INTERNATIONAL STANDARD

ISO/IEC 8571-5

First edition
1990-12-15

Information processing systems — Open Systems Interconnection — File Transfer, Access and Management —

Part 5 :
Protocol Implementation Conformance Statement Proforma

Systèmes de traitement de l'information — Interconnection de systèmes ouverts — Gestion, accès et transfert de fichier —

Partie 5 : Avis de conformité de mise en œuvre du protocole proforma

Reference number
ISO/IEC 8571-5 : 1990 (E)

Contents

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 8571-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

ISO 8571 consists of the following parts, under the general title *Information processing systems — Open Systems Interconnection — File Transfer, Access and Management*:

- *Part 1: General introduction*
- *Part 2: Virtual Filestore Definition*
- *Part 3: File Service Definition*
- *Part 4: File Protocol Specification*
- *Part 5: Protocol Implementation Conformance Statement Proforma*

Annex A forms an integral part of this part of ISO 8571. Annex B is for information only.

Introduction

ISO 8571 is one of a set of International Standards introduced to facilitate the interconnection of computer systems. It is related to other International Standards in the set as defined by the Reference Model for Open Systems Interconnection (ISO 7498). The Reference Model subdivides the area of standardization for interconnection into a series of layers of specification, each of manageable size.

The aim of Open Systems Interconnection is to allow, with a minimum of technical agreement outside the interconnection standards, the interconnection of computer systems

a) from different manufacturers,

b) under different managements,

c) of different levels of complexity,

d) of different ages.

ISO 8571 defines a File Service and specifies a File Protocol available within the application layer of the Reference Model. The service defined is of the category Application Service Element (ASE). It is concerned with identifiable bodies of information which can be treated as files, which may be stored within open systems or passed between application processes.

ISO 8571 defines a basic file service. It provides sufficient facilities to support file transfer, and establishes a framework for file access and file management. ISO 8571 does not specify the interfaces to a file transfer or access facility within the local system.

It is recognised that, with respect to Communication Quality of Service, work is still in progress to provide an integrated treatment of quality of service across all of the layers of the OSI Reference Model and to ensure that the individual treatments in each layer service satisfy overall quality of service objectives in a consistent manner. As a consequence, an addendum may be added to this International Standard at a later time which reflects further quality of service developments and integration.

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given OSI protocol. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

Information processing systems — Open Systems Interconnection — File Transfer, Access and Management —

Part 5:
Protocol Implementation Conformance Statement Proforma

1 Scope

This part of ISO 8571 defines a Protocol Implementation Conformance Statement (PICS) proforma for the detailed expression of the conformance requirements of ISO 8571. This PICS proforma is in compliance with the relevant requirements and in accordance with the relevant guidance for a PICS proforma given in ISO 9646-2. Detail of the use of this proforma is provided in this part of ISO 8571. Implementations claiming conformance to ISO 8571 shall complete the proforma as part of the conformance requirements. The level of detail required in the proforma exceeds that of the protocol specification by requiring details to uniquely identify the implementation and the supplier.

NOTE - PICS are related to base standards and only base standards. PICS structure might be expanded and refined for other documents using the base standards (eg ISPICS)

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 8571. At the time of publication, the editions indicated were valid. All standards are subject to revision, and the parties to agreements based on this part of ISO 8571 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 7498 : 1984, *Information Processing Systems - Open Systems Interconnection - Basic Reference Model.*

ISO/TR 8509 : 1987, *Information Processing Systems - Open Systems Interconnection - Service Conventions.*

ISO 8571-1 : 1988, *Information Processing Systems - Open Systems Interconnection - File transfer, Access and Management - Part 1: General Introduction.*

ISO 8571-2 : 1988, *Information Processing Systems - Open Systems Interconnection - File transfer, Access and Management - Part 2: Virtual Filestore Definition.*

ISO 8571-3 : 1988, *Information Processing Systems - Open Systems Interconnection - File transfer, Access and Management - Part 3: File Service Definition.*

ISO 8571-4 : 1988, *Information Processing Systems - Open Systems Interconnection - File transfer, Access and Management - Part 4: File protocol Specification.*

ISO 8822 :1988, *Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition.*

ISO 8823 : 1988, *Information Processing Systems -Open Systems Interconnection - Connection Oriented Presentation Protocol Specification.*

ISO 9646-1 : [1], *Information technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 1: General Concepts.*

ISO 9646-2 : [1], *Information technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 2: Abstract Test Suite Specification.*

1) To be published.

3 Definitions

Terms used in this part of ISO 8571 are defined in ISO 8571-1. The following terms are defined in ISO 9646

a) Protocol Implementation Conformance Statement (PICS)

b) PICS proforma

4 Abbreviations

Abbreviations used in this part of ISO 8571 are defined in ISO 8571-1 and clause 8. The following abbreviation used in this part of ISO 8571 is defined in ISO 9646

- PICS

5 Conventions

This part of ISO 8571 uses the descriptive conventions in the OSI Service Conventions ISO/TR 8509. The PICS proforma annex has been designed to be a self-contained section of this part of ISO 8571, for use in testing and procurement.

6 Conformance

A conforming PICS shall be technically equivalent to the ISO published PICS proforma and shall preserve the numbering and ordering of the items in the ISO PICS proforma.

A PICS which conforms to this part of ISO 8571 shall

a) describe an implementation which conforms to ISO 8571-4

b) be a conforming PICS proforma, which has been completed in accordance with the instructions for completion given in clauses A.8 and A.10 of annex A

c) include the information necessary to uniquely identify both the supplier and the implementation

7 Description of the proforma

The proforma defined in annex A is divided into the following sections:

a) Implementation detail (see 7.1)

b) General ISO 8571 detail (see 7.2)

c) Syntax detail (see 7.3)

d) Virtual Filestore detail (see 7.4)

e) File Protocol detail (see 7.5)

f) Document Type detail (see 7.6)

Throughout each section, whenever a line contains a requirement for an implementation response, that line is numbered at the left hand side. For the significance of this numbering see clause 9.

