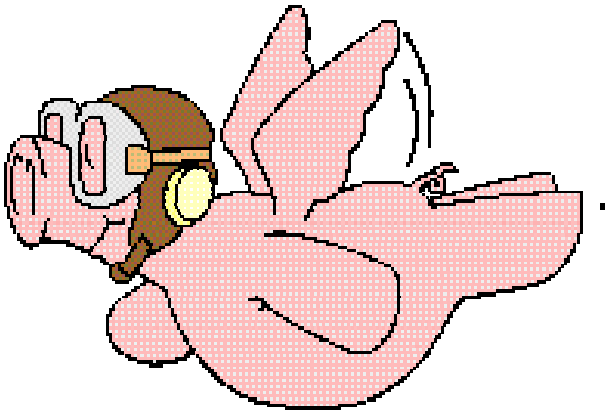
The ATN SARPs



Subvolume One

Introduction and System Level Requirements

Third Edition
(Final Editor's Draft)

Please note that this is the final editor's draft of the "Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) – ICAO DOC 9705/AN956 - as circulated within the ATNP. This text will be passed to ICAO for publication. However, it should be noted that this text in no way replaces the ICAO version, nor can it be considered to be of equal status. The official definitive version is that published in hardcopy by ICAO and all claims of compliance must be made against that version.

This PDF version has been prepared for the ATNP Working Groups by Helios Information Services Ltd. – http://www.helios-is.com

Please check our web site regularly for updates to the draft SARPs

Errata and Disclaimer

Please note that this document has been prepared from a number of separate files and no attempt has been made to ensure continuity of page numbers. You may therefore find some overlap between page numbers.

This document has been prepared on a “best efforts” basis and no warrantee is offered as to its correctness.

FOREWORD

The material contained in this document was originally developed as the detailed part of the first set of Standards and Recommended Practices (SARPs) for the aeronautical telecommunication network (ATN) which has commonly been referred to as the CNS/ATM-1 Package. It was intended to make the material an appendix to the new Chapter 3 of Annex 10, Volume III, Part I, containing broad, general, stable and mostly regulatory-type provisions (the core part of new ATN SARPs).

In December 1997, the Air Navigation Commission (ANC), while conducting the final review of draft ATN SARPs, agreed that the detailed part of ATN SARPs should be published as an ICAO manual (to be updated annually, if necessary), while retaining its SARPs-style language. The ANC has reviewed the status of the document in light of continuing worldwide ATN implementation. The Third Edition includes amendments from implementors and regulatory authorities, as well as four new Sub-Volumes to answer requirements for further standardization, in the interests of safety, regularity and efficiency of international civil aviation.

This document consists of nine Sub-Volumes:

Sub-Volume I — Introduction and System Level Requirements
Sub-Volume II — Air-Ground Applications
Sub-Volume III — Ground-Ground Applications
Sub-Volume IV — Upper Layer Communications Service (ULCS)
Sub-Volume V — Internet Communications Service (ICS)
Sub-Volume VI — System Management (SM)
Sub-Volume VII — Directory Services (DIR)
Sub-Volume VIII — Security (SEC)
Sub-Volume IX — Registration (REG)

Provisions contained in Sub-Volumes II, III, IV, V, VI, VII, VIII, and IX have been developed in accordance with system requirements specified in Sub-Volume I.

In line with the agreement by the ANC that the document should be updated on a yearly basis (if deemed necessary), the Third Edition has been published to incorporate changes necessitated by continuing validation and actual implementation activities.

TABLE OF CONTENTS

SUB-VOLUME I. INTRODUCTION AND SYSTEM LEVEL REQUIREMENTS

SUB-VOLUME II. AIR-GROUND APPLICATIONS

SUB-VOLUME III. GROUND-GROUND APPLICATIONS

SUB-VOLUME IV. UPPER LAYER COMMUNICATIONS SERVICE

SUB-VOLUME V. INTERNET COMMUNICATIONS SERVICE

SUB-VOLUME VI. SYSTEMS MANAGEMENT SERVICE

SUB-VOLUME VII. DIRECTORY SERVICE

SUB-VOLUME VII. SECURITY SERVICES

SUB-VOLUME IX. REGISTRATION SERVICE

1.1 DEFINITIONS AND REFERENCES

1.1.1 DEFINITIONS

Note 1.— The aeronautical telecommunication network (ATN) comprises application entities and communication services which allow ground, air-to-ground and avionics data subnetworks to interoperate by adopting common interface services and protocols based on the International Organization for Standardization (ISO) open systems interconnection (OSI) reference model.

Note 2.— This document addresses the following ATN technical requirements:

a) General and system level requirements;

b) ATN application entity requirements;

1) System application entity requirements;

i) Context management (CM) application;

ii) ATN Directory Services

2) Air-ground application entity requirements;

i) Controller pilot data link communication (CPDLC) application;

ii) Automatic dependent surveillance (ADS) application;

iii) Flight information service (FIS) applications;

3) Ground-ground application entity requirements;

i) Inter-centre communication (ICC) applications;

ii) ATS message handling service (ATSMHS) application;

c) ATN communication service requirements;

1) Upper layer communications service;

2) Internet communications service.

d) ATN systems management requirements;

e) ATN security service requirements;

f) ATN identifier registration requirements

Note 3.— An overview of this document is depicted in Figure 1-1.

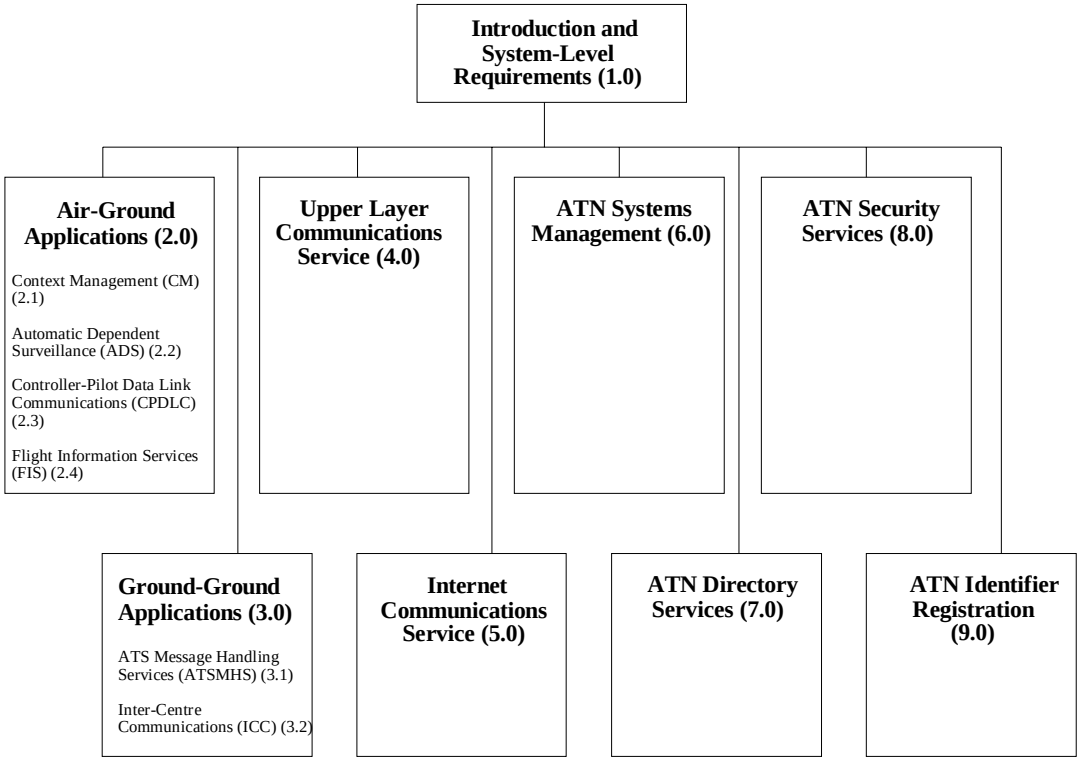


Figure 1.1. Overview of document

When the following terms are used in this document, they have the following meanings:

Abstract service interface. The abstract interface between the application entity (AE) and the application user.

