ISITEP
D6.2.2 - TERMINAL TRAINING TOOL

Document Manager:	George Mitsopoulos	NETFI	Editor

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

Document ID N°:	ISITEP_6.2.2_20160610_V1.0	**Version:**	V1.0
Deliverable:	D6.2.2	**Date:**	10/06/2016
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	George Mitsopoulos (NETFI)
Approved by (WP Leader):	George Mitsopoulos (NETFI)
Approved by (SP Leader):	Dimitris Androutsopoulos (NETFI)
Approved by (Coordinator):	Paolo Di Michele (FNM)
Security Approval (Advisory Board Coordinator):	Etienne Lezaack (BFP)

CONTRIBUTING PARTNERS

Name	Company/Organization	Role/Title
Claudia.OLIVIERI	FNM	Contributing Partner
Federico FROSALI	FNM	Contributing Partner
Serge DELMAS	ADS FR	Contributing Partner
Feiko VERMEULEN	V&J	Contributing Partner
Federica BATTISTI	RM3	Contributing Partner

DISTRIBUTION LIST

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

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V0.1	19/02/2016	All	All	Initial version
V1.0	10/06/2016	All	All	Final for submission

Publishable extended abstract

This document includes a description of the tool and details of use for the Terminal Training Tool (task 6.2.2 Terminal training tool). The Terminal Training Tool will provide a visualized training environment for various handheld terminal. The tool will be accessible from any device (PC, Smartphone, Tablet) and will provide the user with the instructions and visual interactivity for the most common handheld functions.

The document is classified as Public as it does not deal with any potential security frameworks and mechanisms of the ISITEP security solution for network interconnection and there are no national security sensitive issues in the document.

CONTENTS

FIGURES

1 INTRODUCTION

The ISITEP project pursues the vision of allowing first responders of European ISITEP federated countries to seamlessly interoperate by overcoming current operational and technological barriers. New European entrants will be easily federated into the ISITEP European network to achieve seamless interoperability.

To achieve ISITEP's vision the project will develop an operations training tool in order to provide fast and accurate training/education on the procedures that apply at cross-border emergency events.

This document will provide a general description of the Terminal Training Tool.

1.1 Tool Access

You can access the tool in the URL http://gatory.com/isitep/terminal-training/index.php

In order to access the tool functions the user must have valid login credentials.

There are two user levels, Administrators and Users.

To login as a demo user use the following credentials:

E-mail: user@ isiteptools.com

Password: User1@

1.2 Tool Technology

The tool has been built with PHP and javascript programming languages. The JQUERY mobile framework has been used in order to provide cross-device functionality.

MySQL datatabase has been used in order to store user information.

2 DEFINITIONS AND ABBREVIATIONS

2.1 Definitions

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

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

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

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

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

Encryption: the conversion of plain text to cipher text.

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

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

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

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

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

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

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

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

Security assurance: it is the confidence that a network product / terminal / system meet its specific security objectives. Assurance is usually verified by performing an evaluation.

(Security) certificate: it is an official document attesting that the evaluation of the network product / terminal /system against some security assurance specifications was conducted correctly and was successful.

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

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

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

2.2 Abbreviations

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

Acronym	Definition
CCK	Common Cipher Key
CDR	Call Detail Record
DCK	Derived Cipher Key
GTSI	Group TETRA Subscriber Identity
GW	Gateway
IOP	Interoperability Profile
IP	Internet Protocol
MS	Mobile Station
MT	Mobile Terminal
OTAK	Over The Air re-Keying
OTAR	Over The Air Rekeying
PC	Professional Computer
PDA	Personal Digital Assistant
PEI	Peripheral Equipment Interface
PMR	Professional/Private Mobile Radio
PPDR	Public Protection and Disaster Relief
PS	Public Safety
SDS	Short Data Service
TE	Terminal Equipment
TEI	Terminal Equipment Identity
TG	Talk Group
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WS	Work station

3 GENERAL DESIGN AND TOOL ARCHITECTURE

3.1 Tool Architecture

The tool provides a web interface in order to accept user input and return the results. The UI is accessible with a web browser. The web application files are stored in a web server that receives the requests from the client (browser) and returns the results. A database server is used in order to store system data.

