TETRA Interoperability Certificate

AIRBUS DEFENCE AND SPACE, TETRA System Rel7.0, SwMI – Hytera, MT680 Plus, Terminal

Helsinki, April 2017

Latest Certified SwMI SW Release:	Rel7.0 SCD 4.0	**Latest Certified Terminal SW Release:**	V3.08
Latest Certified SwMI HW Release:	M98F (DXTip)	**Latest Certified Terminal HW Release:**	126800

ISCTI (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione) certifies, that the AIRBUS DEFENCE AND SPACE, TETRA System Rel7.0, SwMI and the Hytera, MT680 Plus, 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 (TPD001-01).

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

This certificate has been issued following a fully witnessed single test session between AIRBUS DEFENCE AND SPACE and Hytera on April 2017. Detailed test results are listed in the Test Report associated to this Certificate. Details and explanation about the procedure used to provide verdicts are in the TIC process TPD001-01.

IOP test engineer

Stefano Fransesini

Head of the Procedure

Ivano Luciani

Radio Office Manager

Giuseppe Pierri

ISCTI - V.le America 201, 00144 Rome, Italy
Ph.: +39 06 5444 2135, Fax: +39 06 5410904
e-mail: tetra_ctc.iscom@mise.gov.it,
Web: www.mise.gov.it

Date of issue
18 May 2017
v1

Certified features

Tetra Association TTR001-04:Auth	
SwMI Initiated (non-mutual) Authentication	Certified
SwMI Initiated Authentication made Mutual by MS	Certified
TEI Query	Certified
Tetra Association TTR001-11:AIE	
Security Class 2 Air Interface Encryption	Certified
Security Class 3 Air Interface Encryption	Certified
Security Class 3G Air Interface Encryption	-
Management of CMG and GSKO	-
Key Status demand	-
Change of Security Class for Fallback operation	Certified
Change of Security Class (other than for Fallback operation)	-
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' results depend on a set of sub-features, 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 blue background and the associated sub-features (or second level features) have a white background.

The outcome assigned to a feature as shown on page 2, is derived by the Feature Compliance Report tables.

Outcome	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 outcome is derived from the verdict assigned to a sub feature which 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	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 or sub-feature
Incomplete	Not all Mandated tests (as per TIC-RT indication) have been executed
Failed	At least one of mandated test or steps of tests linked to this functionality failed to match the TIP specification relevant to this feature or sub-feature

The verdict associated to the feature or sub-feature gives also indication about the method used to test that feature or sub-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 "TPD001-01 TETRA Interoperability Certification Process Description" document.

Testing Method	Description
Complete	All mandated tests associated to the feature or sub-feature have been executed
Spot	Only a selection of the mandatory test cases associated to the feature or sub-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 the associated Test Report

Regression	Only a selection of the mandatory test cases associated to the feature or sub-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 the associated Test Report
Regression on spot	The regression method (see the previous item) has been applied at this session on the verdicts from the referenced (previous) session where the spot testing method (see above) had been applied.
Witnessed	The TIP heading lines in the Feature Compliance Report indicate whether each TIP is partially or fully witnessed by the Certification Body. Additionally, for a partially-witnessed TIP, the number of witnessed test cases that passed is shown for each the feature and sub-feature. There may have been some un-witnessed passed tests and they will have been found to be successful based on the log file evaluation

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 + Critical Communications Association web site (https://tandcca.com/interoperability/interoperability-certificates-and-test-reports/).

The feature results are shown in the tables below.

