESK automatically send triggered or periodic use-reports and other information by mail to all users.

Table 3: Used EMDESK desiderata

Currently (at M23) 38 ISITEP documents have been uploaded on EMDESK repository. Most of them are completed, few are draft for future milestones.
Following table reports the status of ISITEP documents currently present on EMDESK repository.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Plan Submission Month (DOW)	WP No.	Del No.	Deliverable Title		Started	Draft	Consolidated	Review	2nd Draft	2nd Review	Final Version	3rd Review	Approved	Editing	Submitted	Completion	Leader	Comment
M01	WP 8.2	**D 8.2.1**	Project logo design	Actual	02.09.13 (M01)	30.09.13 (M01)	05.11.13 (M03)	25.11.13 (M03)			16.12.13 (M04)		30.01.14 (M05)		03.02.14 (M06)	100%		SES
				Planned	16.08.2013 (M00)	26.08.2013 (M00)	31.08.2013 (M00)	05.09.2013 (M01)	10.09.2013 (M01)	15.09.2013 (M01)	20.09.2013 (M01)	25.09.2013 (M01)	27.09.2013 (M01)	29.09.2013 (M01)	30.09.2013 (M01)			
M01	WP 8.2	**D 8.2.6**	News and newsletters	Actual	29.11.13 (M03)	30.05.14 (M09)	30.09.14 (M13)	03.10.14 (M14)			03.11.14 (M15)		07.11.14 (M15)		11.11.14 (M15)	100%		SES
				Planned	16.08.2013 (M00)	26.08.2013 (M00)	31.08.2013 (M00)	05.09.2013 (M01)	10.09.2013 (M01)	15.09.2013 (M01)	20.09.2013 (M01)	25.09.2013 (M01)	27.09.2013 (M01)	29.09.2013 (M01)	30.09.2013 (M01)			
M02	WP 8.2	**D 8.2.2**	Project factsheet	Actual	04.11.13 (M03)	20.12.13 (M04)	13.01.14 (M05)	31.01.14 (M05)			04.02.14 (M06)		14.02.14 (M06)		14.02.14 (M06)	100%		SES
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M02	WP 8.2	**D 8.2.3**	Project presentation	Actual	01.10.13 (M02)	07.11.13 (M03)	20.12.13 (M04)	24.01.14 (M05)			10.02.14 (M06)		12.02.14 (M06)		14.02.14 (M06)	100%		SES
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M02	WP 8.2	**D 8.2.7**	Project website	Actual	01.10.13 (M02)	25.10.13 (M02)	15.11.13 (M03)	29.11.13 (M03)			10.01.14 (M05)		03.02.14 (M06)		03.02.14 (M06)	100%		SES
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M02	WP 2.2	**D 2.2.1**	Draft security requirements	Actual	04.11.13 (M03)	14.11.13 (M03)	26.11.13 (M03)	27.11.13 (M03)			27.11.13 (M03)		28.11.13 (M03)		11.03.15 (M19)	100%	UPC	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M02	WP 2.3	**D 2.3.1**	End-user requirements document draft	Actual	09.12.13 (M04)	12.01.14 (M05)	21.01.14 (M05)	24.01.14 (M05)			27.01.14 (M05)		28.01.14 (M05)		11.03.15 (M19)	100%	BFP	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M03	WP 8.1	**D 8.1.1**	Dissemination plan	Actual	10.10.13 (M02)	13.11.13 (M03)	23.01.14 (M05)	28.02.14 (M06)			17.03.14 (M07)		31.03.14 (M07)		11.03.15 (M19)	100%	SES	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	16.10.2013 (M02)	26.10.2013 (M02)	31.10.2013 (M02)	05.11.2013 (M03)	10.11.2013 (M03)	15.11.2013 (M03)	20.11.2013 (M03)	25.11.2013 (M03)	27.11.2013 (M03)	29.11.2013 (M03)	30.11.2013 (M03)			
M06	WP 1	**D 1.1**	Detailed implementation plan	Actual	20.01.14 (M05)	15.04.14 (M08)	05.05.14 (M09)	19.05.14 (M09)			30.05.14 (M09)		06.06.14 (M10)		26.05.15 (M21)	100%	SES	New version updated according to the NEW REMARKS (after the answers to the first comments) of the Commission (1st Annual Review)
				Planned	02.09.2013 (M01)	01.10.2013 (M02)	14.10.2013 (M02)	31.10.2013 (M02)	04.11.2013 (M03)	29.11.2013 (M03)	06.12.2013 (M04)	20.12.2013 (M04)	13.01.2014 (M05)	10.02.2014 (M06)	28.02.2013 (M00)			