Below is the high level system architecture diagram.

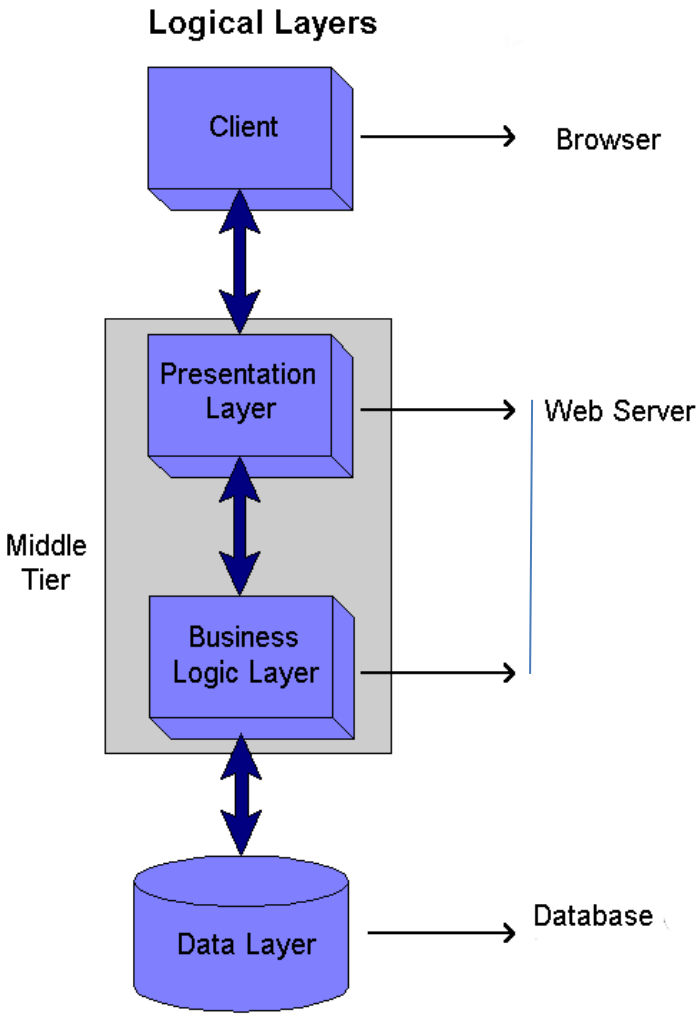

Figure 1. High level system architecture diagram

3.2 Database design

The tool uses a MySQL database. The diagram below shows database tables.

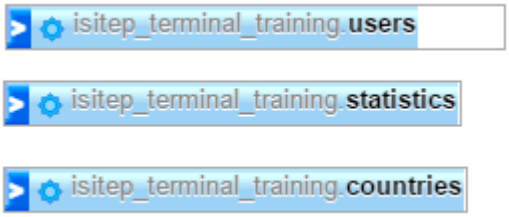

Figure 2. Database Tables

3.2.1 Table "users"

It stores information about system users. The table includes many auxiliary fields for future user.

The most important fields are:

Id

e-mail

password

fullname

country

telephone_number

organization

date_created

friendly_url

role

3.2.2 Table “statistics”

It stores information details on the content that has been visited by the users.

Fields:

Id

terminalid

userid

time

3.2.3 Table “countries”

It stores countries list for use on user profiles

Felds:

Id

code

country

3.3 Main software functions

The main software functions are activated as _GET switch parameters (“sw” parameter).

3.3.1 Logout

User logout

Activation code: if ($sw=="logout")

3.3.2 Manage users

Displays the user management UI to an Administrator.

Activation code: if ($sw=="manage-users")

3.3.3 Login

Login for users.

Activation code: if ($sw=="login")

3.3.4 Contact

Submits contact form to the e-mail addreess that has been defined in ‘functions_settings.php’ file.

