EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

EUROCONTROL SPECIFICATION of Interoperability and Performance Requirements for the Flight Message Transfer Protocol (FMTP)

EUROCONTROL SPECIFICATION DOCUMENT IDENTIFIER: SPEC.COM.FMTP

Edition Number	**:**	**1.0**
Edition Date	**:**	**24/02/2006**
Status	**:**	**Proposed Issue**
Intended for	**:**	**General Public**
Category	**:**	**EUROCONTROL Specification**

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
EUROCONTROL Specification of Interoperability and Performance Requirements for the Flight Message Transfer Protocol (FMTP)		
	Reference:	
Document Identifier	**Edition Number:**	1.0
	Edition Date:	24/02/2006

Abstract

This document specifies the interoperability and performance requirements for implementations of the Flight Message Transfer Protocol (FMTP). The FMTP is used, in a peer-to-peer communications context, for the information exchanges between flight data processing systems. In particular, for the purpose of notification, co-ordination and transfer of flights between air traffic control units and for the purposes of civil-military co-ordination.

Keywords

FMTP | Specification | Peer-to-peer communications

Contact Person(s)	Tel	Unit
Mr Melvyn REES	+32 2 729 3360	DAS/CSM

DOCUMENT STATUS AND TYPE					
Status		**Intended for**		**Category**	
Working Draft	☐	General Public	☑	EUROCONTROL Rule	☐
Draft	☐	Restricted EUROCONTROL	☐	EUROCONTROL Specification	☑
Proposed Issue	☑			EUROCONTROL Guideline	☐
Released Issue	☐				

ELECTRONIC SOURCE		
Path:	P:\DG\RU\SINGLE EUROPEAN SKY\SES MANDATES _ SES TEAM\INTEROPERABILITY\Flight Message Transfer Protocol\EUROCONTROL_Specification\intermediate version	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	369 Kb

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this document.

AUTHORITY	NAME AND SIGNATURE	DATE
Head of Communication & Surveillance Management	Mr Melvyn REES	8th March 2006
Head of Regulatory Unit	Mr Jean-Luc GARNIER	8th March 2006
Director ATM Strategies	Mr Bo REDEBORN	8th March 2006
Director General	Mr Victor AGUADO	

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1	14/02/06		Creation of EUROCONTROL Specification	All
0.2	20/02/06		Minor updates. Addition of List of Tables	i, ii, vi, 1, 2, 3
1.0	24/02/06		Numbering of non-normative paragraphs	2.2, 5.3, 6.3, 8.4

CONTENTS

1. INTRODUCTION 2
1.1 Purpose 2
1.2 Conventions 2
1.3 Abbreviations and Definitions 2
1.3.1 Abbreviations 2
1.3.2 Definitions 3

2. FMTP Identification and Messages 3
2.1 FMTP Identification Values 3
2.2 Identification Validation 4
2.3 Types of Messages 4

3. FMTP MESSAGE FORMAT 4
3.1 General Structure 4
3.2 Header Field 4
3.3 User Data Messages 5
3.4 Identification Messages 6
3.5 System Messages 6

4. FMTP OPERATIONS 7
4.1 General 7
4.2 FMTP Connection Establishment 7
4.3 FMTP Association Establishment 7
4.4 Data Transfer 8
4.5 FMTP Association Release 8
4.6 FMTP Connection Release 8
4.7 Simultaneous FMTP Association and FMTP Connection Release 9
4.8 FMTP Association Integrity 9

5. PROTOCOL STATE TABLES 10
5.1 General 10
5.2 Protocol Events 10
5.3 State Tables 13

6. TCP TRANSPORT INTERFACE AND SETTINGS 18

6.1 Service Assumed 18
6.2 TCP Connection Establishment 18
6.3 TCP Connection Release 18
6.4 Data Transfer 19
6.5 TCP Timer Settings 19
6.6 TCP Ports 19

7. NETWORK PROTOCOL 19
7.1 Service Assumed 19
7.2 IP Addressing 20
7.3 IP Address Validation 20

8. CHARACTER SETS 20

9. BIT-ORDERING FOR DATA TRANSMISSION 20

10. DATA LINK LAYER REQUIREMENTS 21

11. LIST OF REFERENCES TO BE USED IN INTEROPERABILITY AND PERFORMANCE REQUIREMENTS 21

ANNEX A. IMPLEMENTATION CONFORMITY STATEMENT 22

List of Tables

Table 1: FMTP Message Types 4
Table 2: Message Type Values 5
Table 3: ACCEPT and REJECT Identification Message Data 6
Table 4: System Message Data Values 6
Table 5: Protocol Event List 10
Table 6: FMTP-SM Action List 12
Table 7: State Definitions 13
Table 8: State Table for Outgoing FMTP Connection Establishment (Client) 14
Table 9: State Table for Incoming FMTP Connection Establishment (Server) 16
Table 10: State Table for FMTP Association Establishment and Data Transfer 17