Abstract syntax notation One (ASN.1). Abstract syntax notation One is defined in ISO/IEC 8824-1. The purpose of this notation is to enable data types to be defined, and values of those types specified, without determining their actual representation (encoding) for transfer by protocols.

Access control. The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

Accounting management. An ATN systems management facility to monitor users for use of network resources and to limit the use of those resources.

Addressing plan. A plan that provides common address syntax and management of global addresses for the unambiguous identification of all end and intermediate systems in accordance with the rules prescribed in ISO/IEC 7498-3 and ISO/IEC TR 10730.

Administrative domain. A collection of end systems, intermediate systems and subnetworks operated by a single organization or administrative authority. An administrative domain may be internally divided into one or more routing domains..

ADS. The symbol used to designate automatic dependent surveillance.

ADS application. An ATN application that provides ADS data from the aircraft to the ATS unit(s) for surveillance purposes.

ADS Contract. An agreement between the ADS ground-user and the ADS air-user that the latter will provide reports to the former under the conditions specified in the contract.

Aeronautical administrative communication (AAC). Communication used by aeronautical operating agencies related to the business aspects of operating their flights and transport services. This communication is used for a variety of purposes, such as flight and ground transportation, bookings, deployment of crew and aircraft or any other logistical purposes that maintains or enhances the efficiency of overall flight operation.

Aeronautical administrative messages. Messages regarding the operation or maintenance of facilities provided for the safety or regularity of aircraft operation. Messages concerning the functioning of the ATN and messages exchanged between government civil aviation authorities relating to aeronautical services.

Aeronautical fixed telecommunications network (AFTN). A world-wide system of aeronautical fixed circuits provided, as part of the aeronautical fixed service, for the exchange of messages and/or digital data between aeronautical fixed stations having the same or compatible communications characteristics.

Aeronautical industry service communication (AINSC). Communication related to aeronautical industry services including aeronautical operational control communication, aeronautical administrative communication, and aeronautical passenger communication. This communication involves one or more aeronautical industry service administrations. This term is used for purposes of address administration.

Aeronautical information service (AIS) messages. Messages concerning the aeronautical information service defined in ANNEX 15.

Aeronautical mobile-satellite service (AMSS). The AMSS comprises satellites, aeronautical earth stations (AESs), ground earth stations (GESs) and associated ground facilities such as a network coordination center. It uses the satellite subnetwork to provide aeronautical communication services between aircraft and ground users. Technical requirements for the AMSS are contained in Annex 10, Volume III, Part I, Chapter 4. The ATN supports the packet-mode data exchange provided by the AMSS.

Aeronautical operational control (AOC). Communication required for the exercise of authority over the initiation, continuation, diversion or termination of flight for safety, regularity and efficiency reasons.

Aeronautical passenger communication (APC). Communication relating to the non-safety voice and data services to passengers and crew members for personal communication.

AFTN. The symbol used to designate aeronautical fixed telecommunication network

AFTN/AMHS gateway. An end system which provides bi-directional interworking between users of the ATS message service and users connected to the AFTN.

AFTN form address (AF-address). Either an AFTN addressee indicator as specified in Annex 10, Volume II, paragraphs 4.4.3.1.2 and 4.4.16.2.1.3 which is used to locate AMHS users, either direct or indirect, in the AFTN address space or a predetermined distribution addressee indicator (PDAI) as specified in Annex 10, Volume II, 4.4.14.

Note.— An AF-address (AFTN-form) is an ICAO AFTN 8-letter addressee indicator.

AIDC. The symbol used to designate ATS interfacility data communication.

AINSC. The symbol used to designate aeronautical industry service communication.

Air application service element (air-ASE). An abstract part of the aircraft system that performs the communication related functions of the application.

Airborne collision avoidance system (ACAS). An aircraft system based on secondary surveillance radar (SSR) transponder signals which operates independently of ground-based equipment to provide advice to the pilot on potential conflicting aircraft that are equipped with SSR transponders.

Aircraft address. A unique combination of twenty-four bits available for assignment to an aircraft for the purpose of air-ground communications, navigation and surveillance.

Aircraft flight identification. A group of letters, figures or a combination thereof which is either identical to, or the coded equivalent of, the aircraft call sign to be used in air-ground communication and which is used to identify the aircraft in ground-ground air traffic services communication.

Air-ground application. An application that has one peer application on an aircraft and its other peer application on the ground. An air-ground application may require the use of ground-ground subnetworks.

Air traffic control (ATC) clearance. Authorization for an aircraft to proceed under conditions specified by an air traffic control unit.

Note 1.— For convenience the term "air traffic control clearance" is frequently abbreviated to "clearance" when used in appropriate contexts.

Note 2.— The abbreviated term "clearance" may be prefixed by the words "taxi", take-off", "departure", "en-route", "approach" or "landing" to indicate the particular portion of flight to which the air traffic control clearance relates.

Air traffic control (ATC) instruction. Directives issued by air traffic control for the purposes of requiring a pilot to take specific action.

Air traffic control (ATC) service. A service provided for the purposes of:

a) preventing collisions:

1) between aircraft, and

2) on the manoeuvring area between aircraft and obstructions; and

b) expediting and maintaining an orderly flow of traffic.

Air traffic services (ATS). A generic term meaning variously, flight information service, alerting service, air traffic advisory service, air traffic control service (area control service, approach control service or aerodrome control service).

Air user (air-user). The abstract part of the aircraft system that performs the non communication related functions of the application.

AMHS. The symbol used to designate ATS message handling system.

AMHS management domain. An AMHS management domain formed by an ATS organization for the management of that part of the AMHS which is under its responsibility.

AMHS message. An instance of the category of information object defined as message in ISO/IEC 10021-2 and conveyed in the AMHS. It is composed of an envelope and of a content.

AMHS probe. An instance of the category of information object defined as probe in ISO/IEC 10021-2 and conveyed in the AMHS. It is a class of message containing only an envelope which is conveyed by the message transfer agents (MTAs) from one user up to the MTA serving other users, used to determine the deliverability of messages.

AMHS report. An instance of the category of information object defined as report in ISO/IEC 10021-2 and conveyed in the AMHS. It is generated by a message transfer agent (MTA) in order to report on the outcome or progress of a message or probe in the set of interconnected MTAs pertaining to the AMHS.

Application. The ultimate use of an information system, as distinguished from the system itself.

Application entity (AE). Part of an application process that is concerned with communication within the OSI environment. The aspects of an application process that need to be taken into account for the purposes of OSI are represented by one or more AEs.

Application entity (AE) qualifier. That part of the AE title that unambiguously identifies the particular application entity.

Application entity (AE) service interface. The interface between the application users and the application service provider.

Application entity (AE) title. An unambiguous name for an application entity.

Application Information. **Refers to the application names (e.g. AE qualifiers such as ADS and CPC), version numbers, and addresses (the long or short TSAP, as required) of each application.**

Application layer. The seventh layer of the OSI reference model that controls application user access to the communication system and provides services to perform a logical association to other applications.

Application layer structure (ALS). The application layer structure refers to the internal architecture of the OSI application layer as described in ISO/IEC 9545.

Application process (AP). A set of resources, including processing resources, within a real open system which may be used to perform a particular information processing activity.

Application protocol data unit (APDU). An Application protocol data unit is an (N) PDU where N refers to the application layer. An APDU is the basic unit of information exchanged between the airborne application and the ground application.

Application service. The abstract interface between the (N) service and the (N) service user, where N refers to the application layer; thus it is the boundary between the AE and the application user.