Activation code: if ($sw=="contact")

3.3.5 Statistics

Displays statistics of use for terminals and users

Activation code: if ($sw=="statistics")

3.3.6 Adding new terminals

In order to add new terminal to the tool you have to add the terminal files in the "terminals" folder. Once you add properly the files in the "terminals" folder, the system will recognize the fact the a new terminal has been added and will display a link to the terminal in the home page.

The new terminal folder should be named based on the terminal model and should include the following files :

Index.php

settings_php

And a folder named "images" where all the images that will be used for visualizing the training experience should be added.

The file settings.php includes the html code that will load the screen and the training UI for the specific terminal.

The file settings.php includes the following parameters that have to be set in case of a new terminal.

```
$terminal_name= ;                          //set terminal name
$terminal_id=' ';                          //set terminal name. It has to be unique between terminals
$files_path='terminals/{terminal folder}/'; //files path
```

3.4 Web application map

Home Page

Login

Logout

Contact

Manage Users -> Add User

-> Edit Profile

-> Delete User

Terminals/Handhelds

Statistics

4 GRAPHICAL USER INTERFACE DESCRIPTION AND USAGE

4.1 Login

The first screen of the Tool is the login screen. Enter your e-mail and password and click 'Go' in order to login.

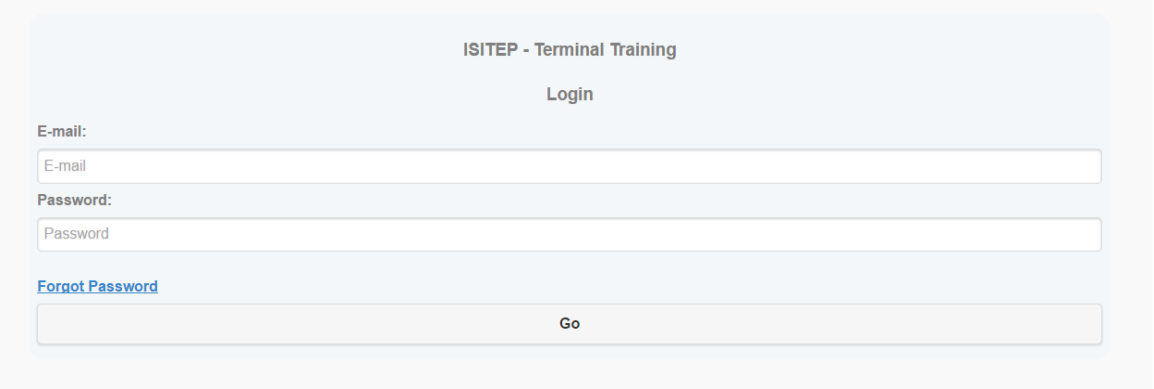

Figure 3. Login Screen

4.2 Tool Home Screen

From the tool home screen you can:

-Manage Tool Users (in case you have login as Admin)