Table A.1: Identification 22
Table A.2: Dynamic Conformity Requirements 23
Table A.3: User Data 24
Table A.4: Message Transfer Protocol 24
Table A.5: Transport Layer 25
Table A.6: Network Layer 25
Table A.7: Data Link Layer 25

EXECUTIVE SUMMARY

This EUROCONTROL Specification defines the interoperability and performance requirements for implementations of the Flight Message Transfer Protocol (FMTP). The FMTP is used, in a peer-to-peer communications context. In particular, for the information exchanges between flight data processing systems for the purpose of notification, co-ordination and transfer of flights between air traffic control units and for the purposes of civil-military co-ordination.

The FMTP is based on industry-standard Transmission Control Protocol / Internet Protocol (TCP/IP) provisions.

An implementation Conformity Statement pro-forma is included as Annex A. Suppliers of systems implementing the FMTP are required to complete the pro-forma tables.

1. INTRODUCTION

1.1 Purpose

This EUROCONTROL Specification defines interoperability and performance requirements for implementations of the Flight Message Transfer Protocol (FMTP). The FMTP is used, in a peer-to-peer communications context, for the information exchanges between flight data processing systems for the purpose of notification, co-ordination and transfer of flights between air traffic control units and for the purposes of civil-military co-ordination.

1.2 Conventions

Throughout this specification, the word “shall” indicates a mandatory requirement, which must be satisfied by all systems claiming conformity to this specification.

1.3 Abbreviations and Definitions

1.3.1 Abbreviations

ASCII	American Standard Code for Information Interchange
FMTP	Flight Message Transfer Protocol
FMTP-SM	Flight Message Transfer Protocol State Machine
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organisation for Standardisation
MT	Message Transfer
RFC	Request For Comments
STD	Internet Standard
TCP	Transmission Control Protocol
UCS	Universal Character Set
UDP	User Datagram Protocol

UTF-8	Universal Character Set Transformation Format 8

1.3.2 Definitions

MT-User	An entity that uses the services delivered by the FMTP for the purpose of exchanging operational flight data messages with a peer MT-User.
FMTP Association	An established relationship between two MT-Users such that the FMTP is in a suitable state to allow the exchange of MT-User messages.
FMTP connection	An established relationship between peer FMTP entities over TCP/IP, in which the peer MT-Users have not yet indicated their readiness to commence the exchange of MT-User messages.
FMTP-Initiator	The FMTP entity that initiates an FMTP connection (TCP/IP client).
FMTP-Responder	The FMTP entity that receives an FMTP connection request from a remote peer (TCP/IP server).
FMTP-SM	Flight message transfer protocol state machine. An abstract entity that implements one end of the FMTP and provides the MT-service to a local MT-User.
Identification value	An octet string identifying the FMTP entity.
Timer Ti	The maximum period of time to receive data during FMTP identification.
Timer Ts	The maximum period of time in which data must be transmitted in order to maintain the FMTP Association.
Timer Tr	The maximum period of time in which data is to be received over an FMTP Association.

2. FMTP IDENTIFICATION AND MESSAGES

2.1 FMTP Identification Values

2.1.1 FMTP identification values are octet strings that shall not exceed 32 octets in length.

2.1.2 The local identification value shall be a configurable parameter.

2.1.3 The known identification values of remote implementations shall be configurable parameters.

2.1.4 The establishment of more than one FMTP connection with a remote MT-User identified by its identification value shall be prohibited.

2.2 Identification Validation

2.2.1 The FMTP implementation shall have access to a local list of identification values corresponding to the remote MT-Users with whom it is necessary to establish communication.

2.2.2 When an Identification message is received, the identification values in the Data field shall be validated against the list of known identification values.

2.2.3 Identification validation shall be deemed successful only if:

a) the received identification values match values indicated in the list, and

b) no active FMTP connection already exists with the remote implementation.

2.3 Types of Messages

2.3.1 The FMTP shall support the types of messages described in Table 1.

Table 1: FMTP Message Types

Message Type	Description
System Messages	Used for FMTP Association integrity (HEARTBEAT message) and FMTP Association control (STARTUP and SHUTDOWN messages).
Operational Messages	Linked to a specific operational context for applications using the FMTP.
Identification Messages	Containing identification values.