7.1 Implementation detail

The implementation detail provides a number of items of information which allow a unique identification of an implementation and the supplier. These are implementor and supplier specific.

7.2 General ISO 8571 detail

The general detail covers general detail of ISO 8571. This includes information on which protocol version numbers, addenda and defect reports have been included in the implementation. Also specified in this section is a statement of which roles have been implemented from the ranges of initiator/responder and sender/receiver.

7.3 Syntax detail

The abstract syntaxes identified are those defined for the basic operation of the protocol and the implementation of the hierarchical file model. Support for abstract syntaxes defined as part of a document type is defined in section six (document type detail).

Conformance to the syntactic elements of the protocol which cannot be exercised because of overriding application semantic constraints is outside the scope of the individual PICS.

7.4 Virtual Filestore detail

The virtual filestore detail provides information on which virtual filestore model has been implemented and if the hierarchical model defined in ISO 8571-2 has been implemented. The section continues to identify the detail of the model. Definition of other filestore models is for future study and the detail in this section may or may not be relevant.

As the virtual filestore is always in the role of responder a certain asymmetry develops within the PICS with some features for the responder implementation being specified

in this Virtual Filestore section while the initiator implementation detail is specified in the protocol section.

7.5 File Protocol detail

Comprising the major portion of the PICS, the file protocol detail section establishes which fields of which PDUs are implemented. It requires a statement of the value range supported and a reference to further detail for many of the fields.

7.6 Document Type detail

Document type detail is included in the PICS to reflect the detail in ISO 8571-2. It is not necessary, for conformance purposes, to implement any of the document types defined in ISO 8571-2. The style of the proforma in this section may be used to specify support of further document types.

8 Notations defined for the proforma

In order to reduce the size of the tables in the PICS proforma notations have been introduced. These have allowed the use of multi-column layout where the columns are headed 'D', 'I' or 'R' - The definition of each of these follows.

8.1 D - column

'D' - Defined in ISO 8571. This column indicates the level of support required for conformance to ISO 8571, it has three distinct sets of values, one for attribute support, one for PDU support and one for parameter support. These are detailed below:

For attributes

'f' - full support of the attribute is required, as defined in ISO 8571-2.

'p' - partial support of the attribute is permitted, as defined in ISO 8571-2.

For PDUs

'm' - mandatory support is required for this protocol data unit.

'c' - support for this protocol data unit is conditional upon the implementation of particular functional units. If the relevant functional unit is implemented the support level for the PDU is mandatory.

For parameters

'm' - mandatory support is required for this parameter for conformance to ISO 8571.

'o' - optional support is permitted for conformance to ISO 8571. Although if implemented it must conform to the specifications and restrictions contained in ISO 8571. These restrictions may affect the optionality of other parameters.

'—' - a of dash to indicate that the item is not applicable.

8.2 I - column

The 'I' column shall be completed by the supplier or implementor to indicate the level of implementation of each feature in the role of initiator. Where this column is pre printed with dashes, representing a non applicable entry, no entry shall be inserted in the 'I' column. Elsewhere entries shall be as defined in 8.4.

8.3 R - column

The 'R' column shall be completed by the supplier or implementor to indicate the level of implementation of each feature in the role of responder. Where this column is pre printed with dashes, representing a non applicable entry, no entry shall be inserted in the 'R' column. Elsewhere entries shall be as defined in 8.4.

Attribute support level columns in section four are specified as either 'R full' or 'R partial'. These shall be completed as defined in 8.4 to indicate wether the file attributes are fully or partially supported as defined in ISO 8571-2.

8.4 Column entries

The PICS proforma has been designed such that the only entries required in the 'I' and 'R' columns are:

Y - yes, the feature has been implemented

N - no, the feature has not been implemented

The 'RANGE OF VALUES' column requires the specification of the range of values implemented for the feature it is alongside, for each role, where relevant. This column has, in some instances, instead of space for a value, a forward reference to a clause providing for more detail.

9 PICS numbers

Each line, within a clause of the PICS proforma, which requires implementation detail to be entered is numbered at the left hand edge of the line. This numbering is included as a means of uniquely identifying all possible implementation detail within the PICS proforma. The need for such unique referencing has been identified by the testing bodies.

All responses shall be referenced by specifying the following sequence:

a) the clause number

b) a solidus character (/)

c) line number

d) line item identifier as defined in ISO 9646-2.

10 Completion of the PICS

The implementor shall complete all entries in the columns marked 'R' and 'I'. In addition other specifically identified information shall be provided by the implementor where requested. No changes shall be made to the proforma except the completion as required. Recognising that the level of detail required may, in some instances, exceed the space available for responses a number of responses specifically allow for the addition of appendices to the PICS.

Annex A [1)]
(normative)

Protocol Implementation Conformance Statement(PICS) Proforma for OSI File Transfer, Access and Management (FTAM)

Section 1 : Implementation Details

A.1 Date of Statement

1	Date of Statement yy-mm-dd

A.2 Implementation detail

Specify the information necessary to uniquely identify the implementation and the systems in which it may reside. This may include details of:

a) supplier, implementation name, operating system, suitable hardware

b) system supplier and/or client of the test laboratory that is to test the implementation

c) information on whom to contact if there are queries concerning the content of this PICS.

d) the relationship between this PICS and the System Conformance Statement for the system (see note 1)

e) Profiles to which conformance is claimed. (see note 2)

NOTES

1) The System Conformance Statement is defined in ISO 9646. It relates to a PICS covering more than one layer of the reference model.