Application service element (ASE). The element in the communication system which executes the application specific protocol. In other words, it processes the application specific service primitive sequencing actions, message creation, timer management, error and exception handling. The application's ASE interfaces only with the application's CF.

Application service element (ASE) service interface. The abstract interface through which the ASE service is accessed.

Note.— In version 1 of the ADS application, the ADS-ASE service interface coincides with the ADS-AE abstract service interface.

Application service object (ASO). An active element within (or equivalent to the whole of) the application-entity embodying a set of capabilities defined for the application layer that corresponds to a specific ASO-type (without any extra capabilities being used). An ASO is a combination of application service elements (ASEs) and ASOs that perform a specific function. An ASO that provides the functions of the establishment and data transfer phases is considered a complete protocol.

Application user. That abstract part of the aircraft or ground system that performs the non-communication related functions of the application.

Association control service element (ACSE). The association control service element is the common mechanism in the application layer structure (ALS) for establishing and releasing application service object (ASO) associations.

ATIS. The symbol used to designate automatic terminal information service.

ATIS application. A FIS application that supports the ATIS.

ATN. The symbol used to designate the aeronautical telecommunication network.

ATN application. Refers to an application that is designed to operate over ATN communication services.

ATN communication services. Composed of the internet communications service and the upper layers communications service.

ATN Directory Services (DIR). A service which provides the capability for an application entity or user in the ATN community to query a distributed directory data base and retrieve addressing, security and technical capabilities information relating to other users or entities within the ATN community.

ATN environment. The environment that relates to functional and operational aspects of the ATN as a complete end-to-end communication system.

ATN identifier registration. The central repository for common identifiers and application addresses used within the ATN domain. Common identifiers include object identifiers and application type identifiers used by various applications, and are defined to avoid duplication and conflicts with the ATN domain. Application addresses are also included in the ATN Identifier Registration in order to provide a common location for the listing of States' ATN addresses.

ATN profile requirement list (APRL). APRLs identify, in a tabular form, requirements together with the options and parameters for protocols used in the ATN. The supplier of an ATN protocol implementation claiming to conform to the ATN technical requirements must indicate conformance to those requirements by preparing a protocol implementation conformance statement (PICS) based on the set of APRLs.

ATN Security Services. A set of information security provisions allowing the receiving end system or intermediate system to unambiguously identify (i.e. authenticate) the source of the received information and to verify the integrity of that information.

ATN systems management (SM). A collection of facilities to control, co-ordinate and monitor the resources which allow communications to take place in the ATN environment. These facilities include fault management, accounting management, configuration management, performance management and security management.

ATS. The symbol used to designate air traffic services.

ATSC. The symbol used to designate air traffic services communication.

ATSC class. The ATSC class parameter enables the ATSC user to specify the quality of service expected for the

offered data. The ATSC class value is specified in terms of ATN end-to-end transit delay at 95% probability.

ATS communication (ATSC). Communication related to air traffic services including air traffic control, aeronautical and meteorological information, position reporting and services related to safety and regularity of flight. This communication involves one or more air traffic service administrations. This term is used for purposes of address administration.

ATS interfacility data communication (AIDC). Automated data exchange between air traffic services units, particularly in regard to co-ordination and transfer of flights.

AIDC application. An ATN application dedicated to exchanges between ATS units (ATSUs) of air traffic control (ATC) information in support of flight notification, flight coordination, transfer of control, transfer of communication, transfer of surveillance data and transfer of general data.

ATS message. A unit of user-data, coded in binary form, which is conveyed from an originator of the data to one or more recipients of the data. It is possible to associate a unique message identifier and a priority with each ATS message.

ATS message handling services (ATSMHS). Procedures used to exchange ATS messages over the ATN such that the conveyance of an ATS message is in general not correlated with the conveyance of another ATS message by the service provider.

ATS message server. An ATN end system which provides the relay function included in the ATS message service. It may also optionally provide the storage function included in the ATS message service.

ATS message handling system (AMHS). The set of computing and communication resources implemented by ATS organizations to provide the ATS message service.

ATS message user agent. An ATN end system which provides an interface to the ATS message service for an ATS message service user.

ATSMHS. The symbol used to designate ATS message handling services.

ATS organization. An ICAO State or organization which administers one or more ATS end and/or intermediate systems.

ATS unit (ATSU). A generic term meaning variously, air traffic control unit, flight information centre or air traffic services reporting office.

Authentication. A process used to ensure the identity of a person/user/network entity.

Authentication exchange. A mechanism intended to ensure the identity of an entity by means of information exchange.

Authentication information. Information used to establish the validity of a claimed identity.

Authorized path. A communication path that the administrator(s) of the routing domain(s) has pre-defined as suitable for a given traffic type and category.

Automatic dependent surveillance (ADS). A surveillance technique in which aircraft automatically provide, via a data link, data derived from on-board navigation and position-fixing systems, including aircraft identification, four-dimensional position, and additional data as appropriate.

Automatic terminal information service (ATIS). The automatic provision of current, routine information to arriving and departing aircraft throughout 24 hours or a specified portion thereof.

Data link-automatic terminal information service (D-ATIS). The provision of ATIS via data link.

Voice-automatic terminal information service (Voice-ATIS). The provision of ATIS by means of continuous and repetitive voice broadcasts.

***Aviation Routine Weather Report Service* (METAR). The provision of routine and special (SPECI)weather observation reports issued at interval of one hour and disseminated on request to local air traffic services. SPECI reports are unscheduled reports containing all METAR data element plus additional plain language information.**

***Basic encoding rules (BER).* Encoding rules as defined in ISO/IEC 8825-1 which have been designed to provide basic encoding of ASN.1 structures.**

Boundary intermediate system (BIS). An intermediate system that is able to relay data between two separate routing or administrative domains.

Certificate authority; certification authority. An authority trusted by one or more users to create and assign certificates.

Certificate path; certification path. An ordered sequence of certificates of objects in the DIT which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

CIDIN. The symbol used to designate common ICAO data interchange network.

CIDIN/AMHS gateway. An end system which provides bi-directional interworking between users of the ATS message service and users connected to the CIDIN.

CM. The symbol used to designate context management.

Confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration management. An ATN systems management facility for managers to change the configuration of remote elements.

Common management information Protocol (CMIP). The management protocol defined by ISO 9596-1.

Connectionless network protocol (CLNP). The protocol responsible for forwarding packets through the ATN internet communications service.

Context management (CM) application. An ATN application that provides a logon service allowing initial aircraft introduction into the ATN and a directory of all other data link applications on the aircraft . It also includes

functionality to forward addresses between ATS units.

Note.— Context management is a recognized OSI presentation layer term. The OSI use and the ATN use have nothing in common.

Context management (CM) server. **An ATS facility that is capable of providing application information relating to other ATSUs to requesting aircraft or ATSUs**.

Controller pilot communication (CPC). In a controlled airspace, continuous listening watch on the appropriate radio frequency (either manual or automatic with signaling devices) and establishment of two-way communication with the appropriate air traffic control (ATC) unit.

Controller pilot data link communication (CPDLC). A means of communication between controller and pilot, using data link for ATC communications.

CPDLC application. An ATN application that provides a means of ATC data communication between controlling, receiving or downstream ATS units and the aircraft, using air-ground and ground-ground subnetworks, and which is consistent with the ICAO phraseology for the current ATC voice communication.

Control function (CF). That abstract part of the AE that performs the mapping between the ASE service primitives, the association control service element (ACSE) service primitives and other elements within the application entity.

Controlling ATSU (C-ATSU). The air traffic control unit exercising legal authority over the initiation, continuation, diversion or termination of flights and providing air traffic control service to controlled flights in the control area under its jurisdiction.

CPDLC. The symbol used to designate controller pilot data link communication.

Credentials. Data that is transferred to establish the claimed identity of an entity.

Cryptographic checkvalue; tag. Information which is derived by performing a cryptographic transformation on the data unit.

