ISITEP
D5.3.1 - SECURITY MANAGER TEST REPORT

Document Manager:	Vincenzo	ABBATE	Editor

Programme:	Inter System Interoperability for Tetra-TetraPol Networks
Project Acronym:	ISITEP
Contract Number:	312484
Project Coordinator:	FNM
SP Leader:	RM3

Document ID N°:	ISITEP_D5.3.2_20160428_V1.0	**Version:**	V1.0
Deliverable:	D5.3.1	**Date:**	28/04/2016
		Status:	Approved

Document classification	**PUblic**

Approval Status	
Prepared by:	Vincenzo ABBATE (EXP)
Approved by (WP Leader):	Vincenzo ABBATE (EXP)
Approved by (SP Leader):	Federica BATTISTI (RM3)
Approved by (Coordinator)	Paolo DI MICHELE (FNM)
Security Approval (Advisory Board Coordinator)	Etienne LEZAACK (BFP)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Marco Carli	RM3	Contributor
Federica Battisti	RM3	Contributor
Massimo Cretaio	RM3	Contributor
Federico Frosali	FNM	Revisor
Claudia Olivieri	FNM	Revisor

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
Federico.Frosali, Claudia.Olivieri, Andrea Campodonico	FNM	WP2.2 participant
Etienne Lezaack, Simon Verdegem, Yves Cawet, Marc Vandenbroeck, Marie Carlsson	BFP	WP2.2 participant
Marianne Storrosten, Michel Duits	DNK	WP2.2 participant
Anita Galin, Anna Falkdrugge, Peter.Hedman, Robert Danelius, David Arnljots	MSB	WP2.2 participant
Ronald Van.Der Wal, Herman Van Sprakelaar, Hans Borgonjen	V&J	WP2.2 participant
Jaakko Saijonmaa, Risto Toikkanen	ADS FI	WP2.2 participant
Serge Delmas, Jean-Pierre Quemard, Herve Mokrani, Eric Lorfeuvre, Dominique Eustache	ADS FR	WP2.2 participant

Daniele Biondini, Luciana Favia, Ivano Luciani, Giuseppe Pierri, Franco Pangallo, Mario Manzi	ISCOM	WP2.2 participant
Theodore Tzamos, Michael Spyridakis, Haritou, Dimitris Androutsopoulos	NETFI	WP2.2 participant
Cor Verkoelen, Frank Fransen, Bram Verheesen, Marcel Vanderlee	TNO	WP2.2 participant
Ramon Ferrús, Oriol Sallent	UPC	WP2.2 participant/Leader
All Company Project Managers	All involved companies	Members of the Steering Committee
Elina MANOVA	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
V0.1	01/03/2016	All	All	Initial version (RM3)
V0.8	11/04/2016	All	All	Revised version (RM3)
V1.0	28/04/2016	All	All	Final revision (RM3)

Publishable extended abstract

In this deliverable, the design of the test set for assessing the effectiveness of the Security Manager (SM) for the new enhanced terminals in the ISITEP project is reported. In this framework, the overall security depends on several factors, such as the secure migration between TETRA and TETRAPOL networks and the use of a secured terminal. In particular, the use of an open source Operating System (i.e., Android) poses severe challenges concerning threats and vulnerabilities that have been addressed in D2.2.2 [1] and integrated in the Security Manager design in D5.3.2 [2]

This WP is devoted to test the Security Software Manager on ISITEP terminals addressing the following issues:

- Test the Security Manager functionalities as described in D5.3.2
- Test on an Android device the SM functionalities.

ABBREVIATIONS

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

Acronym	Definition
API	Application Program Interface
CM	Communication Manager
GUI	Graphic User Interface
REQ	Requirement
SDS	Short Data Service
SM	Security Manager
TEI	Terminal Equipment Identity
TETRA	TErrestrial Trunked Radio
USB	Universal Serial Bus

CONTENTS

1. INTRODUCTION

The aim of WP5.3 is to define and implement a Security Software manager on the new enhanced terminal designed and implemented in the ISITEP project. The enhanced terminal is a bi-technology terminal composed by a TETRA and by a TETRAPOL modem controlled by a single control unit deployed inside an Android device.