M06	WP 2.3	**D 2.3.2**	End-user requirements document candidate release	Actual	01.07.14 (M11)	31.08.14 (M12)	26.09.14 (M13)	15.10.14 (M14)	31.08.14 (M12)		31.10.14 (M14)		07.11.14 (M15)		11.11.14 (M15)	100%		BFP
				Planned	14.01.2014 (M05)	24.01.2014 (M05)	29.01.2014 (M05)	03.02.2014 (M06)	08.02.2014 (M06)	13.02.2014 (M06)	18.02.2014 (M06)	23.02.2014 (M06)	25.02.2014 (M06)	27.02.2014 (M06)	28.02.2014 (M06)			
M06	WP 5.1	**D 5.1.1**	Enhanced terminal requirements	Actual	31.01.14 (M05)	27.02.14 (M06)	02.05.14 (M09)	02.06.14 (M10)			06.06.14 (M10)		09.06.14 (M10)		29.07.14 (M11)	100%		RM3
				Planned	14.01.2014 (M05)	24.01.2014 (M05)	29.01.2014 (M05)	03.02.2014 (M06)	08.02.2014 (M06)	13.02.2014 (M06)	18.02.2014 (M06)	23.02.2014 (M06)	25.02.2014 (M06)	27.02.2014 (M06)	28.02.2014 (M06)			
M06	WP 4.3	**D 4.3.1**	Requirements for TETRA-TETRAPOL interoperability	Actual	07.04.14 (M08)	28.05.14 (M09)	25.07.14 (M11)	22.09.14 (M13)			29.09.14 (M13)		12.11.14 (M15)		11.03.15 (M19)	100%	AD&S FR	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	14.01.2014 (M05)	24.01.2014 (M05)	29.01.2014 (M05)	03.02.2014 (M06)	08.02.2014 (M06)	13.02.2014 (M06)	18.02.2014 (M06)	23.02.2014 (M06)	25.02.2014 (M06)	27.02.2014 (M06)	28.02.2014 (M06)			
M06	WP 4.4	**D 4.4.1**	Requirements for TETRAPOL-TETRAPOL Interoperability	Actual	07.04.14 (M08)	28.05.14 (M09)	25.07.14 (M11)	22.09.14 (M13)			29.09.14 (M13)		27.10.14 (M14)		04.11.14 (M15)	100%	AD&S FR	Technical requirements for TETRAPOL TETRAPOL interoperability
				Planned	14.01.2014 (M05)	24.01.2014 (M05)	29.01.2014 (M05)	03.02.2014 (M06)	08.02.2014 (M06)	13.02.2014 (M06)	18.02.2014 (M06)	23.02.2014 (M06)	25.02.2014 (M06)	27.02.2014 (M06)	28.02.2014 (M06)			
M07	WP 2.1	**D 2.1.1**	Current Status Assessment and Scenario outlines (draft 1)	Actual	01.11.13 (M03)	20.12.13 (M04)	15.01.14 (M05)	24.01.14 (M05)			31.01.14 (M05)		03.02.14 (M06)		03.02.14 (M06)	100%		TNO
				Planned	16.09.2013 (M01)	26.09.2013 (M01)	01.10.2013 (M02)	06.10.2013 (M02)	11.10.2013 (M02)	16.10.2013 (M02)	21.10.2013 (M02)	26.10.2013 (M02)	28.10.2013 (M02)	30.10.2013 (M02)	31.10.2013 (M02)			
M07	WP 1	**D 1.2**	Interim periodic report Y1	Actual	19.02.14 (M06)	05.05.14 (M09)	31.05.14 (M09)	02.06.14 (M10)			16.06.14 (M10)		20.06.14 (M10)		12.03.15 (M19)	100%	SES	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	14.02.2014 (M06)	24.02.2014 (M06)	01.03.2014 (M07)	06.03.2014 (M07)	11.03.2014 (M07)	16.03.2014 (M07)	21.03.2014 (M07)	26.03.2014 (M07)	28.03.2014 (M07)	30.03.2014 (M07)	31.03.2014 (M07)			
M08	WP 8.2	**D 8.2.4**	Brochures	Actual	16.12.13 (M04)	10.02.14 (M06)	05.09.14 (M13)	08.09.14 (M13)			15.09.14 (M13)		19.09.14 (M13)		01.10.14 (M14)	100%		SES
				Planned	16.03.2014 (M07)	26.03.2014 (M07)	31.03.2014 (M07)	05.04.2014 (M08)	10.04.2014 (M08)	15.04.2014 (M08)	20.04.2014 (M08)	25.04.2014 (M08)	27.04.2014 (M08)	29.04.2014 (M08)	30.04.2014 (M08)			
M08	WP 8.2	**D 8.2.5**	Posters	Actual	01.10.13 (M02)	31.10.13 (M02)	20.02.14 (M06)	01.04.14 (M08)			28.04.14 (M08)		05.05.14 (M09)		14.05.14 (M09)	100%		SES
				Planned	16.03.2014 (M07)	26.03.2014 (M07)	31.03.2014 (M07)	05.04.2014 (M08)	10.04.2014 (M08)	15.04.2014 (M08)	20.04.2014 (M08)	25.04.2014 (M08)	27.04.2014 (M08)	29.04.2014 (M08)	30.04.2014 (M08)			