Cryptographic scheme. A cryptographic scheme consists of an unambiguous specification of a set of transformations capable of providing a cryptographic service when properly implemented and maintained.

Current data authority. The ground system that provides for the establishment and maintenance of a transport connection for the purposes of conducting a CPDLC dialogue pertaining to the services of the C-ATSU.

Data authority. A ground system that provides for the establishment and maintenance of a CPDLC transport connection with an aircraft. The transfer of communication from the current data authority to the next data authority is prepared prior to the actual data link switch by designating a next data authority in a specific CPDLC message.

Data communications equipment (DCE). An interface between data terminal equipment and the transmission mechanism.

Data Integrity. The property that data has not been altered or destroyed.

Data link layer. The second layer of the OSI reference model that manages the operations of the physical layer and may utilize special error detection or retransmission techniques to achieve acceptable error rates.

Data origin authentication. The corroboration that the source of data received is as claimed.

Demand contract (DC). A contract between a requestor and a provider of information service, such as ADS or FIS, to provide a single report to the requestor (vs. Continual reports to one request).

Dialogue. A co-operative relationship between elements which enables communication and joint operation.

Dialogue service (DS). The lower service boundary of an ASE; the service allows two ASEs to communicate, such as a CM ground-ASE to communicate with a CM air-ASE.

Digital signature. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.

Directory. A facility that supports on request the retrieval of address information or the resolution of application names.

Distinguished encoding rules (DER). Encoding rules as defined in ISO/IEC 8825-1 which have been designed to restrict the encoding of values to just one of the alternatives provided by BER.

Distinguishing path attribute (DPA). Used to discriminate among multiple routes to a destination, based on differences in the quality of service between the routes (for example, expense, transit delay or residual error probability.)

Domain. A set of end systems and intermediate systems that operate according to the same routing procedures and that is wholly contained within a single administrative domain.

Domain specific part (DSP). An addressing authority is responsible for its own addressing subdomain and network service access point (NSAP) addresses within that addressing domain are distinguished, where necessary, by the value of the DSP.

Downstream ATSU (D-ATSU). D-ATSU handles the coordination of the conditions of transfer for a flight from the controlling ATSU (C-ATSU) which may notify the D-ATSU of a flight's cleared profile prior to its effective transfer to the receiving ATSU (R-ATSU).

Downstream clearance (DSC). Specific clearance request by an aircraft to an ATSU which is not the controlling ATSU. The initiation of the DSC service can only be initiated by an aircraft.

Downstream data authority. The ground system that is permitted to conduct a downstream CPDLC downstream clearance (DSC) dialogue with an aircraft.

DSC. The symbol used to designate downstream clearance.

Edition. The edition of this document indicates the collection of technical provisions as of a specific publication date.

Emergency contract. A contract to provide ADS reports at regular intervals during an emergency situation.

End routing domain (ERD). A routing domain (RD) that only routes protocol data units (PDUs) from/to its own RD.

End system (ES). A system that contains the OSI seven layers and contains one or more end user application processes.

End-to-end. Pertaining or relating to an entire communication path, typically from (1) the interface between the information source and the communication system at the transmitting end to (2) the interface between the communication system and the information user or processor or application at the receiving end.

End user. An ultimate source and/or consumer of information.

Entity. An active element in any layer which can either be a software entity (such as a process) or a hardware entity (such as an intelligent I/O chip).

Estimated time of arrival (ETA). For IFR flights, the time at which it is estimated that the aircraft will arrive over that designated point, defined by reference to navigation aids, from which it is intended that an instrument approach procedure will be commenced, or if no navigation aid is associated with the aerodrome, the time at which the aircraft will arrive over the aerodrome. For VFR flights, the time at which it is estimated that the aircraft will arrive over the aerodrome.

Ethernet. Based on the local area network standard, ISO/IEC 8802-3, carrier sense multiple access with collision detection (CSMA/CD) access method, and physical layer specifications using broadcast technology which may connect as an ATN subnetwork.

Expense. The cost to perform some task. In the context of internetworking, expense is defined in terms of the incremental expense incurred for transfer of a single network service data unit (NSDU) of 512 octets in size.

Extended projected profile. A projected profile extended up to a number of way points.

Fast byte. The capability at any layer of the OSI reference model to negotiate out the capabilities of the base protocol.

Fault Management. An ATN systems management facility to detect, isolate and correct problems.

Figure of merit (FOM). An indication of the level of accuracy of positional information given in an ADS report.

FIS. The symbol used to designate flight information service.

FIS application. An ATN application that provides to aircraft information and advice useful for safe and efficient conduct of flight.

FIS contract. An agreement between a FIS air-user and a FIS ground-user that the latter will provide FIS reports under the conditions specified in the FIS contract.

Flight information region (FIR). An airspace of defined dimensions within which flight information service and alerting service are provided.

Flight information service (FIS). A service provided for the purpose of giving advice and information useful for the safe and efficient conduct of flights.

Flight plan. Specified information provided to air traffic services units, relative to an intended flight or portion of a flight of an aircraft.

Note.— Specifications for flight plans are contained in Annex 2. A model Flight Plan Form is contained in Appendix 2 to PANS-RAC (Doc 4444).

Flow control. A function that controls the flow of data to perform buffer management within a layer or between adjacent layers.

Forward contract. A contract to provide a ground ADS system with ADS reports.

Forwarding information base (FIB). The information base that is maintained by each router and contains the set of forwarding paths reflecting the various policy and QoS rankings available to reach each known destination.

Function. A coherent set of activities which fulfils, by itself or together with other functionality, a concept. Examples of functions: conflict free planning; electronic representation of the flight.

Functional requirements. Requirements that determine what function a system should perform. They can usually be expressed by a verb applying to a type of data, e.g., display aircraft position.

Gateway. A system used to interconnect dissimilar networks. A gateway may contain all seven layers of the OSI reference model.

General communication. A category of communications which includes APC, public correspondence and other non-operational and non-administrative communication.

Ground application service element (ground-ASE). An abstract part of the ground system that performs the communication related functions of the application.

Ground user (ground-user). The abstract part of the ground system that performs the non-communication related functions of the application.

Ground earth station (GES). An earth station in the fixed satellite service, or, in some cases, in the aeronautical mobile-satellite service, located at a specified fixed point on land to provide a feeder link for the aeronautical mobile-satellite service.

Note.— This definition is used in the ITU's Radio Regulations under the term "aeronautical earth station." The definition herein as "GES" for use in the SARPs is to clearly distinguish it from an aircraft earth station (AES), which is a mobile station on an aircraft.

Ground forwarding function. The capability for a ground system to forward a CPDLC message to another ground system via a CPDLC message with an indication of success, failure or non-support from the receiving ground system. This function may be invoked by the current data authority in order to avoid retransmission of a request by an aircraft by forwarding the information to the next data authority. The downstream data authority may use this function in order to relay a message to the current data authority which then performs the actual transmission

to the aircraft.

Ground-ground application. An application that has both of its peer applications on the ground.

Hash function. A (mathematical) function which maps values from a large (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range.

ICAO Facility Designation. A four to eight-letter code group formulated in accordance with rules prescribed by ICAO and assigned to the ATS end system executing an application process.

ICC. The symbol used to designate inter-centre communication.

ICS. The symbol used to designate the internet communication services.

Initial domain part (IDP). The addressing authority responsible for an addressing subdomain that assigned the network service access point (NSAP) address and that specified the abstract syntax and structure of the remainder of the NSAP address.

Inter-centre communication (ICC). ICC is data communication between ATS units to support ATS, such as notification, coordination, transfer of control, flight planning, airspace management and air traffic flow management.

Intermediate system (IS). A system which performs relaying and routing function and comprises the lowest three layers of the OSI reference model.

International Alphabet No. 5 (IA5). International Alphabet Number 5 defined by ITU-T.