Some security functions are provided by the TETRA and TETRAPOL modems. In particular:

- authentication of the modem on the actual Network Infrastructure;
- confidentiality of communications through encryption mechanisms;
- protection against eavesdropping or poisoning information from a stolen or loss terminal through Enable / Disable functionalities.

In this document are reported the design and report of the test implemented for evaluating the effectiveness of the security mechanisms implemented for improving the security of the Android device. The security mechanisms have been designed by following the requirements established in D.5.3.2[2].

The document is organized as follows:

- Section 1: Introduction
- Section 2: Testing environment
- Section 3: Test case
- Section 4: Requirements mapping
- Section 5: Test report
- Section 6: Issue list
- Section 7: References

2. TESTING ENVIRONMENT

2.1 Test Environment Architecture

The test reported in this document have been performed on two different terminals, Galaxy S4 (Android 5.0.1, API 21) and Nexus 4 (Android 5.1.1, API 22).

Test involving communication with other application of ISITEP framework, through Android Broadcast Bus, that are not available, have been simulated.

In more details, the application behavior has been simulated through a simple test Application (sending expected intent on the broadcast bus) and a receiver (showing the expected response).

3. TEST CASE

3.1 Test Security Manager GUI

3.1.1 SM_GUI_1 – First Launch

Security Manager GUI		
SM_GUI_1 **First Launch**		
Objective(s)		
Setting administrator password		
Pre-Conditions		
○ The Security Manager GUI has never been executed ○ The administrator password has not been set in the enhanced terminal		
Test procedure		
Action		**Expected Result**
1	Tap on Security Manager GUI icon	Security Manager Administrator Login is opened A dialog for setting administrator password is shown.
2	Go to first field “Set Administrator password”, enter a password of length lower than **8** characters and tap on “Save Configuration” button (or “save” button on keyboard layout)	An error message **“Invalid password**” is shown.
3	Go to first field “Set Administrator password” enter at least **8** characters. Go to second field “Confirm administrator password”, enter a different password and press the save button.	An error message “**Confirm password does not match**” is shown.
4	Go to second field “Confirm administrator password”, enter the same password and press the save button.	The dialog is closed and a message “Administrator password saved” is shown.

3.1.2 SM_GUI_2 – Login Administrator

Security Manager GUI		
SM_GUI_2 **Login Administrator**		
Objective(s)		
Login as administrator for setting up the preference of Security Manager		
Pre-Conditions		
○ The administrator password has been set		
Test procedure		
Action		**Expected Result**
1	Tap on Security Manager GUI icon	Security Manager Administrator Login is opened. Below the field to enter password, the number of available login tentative is shown.
2	Go to field “Enter Administrator password”, enter less than **8** characters and tap on “Sign In” button (or “Sign in” button on keyboard layout)	An error label “**Invalid password**” appears on field. The number of available login tentative does not change
3	Go to field “Enter Administrator password”, enter a wrong password with at least **8** characters and tap on “Sign In” button (or “Sign in” button on keyboard layout)	An error label “**Incorrect password**” appears on field. The number of available login tentative is decremented by one. If the number of available login tentative reach zero, the device shall be wiped.
4	Go to field “Enter Administrator password”, enter a correct password and tap on “Sign In” button (or “Sign in” button on keyboard layout)	The preference of Security Manager is opened

3.1.3 SM_GUI_3 – Setting Security Manager Preference

Security Manager GUI		
SM_GUI_3 **Setting Security Manager Preferences**		
Objective(s)		
Set and save Security Manager preferences		
Pre-Conditions		
○ The administrator was logged in and the preference of Security Manager is opened ○ The Security Manager is not active as device administrator. ○ The USB debug mode is disabled		
Test procedure		
Action		**Expected Result**
1	Go to field “Set User Pin”, enter less then **4** characters and tap on “Save Configuration” button (or “Save” button on keyboard layout)	An error message “**Invalid pin**” is shown.
2	Go to first field “Set User Pin” enter at least **4** characters. Go to second field “Confirm User Pin”, enter a different pin and save	An error message “**Confirm pin does not match**” is shown
3	Go to second field “Confirm User Pin”, enter the same pin. Change the default value of Max Admin and User Login Attempts Change the default value of user authentication session timeout Save	A message “**Configuration saved**” is shown
4	Check “Enable Device Admin”	A system dialog is opened to activate Security Manager as device administrator (*).
5	Check “Enable USB Debug Mode”	A message to confirm that USB is on debug mode is shown(**)
Comment		
(*) This will allow Security Manager to erase all data from device (wipe to factory reset), otherwise a security exception will occur when Security Manager will try to perform this operation (**) In order to be able setting USB in debug mode Security Manager must be signed with platform key otherwise a security exception will occur.		

