ISITEP
D8.5.2 – First 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_D8.5.2_20141107_V1.0	**Version:**	V1.0
Deliverable:	D8.5.2	**Date:**	07/11/2014
		Status:	Approved

Document classification	**Public**

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

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Federico Frosali, Paolo Di Michele, Fiorella Lamberti	SES	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

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V1.0	07/11/2014	All	All	First issue

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

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.

CONTENTS

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.

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, these issues, are strictly bounded to ethical and legal norms, addressed in 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).

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.

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.

5 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.

5.1 MANDATORY FUNCTIONS

5.1.1 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.

5.1.2 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.

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.

5.1.3 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.

5.1.4 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.

5.2 ADDITIONAL DESIDERATA

5.2.1 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.

5.2.2 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.

5.2.3 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 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.

5.2.4 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…

6 MEETING PLATFORM TOOL

The nature of ISITEP project and the presence of several international project-partners, working together to the various tasks, lead 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.

6.1 COMMUNICATIONS TOOL NEEDED FUNCTIONS

6.1.1 GROUP COMMUNICATIONS AND MESSAGING

An effective meeting platform allows 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.

6.1.2 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.

6.1.3 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.

6.1.4 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 5.1.1 and 5.1.2).

7 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.

7.1 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 projects partners that is facilitates through tools e.g. mailing lists, shared calendar and a document manager.

7.1.1 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.

7.1.2 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.

7.1.3 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.

7.1.4 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].

7.1.5 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

		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

7.2 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.

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

7.2.1 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 communications 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 encryption protocol

Table 2: accomplishment of desiderata for the digital meeting platform

8 BIBLIOGRAPHY

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