Note.— ATN uses the "6 bit ASCII" subset of 1A5, as used in SSR Mode S specifications.

Internet communications service (ICS). The internet communications service is an internetwork architecture which allows ground, air-to-ground and avionics data subnetworks to interoperate by adopting common interface services and protocols based on the ISO OSI reference model.

Internetwork. A set of interconnected, logically independent heterogeneous subnetworks. The constituent subnetworks are usually administrated separately and may employ different transmission media.

Internetwork protocol (IP). A protocol that performs the basic end-to-end mechanism for the transfer of data packets between network entities. In the ATN internet communications service, the ISO/IEC 8473 internetwork protocol is used.

Interoperability. Describes the ability of the ATN to provide, as a minimum, a transparent data transfer service between end systems even though the ATN comprises various ground, air-to-ground and avionics subnetworks. The ability to interoperate between end systems can be extended to include commonality of upper layer protocols.

ISO. The symbol used to designate International Organization for Standardization.

ITU-T. The symbol used to designate International Telecommunication Union-Telecommunication Standardization

Sector.

IETF. The symbol used to designate Internet Engineering Task Force.

Key agreement. A method for negotiating a key value on-line without transferring the key, even in an encrypted form, e.g., the Diffie-Hellman technique.

Key agreement scheme. A scheme in which the keying data established is a function of contributions provided by both entities in such a way that neither party can predetermine the value of the keying data.

Key derivation function. A key derivation function is a function which takes as input a shared secret value and outputs keying data suitable for later cryptographic use.

Long transport service access point (TSAP). Composed of the router domain part (RDP) and the short TSAP.

Lower layers. The physical, data link, network and transport layers of the OSI reference model.

Managed object. Data processing and data communication resources that may be managed through the use of the OSI management protocol.

Management agent. Performs management operations on managed objects within its local environment as a consequence of management operations communicated from a manager. A management agent may also forward notifications emitted by managed objects to a manager.

Management domain (MD). Resources that for systems management purposes are represented by managed objects. A management domain possesses at least the following quantities: a name that uniquely identifies that management domain, identification of a collection of managed objects that are members of the domain and identification of any inter-domain relationships between this domain and other domains.

Management information base (MIB). Data structure containing MO abstractions and providing access points to real managed objects.

Manager. The term given to a system that requests or otherwise receives information about managed objects.

Manipulation. The replacement, insertion, deletion, or misordering of user data during a communication by an unauthorized user.

Message. Basic unit of user information exchanged between an airborne application and its ground counterpart or between two ground applications. Messages are passed in one or more data blocks from one end user to another through different subnetworks.

Message authentication code or MAC scheme. A message authentication code or MAC scheme is a cryptographic scheme capable of providing data origin authentication and data integrity.

Message element. A component of a message used to define the context of the information exchanged.

Message element identifier. The ASN.1 tag of the ATCUplinkMsgElementId or the ATCDownlinkMsgElementId.

Message handling system (MHS)-form address. An instance of the AMHS address form which is used to locate a direct or indirect AMHS user in the AMHS address space.

Message header. The control information used to maintain synchronization between the two end systems.

METAR. The symbol used to designate **Aviation Routine Weather Report Service**

METAR application. A FIS application that supports the METAR.

Mobile routing domains. Formed from ATSC and AINSC systems onboard an aircraft (or any other mobile platform), within the aircraft operator's administrative domain. A mobile RD is characterized as an end routing domain (ERD).

Mobile subnetwork. A subnetwork connecting a mobile system with another system not resident in the same mobile platform. These subnetworks tend to use free-radiating media (e.g. VHF/UHF radio, D band satellite or D band secondary surveillance radar) rather than contained media (e.g. wire or coaxial cable); thus they exhibit broadcast capabilities in the truest sense.

Mode select (Mode S). An enhanced mode of secondary surveillance radar (SSR) which permits the selective interrogation of Mode S transponders, the two-way exchange of digital data between Mode S interrogators and transponders and also the interrogation of Mode A or Mode C transponders.

Naming plan. A plan that provides common naming conventions and designations for the unambiguous identification of all end and intermediate systems in accordance with the rules prescribed in ISO/IEC 7498-3, ISO/IEC TR 10730 and ISO/IEC 9545.

Network addressing domain. A subset of the global addressing domain consisting of all the NSAP addresses allocated by one or more addressing authorities.

Network entity (NE). A functional portion of an internetwork router or host computer that is responsible for the operation of internetwork data transfer, routing information exchange and network layer management protocols.

Network entity title (NET). The global address of a network entity.

Network layer (NL). Provides a uniform service interface for the transfer of data among end systems and intermediate systems (ISs) utilizing the ISO protocol architecture.

Network management (NM). The set of functions related to the management of various OSI resources and their status across the Network Layer of the OSI architecture.

Network service access point (NSAP). Point within the ISO protocol architecture at which global end users may be uniquely addressed on an end-to-end basis.

Network service access point (NSAP) address. A hierarchically organized global address, supporting international, geographical and telephony-oriented formats by way of an address format identifier located within the protocol header. Although the top level of the NSAP address hierarchy is internationally administered by ISO, subordinate address domains are administered by appropriate local organizations.

Network service access point (NSAP) address prefix. Used to identify groups of systems that reside in a given routing domain or confederation. An NSAP prefix may have a length that is either smaller than or the same size as the base NSAP address.

Network topology map. Provides an overall view of the global network connectivity and is used in path computations by the operative routing algorithm.

Next data authority. The ground system that provides for the establishment and maintenance of a transport connection for the purposes of conducting a CPDLC dialogue pertaining to the services of the receiving ATS unit (R-ATSU).

NOTAM. A notice containing information concerning the establishment, condition or change in any aeronautical facility, service, procedure or hazard, the timely knowledge of which is essential to personnel concerned with flight operations.

Open systems interconnection (OSI) protocol architecture. A set of protocols used to implement the OSI reference model.

Open systems interconnection (OSI) reference model. A model providing a standard approach to network design introducing modularity by dividing the complex set of functions into seven more manageable, self-contained, functional layers. By convention these are usually depicted as a vertical stack.

Operational requirement. A statement of the operational attributes of a system needed for the effective and/or efficient provision of air traffic services to users.

OSI. The symbol used to designate open systems interconnection.

Packed encoding rules (PER). Encoding rules as defined in ISO/IEC 8825-2 which have been designed to minimize the number of bits transmitted.

Peer-entity authentication. The corroboration that a peer entity in an association is the one claimed.

Performance management. An ATN systems management facility to monitor and evaluate the performance of the systems.

Performance requirements. Requirements that define a function's characteristics, such as reliability, availability, response time, processing delay, integrity, that are necessary to meet the operational requirements for a specific application of the function.

Periodic contract (PC). A contract to provide ADS reports at regular intervals.

Physical layer. The layer of the OSI reference model that controls access to the transmission medium which forms the basis for the communication system.

Presentation address (PA). The presentation address must, as a minimum, include a network service access point (NSAP) address and a transport service access point (TSAP) selector and may include a presentation service access point (PSAP) selector and session service access point (SSAP) selector based on the addressing structure adopted within the end system (ES) and whether the application requires the OSI session or presentation protocol.

Presentation data value (PDV). The unit of information specified in an abstract syntax, which is transferred by the

OSI presentation-service (ISO/IEC 8822).

Presentation layer. The layer of the OSI reference model that controls the coding, format and appearance of the data transferred to and from the application layer.

Presentation service access point (PSAP) selector. The element of the presentation address that identifies the user of the presentation protocol entity.

Priority (P). The relative importance of a particular protocol data unit (PDU) relative to other PDUs in transit and used to allocate resources which become scarce during the transfer process.

Private key; secret key (deprecated). In a public key cryptosystem that key of a user's key pair which is known only by that user.

Profile. Defines implementation conformance constraints on a set of reference specifications.

Projected profile. An indication of where and when the aircraft anticipates it will be at the following two way-points.