3.1.4 SM_GUI_4 – Logout Administrator

Security Manager GUI		
SM_GUI_4 **Logout Administrator**		
Objective(s)		
Logout administrator		
Pre-Conditions		
○ The administrator was logged in and the preference of Security Manager is opened		
Test procedure		
Action		**Expected Result**
1	Tap on “Logout” button	The preference of Security Manager is closed. All services with category “eu.isitep.SERVICE" are launched and a notification for each of them is shown(*)
Comment		
(*) This ensure that service with no GUI and configured to start at boot are loaded from system in order to enable receiver with filter action “android.intent.action.BOOT_COMPLETED”		

3.2 Test Security Manager Service

3.2.1 SM_SERV_1 – Security Manager Run As Service

Security Manager Service		
SM_SERV_1 **Security Manager Run As Service**		
Objective(s)		
Verify that Security Manager run as Service starting on boot device		
Pre-Conditions		
○ The administrator password was set (this ensure that SM GUI was launched)		
Test procedure		
Action		**Expected Result**
1	Reboot device	At boot completed a notification appears with Security Manager service status

3.2.2 SM_SERV_2 – End-User Authentication Request (need enter user pin)

Security Manager Service		
SM_SERV_2 **User Authentication Request**		
Objective(s)		
Security Manager authenticate the end-user		
Pre-Conditions		
○ End-user is not authenticated on terminal or session timeout is reached after last authentication request		
Test procedure		
Action		**Expected Result**
1	An added value application requests authentication by sending an “authenticateOpReq” message on Android Broadcast Bus	SM receive message “authenticateOpReq” from bus. The activity to enter user pin is opened
2	In the “Enter User Pin” field, enter less than **4** characters and tap on “Sign In” button (or “Sign in” button on keyboard layout)	An error message “**Invalid pin**” is shown on the screen. The number of available login tentative does not change
3	Go to field “Enter User Pin”, enter a wrong pin with at least 4 characters, and Sign in	An error label “**Incorrect pin**” is shown on the screen. The number of available login tentative is decremented by one. A message “authFailed” is sent on bus. If the number of available login tentative to zero the device shall be wiped.
4	Tap on “Cancel” Button	A message “authCancel” is sent on bus.
5	Go to field “Enter User Pin”, enter a correct pin and Sign in	A message “activateCM” is sent on Android Broadcast Bus. All services with category “eu.isitep.SERVICE" are launched and a notification for each of them is shown(*) A message “authSuccesful” is sent on Android Broadcast Bus.
Comment		
(*) This ensure that all service of ISITEP system are running after login		

3.2.3 SM_SERV_3 – End-User Authentication Request (don't need enter user pin)

Security Manager Service		
SM_SERV_3 **User Authentication Request**		
Objective(s)		
Security Manager authenticate the end-user		
Pre-Conditions		
○ End-user was authenticated and no session timeout is reached after last authentication request		
Test procedure		
Action		**Expected Result**
1	An added value application request authentication sending a "authenticateOpReq" message on Android Broadcast Bus	SM receive message "authenticateOpReq" from bus. A message "authSuccesful" is sent on Android Broadcast Bus.

3.2.4 SM_SERV_4 – Security Manager receive notification about network availability

Security Manager Service		
SM_SERV_4 **Security Manager receive notification about network availability**		
Objective(s)		
Security Manager update its status base on network availability		
Pre-Conditions		
○ End-User was logged on terminal		
Test procedure		
Action		**Expected Result**
1	A message "commServiceAvailIndication" is sent on bus from CM.	SM receive message "commServiceAvailIndication" from bus and update its status and shown a notification.

