TETRA ASSOCIATION

ISCTI

TETRA Interoperability Certificate

Motorola, Dimetra IP, SwMI – Cassidian, THR880i, Terminal

Copenhagen, January 2011

Latest Certified SwMI SW Release:	7.1	**Latest Certified Terminal SW Release:**	6.H1-2_016
Latest Certified SwMI HW Release:	7.1	**Latest Certified Terminal HW Release:**	RC-10

ISCTI (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) certifies, that the Motorola, Dimetra IP, SwMI and the Cassidian, THR880i, terminal have been subject to interoperability testing for the "certified" features listed on second page of this certificate, in accordance with the TETRA Interoperability Profiles, TIP compliance Test Plan and related TETRA interoperability requirement tables.

The table lists all the available TETRA interoperability profiles, and summarizes the main functionalities of every profile according to the TETRA interoperability requirement tables.

A feature is **"Certified"** when it has been successfully tested during the last test session with one of the testing method described in the TETRA process document part 1 (TPD001).

A breakdown into the feature details is given in the Feature Compliance Overview section of this certificate.

Detailed test results and explanation about the procedure used to provide verdicts are listed in the Test Report associated to this Certificate.

IOP test engineer
Franco Pangallo

IOP test engineer
Ivano Luciani

Radio Office Manager
Giuseppe Pierri

Date of issue:
24 June 2011
v 01

ISCTI - V.le America 201, 00144 Rome, Italy
Ph.: +39 06 5444 2663, Fax: +39 06 5410904
e-mail: tetra_ctc.iscom@sviluppoeconomico.gov.it,
Web: www.sviluppoeconomico.gov.it

Certified features

Tetra Association TTR001-04:Auth	
SwMI Initiated (non-mutual) Authentication	Partial
SwMI Initiated Authentication made Mutual by MS	Certified
TEI Query	-
Tetra Association TTR001-11:AIE	
Security Class 2 Air Interface Encryption	-
Security Class 3 Air Interface Encryption	-
Security Class 3G Air Interface Encryption	-
Change of CMG and GSKO	Certified
Key Status demand	Certified
Change of Security Class for Fallback operation	Certified
Change of Security Class (other than for Fallback operation)	Certified
Key Management for Secure Direct Mode Operation	-

Feature Compliance Overview

The first pages of this certificate provide an indication about the main interoperable TETRA features for each TIP specification (as described in the TIC-RT). The main interoperable TETRA features result depend on a set of sub-feature, the verdicts associated to each sub-feature are directly derived from the analysis of the performed test cases.
The results associated to each feature and sub-feature are shown in the "Feature compliance report" table below. The main features are indicated with grey background and the associated sub-features (or second level features) have white background.

The verdict assigned to a sub-feature as shown on page 2, is derived by the Feature compliance report tables.

Verdict	Definition
Certified	All required tests have been performed and passed
Partial	Not all the required tests have been performed but none have failed
–	Feature cannot be certified e.g. it is not supported by at least one product, no tests were performed, or some tests were performed but at least one failed

The verdict assigned to a sub feature is the result of an analysis of the test case results listed in the Test Report. The verdict assigned to each sub-feature is derived from one or several test case results or test steps result, the TETRA Interoperability requirement tables (TIC-RTs) indicate the link between sub-features and test cases for the certified set of equipment capabilities (see Test Report)

Verdict	Definition
Passed (note x)	All mandated tests or steps of tests linked to this functionality (as per TIC-RT indication) are compliant with the TIP specification relevant to this feature. A note can be associated to this result, if further clarification on the behaviour of the equipment is needed
Time_limited	Not all Mandated tests (as per TIC-RT indication) have been executed (ran out of time)

The verdict associated to the feature gives also indication about the method used to test that feature. The allowed testing Methods are listed in the table below, a complete description of the procedures and constraints associated to each of them can be found in the "TPD001 TETRA Interoperability Certification Process

Description" document.

Testing Method	Description
Complete	All mandated tests associated to the feature have been executed
Spot	Only a selection of the mandatory test cases associated to the feature has been executed during the test session. These tests are a subset of the tests performed on an equivalent software which has been "completely" tested against the same functionality on a different equipment, see manufacturer declaration in annex A
Regression	Only a selection of the mandatory test cases associated to the feature has been executed during the test session. These tests are a subset of the tests performed on a previous version of the same software which has been "completely" tested in a previous test session against the same functionality, see manufacturer definition in annex A
Regression on spot	The regression method has been applied on the verdicts based on the spot testing method

Depending on equipment capabilities declared by the manufacturer, some features or sub features cannot be tested. The following table describes meaning of the used abbreviation

Indication	Definition
Not Supported	The SwMI and/or MS do not support the minimum features required to verify these items.

ISCTI has made every effort to ensure that every result has been correctly evaluated in accordance with the relevant TIPs, Test Plans and TIC-RTs. ISCTI has no liability for the test results, or towards the manufacturers,

The table on the following page lists HW and SW releases of SwMI and Terminal under test in the last four test sessions and the used TIP specifications, Test Plans and TIC-RTs

This Certificate and Certificates from previous test sessions are available on the TETRA Association web site (http://www.tetra-association.com/tetramou.aspx?&id=2636).