-View brief instructions on how to use the tool

-Access the available handheld training screens

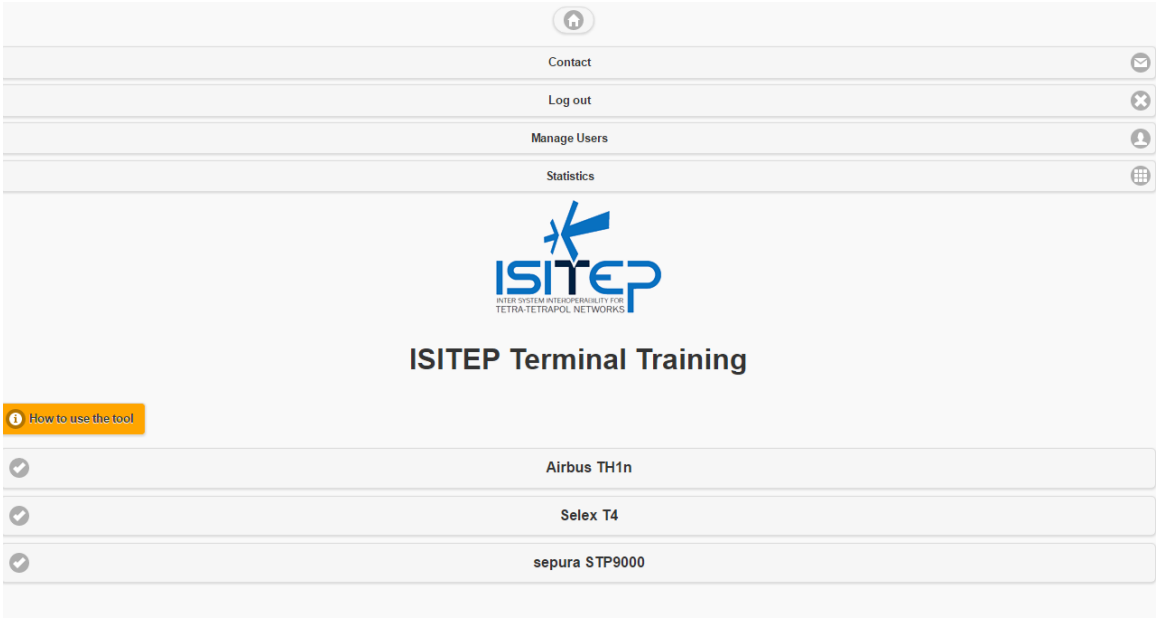

Figure 4. Home Screen

4.3 Manage Users

From the user management screen (accessible from the tool homepage) you can

-Add new User

-Delete Existing User

-Edit existing user by clicking on his/her full name

-Return to the Homepage by clicking the home icon on the top of the page

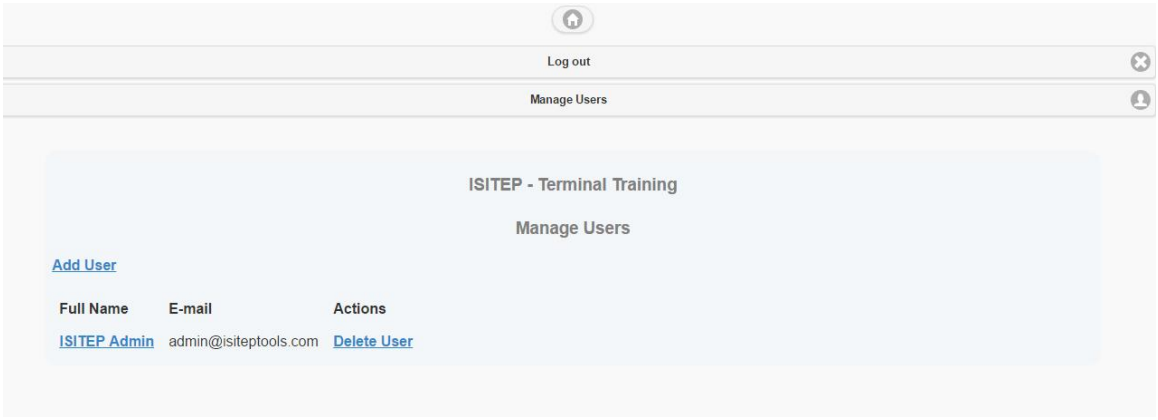

Figure 5. User Management Main Screen

4.4 Statistics

From the statistics screen (accessible from the tool homepage) you can view usage statistics per user and per terminal.