M10	WP 2.1	**D 2.1.2**	Current Status Assessment and Scenario outlines (draft 2)	Actual	04.02.14 (M06)	01.10.14 (M14)	31.10.14 (M14)	03.11.14 (M15)			05.11.14 (M15)		07.11.14 (M15)		11.11.14 (M15)	100%		BFP
				Planned	14.01.2014 (M05)	24.01.2014 (M05)	29.01.2014 (M05)	03.02.2014 (M06)	08.02.2014 (M06)	13.02.2014 (M06)	18.02.2014 (M06)	23.02.2014 (M06)	25.02.2014 (M06)	27.02.2014 (M06)	28.02.2014 (M06)			
M10	WP 4.5	**D 4.5.1**	Requirements for mobile gateway	Actual	30.04.14 (M08)	28.05.14 (M09)	25.07.14 (M11)	22.09.14 (M13)			29.09.14 (M13)		27.10.14 (M14)		04.11.14 (M15)	100%	AD&S FR	Specific requirements for deployable gateway and its connections to national networks through SAT links.
				Planned	16.05.2014 (M09)	26.05.2014 (M09)	31.05.2014 (M09)	05.06.2014 (M10)	10.06.2014 (M10)	15.06.2014 (M10)	20.06.2014 (M10)	25.06.2014 (M10)	27.06.2014 (M10)	29.06.2014 (M10)	30.06.2014 (M10)			
M12	WP 8.3	**D 8.3.1**	Preliminary ?Who is Who? (enriched database)	Actual	01.07.14 (M11)	01.08.14 (M12)	05.09.14 (M13)	06.10.14 (M14)			03.11.14 (M15)		07.11.14 (M15)		11.03.15 (M19)	100%	SES	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 2.2	**D 2.2.2**	Candidate security requirements	Actual	13.12.13 (M04)	19.05.14 (M09)	15.07.14 (M11)				01.08.14 (M12)		20.10.14 (M14)		27.10.14 (M14)	100%		UPC
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 2.4	**D 2.4.1**	System subsystem design description (SSDD) candidate Release	Actual	22.01.14 (M05)	02.08.14 (M12)	28.08.14 (M12)				08.09.14 (M13)		20.10.14 (M14)		27.10.14 (M14)	100%		UPC
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 2.4	**D 2.4.3**	Network architecture candidate release	Actual	22.01.14 (M05)	01.08.14 (M12)	29.08.14 (M12)				08.09.14 (M13)		20.10.14 (M14)		27.10.14 (M14)	100%		UPC
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 4.3	**D 4.3.2**	TETRA-TETRAPOL gateway interfaces design	Actual	07.04.14 (M08)	28.05.14 (M09)	25.07.14 (M11)	22.09.14 (M13)			29.09.14 (M13)		11.11.14 (M15)		11.11.14 (M15)	100%		AD&S FR
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 4.6	**D 4.6.1**	Analysis of potential security frameworks and solutions	Actual	23.01.14 (M05)	02.08.14 (M12)	25.08.14 (M12)				01.09.14 (M13)		20.10.14 (M14)		11.03.15 (M19)	100%	UPC	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 4.7	**D 4.7.1**	Gateways Integration and test plan	Actual	28.04.14 (M08)	30.05.14 (M09)	21.07.14 (M11)	08.09.14 (M13)			29.09.14 (M13)		29.10.14 (M14)		11.03.15 (M19)	100%	AD&S FI	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 4.2	**D 4.2.1**	E1 ISI TETRA gateway interface design documentation	Actual	01.07.14 (M11)	10.11.14 (M15)	01.12.14 (M16)	08.12.14 (M16)			10.12.14 (M16)		15.12.14 (M16)		15.01.15 (M17)	100%		MOT
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 8.5	**D 8.5.1**	Detailed report on the ethical, legal and societal aspects of the project	Actual	07.07.14 (M11)	08.09.14 (M13)	13.10.14 (M14)				03.11.14 (M15)		07.11.14 (M15)		11.03.15 (M19)	100%	SES	New version updated according to the remarks of the Commission (1st Annual Review)
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 8.5	**D 8.5.2**	First report on security, integrity and availability	Actual	07.07.14 (M11)	15.09.14 (M13)	13.10.14 (M14)				03.11.14 (M15)		07.11.14 (M15)		13.11.14 (M15)	100%		SES