The feature results are shown in the tables below

Information on equipment under test and document references

Test Session Date/Place	Motorola Copenhagen January 2011	Motorola Copenhagen January 2009		
SwMI Type	Dimetra IP	Dimetra IP 6.2SSR		
SwMI HW Release	7.1	Dimetra IP		
SwMI SW Release	7.1	6.2SSR		
Terminal Type	THR880i	THR880i		
Terminal HW Release	RC-10	RC-10		
Terminal SW Release	6.H1-2-016	6.29-2-004		
TIP Specs and TIP Compliance Test Plans				
Auth	TTR001-04 v3.0.0 IOP001-04 v2.0.0 TIC-RT001-04 v222	Not Tested		
AIE	TTR001-11 v3.0.0 IOP001-11 v3.0.0 TIC-RT001-11 v3018	Not Tested		

Feature compliance report

Test Session	Motorola Copenhagen January 2011	Motorola Copenhagen January 2009		
Authentication				
SwMI Initiated (non-mutual) Authentication	PASSED No_Equipment 1_pass_of_3	-		
Attach with authentication	No_Equipment 0_pass_of_1	-		
Roaming with authentication	No_Equipment 0_pass_of_1	-		
SwMI rejects MS during authentication	PASSED Complete 1_pass_of_1	-		
MS rejects SwMI during authentication	Not Supported	-		
SwMI Initiated Authentication made Mutual by MS	PASSED Complete 2_pass_of_2	-		
Attach with authentication	PASSED Complete 1_pass_of_1	-		
Roaming with authentication	PASSED Complete 1_pass_of_1	-		
TEI Query		-		
TEI Query Operation	Not Supported	-		
Air Interface Encryption				
Security Class 2 Air Interface Encryption	FAILED Complete 15_pass_of_18	-		
Location Updating and AI Signalling Protection	FAILED Complete 5_pass_of_7	-		
TM-SCK provisioning during location updating	FAILED Complete 1_pass_of_2	-		
Communications between parties using encryption	PASSED Complete 2_pass_of_2	-		
Communications between clear and encrypted parties	PASSED Complete 3_pass_of_3	-		

Communications between encrypted parties on a channel designated to operate in clear	PASSED Complete 2_pass_of_2	-		
OTAR and Change of TM-SCK	FAILED Complete 3_pass_of_4	-		
Security Class 3 Air Interface Encryption	FAILED Complete 17_pass_of_18	-		
Location Updating and AI Signalling Protection	PASSED Complete 7_pass_of_7	-		
DCK Forwarding at MS request	Not Supported	-		
DCK Forwarding by SwMI (without MS request)	Not Supported	-		
DCK Retrieval	PASSED Complete 4_pass_of_4	-		
CCK provisioning during location updating	PASSED Complete 3_pass_of_3	-		
Communications between parties using encryption	PASSED Complete 2_pass_of_2	-		
Communications between clear and encrypted parties	PASSED Complete 3_pass_of_3	-		
Communications between encrypted parties on a channel designated to operate in clear	PASSED Complete 2_pass_of_2	-		
OTAR and Change of CCK	FAILED Complete 3_pass_of_4	-		
Security Class 3G Air Interface Encryption	FAILED Complete 7_pass_of_8	-		
GCK Key Association setting	PASSED Complete 2_pass_of_2	-		
Communications between parties using encryption	PASSED Complete 2_pass_of_2	-		
Communications between clear and encrypted parties	PASSED Complete 1_pass_of_1	-		
OTAR and Change of GCK	FAILED Complete 2_pass_of_3	-		
Change of CMG and GSKO	PASSED Complete 5_pass_of_5	-		
OTAR and change of CMG and GSKO	PASSED Complete 5_pass_of_5	-		
Key Status demand	PASSED Complete 3_pass_of_3	-		
SCK Key Status demand	PASSED Complete	-		

	1_pass_of_1			
GCK Key Status demand	PASSED Complete 1_pass_of_1	-		
GSKO Key Status demand	PASSED Complete 1_pass_of_1	-		
Change of Security Class for Fallback operation	PASSED Complete 12_pass_of_12	-		
Seamless change to Security Class 2 for BS Fallback operation	PASSED Complete 10_pass_of_10	-		
Non-seamless change to Security Class 2 for BS Fallback operation	Not Supported	-		
Provisioning of TM-SCK for fallback to Security Class 2 operation	PASSED Complete 2_pass_of_2	-		
Change to Security Class 1 for BS Fallback operation	Not Supported	-		
Change of Security Class (other than for Fallback operation)	PASSED Complete 5_pass_of_5	-		
Change between Security Class 3 and Security Class 3G	PASSED Complete 2_pass_of_2	-		
Change between Security Class 2 and Security Class 3	PASSED Complete 2_pass_of_2	-		
Change from Security Class 3G to Security Class 2	PASSED Complete 1_pass_of_1	-		
Key Management for Secure Direct Mode Operation		-		
OTAR and change of DM-SCK	Not Supported	-		