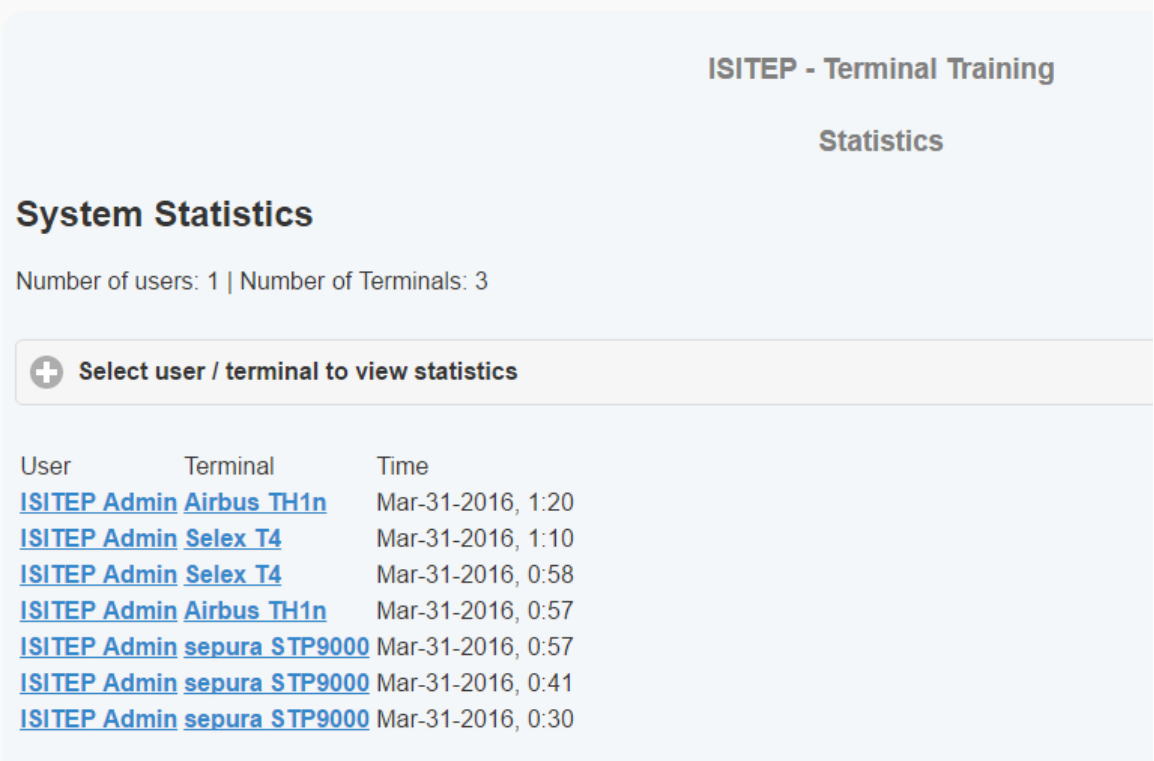

Figure 6. Statistics

4.5 The Terminal Training Screen

Below there is an example of the Terminal Training Interface with details on the screen areas and usage.

Figure 7. Terminal Training Interface

5 TESTS PERFORMED

Functions Tested	Date	Status
Login	2016.02.26	Passed
Logout	2016.02.26	Passed
Forgot Password	2016.02.26	Passed
Home Button Click	2016.02.26	Passed
Manage users Button	2016.02.26	Passed
Handheld Access Buttons	2016.02.26	Passed
Handheld training screen flows	2016.02.26	Passed
Add user Function	2016.02.26	Passed
Delete user Function	2016.02.26	Passed
Edit user Function	2016.02.26	Passed
Statistics	2016.02.26	Passed
Contact Form	2016.02.26	Passed

6 SETUP INSTRUCTIONS

In order to set up the tool you need to have installed a MySQL database server and an Apache web server.

Once you have the environemt running, follow the next steps:

-Unzip the contents of terminal_training_tool_setup.zip.

-Create an empty database in your MySQl server.

-Run the setup_database.sql file that you can find in your unzipped folder to your new database. This will publish the required tables and initial data.

-Edit the file functions_settings.php in the HTML folder and set the database connection details $db_host, $db_pass, $db_name and the rest of options in the same setting paragraph of the file based on the examples of the file.

-Save and close the functions_settings.php file.

-Upload the contents of the HTML folder to your root folder of your web server.

-Point your browser to the root of your web server to start using the tool.