2) The list of profile names is not necessarily a fully inclusive set of those covered by this implementation.

1	

---

1) Copyright release for PICS proformas

Users of this International Standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

Section 2 : General ISO 8571 Detail

A.3 ISO 8571 Protocol versions implemented

1	FTAM protocol version number(s)

A.4 ISO 8571 Addenda implemented

1	ISO 8571-1
2	ISO 8571-2
3	ISO 8571-3
4	ISO 8571-4
5	ISO 8571-5

A.5 Defect report numbers and amendments implemented

The numbers of any approved defect reports or amendments which have been implemented shall be stated below.

1	ISO 8571-1
2	ISO 8571-2
3	ISO 8571-3
4	ISO 8571-4
5	ISO 8571-5

A.6 Global statement of conformance

1	Does the implementation referred to by this PICS conform to ISO 8571? yes or no

A.7 Initiator / Responder capability

State which combination of roles are, and which are not, implemented and specified in this PICS.

	ROLES	D	I	R	
1	Sender	o			
2	Receiver	o			

A.8 Application Context Name details

List the names of the Application Context Names recognized or provided by this implementation.

1	

Section 3 : Syntax Detail

A.9 Abstract syntaxes

	Object descriptor	Object identifier	D	I	R
1	FTAM PCI	{iso standard 8571 abstract-syntax (2) ftam-pci (1)	m		
2	FTAM FADU	{iso standard 8571 abstract-syntax (2) ftam-fadu (2)}	o		
3		{joint-iso-ccitt association-control(2) abstract-syntax(1) apdus(0) version1(1)}	m		
4		{iso standard 8571 abstract-syntax(2) unstructured-text(3)}	o		
5		{iso standard 8571 abstract-syntax(2) unstructured-binary(4)}	o		

NOTE - ISO 8571 requires the presence of the transfer syntax derived from the "Basic Encoding of a single ASN.1 type "{joint-iso-ccitt asn1 (1) basic-encoding (1)} encoding rules for transfer of the "FTAM PCI" and the "FTAM FADU" abstract syntaxes. Implementation detail of this transfer syntax, and other transfer syntaxes supported, is specified in the PICS of ISO 8823.

Section 4 : Virtual Filestore Detail

A.10 Virtual filestore

This clause details the conformance to the file model, file attribute support and to file structure support.
State whether the hierarchical file model (see ISO 8571-2) is supported, and, if so, which constraint sets and, where relevant, the maximum depth of hierarchy supported.

A.10.1 File model

	FILE MODEL	D R	
1	Hierarchical	o	
2	Other models (specify or detail in an appendix)		

A.10.2 Attributes

A.10.2.1 Attribute groups implemented

State which file attribute groups are implemented, and which are not implemented. The level of support within each group shall be stated in A.10.2.2.

	ATTRIBUTE GROUP NAME	D I R	
1	Kernel	m	
2	Storage	o	
3	Security	o	
4	Private	o	

A.10.2.2 Attribute values

Complete the tables for all attribute groups, shown as supported in A.10.2.1, indicating for the initiator role whether the attribute is fully supported or not, and for the responder role whether the attribute is fully or partially supported. If a group is implemented the range of values of each attribute in that group shall be stated in the 'RANGE OF VALUES' column, or a forward reference included, possibly to an appendix, giving further details of the supported value range.
Conformance to ISO 8571 requires, that for attribute groups supported, at least the minimum range of attribute values defined in ISO 8571-2, be supported. An initiator shall not partially support attributes.

On any single line in a responder table in A.10.2 an entry shall only be made for R (full) or R (partial) not for both.

	KERNEL GROUP (INITIATOR)	D I full	RANGE OF VALUES
1	Filename	f	see A.10.2.3
2	Permitted Actions	f	
3	Contents Type	f	see A.12.7

	KERNEL GROUP (RESPONDER)	D R full	RANGE OF VALUES
4	Filename	f	see A.10.2.3
5	Permitted Actions	f	
6	Contents Type	f	see A.12.7

	STORAGE GROUP (INITIATOR)	D I full	RANGE OF VALUES
7	Storage account	f	
8	Date and time of creation	f	
9	File availability	f	
10	Future filesize	f	

	STORAGE GROUP (RESPONDER)	D R full R partial	RANGE OF VALUES
11	Storage account	p	
12	Date and time of creation	p	
13	Date and time of last modification	p	
14	Date and time of last read access	p	
15	Date and time of last attribute modification	p	
16	Identity of creator	p	
17	Identity of last modifier	p	
18	Identity of last reader	p	
19	Identity of last attribute modifier	p	
20	File availability	p	
21	Filesize	p	
22	Future filesize	p	

	SECURITY GROUP (INITIATOR)	D I full	RANGE OF VALUES
23	Access control	f	see A.12.2
24	Legal qualifications	f	

	SECURITY GROUP (RESPONDER)	D R full R partial	RANGE OF VALUES
25	Access control	p	see A.12.2
26	Legal qualifications	p	

	PRIVATE GROUP (INITIATOR)	D	I full	RANGE OF VALUES
27	Private use	f		

NOTE - If the private use attribute is implemented, then the details of the values and their semantics should be stated in an appendix.

	PRIVATE GROUP (RESPONDER)	D	R full	R partial	RANGE OF VALUES
28	Private use	p			

NOTE - If the private use attribute is implemented, then the details of the values and their semantics should be stated in an appendix.

A.10.2.3 Filename detail

Specify what restrictions, including filename conventions if any, apply to the filename.