2.3.2 The ATC units implementing FMTP shall specify in their letter of agreement whether they will use free text Operator Messages.

3. FMTP MESSAGE FORMAT

3.1 General Structure

3.1.1 All FMTP messages exchanged over the supporting transport connection shall consist of a header field immediately followed by a data field.

3.2 Header Field

3.2.1 The header shall consist of four fields entitled VERSION, RESERVED, LENGTH and TYP fields and appearing in that order.

3.2.2 The VERSION field shall consist of a single octet representing a numerical quantity indicating the header version.

3.2.3 The value of the VERSION field shall be set to 2 for this version of the FMTP.

3.2.4 The RESERVED field shall consist of a single octet representing a numerical quantity.

3.2.5 The value of the RESERVED field shall be set to 0 for this version of the FMTP.

3.2.6 The LENGTH field shall consist of a double octet representing a numerical quantity.

3.2.7 The LENGTH field shall indicate the combined length in octets of the VERSION, RESERVED, LENGTH, TYP and Data fields.

3.2.8 The TYP field shall consist of a single octet representing a numerical quantity.

3.2.9 The TYP field shall be used to indicate the message type that is being transmitted or received, using the TYP values indicated in Table 2.

Table 2: Message Type Values

TYP value	Message Type
1	Operational message
2	Operator message
3	Identification message
4	System message

3.3 User Data Messages

3.3.1 When sending MT-User data, the message type value in the FMTP message shall be set to Operational message or Operator message, depending on the type of data that are to be sent.

3.3.2 When the local user requests to send data, the user data shall be mapped unaltered to the Data field of an FMTP message.

3.3.3 When delivering user data to the local user, the Data field of the received FMTP message shall be provided unaltered.

3.3.4 The FMTP shall support the transmission of MT-User data up to and including 10 240 octets in length.

3.3.5 The FMTP shall prohibit the concatenation of several MT-User data messages into a single DATA field.

3.3.6 The FMTP shall prohibit the segmentation of a MT-User data message into several DATA fields with separate headers.

3.3.7 If Operator messages are supported, a user interface shall be provided to display received messages and to allow the composition of messages for transmission.

3.3.8 The data field of Operator messages shall contain only printable ASCII characters.

3.4 Identification Messages

3.4.1 Apart from ACCEPT and REJECT Identification messages, the Data field of Identification messages shall include:

a) identification value of the sending system, followed by

b) a single hyphen (-), followed by

c) identification value of the intended recipient.

3.4.2 The fixed value Identification Messages (TYP = 3) indicated in Table 3 shall be supported:

Table 3: ACCEPT and REJECT Identification Message Data

Message	Data field contents
ACCEPT message	‘41’H ‘43’H ‘43’H ‘45’H ‘50’H ‘54’H (characters “ACCEPT”)
REJECT message	‘52’H ‘45’H ‘4A’H ‘45’H ‘43’H ‘54’H (characters “REJECT”)

3.5 System Messages

3.5.1 The fixed value System messages (TYP = 4) indicated in Table 4 shall be supported:

Table 4: System Message Data Values

Message	Data field contents
Startup message	'30'H '31'H (characters 01)
Shutdown message	'30'H '30'H (characters 00)
Heartbeat message	'30'H '33'H (characters 03)

4. FMTP OPERATIONS

4.1 General

Note: This section describes the operation of a single MT-User initiated FMTP Association. Further FMTP Associations may be supported on the same network interface by invoking these procedures for each underlying TCP transport connection.

4.1.1 For the protocol to function correctly, the initial value of the timer Ts shall be smaller than the initial value of timer Tr of the FMTP peer.

4.2 FMTP Connection Establishment

4.2.1 When the FMTP-Initiator requests the establishment of an FMTP connection, the FMTP shall initiate the following normal sequence of events:

a) a TCP Transport connection is established between the FMTP entities at each end of the FMTP connection;

b) the FMTP-Responder starts a local timer Ti;

c) the FMTP-Initiator sends an Identification message, and starts a local timer Ti;

d) the FMTP-Responder validates the received Identification message, replies by sending an Identification message back to the FMTP-Initiator, and resets Ti;

e) the FMTP-Initiator validates the received Identification message, sends an Identification ACCEPT message to the FMTP-Responder, and stops Ti;

f) the FMTP-Responder receives the Identification ACCEPT message and stops Ti;

g) both MT-Users are informed that the connection is established.