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M12	WP 4.4	**D 4.4.2**	TETRAPOL-TETRAPOL gateway Interfaces design	Actual	12.05.14 (M09)	09.06.14 (M10)	23.06.14 (M10)	25.06.14 (M10)			30.06.14 (M10)		03.11.14 (M15)		11.11.14 (M15)	100%	AD&S FR	Interface design for connecting the gateway to TETRAPOL networks.
				Planned	17.07.2014 (M11)	27.07.2014 (M11)	01.08.2014 (M12)	06.08.2014 (M12)	11.08.2014 (M12)	16.08.2014 (M12)	21.08.2014 (M12)	26.08.2014 (M12)	28.08.2014 (M12)	30.08.2014 (M12)	31.08.2014 (M12)			
M14	WP 4.5	**D 4.5.2**	Deployable gateway design capabilities	Actual	09.02.15 (M18)	27.02.15 (M18)	20.03.15 (M19)	06.04.15 (M20)			15.04.15 (M20)		19.06.15 (M22)		22.06.15 (M22)	100%		AD&S FR
				Planned	16.09.2014 (M13)	26.09.2014 (M13)	01.10.2014 (M14)	06.10.2014 (M14)	11.10.2014 (M14)	16.10.2014 (M14)	21.10.2014 (M14)	26.10.2014 (M14)	28.10.2014 (M14)	30.10.2014 (M14)	31.10.2014 (M14)			
M16	WP 8.3	**D 8.3.3**	Report on 1st ISITEP workshops	Actual	17.11.14 (M15)	01.12.14 (M16)	08.12.14 (M16)	10.12.14 (M16)			12.12.14 (M16)		15.12.14 (M16)		05.02.15 (M18)	100%		SES
				Planned	16.11.2014 (M15)	26.11.2014 (M15)	01.12.2014 (M16)	06.12.2014 (M16)	11.12.2014 (M16)	16.12.2014 (M16)	21.12.2014 (M16)	26.12.2014 (M16)	28.12.2014 (M16)	30.12.2014 (M16)	31.12.2014 (M16)			
M18	WP 6.1	**D 6.1.1**	Open public functional specifications	Actual	07.11.14 (M15)	26.03.15 (M19)	08.04.15 (M20)				20.04.15 (M20)		19.06.15 (M22)		22.06.15 (M22)	100%		UPC
				Planned	14.01.2015 (M17)	24.01.2015 (M17)	29.01.2015 (M17)	03.02.2015 (M18)	08.02.2015 (M18)	13.02.2015 (M18)	18.02.2015 (M18)	23.02.2015 (M18)	25.02.2015 (M18)	27.02.2015 (M18)	28.02.2015 (M18)			
M18	WP 6.2	**D 6.2.1**	Open public functional specifications	Actual	09.02.15 (M18)	23.02.15 (M18)	19.03.15 (M19)	31.03.15 (M19)			21.05.15 (M21)		19.06.15 (M22)		22.06.15 (M22)	100%		NETTECHN
				Planned	14.01.2015 (M17)	24.01.2015 (M17)	29.01.2015 (M17)	03.02.2015 (M18)	08.02.2015 (M18)	13.02.2015 (M18)	18.02.2015 (M18)	23.02.2015 (M18)	25.02.2015 (M18)	27.02.2015 (M18)	28.02.2015 (M18)			
M24	WP 4.1	**D 4.1.2.b**	Gateway prototype SELEX ES network	Actual	19.02.14 (M06)	19.02.14 (M06)										10%		SES
				Planned	17.07.2015 (M23)	27.07.2015 (M23)	01.08.2015 (M24)	06.08.2015 (M24)	11.08.2015 (M24)	16.08.2015 (M24)	21.08.2015 (M24)	26.08.2015 (M24)	28.08.2015 (M24)	30.08.2015 (M24)	31.08.2015 (M24)			
M27	WP 4.1	**D 4.1.3**	Procedures for Interoperability testing and prototypes test report	Actual	26.01.15 (M17)											5%		ISCOM
				Planned	16.10.2015 (M26)	26.10.2015 (M26)	31.10.2015 (M26)	05.11.2015 (M27)	10.11.2015 (M27)	15.11.2015 (M27)	20.11.2015 (M27)	25.11.2015 (M27)	27.11.2015 (M27)	29.11.2015 (M27)	30.11.2015 (M27)			
M33	WP 4.8	**D 4.8.1**	Procedures for testing interoperability and test reports	Actual	03.02.15 (M18)											5%		ISCOM
				Planned	16.04.2016 (M32)	26.04.2016 (M32)	01.05.2016 (M33)	06.05.2016 (M33)	11.05.2016 (M33)	16.05.2016 (M33)	21.05.2016 (M33)	26.05.2016 (M33)	28.05.2016 (M33)	30.05.2016 (M33)	31.05.2016 (M33)			
M33	WP 4.1	**D 4.1.4.b**	Gateway prototype SELEX Es network final release	Actual	19.02.14 (M06)											5%		SES
				Planned	16.04.2016 (M32)	26.04.2016 (M32)	01.05.2016 (M33)	06.05.2016 (M33)	11.05.2016 (M33)	16.05.2016 (M33)	21.05.2016 (M33)	26.05.2016 (M33)	28.05.2016 (M33)	30.05.2016 (M33)	31.05.2016 (M33)			