	FILENAME - INITIATOR
1	How many filename elements are supported
2	Which graphic repertoires are supported
3	Which graphic characters, if any, are excluded
4	What is the maximum string length of each filename element
5	Other restrictions

	FILENAME - RESPONDER
6	How many filename elements are supported
7	Which graphic repertoires are supported
8	Which graphic characters, if any, are excluded
9	What is the maximum string length of each filename element
10	Other restrictions

A.10.3 File structures

A.10.3.1 Constraint sets

If the Contents type 'Abstract Syntax/Constraint Set' is implemented state which constraint sets are, and which are not, implemented. Where applicable an integer figure shall be supplied to indicate the maximum depth of hierarchy which the implementation supports.

	CONSTRAINT SET NAME	D I R	DEPTH
1	Unstructured	o	NOT APPLICABLE
2	Sequential Flat	o	NOT APPLICABLE
3	Ordered flat	o	NOT APPLICABLE
4	Ordered flat with unique names	o	NOT APPLICABLE
5	Ordered hierarchical	o	
6	General hierarchical	o	
7	General hierarchical with unique names	o	

NOTE - If the actions allowed and/or the permissible FADU identities are restricted within a specific constraint set beyond the restrictions given by the specified support of the permitted actions file attribute and the document type supported, such restrictions should be stated in an appendix.

A.10.3.2 File and filestore actions

A.10.3.2.1 Filestore Actions

Support for filestore actions is dependent upon the functional units implemented (see A.12.4 and A.12.5)

A.10.3.2.2 File Actions

State whether the action is, or is not, supported within a file open regime, for the constraint sets implemented in the responder role.

		CONSTRAINT SET											
		unstructured		sequential flat		ordered flat		ordered flat with unique names		ordered hierarchical		general hierarchical		general hierarchical with unique names	
	ACTION	D	R	D	R	D	R	D	R	D	R	D	R	D	R
1	Locate	—	—	o		o		o		o		o		o	
2	Read	o		o		o		o		o		o		o	
3	Insert	—	—	o		o		o		o		o		o	
4	Replace	o		—	—	o		o		o		o		o	
5	Extend	o		—	—	o		o		o		o		o	
6	Erase	o		o		o		o		o		o		o	

A.10.3.2.3 Access contexts implemented

	ACTION CONTEXT	CONSTRAINT SET													
		unstructured		sequential flat		ordered flat		ordered flat with unique names		ordered hierarchical		general hierarchical		general hierarchical with unique names	
		D	R	D	R	D	R	D	R	D	R	D	R	D	R
1	US	—	—	—	—	—	—	—	—	o		o		o	
2	UA	o		o		o		o		o		o		o	
3	FS	—	—	—	—	—	—	—	—	o		o		o	
4	FL	—	—	—	—	—	—	—	—	o		o		o	
5	FA	—	—	o		o		o		o		o		o	
6	HN	—	—	—	—	—	—	—	—	o		o		o	
7	HA	—	—	—	—	o		o		o		o		o	

A.10.4 Additional information

State whether there are any circumstances under which the existence of a file, its contents, or the values of the supported attributes may change, between separate accesses using the FTAM protocol.

1	State details here or in an appendix

State whether there are any circumstances under which modifications to the file contents or the values of the file attributes by FTAM protocol exchanges will not subsequently be available for use.

2	State details here or in an appendix

A.10.5 Override

State the implemented filestore capability.

	RESPONDER OVERRIDE	D	R
1	Create failure	o	
2	Select old file	o	
3	Delete and recreate with old attributes	o	
4	Delete and create with new attributes	o	

NOTE - The specification of the role of initator is to be given in section five (file protocol detail).

Section 5 : File Protocol Detail

A.11 File protocol

Detail the level of support for the FTAM protocol, i.e. PDUs and PDU fields. Indicate which PDUs are, and which are not, implemented. Also state which fields are, and which are not, implemented for each supported PDU.

If a PDU field is implemented then, its range of values shall be specified, or, if applicable, the reference completed. Fields not implemented shall be so marked.

Subclauses A.11.2 to A.11.24 require an indication of which PDUs are implemented. The conformance requirements for PDUs are dependent on the particular functional units implemented. PDUs indicated in A.11.8 to A.11.24 as conditional shall be considered as mandatory when a particular functional unit is implemented, according to the following table.

PDUs	Clause	Functional Units								
		Kernel	Read	Write	Access	L F M	E F M	Grouping	Recovery	Restart
F-CREATE	A.11.8					m				
F-DELETE	A.11.9					m				
F-READ-ATTRIB	A.11.10					m				
F-CHANGE-ATTRIB	A.11.11						m			
F-OPEN	A.11.12		m	m						
F-CLOSE	A.11.13		m	m						
F-BEGIN-GROUP	A.11.14							m		
F-END-GROUP	A.11.15							m		
F-RECOVER	A.11.16								m	
F-LOCATE	A.11.17				m					
F-ERASE	A.11.18				m					
F-READ	A.11.19		m							
F-WRITE	A.11.20			m						
F-DATA-END	A.11.21		m	m						
F-TRANSFER-END	A.11.22		m	m						
F-CANCEL	A.11.23		m	m						
F-RESTART	A.11.24									m

NOTES

1) In order to keep the protocol tables compact some forward references have been introduced to clauses which expand upon the detail of field support.

2) The FTAM protocol will require a number of optional lower layer services to be available (e.g. Application Entity Titles in ACSE). This requirement is outside the scope of this PICS proforma.

A.11.1 GraphicString support

State the supported coded character sets for the GraphicString fields of the PDUs implemented and the maximum length of the string, if such a restriction applies. If the support for initiator and responder roles is not the same state each restriction separately.

1	

NOTES

1) If the level of support of this feature varies with the different fields in which GraphString is used full detail should be given in an appendix.

2) The character set support for Document Types is specified in Section 6.