4.2.2 At the FMTP-Responder, incoming TCP transport connection requests shall be serviced independently of each other.

4.2.3 An FMTP implementation shall be capable of initiating an FMTP connection or servicing an incoming FMTP connection request.

4.3 FMTP Association Establishment

4.3.1 Following FMTP connection establishment, an FMTP Association between two MT-Users shall be established when:

a) each MT-User requests the establishment of an FMTP Association, causing a STARTUP message to be sent over the FMTP connection;

b) each FMTP entity receives a STARTUP message over the FMTP connection and indicates to the local MT-User that the MT-Association is established.

4.3.2 A local timer Tr shall be started or reset when the STARTUP message is sent.

4.3.3 A local timer Ts shall be started when the STARTUP message is received.

4.4 Data Transfer

4.4.1 When it is necessary to send an Operational message or Operator message over an established FMTP Association, the FMTP shall initiate the following normal sequence of events:

a) the local FMTP entity forms an FMTP message with appropriate header and Data fields, and resets timer Ts;

b) the FMTP message is sent over the FMTP Association;

c) on receiving the FMTP message, the FMTP entity at the recipient side validates the message header, provides the Data field to the local user, and resets Tr.

4.5 FMTP Association Release

4.5.1 If an MT-User wishes to end an established FMTP Association, the FMTP shall initiate the following normal sequence of events:

a) the local FMTP entity forms a SHUTDOWN message, sends it over the FMTP Association, and stops timers Ts and Tr;

b) on receiving the SHUTDOWN message, the FMTP entity at the recipient side informs the MT-User that the FMTP Association is ending, stops timer Ts and resets timer Tr;

c) the FMTP connection still exists and a new FMTP Association may be established if required.

4.5.2 To re-establish an ended FMTP Association, the MT-User that requested the end of the Association shall request a new Association, resulting in the transmission of a STARTUP message as above.

4.6 FMTP Connection Release

4.6.1 If an MT-User wishes to end an established FMTP connection, the FMTP shall initiate the following normal sequence of events:

a) the local FMTP entity releases the underlying transport connection;

b) the peer FMTP entity confirms the transport disconnection and informs its local MT-User that the connection is terminated.

4.7 Simultaneous FMTP Association and FMTP Connection Release

4.7.1 If an MT-User wishes to release both an established FMTP Association and the underlying connection, the FMTP shall initiate the following normal sequence of events:

a) the local FMTP entity forms a SHUTDOWN message, sends it over the FMTP Association, and stops timers Ts and Tr;

b) the local FMTP entity requests the release of the underlying transport connection;

c) on receiving the SHUTDOWN message, the FMTP entity at the recipient side informs the MT-User that the FMTP Association is ending, stops timer Ts and resets timer Tr;

d) on receiving notification that the transport service user requested release, the FMTP entity at the recipient side confirms the transport disconnection, informs the MT-User that the FMTP connection is ending and stops timer Tr.

4.8 FMTP Association Integrity

4.8.1 The integrity of the FMTP Association between two MT-Users shall be ensured by the periodic exchange of HEARTBEAT messages at times when no other messages are being exchanged.

4.8.2 The FMTP-SM shall start a configurable timer Ts when the FMTP Association is first established and reset timer Ts when sending any Operational message or Operator message over the FMTP Association.

4.8.3 The FMTP-SM shall start a configurable timer Tr when the FMTP Association is first established and reset timer Tr upon receiving any Operational, Operator, HEARTBEAT or SHUTDOWN message over the FMTP Association.

4.8.4 If the timer Ts expires while an FMTP Association is established, the FMTP entity shall form a HEARTBEAT message, send it over the FMTP Association and reset timer Ts.

5. PROTOCOL STATE TABLES

5.1 General

5.1.1 The FMTP shall behave in accordance with the state tables specified in this section.

5.1.2 In case of discrepancy with the textual description of the FMTP, the state table shall take precedence.

5.2 Protocol Events

5.2.1 The FMTP-SM shall respond to events which are:

a) requested by the local MT-User,

b) indicated by the underlying transport service, using TCP service indication primitives, and

c) occurring when specified periods of time elapse.

5.2.2 The FMTP-SM shall support the protocol events specified in Table 5.

Table 5: Protocol Event List

Event Name	Event Description
MT-CON rq	The MT-User requests the establishment of an FMTP connection.
MT-DIS rq	The MT-User requests to stop an existing FMTP Association and release the underlying connection.
MT-DATA rq	The MT-User requests that data (Operational or Operator message) be sent from the local to the remote user over an existing FMTP Association.
MT-STOP rq	The MT-User requests to stop an existing FMTP Association without releasing the underlying connection.
MT-ASSOC rq	The MT-User requests the establishment of an FMTP Association over an established FMTP connection.
R_setup	A TCP transport connection establishment indication has been received by the TCP client or server (T-Connect→Ind).
R_disconnect	A TCP transport connection release indication has been received (T-Disconnect→Ind).