Protocol. A set of rules and formats (semantic and syntactic) which determines the communication behavior between peer entities in the performance of functions at that layer.

Protocol control information (PCI). Information included in a layer header which contains service primitives specific to that layer.

Protocol data unit (PDU). (1) A unit of data transferred between peer entities within a protocol layer consisting of protocol control information and higher layer user data (i.e. service data units). (2) A unit of data specified in an (N) protocol and consisting of (N) protocol control information and possibly (N) user data, where N indicates the layer.

Protocol implementation conformance statement (PICS). A protocol implementation conformance statement enables conformance testing of protocols. As recommended by ISO/IEC 9646-2, PICS proforma, tailored to ATN context, have been developed as ATN profile requirement list (APRLs) to provide an effective basis for conformance testing of implementations.

Public key. In a public key cryptosystem that key of a user's key pair which is publicly known.

Quality of service (QoS). Information relating to data transfer characteristics (for example, requested throughput and priority) used by a router to perform relaying and routing operations across the subnetworks which make up a network.

Replay. The recording and subsequent replay of a communication at some later time.

RFC. The symbol to designate Request for Comments.

Receiving ATSU (R-ATSU). The next air traffic control unit which is the process of accepting the control authority and communication responsibility for a flight transferred by the controlling ATSU (C-ATSU).

Relaying. The process of transferring packets across subnetworks including any necessary packet conversion.

Requested QoS. The service characteristics desired by the service user.

Reserved value. Legal values for the respective fields (have not yet been assigned specific meanings by ICAO). These values should be processed normally in order to allow future assignment. Meanings may be assigned in the future and are not available for local use. The allocation of these values requires no change in the version identifier.

Residual error probability. Indicates the likelihood that a protocol data unit (PDU) will be lost, duplicated or corrupted. This probability is defined as the ratio of lost, duplicated or corrupted network service data units (NSDUs) to the total number of NSDUs transmitted by an ATN network service (NS) provider, normalized for an NSDU size of 512 octets.

Residual error rate (RER). The ratio of messages mis-delivered, non-delivered or delivered with an error undetected by the system, to the total number of messages delivered to the system during a measurement period (adapted from ISO/IEC 8072).

Note.— For the ATN, detected mis-delivered and non-delivered messages are not included in the ratio.

Route. The set of addresses that identifies the destinations reachable over the router and information about the route's path including the QoS and security available over the route.

Router. The communication element that manages the relaying and routing of data while in transit from an originating end system to a destination end system. A router comprises an OSI intermediate system and end system supporting a systems management agent.

Routing. A function within a layer that uses the address to which an entity is attached in order to define a path by which that entity can be reached.

Routing area (RA). A routing subdomain comprising one or more intermediate systems (ISs) and optionally one or more end systems (ESs).

Routing domain (RD). A set of end systems and intermediate systems that operate the same routing protocols and procedures and that are wholly contained within a single administrative domain. A routing domain may be divided into multiple routing subdomains.

Routing domain confederation (RDC). A set of routing domains and/or RDCs that have agreed to join together. The formation of a RDC is done by private arrangement between its members without any need for global coordination.

Routing domain identifier (RDI). A generic network entity title (NET) as described in ISO/IEC 7498 and is assigned statically in accordance with ISO/IEC 8348. An RDI is not an address and cannot be used as a valid destination of an ISO/IEC 8473 PDU. However, RDIs are, like ordinary NETs, assigned from the same addressing domain as network service access point (NSAP) addresses.

Routing information base (RIB). A data base that is maintained by each router and comprises the information regarding the connectivity and topology of the end systems (ESs) and intermediate systems (ISs) within a particular routing domain and path information pertinent to paths interconnecting routing domains. It is maintained by way of the information received by a routing information exchange protocol. Each routing information exchange protocol has its own RIB specification.

Routing information exchange protocol. The protocol used to exchange subnetwork connectivity information between end systems and intermediate systems and between intermediate systems and intermediate systems.

Routing policy. A set of rules that control the selection of routes and the distribution of routing information by boundary intermediate systems (BISs). These rules are based on policy criteria rather than on performance metrics such as hop count, capacity, transit delay, cost, etc. which are usually applied for routing. There are two groups of routing policy in the ATN:

a) general routing policy to ensure necessary connectivity at a reasonable routing information update rate, and

b) user specified routing policy, i.e. individual policy rules which may be additionally implemented in BISs by administrations and organizations to meet their specific operational and policy needs.

Runway visual range (RVR). The range over which the pilot of an aircraft on the centre line of a runway can see the runway surface markings or the lights delineating the runway or identifying its centre line.

Secondary surveillance radar (SSR). A surveillance radar system which uses transmitters/receivers (interrogators) and transponders.

Security label. May indicate requirements for protection of a protocol data unit (PDU) and provide information used by network layer access control functions.

Security management. An ATN systems management facility for access control, authentication and data integrity.

Service data unit (SDU). A unit of data transferred between adjacent layer entities, which is encapsulated within a protocol data unit (PDU) for transfer to a peer layer.

Service primitive. A function of an application service element (ASE) that is not broken down further into subfunctions and is presented as part of the abstract service interface (i.e. request, indication, response or confirmation).

Service provider. The ground and airborne application entities (AEs) for the application, all underlying data communication protocol entities and the physical media. As a consequence, it encompasses everything between the application-AE service interfaces of the end users of the application.

Session key. A key established by a key establishment scheme.

Session layer. The layer of the OSI reference model that establishes the rules of dialogue between two end user entities.

Session service access point (SSAP) selector. The element of the session address that identifies the user of the session protocol entity.

Shared secret value. An intermediate value in a key establishment scheme from which keying data is derived.

Short transport service access point (TSAP). Composed of the administrative region selector (ARS), (Optional), the

location identifier (LOC), the system identifier (SYS), the network selector (SEL), and the transport selector (TSAP selector).

Signature scheme. A signature scheme is a cryptographic scheme capable of providing data origin authentication, data integrity, and non-repudiation.

Simple authentication. Authentication by means of simple password arrangements.

Stack (or protocol stack). A set of cooperating OSI protocols selected from different layers of the basic reference model. Hence, upper layer stack refers to session, presentation and application protocols, while lower layer stack refers to physical, data link, network and transport protocols.

Strong authentication. Authentication by means of cryptographically derived credentials

Subnetwork (SN). An actual implementation of a data network that employs a homogeneous protocol and addressing plan and is under control of a single authority.

Subnetwork access protocol (SNAcP). The actual protocol used to receive services for a particular sub-network. For example, the subnetwork access protocol to many public data networks is X.25.

Subnetwork dependent convergence function (SNDCF). The set of rules and procedures needed to convert the data transfer needs of the subnetwork independent convergence protocol to the actual services provided by a subnetwork.

Subnetwork (SN) domain. The set of end systems and intermediate systems connected to the same physical network.

Subnetwork independent convergence function (SNICF). The common protocol for all host computers and routers that is used for the transfer of data. The SNICF is the connectionless network protocol defined by ISO/IEC 8473.

Subnetwork point of attachment (SNPA). The point at which a real end system, interworking unit or real subnetwork is attached to a real subnetwork and is a conceptual point within an end or intermediate system at which the subnetwork service is offered.

Subnetwork point of attachment (SNPA) address. Provides information used in the context of a particular real subnetwork to identify a SNPA. An SNPA address is a subnetwork address such as X.25 data terminal equipment (DTE) addresses, ethernet MAC addresses, etc.

Subset. An implementation of an application air or ground service conforming to the application SARPs which supports a defined, technically acceptable but not complete application functionality.

Subsetting rules. Formal instructions relating to the requirement for combinations of elements within an application SARPs, constituting limited application functionality.

System application. An application supports the operation of the air-ground applications, ground-ground applications, or communication services. A system application can take the form of either an air-ground application or a ground-ground application.