Table 4: Documents present on EMDESK repository at M23

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

9.2 JOIN.ME

Join.me has been mainly used as audio conferencing platform, since its flexibility; it is in fact possible to join the conference by phone (using local numbers) or through the internet (via VoIP).
The access to join.me services are subordinated to a registration, for users joining the conference with the software or through the website, while a conference PIN-code is requested to user calling by phone. To be noted that the maximum number of supported participant to a conference is 250, number never reached during meetings so far.

Characteristic	Used	Note
Group communication and messaging	Yes	Mainly audio conferencing, directly by phone and/or trough the internet.
User identification	Yes	Online users are identified; users joining conference calls by phone are requested to digit a multi-digit code.
PC screen sharing	No/Yes	Official events and plenary meeting just use audio conferencing. Possible multimedia data or presentation are uploaded on EMDESK or, in some cases, distributed by mail. PC screen sharing can be anyway used by project partners for operative meetings, according to their company policies.
Communication Security	Yes	Users accessing to audio conferences via VoIP are protected by https protocol for the access of the web virtual meeting area.

Table 5: Used Join.me desiderata

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

10 SECURITY, INTEGRITY AND AVAILABILITY ASPECTS IN DISSEMINATION ACTIVITIES

Beside the arguments described in previous sections, also dissemination could present security, integrity and availability issues in information treatment, since this activity exposes data to a wide public and involves the use of web and social networks to publish news, information and documents.

Dissemination activities of ISITEP Project are performed resorting to various types of channel and media. In particular, the chosen tools (together with their web addresses) are:

- ISITEP Website: www.isitep.eu
- Twitter: twitter.com/isitep
- Facebook: www.facebook.com/ISITEP
- LinkedIN: www.linkedin.com/groups/ISITEP-5183355
- Youtube: www.youtube.com/user/isitep
- Newsletter: published on isitep.eu/news-and-events/blog and distributed through other media (e-mail, social networks...)
- Publications: papers on journals and magazines or presented to conferences, book chapters and similar.

In dissemination context, major issues that could arise concern the possibility of making public confidential information, documents, or research results belonging to other parties. For this reason it is important to foreseen specific figures that are responsible of manage the security aspects of dissemination, especially through Web 2.0 technologies, together with methodologies and procedures to be followed in order to guarantee confidentiality, integrity and availability of published information.

In general, project documents could be considered confidential. In particular, they shall be handled in compliance with the confidentiality principle and rules depicted in Contract and Consortium Agreement.
Documents that should to considered confidential are:

- program documents, such as program schedules, management information and documentation;
- technical documents such as the results of ISITEP studies, documentation on hardware components, applications, tools, integration, validation and acceptance tools and reports, minutes of reviews and meetings,

In the other hand, not confidential documents are:

- exchanges of dates and places for meetings organization and preparation,
- dissemination data,
- other data specifically approved for publication by the PMT.

Not confidential documents are the only that can be freely published, while the other shall be treated only by consortium members.

Taking into account these general considerations, guidelines for the approach to dissemination activities have been defined. As a general rule, the control and authorization functions are performed by all partners or by their representative in PMT. Moreover, for each dissemination tool some Media Dissemination Managers (MDMs) have been designed. A same person can act as manager of different media, in collaboration with others. Two or more people are responsible for one dissemination channel, to ensure redundancy in services access and in publishing operations control. They are in contact with coordinator that leads dissemination activities and with all partners.
Media Dissemination Managers shall respect a code of conduct. In particular they shall:

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

- be aware that data published on the web are free to be shared or reposted, they become therefore persistent even if deleted from the original source. For this reason MDMs shall carefully verify the correctness of all information;
- interact with partners to avoid mistakes;
- be transparent with partners and public;
- be always available to publish news and to interact with public, providing additional clarifications and eventually avoiding misinformation;
- avoid spam;
- respect social networks netiquette;
- respect users and their privacy.

10.1 WEB SITE AND SOCIAL MEDIA

ISITEP website makes all published information available for general public, for web consultation or download. The official ISITEP website collect al submitted public deliverable as well (at: http://isitep.eu/resources/project-deliverables.php).