Event Name	Event Description
R_data	An FMTP message (Operational or Operator message type) has been received from the remote user.
R_accept	An ACCEPT identification message has been received from the remote peer.
R_reject	A REJECT identification message has been received.
R_id (valid)	An identification message containing a valid identification value for the peer MT-User has been received.
R_id (bad)	An identification message which fails the identification value validation test has been received.
R_heartbeat	A HEARTBEAT message has been received from the remote system.
R_shutdown	A SHUTDOWN message has been received from the remote system.
R_startup	A STARTUP message has been received from the remote system.
Ts_timeout	Expiry of timer Ts for sending a HEARTBEAT to the remote user.
Tr_timeout	Expiry of timer Tr when a HEARTBEAT or a data message is expected.
Ti_timeout	Expiry of timer Ti when an Identification message is expected.

5.2.3 The FMTP-SM shall support the actions specified in Table 6.

Table 6: FMTP-SM Action List

Action Name	Action Description
T-CON rq	Issue T-Connect→Req service primitive
T-Dis rq	Issue T-Disconnect→Req service to release the TCP transport connection
T-DAT rq	Issue T-Data→Req service primitive with MT-User data as parameter
IDENT	Issue T-Data→Req service primitive with Identification message as user data
ACCEPT	Issue T-Data→Req service primitive with ACCEPT identification message as user data
REJECT	Issue T-Data→Req service primitive with REJECT message as user data
STARTUP	Issue T-Data→Req service primitive with STARTUP message as user data
SHUTDN	Issue T-Data→Req service primitive with SHUTDOWN message as user data
HEARTBT	Issue T-Data→Req service primitive with HEARTBEAT message as user data
MT-CON ind	Indication to the local MT-User that an FMTP connection request has been received
MT-DIS ind	Indication to the local MT-User that an FMTP disconnection request has been received
MT-ASS ind	Indication to the local MT-User that an FMTP Association establishment request has been received
MT-STOP ind	Indication to the local MT-User that an FMTP Association release request has been received
MT-DATA ind	Received MT-User data are provided to the local MT-User
Start Ti	Timer Ti is started or, if already running, reset.
Stop Ti	Timer Ti is stopped, no timeout event occurs.

Action Name	Action Description
Start Tr	Timer Tr is started or, if already running, reset.
Stop Tr	Timer Tr is stopped, no timeout event occurs.
Start Ts	Timer Ts is started or, if already running, reset.
Stop Ts	Timer Ts is stopped, no timeout event occurs.

5.3 State Tables

5.3.1 The FMTP shall behave as though each local protocol entity contains a state machine that can exist only in one of the states indicated in Table 7.

Table 7: State Definitions

State Name	Abbreviation	Description
IDLE	IDLE	No protocol instance exists. TCP server is bound to the TCP listening port; this corresponds to the TCP LISTEN state. TCP client can launch a TCP transport connection request.
CONNECTION_PENDING	CONN_P	The TCP client has launched the TCP 3-way handshake and is waiting for establishment of an FMTP connection. This state is applicable to the MT-Initiator system only.
SYSTEM_ID_PENDING	SYSID_P	TCP transport connection established on TCP server and awaiting remote system identification message. This state is applicable to the MT-Responder system only.
ID_PENDING	ID_P	TCP transport connection is established, awaiting a response for the transmitted system identification message.
READY	READY	TCP transport connection is established, system identification completed, FMTP Association ready to be established by local user.
ASSOCIATION_PENDING	ASSOC_P	Waiting for remote STARTUP to enter DATA_READY.
DATA_READY	DATA_RY	Ready to exchange operational messages.

5.3.2 Initially the FMTP-SM shall be in the IDLE state.

Note: In the state tables Table 8, Table 9 and Table 10, the intersection of an incoming event (row) and a state (column) forms a cell. A non-blank cell represents an incoming event and state combination that is defined for the FMTP-SM. Such a cell contains a mandatory action list, which contains:

a) a list of actions, and

b) a resultant state, indicated by an arrow symbol (->) and the name of the new state.

5.3.3 When an incoming event occurs, the FMTP-SM shall perform the action(s) indicated then make the transition to the new state, as indicated by the cell corresponding to the combination of incoming event and current state.