Information on equipment under test and document references

Test Session Date/Place	AIRBUS DEFENCE AND SPACE, Helsinki, April 2017			
SwMI Type	TETRA System Rel7.0			
SwMI HW Release	M98F (DXTip)			
SwMI SW Release	Rel7.0 SCD 4.0			
Terminal Type	MT680 Plus			
Terminal HW Release	126800			
Terminal SW Release	V3.08			
TIP Specs and TIP Compliance Test Plans				
Auth	TTR001-04 v3.0.0 IOP001-04 v2.0.0 TIC-RT001-04 v230			
AIE	TTR001-11 v3.0.3 IOP001-11 v3.1.0 TIC-RT001-11 v331			

b

Feature compliance report

Test Session	AIRBUS DEFENCE AND SPACE, Helsinki, April 2017			
Auth - Fully Witnessed Testing				
SwMI Initiated (non-mutual) Authentication	Spot 0_pass_of_3			
Attach with authentication	Spot 0_pass_of_1			
Roaming with authentication	Spot 0_pass_of_1			
SwMI rejects MS during authentication	Spot 0_pass_of_1			
MS rejects SwMI during authentication	Not Supported			
SwMI Initiated Authentication made Mutual by MS	Spot 0_pass_of_2			
Attach with authentication	Spot 0_pass_of_1			
Roaming with authentication	Spot 0_pass_of_1			
TEI Query	PASSED Complete 1_pass_of_1			
TEI Query Operation	PASSED Complete 1_pass_of_1			
AIE - Fully Witnessed Testing				
Security Class 2 Air Interface Encryption	PASSED Spot 1_pass_of_2			
Location Updating and AI Signalling Protection	PASSED Complete 1_pass_of_1			
TM-SCK provisioning during location updating	Not Supported			
Communications between parties using encryption	Spot 0_pass_of_1			
Communications between clear and encrypted parties	Not Supported			
Communications between encrypted parties on a channel designated to operate in clear	Not Supported			
OTAR of TM-SCK	Not Supported			

Change of TM-SCK	Not Supported			
Packet Data with Class 2 Air Interface Encryption	Not Supported			
Tolerance of SwMI not supporting SCK-OTAR	Not Supported			
Security Class 3 Air Interface Encryption	PASSED Spot 4_pass_of_18			
Clear Location Updating and AI Signalling Protection	PASSED Spot 1_pass_of_3			
Encrypted Location Updating and AI Signalling Protection	PASSED Spot 1_pass_of_4			
DCK Forwarding at MS request	PASSED Spot 1_pass_of_3			
DCK Forwarding by SwMI (without MS request)	Not Supported			
DCK Retrieval	Spot 0_pass_of_1			
CCK provisioning during location updating	PASSED Spot 1_pass_of_3			
Communications between parties using encryption	PASSED Spot 1_pass_of_2			
Communications between clear and encrypted parties	Spot 0_pass_of_3			
Communications between encrypted parties on a channel designated to operate in clear	PASSED Spot 1_pass_of_2			
OTAR of CCK	Spot 0_pass_of_2			
Change of CCK	Spot 0_pass_of_3			
Packet Data with Class 3 Air Interface Encryption	Spot 0_pass_of_1			
Security Class 3G Air Interface Encryption				
GCK Key Association setting	Not Supported			
Communications between parties using encryption	Not Supported			
Communications between clear and encrypted parties	Not Supported			
OTAR of GCK	Not Supported			
Change of GCK	Not Supported			
Management of CMG and GSKO				
OTAR and change of CMG and GSKO	Not Supported			
Key Status demand				
SCK Key Status demand	Not Supported			
GCK Key Status demand	Not Supported			
GSKO Key Status demand	Not Supported			

Change of Security Class for Fallback operation	PASSED Spot 1_pass_of_4			
Seamless change to Security Class 2 for BS Fallback operation	Not Supported			
Non-seamless change to Security Class 2 for BS Fallback operation	PASSED Spot 1_pass_of_3			
Provisioning of TM-SCK for fallback to Security Class 2 operation	Not Supported			
Change to Security Class 1 for BS Fallback operation	Spot 0_pass_of_1			
Change of Security Class (other than for Fallback operation)				
Change between Security Class 3 and Security Class 3G	Not Supported			
Change between Security Class 2 and Security Class 3	Not Supported			
Change from Security Class 3G to Security Class 2	Not Supported			
Key Management for Secure Direct Mode Operation				
OTAR of DM-SCK	Not Supported			
Change of DM-SCK	Not Supported			