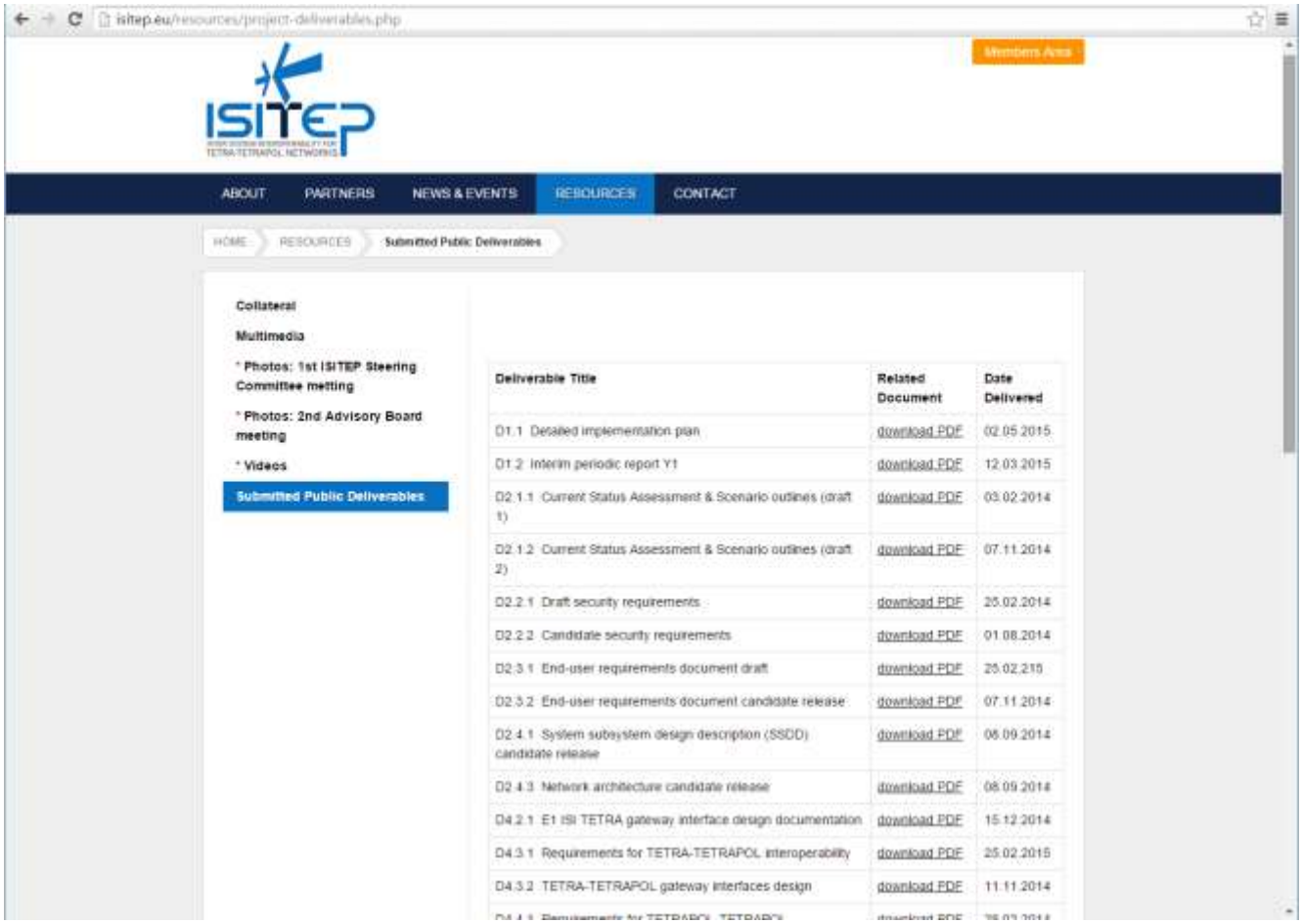

Figure 6: It is possible to download a PDF version of all public deliverables directly on ISITEP website

Social media, on the other hand, can be used to publish news, events, and have available a feedback channel from general audience.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

The various media have different characteristics, which make them more suitable to the diffusion of some kinds of information differing in contents and forms, e.g.:

- Twitter is mainly used to communicate with persons with similar interests, regardless of whether users know one another off Twitter. It based on the concept of short messages, and all communication (the “tweets”) are limited to 140 characters. The “tweets” enable fast and real time communications; users’ interaction on arguments identified by hashtags (#). Even if it’s possible to share images and videos, Twitter is text-oriented.
- Facebook is the most popular, widespread and general purpose social network. It is mainly used by individuals who wish to stay connected with people that they know offline, but with the presence of “pages” can also be effectively adopted for promoting projects. It’s a media-share oriented social network, and posts containing images or videos have generally more visibility. Facebook is also suitable for event promotion.
- LinkedIn is a professional social network that facilitates relationships with project partners and other stakeholders.

All partner can propose information to be shared on social networks or on the website, but few users have the credentials to actual publish on official ISITEP website and social pages, increasing the control on dissemination activity.
This allows to verify that confidential documents or sensitive information are not publically shared. Data integrity and correctness checked as well.
The continuous communications between people allowed to publish and other ISITEP partners, permits to maintain shared information updated.
Some social networks, as Facebook or LinkedIn, permit people to publish posts on ISITEP virtual wall; in this case the author is identified by his own name and is not officially publishing as ISITEP. Users managing the page can act as moderator to filter post on ISITEP wall or comments to ISITEP activities, if necessary.
After the publication, data availability is demanded to third parties (e.g. web provider, Facebook, Twitter, LinkedIn).