5.3.4 A blank cell represents the combination of an incoming event and a state that is not defined for the FMTP-SM; such events shall not cause a state transition or any action that is visible to MT-Users.

5.3.5 When the FMTP-SM is in a given state, any incoming event that is not specified for that state shall be treated as a blank cell.

Table 8: State Table for Outgoing FMTP Connection Establishment (Client)

Incoming Event	**FMTP-SM State**		
	IDLE	**CONN_P**	**ID_P**
MT-CON rq	T-Con rq -> CONN_P		
R_setup		IDENT Start Ti -> ID_P	
MT-DIS rq		T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_disconnect		T-Dis rq MT-DIS ind -> IDLE	T-Dis rq Stop Ti MT-DIS ind -> IDLE
R_data			Stop Ti T-Dis rq MT-DIS ind -> IDLE
R_accept			Stop Ti T-Dis rq MT-DIS ind -> IDLE

Incoming Event	FMTP-SM State		
	IDLE	CONN_P	ID_P
R_reject			Stop Ti T-Dis rq MT-DIS ind -> IDLE
R_id (valid)			Stop Ti ACCEPT MT-CON ind -> READY
R_id (bad)			REJECT Stop Ti T-Dis rq MT-DIS ind -> IDLE
R_heartbeat			Stop Ti T-Dis rq MT-DIS ind -> IDLE
R_shutdown			Stop Ti T-Dis rq MT-DIS ind -> IDLE
R_startup			Stop Ti T-Dis rq MT-DIS ind -> IDLE
Ti_timeout			T-Dis rq MT-DIS ind -> IDLE

Table 9: State Table for Incoming FMTP Connection Establishment (Server)

Incoming Event	FMTP-SM State		
	IDLE	**SYSID_P**	**ID_P**
R_setup	Start Ti -> SYSID_P		
MT-DIS rq		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_disconnect		T-Dis rq Stop Ti -> IDLE	T-Dis rq Stop Ti -> IDLE
R_data		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_accept		Stop Ti T-Dis rq -> IDLE	Stop Ti MT-CON ind -> READY
R_reject		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_id (valid)		IDENT Start Ti -> ID_P	Stop Ti T-Dis rq -> IDLE
R_id (bad)		REJECT Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_heartbeat		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_shutdown		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
R_startup		Stop Ti T-Dis rq -> IDLE	Stop Ti T-Dis rq -> IDLE
Ti_timeout		T-Dis rq -> IDLE	T-Dis rq -> IDLE

Table 10: State Table for FMTP Association Establishment and Data Transfer

Incoming Event	FMTP-SM State		
	READY	**ASSOC_P**	**DATA_RY**
MT-DIS rq	T-Dis rq -> IDLE	SHUTDN Stop Tr T-Dis rq -> IDLE	SHUTDN Stop Tr, Stop Ts T-Dis rq -> IDLE
R_disconnect	T-Dis rq MT-DIS ind -> IDLE	Stop Tr T-Dis rq MT-DIS ind -> IDLE	Stop Tr, Stop Ts T-Dis rq MT-DIS ind -> IDLE
MT-DATA rq			Start Ts T-DAT rq -> DATA_RY
MT-STOP rq		SHUTDN Stop Tr -> READY	SHUTDN Stop Tr, Stop Ts -> READY
MT-ASSOC rq	Start Tr STARTUP -> ASSOC-P		
R_data			Start Tr MT-DATA ind -> DATA_RY
R_heartbeat			Start Tr -> DATA_RY
R_shutdown			Stop Ts, Start Tr MT-STOP ind -> ASSOC_P
R_startup		STARTUP Start Tr, Start Ts MT-ASS ind -> DATA_RY	
Ts_timeout			HEARTBT Start Ts -> DATA_RY
Tr_timeout		STARTUP Start Tr -> ASSOC_P	Stop Ts, Stop Tr T-Dis rq MT-DIS ind -> IDLE

6. TCP TRANSPORT INTERFACE AND SETTINGS

6.1 Service Assumed

6.1.1 The FMTP shall operate over a TCP connection-mode transport service, as defined in Internet standard STD 0007 or RFC 793.

6.1.2 The TCP service shall satisfy the transport layer requirements of RFC 1122, section 4.2.

6.1.3 The following TCP services and primitives shall be provided:

a) T-Connect request and indication, for TCP connection establishment

b) T-Data request and indication, for data transfer over an established connection

c) T-Disconnect request and indication, for TCP connection release.

6.2 TCP Connection Establishment

6.2.1 Systems implementing the FMTP shall be capable of supporting multiple simultaneous TCP transport connections.

Note: Systems may use the IP stack for other TCP or UDP applications.