A.11.2 FTAM regime establishment

	F-INITIALIZE PDU	D m	I	D m	R	
	FIELD NAME					RANGE OF VALUES OR REFERENCE
2	State result	—	—	m		all values defined in ISO 8571
3	Action result	—	—	m		all values defined in ISO 8571
4	Protocol version	m		m		see Section 2
5	Implementation information	o		o		see A.12.1
6	Presentation context management	m		m		see note 1
7	Service class	m		m		see A.12.4
8	Functional units	m		m		see A.12.5
9	Attribute groups	m		m		see A.10.2
10	Shared ASE information	o		o		see A.12.9
11	FTAM Quality of Service	m		m		see A.12.8
12	Contents type list	o		o		see A.12.7.1
13	Initiator identity	o		—	—	
14	Account	o		—	—	
15	Filestore password	o		—	—	see A.12.11
16	Diagnostic	—	—	o		see A.12.6
17	Checkpoint window	m		m		see note 2

NOTES

1) The values available for the presentation context management field depend upon the functional units implemented in ISO 8823.

2) Checkpoint window field is indicated as mandatory in accordance with ISO 8571-4. The field is defaulted to the value 1.

A.11.3 FTAM regime termination (orderly)

	F-TERMINATE PDU	D m	I	D m	R	
	FIELD NAME					RANGE OF VALUES OR REFERENCE
2	Shared ASE information	o		o		see A.12.9
3	Charging	—	—	o		see A.12.10

A.11.4 FTAM regime termination (abrupt) by service user

	F-U-ABORT PDU	D m	I	R	
	FIELD NAME				RANGE OF VALUES OR REFERENCE
2	Action result	m			all values defined in ISO 8571
3	Diagnostic	o			see A.12.6

A.11.5 FTAM regime termination (abrupt) by service provider

	F-P-ABORT PDU	D m	I	R	
	FIELD NAME				RANGE OF VALUES OR REFERENCE
2	Action result	m			all values defined in ISO 8571
3	Diagnostic	o			see A.12.6

A.11.6 File selection

	F-SELECT PDU	D m	I	D m	R	
	FIELD NAME					RANGE OF VALUES OR REFERENCE
2	State result	—	—	m		all values defined in ISO 8571
3	Action result	—	—	m		all values defined in ISO 8571
4	Attributes	m		m		see A.10.2
5	Requested access	m		—	—	see A.12.16
6	Access passwords	o		—	—	see A.12.3.5
7	Concurrency control	o		—	—	see A.12.13
8	Shared ASE information	o		o		see A.12.9
9	Account	o		—	—	
10	Diagnostic	—	—	o		see A.12.6

A.11.7 File deselection

	F-DESELECT PDU	D I	D R	
1		m	m	
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	Charging	— —	o	see A.12.10
4	Shared ASE information	o	o	see A.12.9
5	Diagnostic	— —	o	see A.12.6

A.11.8 File creation

	F-CREATE PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	State result	— —	m	all values defined in ISO 8571
3	Action result	— —	m	all values defined in ISO 8571
4	Override	m	— —	see A.12.15
5	Initial attributes	m	m	see A.10.2
6	Create password	o	— —	see A.12.12
7	Requested access	m	— —	see A.12.16
8	Access passwords	o	— —	see A.12.3.5 and 12.3.6
9	Concurrency control	o	— —	see A.12.13
10	Shared ASE information	o	o	see A.12.9
11	Account	o	— —	
12	Diagnostic	— —	o	see A.12.6

A.11.9 File deletion

	F-DELETE PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	Shared ASE information	o	o	see A.12.9
4	Charging	— —	o	see A.12.10
5	Diagnostic	— —	o	see A.12.6

A.11.10 Read attributes

	F-READ-ATTRIB PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	Attribute names	m	— —	
4	Attributes	— —	o	see A.10.2
5	Diagnostic	— —	o	see A.12.6

A.11.11 Change attributes

	F-CHANGE-ATTRIB PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	Attributes	m	o	see A.10.2
4	Diagnostic	— —	o	see A.12.6

A.11.12 File open

	F-OPEN PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	State result	— —	m	all values defined in ISO 8571
3	Action result	— —	m	all values defined in ISO 8571
4	Processing mode	m	— —	see A.12.17
5	Contents type	m	m	see A.12.7.2
6	Concurrency control	o	o	see A.12.13
7	Shared ASE information	o	o	see A.12.9
8	Enable FADU locking	m	— —	see note 3
9	Activity identifier	o	— —	
10	Diagnostic	— —	o	see A.12.6
11	Recovery mode	m	m	see A.12.18
12	Remove contexts	o	— —	max number of presentation contexts =
13	Define contexts	o	— —	
14	Presentation action	— —	m	see notes 1 and 2

NOTES

1) The values available for the presentation action field depend upon the functional units implemented in ISO 8823.

2) Presentation action field is indicated as mandatory in accordance with ISO 8571-4. The field is defaulted to no action.

3) Enable FADU Locking field is indicated as mandatory in accordance with ISO 8571-4. The field is defaulted to false.

A.11.13 File close

	F-CLOSE PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	m	m	all values defined in ISO 8571
3	Shared ASE information	o	o	see A.12.9
4	Diagnostic	o	o	see A.12.6

A.11.14 Beginning of grouping

	F-BEGIN-GROUP PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Threshold	m	— —	

A.11.15 End of grouping

	F-END-GROUP PDU	D I	D R	
1		c	c	see A.11
	The F-END-GROUP PDU carries no fields			

A.11.16 Regime recovery

	F-RECOVER PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	State result	— —	m	all values defined in ISO 8571
3	Action result	— —	m	all values defined in ISO 8571
4	Activity identifier	m	— —	
5	Bulk transfer number	m	— —	
6	Requested access	m	— —	see A.12.16
7	Access passwords	o	— —	see A.12.3.5 A.12.3.6
8	Contents type	— —	m	see A.12.7.2
9	Recovery point	m	m	
10	Diagnostic	— —	o	see A.12.6
11	Remove contexts	o	— —	see notes
12	Define contexts	o	— —	see notes
13	Presentation action	— —	m	see notes

NOTES
1) The values available for the presentation action field depend upon the functional units implemented in ISO 8823.
2) Presentation action field is indicated as mandatory in accordance with ISO 8571-4. The field is defaulted to no action.