Information publishing follows a well defined redaction/authorization/publishing procedure:

1. Data collection: different types of information can be distributed on online channels. Data can be made available through different ways:
    a. Spontaneously sent by partners, which have relevant communications to share.
    b. Requested by MDMs in order to maintain dissemination tools always up to dated or in correspondence of specific deadlines (e.g. Newsletter issues, events, etc.).
    c. Autonomously produced by MDMs, according to news and facts related to project or to PPDR world in general.
2. News redaction by MDMs or partners.
3. Data validation: when needed, info to be published are shared with all partners to confirm their accuracy, and to verify that they respect the restrictions on confidentiality.
4. Media choice: in accordance with the characteristics of various media and the contents which have to be published, MDMs identify the most suitable social media to be used for the news in object.
5. Adaptation and publishing: MDMs adapt the text/format to the particular channel, considering the media characteristics/restrictions, and publish the news.

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

Figure 7: ISITEP redaction, authorization and publishing procedure

10.2 NEWSLETTER

A similar procedure has been foreseen for the newsletter publication in deliverable D82.6 – "News and newsletter" (see Figure 8). In facts, also the newsletter follows a procedure of contents' collection, validation and publishing.

In this case the information to be published come mainly from partners. As described in deliverable D82.6, when they are interested in publishing, they can submit an article, comprising an abstract, a list of authors, the topics related to the project, and some keywords, to PMT composed by SPs' leaders. PMT checks the correctness and the confidentiality of the contents and eventually suggests some modifications. Finally, the article is provided to the editorial board composed of MDMs to be published.

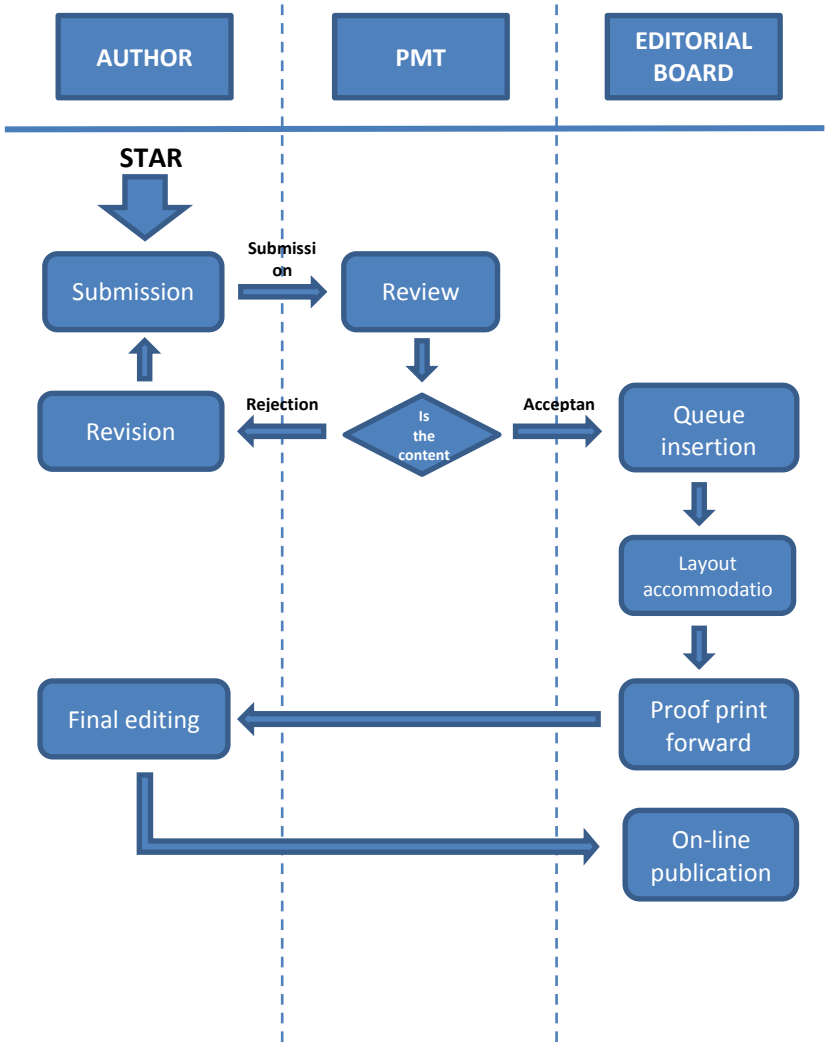

Figure 8: Newsletter authorization procedure

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

10.3 EDITORIAL PUBLICATIONS

The dissemination activities are in some case also autonomously performed by single or group of partners, for example participating to conferences or writing papers, magazines' articles and other editorial products. In this case, each partner is responsible of what is publishing.
In this case, they shall inform the consortium of the activity in order to obtain possible feedback and/or authorizations (if needed), at the same time they shall refer to its internal rules/policies and adhere to copyrights agreements requested by editor.

In order to preserve confidentiality of information concerning the project or belonging to partners, authors should:

- check that the content of the publication does not infringe any other author's copyrights;
- patent every invention, that can be patented before publication;
- include in each publication the following sentence: "*The research leading to these results has been partially funded by the European Community's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement n° 312484. The ISITEP (Inter System Interoperability for Tetra-TetraPol Networks) project is a Collaborative Project for the FP7 THEME [SEC-2012.5.3-4] [Global solution for interoperability between first responder communication systems - Integration Project]. The project has 15 partners and started on 1st September 2013*".