3.2.5 SM_SERV_5 – Security Manager encrypt data

Security Manager Service	
SM_SERV_5 **Security Manager encrypt data**	
Objective(s)	
Security Manager encrypts data	
Pre-Conditions	
○ End-User was logged on terminal	
Test procedure	
Action	**Expected Result**
1 A message “archiveData” is sent on bus from an Added Value Application Testing with ISITEP Test App go to “Data Security” tab, enter some text in “Plain Text” field and tap on “ARCHIVEDATA” button	SM receive message “archiveData” from bus. SM encrypts content of message and sends a message “storeEncryptedData” on bus with encrypted data. Testing with ISITEP Test App the “storeEncryptedData” message is received and encrypted message is shown on “Encrypted Data” field.

3.2.6 SM_SERV_6 – Security Manager decrypt data

Security Manager Service	
SM_SERV_6 **Security Manager decrypt data**	
Objective(s)	
Security Manager decrypts data	
Pre-Conditions	
○ End-User was logged on terminal	
Test procedure	
Action	**Expected Result**
1 A message “retrieveArchive” is sent on bus from an Added Value Application	SM receive message “retrieveArchive” from bus. If session timeout is reached after last authentication request, the end-user authentication procedure is performed. SM decrypts content of message and sends a message “decryptedData” on bus with data decrypted

	Testing with ISITEP Test App after perform test SM_SERV_5 clear content of "Plain Text" and tap on "RETRIEVEDATA" button	Testing with ISITEP Test App the "decryptedData" message is received and decrypted message is shown on "Plain Text" field.

3.2.6 SM_SERV_7 – Security Manager remote request of wipe device

Security Manager Service		
SM_SERV_7 **Security Manager remote request of wipe device**		
Objective(s)		
Security Manager wipe device after receives a remote request		
Pre-Conditions		
○ Network is available		
Test procedure		
Action		**Expected Result**
1	An SDS request is sent from SM server-side	SM verifies network availability. SM sends a SDS to confirm received request SM wipes the device

3.2.6 SM_SERV_8 – Logout User

Security Manager Service		
SM_SERV_8 **Logout User**		
Objective(s)		
Security Manager deactivate CM and notify HMI to logout		
Pre-Conditions		
○ End-User was logged on terminal		
Test procedure		
Action		**Expected Result**
1	A message "logoutCurrentUser" is sent on bus from HMI	SM receive message "logoutCurrentUser" from bus. SM send message "deactivateCM" on bus. SM send message "logoutSuccesful" on bus. HMI receive message "logoutSuccesful" and close itself

4 REQUIREMENT MAPPING

In this section, the test cases are mapped on the project requirements.

Each test suite is mapped over a requirement and contains several test cases.

4.1 Test Security Manager GUI

REQUIREMENT ID	REQUIREMENT DESCRIPTION	TEST CASE ID
REQ#4	The SM shall be able to configure the USB port as device	SM_GUI_3

4.1 Test Security Manager Service

REQUIREMENT ID	REQUIREMENT DESCRIPTION	TEST CASE ID
REQ#1	The SM shall run as service	SM_SERV_1
REQ#2	The SM shall be able to activate CM on user authentication	SM_SERV_2
REQ#3	The SM shall be able to receive form CM availability of the TETRA/TETRAPOL network	SM_SERV_4
REQ#5	SM shall be able to encrypt data	SM_SERV_5
REQ#6	SM shall be able to decrypt data	SM_SERV_6

5 TEST REPORT

TEST ID	TEST TITLE	EXECUTION DATE	RESULT	BUG ID	NOTE
SM_GUI_1	Test Security Manager GUI	30/03/2016	Passed		
SM_GUI_2	Login Administrator	30/03/2016	Passed		
SM_GUI_3	Setting Security Manager Preference	30/03/2016	Passed		
SM_GUI_4	Logout Administrator	19/04/2016	Passed		
SM_SERV_1	Security Manager Run As Service	06/04/2016	Passed		
SM_SERV_2	End-User Authentication Request	11/04/2016	Passed		
SM_SERV_3	End-User Authentication Request	11/04/2016	Passed		
SM_SERV_4	Security Manager receive notification about network availability	11/04/2016	Passed		
SM_SERV_5	Security Manager encrypt data	11/04/2016	Passed		
SM_SERV_6	Security Manager decrypt data	11/04/2016	Passed		
SM_SERV_7	Security Manager remote request of wipe device	11/04/2016	Passed		
SM_SERV_8	Logout User	19/04/2016	Passed		

6 REFERENCES

[1] ISITEP D 2.2.2 Security Requirements
[2] ISITEP D 5.3.2 Security Manager Design Description