A.11.17 Locate file access data unit

	F-LOCATE PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	FADU identity	m	o	
4	FADU lock	o	— —	see A.12.14
5	Diagnostic	— —	o	see A.12.6

A.11.18 Erase file access data unit

	F-ERASE PDU	D I	D R	
1		c	c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	FADU identity	m	— —	
4	Diagnostic	— —	o	see A.12.6

A.11.19 Read bulk data

1	F-READ PDU	D I c	see A.11
	FIELD NAME		RANGE OF VALUES OR REFERENCE
2	FADU identity	m	
3	Access context	m	see A.10.3.2.3
4	FADU lock	o	see A.12.14

A.11.20 Write bulk data

1	F-WRITE PDU	D I c	see A.11
	FIELD NAME		RANGE OF VALUES OR REFERENCE
2	FADU operation	m	
3	FADU identity	m	
4	FADU Lock	o	see A.12.14

A.11.21 End of data transfer

1	F-DATA-END PDU	D I R c	see A.11
	FIELD NAME		RANGE OF VALUES OR REFERENCE
2	Action result	m	all values defined in ISO 8571
3	Diagnostic	o	see A.12.6

A.11.22 End of transfer

1	F-TRANSFER-END PDU	D I c	D R c	see A.11
	FIELD NAME			RANGE OF VALUES OR REFERENCE
2	Action result	— —	m	all values defined in ISO 8571
3	Shared ASE information	o	o	see A.12.9
4	Diagnostic	— —	o	see A.12.6

A.11.23 Cancel data transfer

	F-CANCEL PDU	D I R	
1		c	see A.11
	FIELD NAME		RANGE OF VALUES OR REFERENCE
2	Action result	m	all values defined in ISO 8571
3	Shared ASE information	o	see A.12.9
4	Diagnostic	o	see A.12.6

A.11.23.1 F-CANCEL mapping

If the following two conditions are met ISO 8571 requires that F-CANCEL maps to P-RESYNC.

a) either or both of the read and write functional units are implemented

b) P-RESYNC and P-SYNC-MINOR functional units are available. See ISO 8023 PICS.

1	The F-CANCEL service primitive maps to P-RESYNC YES/NO

A.11.24 Restart data transfer

	F-RESTART PDU	D I R	
1		c	see A.11
	FIELD NAME		RANGE OF VALUES OR REFERENCE
2	Checkpoint identifier	m	

A.12 Expanded PDU field and filestore detail

This clause identifies further PDU field and filestore detail to expand on that given in 10 and 11.

A.12.1 Implementation information detail

Complete the following if support is claimed for the implementation information field of the F-INITIALIZE request or response PDUs.

1	State the graphic repertoires implemented and the maximum length of the string
2	Optional details of the semantics of this parameter (may be included in an appendix)

NOTE - This parameter is not subject to conformance testing.

A.12.2 Access control detail

This clause shall be completed if implementation of both the following is claimed:

a) the security attribute group

b) full support of the access control attribute

	Access control element terms	D I R	RANGE OF VALUES
1	Action list	m	see A.12.3.1 and A.12.3.2
2	Concurrency access	o	see A.12.3.3
3	Identity	o	see A.12.3.4
4	Passwords	o	see A.12.3.5 and 12.3.6
5	Location	o	see A.12.3.7

6	Maximum number of access control elements supported

A.12.3 Access control element detail

A.12.3.1 Action list detail (initiator)

	Initiator Combinations							
	Read	Insert	Replace	Extend	Erase	Read Attribute	Change Attribute	Delete File
1								
2								
3								
4								
5								

NOTE - Further combinations, including reference numbers, should be detailed in an appendix.

A.12.3.2 Action list detail (responder)

	Responder Combinations							
	Read	Insert	Replace	Extend	Erase	Read Attribute	Change Attribute	Delete File
1								
2								
3								
4								
5								

NOTE - Further combinations, including reference numbers, should be detailed in an appendix.

A.12.3.3 Concurrency access term

If the concurrency access term is implemented in the access control element complete details of the concurrency control available with each action.

	Action	not required			shared			exclusive			no access		
		D	I	R	D	I	R	D	I	R	D	I	R
1	Read	o			o			o			o		
2	Insert	o			o			o			o		
3	Replace	o			o			o			o		
4	Extend	o			o			o			o		
5	Erase	o			o			o			o		
6	Read attributes	o			o			o			o		
7	Change attributes	o			o			o			o		
8	Delete file	o			o			o			o		

NOTE - Further restrictions and combinations should be detailed in an appendix.

A.12.3.4 Identity term

If the identity term of the access control element is implemented enter details of the identity control available with each action, or reference an appendix containing the detail.

	Initiator	Responder
1		

A.12.3.5 Initiator Access passwords

If the passwords term of the access control element is implemented the following table shall be completed for the initiator role.

	Initiator Access passwords	D	I
1	OctetString	o	
2	GraphicString	o	
3	State general initiator restrictions which may apply to the range of access passwords (e.g. GraphicString character sets and string lengths).		

A.12.3.6 Responder Access Passwords

If the passwords term of the access control element is implemented the following table shall be completed for the responder role.