For journal and conference papers, the procedure is the following:

1. One among the authors has to inform all consortium partners about a possible publication specifying title and co-authors of the publication, name and date of the planned conference/journal, first submission date, final submission date and the responsible SP or WP for the work's origin;
2. About 45 days before the first submission deadline, an abstract of the publication describing also the scope of the work, the aspects of the project which will be discussed, and the results which will be presented, should be provided to the consortium.
3. All partners can object about the inclusion of specific results or aspects of the project within 30 days before the first submission deadline. If there are no objections, the general contents of the publication are approved.
4. The final version of the manuscript for the first submission should be provided to the consortium at least 21 days (3 weeks) before the deadline for the dissemination activity (workshop, conference or journal), in order to let all the partners check with enough detail if any violation of confidentiality or access rights occurs;
5. All partners can object within one week before the first submission deadline (they can check the final manuscript for two weeks). If there are no objections, then the contribution is approved (so called silent approval procedure);
6. Once the paper has been submitted, if significant reviews of the paper are required for acceptance (especially in case of journal papers), the revised paper should be submitted again to the consortium. Any partner can object (within one week from the reception of the

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

manuscript) on the submission of the modified paper with the modalities specified in the previous point.

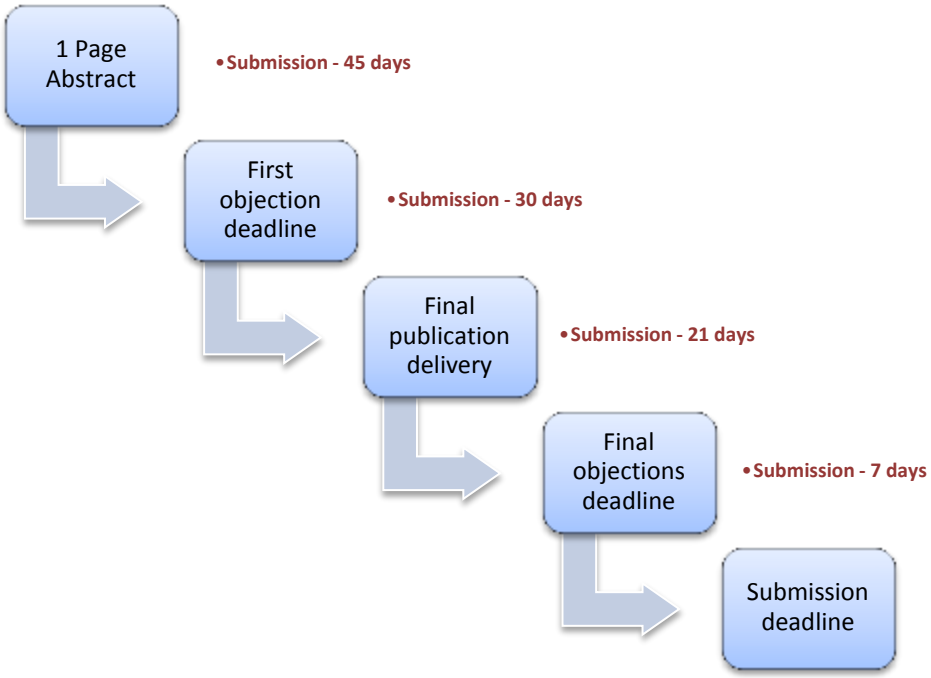

Figure 9: Editorial products approval procedure

If the publication deadline is sooner than 45 days, a short procedure may be followed. This procedure is the same as for journal and conference except for the period for objections reduced to 14 days (instead of 30 days) before the submission date.

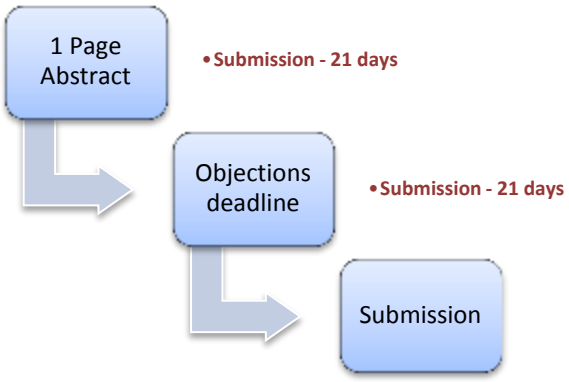

Figure 10: Editorial products short approval procedure

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee

11 BIBLIOGRAPHY

[1] http://www.emdesk.com/en/Security.html
[2] join.me architecture whitepaper, https://secure.join.me/.../joinme_architecture.pdf
[3] www.join.me

This document is produced under the EC contract 312484. It is the property of the ISITEP Parties and shall not be distributed or reproduced without the formal approval of the ISITEP Steering Committee