6.2.2 Systems implementing the FMTP shall be capable of initiating a TCP transport connection or servicing an incoming TCP transport connection request.

6.2.3 For a system to handle incoming TCP transport connection requests there shall be a passive OPEN command executed on the TCP transport service interface.

6.2.4 The T-Connect→Req service primitive shall be implemented using the active OPEN command of the TCP transport service.

6.2.5 The T-Connect→Ind service primitive shall be signalled upon receipt of the TCP acknowledgement segment which establishes the TCP transport connection which brings the TCP protocol to its ESTABLISHED state.

6.2.6 Systems implementing FMTP shall predefine in their letter of agreement client or server roles to ensure that no more than one TCP transport connection exists between two systems.

6.3 TCP Connection Release

6.3.1 The T-Disconnect→Req service primitive shall be implemented by using the CLOSE command of the TCP transport service.

6.3.2 The T-Disconnect→Req shall not terminate the main process listening for incoming TCP connection requests.

6.3.3 The T-Disconnect→Req shall release the transport connection and initiate the termination of the TCP socket and any other processes or threads.

6.3.4 The T-Disconnect→Ind service primitive shall be signalled upon receipt of a TCP transport connection termination segment.

6.4 Data Transfer

6.4.1 The T-Data→Req service primitive shall be implemented by using the SEND command of the TCP transport service.

6.4.2 The T-Data→Ind service primitive shall be signalled when the RECEIVE command of the TCP transport service is invoked.

6.4.3 The T-Data service shall be restricted to the transfer of character-oriented data.

6.5 TCP Timer Settings

6.5.1 RFC 1122, section 4.2.2.15 shall apply to the definition of the retransmission timeout default values and algorithms.

6.6 TCP Ports

6.6.1 FMTP shall reserve and make use of TCP port number 8500 for operational data exchange, as this port number is used to serve incoming TCP transport connection requests for the purpose of the FMTP.

6.6.2 TCP port values defined for the purpose of FMTP shall be configurable parameters.

7. NETWORK PROTOCOL

7.1 Service Assumed

7.1.1 Systems implementing the FMTP shall operate TCP transport connections over IP.

7.1.2 Systems implementing the FMTP shall interoperate over IP version 6.

7.2 IP Addressing

7.2.1 The authority responsible for the FMTP implementations shall be in charge of assigning the required IP address(es).

7.2.2 The IP address values used for peer-to-peer communication shall be configurable parameters.

7.3 IP Address Validation

7.3.1 The source IP address and TCP destination port number shall be validated against a local list of valid remote addresses for the system.

7.3.2 If an invalid address is detected, the incoming IP packets shall be discarded.

8. CHARACTER SETS

8.1 For character-oriented fields, the character set shall be as defined by ISO 646, ISO 8859-1 or ISO 10646-1.

8.2 FMTP information exchange shall be restricted to characters that are common to all character sets, so that only characters defined in ISO 10646-1 BASIC LATIN are exchanged.

8.3 Characters shall be encoded in a single-octet in the range of ‘20’H to ‘7E’H, as defined in ISO 10646-1, Amendment 2, to ensure character set bit encoding compatibility between the ISO 646, ISO 8859 and ISO 10646-1 character sets.

Note: Use of the UCS defined by ISO 10646-1 combined with the UCS Transformation Format 8 (UTF-8) character-encoding scheme described in Annex R to that standard is recommended.

9. BIT-ORDERING FOR DATA TRANSMISSION

9.1 FMTP data shall be transmitted as a stream of octets, as mandated by the Transmission Control Protocol RFC 793, section 1.5.

9.2 The binary conversion of numerical values shall be compatible with big-endian computer systems before the transmission over the transport interface.

9.3 Single or multiple octets representing numerical quantities received through the transport protocol interface shall be assumed to be compatible with big-endian computer systems.

10. DATA LINK LAYER REQUIREMENTS

10.1 Systems implementing the FMTP shall satisfy the data link layer requirements of RFC 1122, section 2.

11. LIST OF REFERENCES TO BE USED IN INTEROPERABILITY AND PERFORMANCE REQUIREMENTS

11.1 Internet Engineering Task Force (IETF) STD 0007, RFC 793:1981, Transmission Control Protocol.

11.2 Internet Engineering Task Force (IETF) STD 0003, RFC 1122:1989, Requirements for Internet Hosts - Communication Layers.