	Responder Access passwords	OctetString		GraphicString	
		D	R	D	R
1	Read-password	o		o	
2	Insert-password	o		o	
3	Replace-password	o		o	
4	Extend-password	o		o	
5	Erase-password	o		o	
6	Read-attribute-password	o		o	
7	Change-attribute-password	o		o	
8	Delete-password	o		o	
9	State general Responder restrictions which may apply to the range of access passwords (e.g. GraphicString repertoires and string lengths).				

A.12.3.7 Location term

If the location term is implemented in the access control element complete details of the location control available with each action and provide details of the Application Entity Titles supported.

	Initiator - Location control detail	Responder - Location control detail
1		

A.12.3.7.1 Application Entity Titles detail

	Initiator	Responder
1		

A.12.3.8 Access control element combinations

State which combinations of access control terms are, and which are not, implemented.

	Combinations			D	R
1	Identity	Password	Location	o	
2	Identity	Password		o	
3	Identity		Location	o	
4		Password	Location	o	
5	Identity			o	
6		Password		o	
7			Location	o	

NOTE - Implementation of access control without any of the above combinations is valid.

A.12.4 Service class field detail

		D I R
1	Transfer class	o
2	Access class	o
3	Management class	o
4	Transfer and management class	o
5	Unconstrained class	o

NOTE - A conformant initiator is only permitted to specify those combinations defined in ISO 8571-3.

A.12.5 Functional unit field detail

State the functional units implemented in each service class.

		SERVICE CLASSES											
		Transfer			Access			Management			Transfer and Management			Unconstrained		
	FUNCTIONAL UNITS	D	I	R	D	I	R	D	I	R	D	I	R	D	I	R
1	Kernel	m			m			m			m			m		
2	Read (see note 2)	c			m			—	—	—	c			m		
3	Write (see note 2)	c			m			—	—	—	c			o		
4	File Access	—	—	—	m			—	—	—	—	—	—	o		
5	Limited File Management	o			o			m			m			o		
6	Enhanced File Management	o			o			o			o			o		
7	Grouping	m			o			m			m			o		
8	FADU Locking	—	—	—	o			—	—	—	—	—	—	o		
9	Recovery	o			o			o			o			o		
10	Restart	o			o			o			o			o		

NOTES

1) The recovery and the restart functional units are only available at the internal file service interface and should only be explicitly referenced in the protocol.

2) The c indicates that either or both of the read and write functional units are to be implemented in the particular service class.

A.12.6 Diagnostic field detail

This clause shall be completed if any diagnostic field is indicated as implemented. The following tables assume that all diagnostic fields have the same implementation details. If this is not so the tables of this clause shall be repeated as necessary in an appendix.

		D I R
1	Diagnostic type	m
2	Error identifier	m
3	Error observer	m
4	Error source	m
5	Suggested delay	o
6	Further details	o
7	If the further details parameter is implemented detail the GraphicString restrictions and maximum string length, if applicable	

A.12.7 Contents type detail

This clause shall be completed if any of the following are implemented:

a) the contents type list field of F-INITIALIZE
b) the contents type field is implemented in F-OPEN
c) the contents type field is implemented in F-RECOVER

A.12.7.1 Contents type list field

If the implementation supports the contents type list field on the F-INITIALIZE PDU complete the following support details.

		D I R	Maximum number of elements
1	document type specifications	o	
2	abstract syntax specifications	o	

A.12.7.2 Contents type field

If the implementation supports the contents type field on the F-OPEN, F-CREATE and/or F-RECOVER PDUs complete the following support details.

		D I R
3	document type specifications	o
4	abstract syntax / constraint set pair specifications	o

NOTE - The detail of document types supported is contained in section 6.

A.12.8 FTAM Quality of service details

A.12.8.1 Initiator

State all possible combinations of FTAM quality of service and the recovery or restart functional units which the initiator is capable of generating.

	Initiator FTAM Quality of service	Functional Units (in request) Neither	Restart	Recovery	Both
1	No recovery	m	— —	— —	— —
2	Class 1	o	o	o	o
3	Class 2	o	o	o	o
4	Class 3	o	o	o	o

A.12.8.2 Responder

State what responses may be returned by the responder implementation for all valid incoming request combinations of FTAM quality of service and the recovery or restart functional units.

	Request		Response							
	FTAM QoS supported Values	Recovery or restart FUs Supported	FTAM QoS values	supported FTAM Qos values	Functional units					
					Neither		Restart		Recovery		Both	
1	0	Neither	0	m	m		—	—	—	—	—	—
2	1	Neither	1	o	o		—	—	—	—	—	—
3	1	Neither	0	o	o		—	—	—	—	—	—
4	1	Restart	1	o	o		o		—	—	—	—
5	1	Restart	0	o	o		o		—	—	—	—
6	1	Recovery	1	o	o		—	—	o		—	—
7	1	Recovery	0	o	o		—	—	o		—	—
8	1	Both	1	o	o		o		o		o	
9	1	Both	0	o	o		o		o		o	
10	2	Neither	2	o	o		—	—	—	—	—	—
11	2	Neither	1	o	o		—	—	—	—	—	—
12	2	Neither	0	o	o		—		—	—	—	—
13	2	Restart	2	o	o		o		—	—	—	—
14	2	Restart	1	o	o		o		—	—	—	—
15	2	Restart	0	o	o		o		—	—	—	—
16	2	Recovery	2	o	o		—	—	o		—	—
17	2	Recovery	1	o	o		—	—	o		—	—
18	2	Recovery	0	o	o		—	—	o		—	—
19	2	Both	2	o	o		o		o		o	
20	2	Both	1	o	o		o		o		o	
21	2	Both	0	o	o		o		o		o	
22	3	Neither	3	o	o		—	—	—	—	—	—
23	3	Neither	2	o	—	—	—	—	—	—		
24	3	Neither	1	o	o		—	—	—	—	—	—
25	3	Neither	0	o	o		—	—	—	—	—	—
26	3	Restart	3	o	o		o		—	—	—	—
27	3	Restart	2	o	o		o		—	—	—	—
28	3	Restart	1	o	o		o		—	—	—	—
29	3	Restart	0	o	o		o		—	—	—	—
30	3	Recovery	3	o	o		—	—	o		—	—
31	3	Recovery	2	o	o		—	—	o		—	—
32	3	Recovery	1	o	o		—	—	o		—	—
33	3	Recovery	0	o	o		—	—	o		—	—
34	3	Both	3	o	o		o		o		o	
35	3	Both	2	o	o		o		o		o	
36	3	Both	1	o	o		o		o		o	
37	3	Both	0	o	o		o		o		o	

Alternatively details of the response FTAM QoS details may be attached as an appendix.