System level requirement. The system level requirement is a high-level technical requirement that has been derived from operational requirements, technological constraints and regulatory constraints (administrative and

institutional). The system-level requirements are the basis for the functional requirements and lower level requirements.

System security object (SSO). The System Security Object provides a set of abstract services for the generation and verification of security items.

Traffic category. A subdivision of the operational communication traffic type used to distinguish between ATS communication and aeronautical operational control (AOC).

Traffic type. A means used to distinguish different types of message traffic for the purposes of establishing communication paths to support operational and legal requirements. There are four traffic types:

a) the operational communication traffic type is subdivided into two cateogries representing safety and regularity of flight communication:

   1) ATS communication

   2) Aeronautical operational control

b) administrative communication representing non-safety and regularity of flight communication sent by aircraft operating agencies and ATS administrations

c) general communication, representing APC, public correspondence and other non-operational and non administrative communication, and

d) systems management communication representing systems management information that is critical for support of network operations.

Note.— The differentiation of traffic types is required because different data traffic may have different access to subnetworks. The traffic type is conveyed in the ATN security label of ISO/IEC 8473 and ISO/IEC 10747. It is used to qualify connectionless mode network protocol (CLNP) data packets and (inter-domain) routes according to the class of traffic that they carry. Based on this qualification, access of subnetworks is controlled by the ATN internet communications service.

Transit delay. In packet data systems, the elapsed time between a request to transmit an assembled data packet and an indication at the receiving end that the corresponding packet has been received and is ready to be used or forwarded.

Transit routing domain (TRD). A domain whose policies permit its boundary intermediate systems (BISs) to provide relaying for protocol data units (PDUs) whose source is located in either the local routing domain or in a different routing domain.

Transport layer. The fourth layer of the OSI reference model which ensures that the data are reliably delivered to the correct destination regardless of which network layer protocol and underlying subnetworks are being used.

Transport protocol class 4 (TP-4). Transport protocol class 4 is defined in ISO/IEC 8073 and profiled for ATN context to provide the connection mode transport service as described in ISO/IEC 8072.

Transport service access point (TSAP). The logical access point to the transport layer.

Transport service access point (TSAP) address. The complete communication address which unambiguously defines a transport service user. The TSAP address comprises the NSAP address and a TSAP selector.

Transport service data unit (TSDU). The data presented to the transport layer for transmission over the ATN internet communications service.

Update contract (UC). A contract to provide a piece of FIS information and any update of this information.

Upper layer (UL) communications service. A term pertaining to the session, presentation and application layers of the OSI reference model.

User. That abstract part of the aircraft or ground system that performs the non-communication related functions of the application. The direct user of the ATN is an application within an end system supporting ATS or aeronautical industry services. The air traffic controller, other ground staff or the pilot are users of the ATN. The user may also be seen more on the abstract level as an organization, e.g. airline or service provider

User certificate; public key certificate; certificate. The public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it.

User requirements. Requirements that are allocated to the user to ensure the interoperability of the communication services and application entities.

UTC. The symbol used to designate coordinated universal time.

Version. The ATN specific protocols and the ATN applications are subject to version control. A version number is incremented only if the protocol/application needs to negotiate with a prior version of that protocol/application in order to achieve interoperability.

Very high frequency (VHF) digital link (VDL). Packet data communication to aircraft and ground users comprised of airborne VHF data radios (VDRs), VHF ground stations and connectivity to routers on the aircraft and the ground.

X.25 packet switched data network (PSDN). A communication network that provides a network access service in compliance with CCITT recommendation X.25.

1.1.2 REFERENCES

When the following reference designators are cited in the Standards and Recommended Practices (SARPs) for the ATN they are referring to the following editions and/or versions:

ANSI X9.63: 1999. Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, Draft.

ANSI X9.62: 1999. Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

Association for Computing Machinery (ACM) - Proceeding of SIGCOM '88, August 1988. Congestion Avoidance and Control, Van Jacobson

Association for Computing Machinery (ACM) - Transactions on Computer Systems, Volume 9, Number 4, November 1991. Improving Round-Trip Time Estimates in Reliable Transport Protocols, Phil Karn

CCITT Recommendation M.3100 (1992). Maintenance: Telecommunications Management Network - Generic Network Information Model

CCITT Rec X.121 (1992). International numbering plan for public data networks.

CCITT Rec X.400 (1992). Message handling system and service overview.

CCITT Rec X.402 (1992). Message handling systems: Overall architecture.

CCITT Rec X.408 (1988). Message handling systems: Encoded information type conversion rules.

CCITT Rec X.410 (1984). Information technology – Text communication – Message handling systems – Reliable transfer service

CCITT Rec X.411 (1992). Message handling systems: Message transfer system: Abstract service definition and procedures.

CCITT Rec X.413 (1992). Message handling systems: Message store: Abstract service definition.

CCITT Rec X.419 (1992). Message handling systems: Protocol specifications.

CCITT Rec X.420 (1992). Message handling systems: Interpersonal messaging system.

IETF RFC 1320. The MD4 Message — Digest Algorithm, R. Rivest, April 1992.

IETF RFC 1951. DEFLATE Compressed Data Format Specification (Version 1.3), P. Deutsch, May 1996.

IETF RFC 2459 (1999). Internet X.509 Public Key Infrastructure Certificate and CRL profile

IETF RFC 2527 (1999). Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

ISO/IEC 646:1991. Information Technology — ISO 7-bit coded character set for information interchange.

ISO/IEC 3166:1993. Codes for the representation of names and countries.

ISO/IEC 6523:1994. Data interchange — Structures for the identification of organizations (Registration of International Code Designators).

ISO/IEC 7498-1:1994. Information technology — Open Systems Interconnection — Basic Reference Model. Reference: ITU-T Rec. X.200 (1994)

ISO/IEC 7498-2:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture.

ISO/IEC 7498-3:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 3: Naming and Addressing. Reference: ITU-T Rec. X.650 (1992).

ISO/IEC 7498-4:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework.

ISO/IEC 8072:1994. Information technology — Open Systems Interconnection — Transport service definition (second edition). Reference: ITU-T Rec. X.214 (1993).

ISO/IEC 8073:1992. Information technology — Telecommunications and information exchange between systems — Open Systems Interconnection — Protocol for providing the connection-mode transport service.

ISO/IEC 8073/PDAM5:1992. Information technology — Telecommunications and information exchange between systems — Open Systems Interconnection — Protocol for providing the connection-mode transport service — Amendment 5: Provision of Non-blocking Expedited Service.

ISO/IEC 8208:1995. Information technology — Data communications — X.25 Packet Layer Protocol for Data Terminal Equipment (Revision of ISO/IEC 8208:1990).

ISO/IEC 8326:1994. Information technology — Open Systems Interconnection — Basic Session Service Definition (second edition). Reference: ITU-T Rec. X.215 (1994).

ISO/IEC 8326:1994/Amd. 1:1997. Information Technology — Open Systems Interconnection — Basic Session Service Definition — Amendment 1: efficiency enhancements.

ISO/IEC 8327-1:1994. Information Technology — Open Systems Interconnection — Basic Connection Oriented Session Protocol: Part 1 — Protocol Specification (second edition). Reference: ITU-T Rec. X.225 (1994).

ISO/IEC 8327-1:1995/Amd. 1:1997. Information Technology — Open Systems Interconnection — Basic Connection Oriented Session Protocol: Part 1 — Protocol Specification — Amendment 1: efficiency enhancements.

ISO/IEC 8327-2:1994. Information technology — Open Systems Interconnection — Basic connection oriented session protocol specification — Part 2: Protocol Implementation Conformance Statement (PICS) Proforma.

ISO/IEC 8348:1993. Information technology — Open Systems Interconnection — Network Service Definition.

ISO/IEC 8473-1:1994. Information technology — Protocol for providing the connectionless-mode network service: Protocol specification.