11.3 Internet Engineering Task Force (IETF) RFC 2460:1998, Internet Protocol, Version 6 (IPv6) Specification.

11.4 ISO/IEC 646:1991 (3rd Edition), Information technology – 7-bit coded character set for information exchange.

11.5 ISO/IEC 8859-1:1987 (1st edition), Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1.

11.6 ISO/IEC 10646-1:1993 (1st edition), Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane.

11.7 ISO/IEC 10646:1993/Amd.2:1996 (1st edition), Information technology – Universal Multiple-Octet Coded Character Set (UCS) – Part 1: Architecture and Basic Multilingual Plane, Amd. 2:UCS Transformation Format (UTF-8).

ANNEX A: IMPLEMENTATION CONFORMITY STATEMENT

A.1 Introduction

The tables in this Annex comprise the Implementation Conformity Statement (ICS) proforma for FMTP systems. The ICS, when accurately completed, facilitates an assessment of whether the subject FMTP system conforms to the requirements of this EUROCONTROL Specification. Comparing the completed ICS of two FMTP implementations gives an initial indication of whether the two systems will be capable of interoperating.

A.2 Conformity Overview

Table A.1: Identification

Supplier	
Contact point for queries about this Conformity Statement	
Implementation name/version	
Machine name/version	
Operating system name/version	
Other hardware and operating systems claimed	
System name (if applicable)	
Date of statement	
Have all the mandatory items of this specification been implemented?	Yes ☐
NOTE - *Failure to respond 'Yes' to this question indicates a failure of conformity*	

A.3 Dynamic Conformity Requirements

Table A.2: Dynamic Conformity Requirements

Are local implementation identification values configurable?	Yes ☐
Are remote implementation identification values configurable?	Yes ☐
Can the implementation identify different identification values for co-hosted MT-Users?	Yes ☐ N/A ☐
Are the TCP port values to service incoming connection establishments configurable?	Yes ☐
Is the implementation IP version independent?	Yes ☐ N/A ☐
Are the IP addresses of local and remote implementations configurable?	Yes ☐
Are user message sizes up to and including 10 240 octets supported?	Yes ☐
NOTE - *Failure to respond to all of these questions indicates a failure of conformity*	

A.4 Upper Layer Requirements

Table A.3: User Data

Is the character set of user data restricted to those of ISO 10646-1 Basic Latin?	Yes ☐
Are characters encoded according to ISO 10646 Amendment 2?	Yes ☐
NOTE - *Failure to respond to all of these questions indicates a failure of conformity*	

Table A.4: Message Transfer Protocol

Are the establishment of outgoing FMTP connections and FMTP Associations described in this specification supported?	Yes ☐
Are the establishment of incoming FMTP connections and FMTP Associations described in this specification supported?	Yes ☐
Are simultaneous FMTP Associations, as described in this specification supported?	Yes ☐ No ☐ If YES maximum number of simultaneous FMTP Associations: …
Is the establishment of more than one FMTP connection between the same FMTP entity peers prohibited?	Yes ☐
Are operator messages supported?	Yes ☐ No ☐
NOTE - *Failure to respond to all of these questions indicates a failure of conformity*	

A.5 Lower Layer Requirements

Table A.5: Transport Layer

Does the TCP implementation comply with RFC 1122, section 4.2?	Yes ☐
Are simultaneous FMTP connections with different peers supported?	Yes ☐ No ☐ If YES maximum number of simultaneous FMTP connections: …
Is TCP port 8500 reserved to service incoming operational connections?	Yes ☐
Can alternative TCP ports be reserved to serve other purposes, e.g. test connections?	Yes ☐ No ☐
Does the bit-order of transmitted user data comply to big-endian systems?	Yes ☐
Does the bit-order of received user data comply to big-endian systems?	Yes ☐
Can a TCP keep-alive mechanism be enabled for associations with a given remote implementation?	Yes ☐ No ☐
NOTE - *Failure to respond to all of these questions indicates a failure of conformity*	

Table A.6: Network Layer

Does the IP implementation comply with RFC 2460?	Yes ☐
Are remote IP addresses validated during connection establishment?	Yes ☐
Can several IP addresses be assigned for a given remote implementation?	Yes ☐ No ☐
Can the flow label be set?	Yes ☐ No ☐ If YES, default value: ....
Are Differentiated Services enabled?	Yes ☐ No ☐ If YES, default Traffic Class value: ....
NOTE - Failure to respond to all of these questions indicates a failure of conformity	

Table A.7: Data Link Layer

Does the IP implementation comply with RFC 1122, section 2?	Yes ☐
NOTE - *Failure to respond to all of these questions indicates a failure of conformity*	