A.12.9 Details of shared ASE information

The mode of use of the shared ASE information field will be highly dependent upon the nature of the symbiotic ASE. Implementations claiming to support the shared ASE information field shall include a reference here to an appendix providing complete details of its use.

A.12.10 Details of charging

State charging details if the charging parameter is implemented.

	Charging	D R
1	Resource identifier term	m
2	Charging unit term	m
3	Charging value term	m
4	Further charging details including the number of charging elements supported	

A.12.11 Filestore password detail

State what restrictions apply to the range of filestore passwords supported.

	Filestore password detail	D I R
1	OctetString	o
2	GraphicString	o
3	State general initiator restrictions which may apply to the range of filestore passwords (e.g. GraphicString character sets and string lengths).	

A.12.12 Create password detail

State what restrictions apply to the range of create passwords supported.

	Create password detail	D I R
1	OctetString	o
2	GraphicString	o
3	State general initiator restrictions which may apply to the range of create passwords (e.g. GraphicString character sets and string lengths).	

A.12.13 Concurrency control

If an implementation does not support access control but does claim support of concurrency control this clause shall be completed to indicate which concurrency locks may be set from the initiator role and which set in the responder role. Further, state the default values applied by the responder, if the concurrency control field is not implemented.

A.12.13.1 Implemented values

	Action	Concurrency control implemented values											
		not required			shared			exclusive			no access		
		D	I	R	D	I	R	D	I	R	D	I	R
1	Read	o			o			o			o		
2	Insert	o			o			o			o		
3	Replace	o			o			o			o		
4	Extend	o			o			o			o		
5	Erase	o			o			o			o		
6	Read attrib	o			o			o			o		
7	Change attrib	o			o			o			o		
8	Delete file	o			o			o			o		

A.12.13.2 Responder Default values

	Action	Concurrency control responder default values							
		not required		shared		exclusive		no access	
		D	R	D	R	D	R	D	R
1	Read	o		o		o		o	
2	Insert	o		o		o		o	
3	Replace	o		o		o		o	
4	Extend	o		o		o		o	
5	Erase	o		o		o		o	
6	Read attrib	o		o		o		o	
7	Change attrib	o		o		o		o	
8	Delete file	o		o		o		o	

A.12.14 FADU Locking

If FADU locking is implemented, complete the following table to indicate which FADU concurrency locks may be set from the implementation while FADU locking is enabled from the F-OPEN assuming no additional access control restrictions.

		FADU Locking Support Values											
		Not required			Shared			Exclusive			No Access		
		D	I	R	D	I	R	D	I	R	D	I	R
1	Read	o			o			o			o		
2	Insert	o			o			o			o		
3	Replace	o			o			o			o		
4	Extend	o			o			o			o		
5	Erase	o			o			o			o		

A.12.15 Initiator Override

State which values of override are implemented in the role of initiator.

	Initiator override	D	I
1	Create failure	o	
2	Select old file	o	
3	Delete and recreate with old attributes	o	
4	Delete and create with new attributes	o	

NOTE - The specification of the role of responder is to be given in A.10.5.

A.12.16 Requested Access

	Action	D	I	R
1	Read	o		
2	Insert	o		
3	Replace	o		
4	Extend	o		
5	Erase	o		
6	Read attribute	o		
7	Change attribute	o		
8	Delete file	o		

A.12.17 Processing mode

State which processing modes are capable of being specified, and which accepted. The validity and applicability of these for any instances of communication will be subject at least to the constraints of ISO 8571.

	Processing mode	D I R	
1	Read	o	
2	Insert	o	
3	Replace	o	
4	Extend	o	
5	Erase	o	

A.12.18 Recovery mode

If the recovery mode parameter is implemented state the implemented values for initiator and responder shall be stated here.

	Recovery mode	D I R
1	None	o
2	At start of file	o
3	Any active checkpoint	o

Section 6 : Document Type Detail

A.13 Document types

Conformance to document types is given at two levels. The following table shall be completed to indicate which document types have some level of support. The detail of that level of support shall be stated in the following tables.

	Entry number	FTAM-1	D I R
1	Object descriptor Object identifier	ISO FTAM unstructured text {iso standard 8571 document-type (5) unstructured-text (1)}	o

	Entry number	FTAM-2	D I R
2	Object descriptor Object identifier	ISO FTAM sequential text {iso standard 8571 document-type (5) sequential-text (2)}	o

	Entry number	FTAM-3	D I R
3	Object descriptor Object identifier	ISO FTAM unstructured binary {iso standard 8571 document-type (5) unstructured-binary (3)}	o

	Entry number	FTAM-4	D I R
4	Object descriptor Object identifier	ISO FTAM sequential binary {iso standard 8571 document-type (5) sequential-binary (4)}	o

In the following tables state the detailed level of support for each document type for which a level of support has been indicated above.
Registration information, when available, shall be included.

NOTES

1) The implementation of additional document types may be specified in a similar fashion.
2) No entry is specified for FTAM-5 because FTAM-5 is an incomplete document type, and therefore cannot be implemented on its own.