ISO/IEC 8473-2:1994. Information technology — Protocol for providing the connectionless-mode network service — Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork.

ISO/IEC 8473-3:1995. Information technology — Protocol for providing the connectionless-mode network service — Part 3: Provision of the underlying service by an X.25 subnetwork.

ISO/IEC 8473-4:1995. Information technology — Protocol for providing the connectionless-mode network service — Part 4: Provision of the underlying service by a subnetwork that provides the OSI data link service.

ISO/IEC TR 8509:1987. Information processing systems — Open Systems Interconnection — OSI Service Conventions.

ISO/IEC 8602:1995. Information technology — Protocol for providing the OSI connectionless-mode transport service.

ISO/IEC 8648:1988. Information processing systems — Open Systems Interconnection — Internal organization of the Network Layer.

ISO/IEC 8649:1996. Information processing systems — Open Systems Interconnection — Service definition for the Association Control Service Element (second edition). Reference: ITU-T Rec. X.217 (1992).

ISO/IEC 8649:1996/ Amd. 1:1997. Information technology — Open Systems Interconnection — Service definition for the Association Control Service Element — Amendment 1: Support of authentication mechanisms for the connectionless mode.

ISO/IEC 8650-1:1996. Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element (second edition). Reference: ITU-T Rec. X.227 (1994).

ISO/IEC 8650-1/Amd. 1:1997 Information processing systems — Open Systems Interconnection — Protocol specification for the Association Control Service Element — Amendment 1: Incorporation of extensibility markers.

ISO/IEC 8650-2:1997. Information technology — Open Systems Interconnection — Protocol specification for the Association Control Service Element — Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

ISO/IEC 8802-3:1990. Carrier Sense Multiple Access with Collision Detect Access method and Physical Layer Specifications.

ISO/IEC 8822:1994. Information technology — Open Systems Interconnection — Presentation service definition (Second edition). Reference: ITU-T Rec. X.216 (1994).

ISO/IEC 8822:1994/Amd. 1:1997. Information technology — Open Systems Interconnection — Presentation service definition — Amendment 1: efficiency enhancements.

ISO/IEC 8823-1:1994. Information technology — Open Systems Interconnection — Basic connection-oriented

presentation protocol — Part 1: Protocol specification (second edition). Reference: ITU-T Rec. X.226 (1994).

ISO/IEC 8823-1:1994/Amd. 1:1997. Information technology — Open Systems Interconnection — Basic connection-oriented presentation protocol — Part 1: Protocol specification — Amendment 1: Efficiency enhancements.

ISO/IEC 8823-2:1995. Information technology — Open Systems Interconnection — Basic connection-oriented presentation protocol — Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

ISO/IEC 8824-1:1994. Information Technology — OSI Abstract Syntax Notation One (ASN.1). — Specification of basic notation. Reference: ITU-T Rec. X.682 (1994).

ISO/IEC 8824-1/Amd.1:1995. Information Technology — Open Systems Interconnection — Abstract Syntax Notation One (ASN.1) — Specification of Basic Notation — Amendment 1: Rules for Extensibility.

ISO/IEC 8824-2:1995. Information technology Open Systems Interconnection Abstract Syntax Notation One (ASN.1) Part 2: Information object specification.

ISO/IEC 8824-3:1995. Information technology Open Systems Interconnection Abstract Syntax Notation One (ASN. 1) Part 3: Constraint specification.

ISO/IEC 8824-4:1995. Information technology Open Systems Interconnection Abstract Syntax Notation One (ASN. 1) Part 4: Parameterization of ASN.1 Specifications.

ISO/IEC 8825-1:1995. Information technology — ASN.1 encoding rules — Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Reference: ITU-T Rec. X.691 (1993).

ISO/IEC 8825-2:1996. Information technology — Open Systems Interconnection — Encoding Rules for Abstract Syntax Notation One (ASN.1) — Part 2: Packed encoding rules. Reference: ITU-T Rec. X.691 (1995).

ISO/IEC 8859-1:1987. Information processing — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1.

ISO/IEC 8878:1992. Information technology — Telecommunications and information exchange between systems — Use of X.25 to provide the OSI Connection-mode Network Service.

ISO/IEC 9072-1 : 1989\|CCITT Recommendation X.219 (1988). Information processing systems – Text communication – Remote operations – Part 1. Model, notation and service definition

ISO/IEC 9072-2 : 1989\|CCITT Recommendation X.229 (1988). Information processing systems – Text communication – Remote operations – Part 2. Protocol specification

ISO/IEC 9542:1988. Information processing systems — Telecommunications and information exchange between systems — End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO/IEC 8473).

ISO/IEC 9542/DAM1:1988. Information processing systems — Telecommunications and information exchange

between systems — End system to Intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO/IEC 8473) — Amendment 1: Dynamic Discovery of OSI NSAP Addresses by End Systems.

ISO/IEC 9545:1994. Information technology — Open Systems Interconnection — Application Layer structure (second edition).

ISO/IEC 9548-1:1993. Information Technology — Open Systems Interconnection — Connectionless Session Protocol Specification Part 1.

ISO/IEC 9548-2:1995. Information technology — Open Systems Interconnection — Connectionless session protocol specification — Part 2: Protocol implementation conformance statement (PICS) proforma.

ISO/IEC TR 9575:1995. Information technology — Telecommunications and information exchange between systems — OSI Routing Framework.

ISO/IEC 9576-1:1995. Information technology — Open Systems Interconnection — Connectionless presentation protocol specification.

ISO/IEC 9576-1:1996/Amd.1:1998. Information Technology - Open Systems Interconnection - Connectionless Presentation Protocol : Protocol Specification Amendment 1 : Efficiency Enhancements.

ISO/IEC 9576-2:1995. Information technology — Open Systems Interconnection — Connectionless presentation protocol specification — Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

ISO/IEC TR 9577:1993. Information technology — Telecommunications and information exchange between systems — Protocol identification in the network layer.

ISO/IEC 9594:1993 | ITU-T Rec. X.500 (1993). Information Technology - Open Systems Interconnection -The Directory: Overview of Concepts, Models and Services.

ISO/IEC 9594-2:1993 | ITU-T Rec. X.501 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Models.

Technical Corrigendum 1 to Rec. X.501 (1993) | ISO/IEC 9594-2:(1995) (addressing DRs 9594/088, 089, 090, 091, 102, 125)

Draft Technical Corrigendum 2 to Rec.X.501 (1993) | ISO/IEC 9594-2:(1995) (addressing DRs 9594/134,136)

ISO/IEC 9594-3:1993 | ITU-T Rec. X.511 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Abstract Service Definition.

Technical Corrigendum 1 to Rec. X.511 (1993) | ISO/IEC 9594-3:(1995) (addressing DR 9594/085)

Draft Technical Corrigendum 2 to Rec. X.511 (1993)| ISO/IEC 9594-3:(1995) (addressing Defect Reports 9594/119,133)

ISO/IEC 9594-4:1993 | ITU-T Rec. X.518 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Procedures for Distributed Operations.

Technical Corrigendum 1 to Recommendation X.518 (1993) | ISO/IEC 9594-4:(1995) (addressing DRs 9594/094, 106, 108, 109, 111, 112, 113, 114, 115)

Draft Technical Corrigendum 2 to Recommendation X.518 (1993) | ISO/IEC 9594-4:(1995) (addressing DRs 9594/116, 117, 118, 119, 120, 121, 130)

ISO/IEC 9594-5:1993 | ITU-T Rec. X.519 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Protocol Specifications.

Technical Corrigendum 1 to Recommendation X.519 (1993) | ISO/IEC 9594-5:(1995) (addressing DRs 9594/075, 124)

ISO/IEC 9594-6:1993 | ITU-T Rec. X.520 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Selected Attribute Types.

Technical Corrigendum 1 to Recommendation X.520 (1993) | ISO/IEC 9594-6:(1995) (addressing DRs 9594/076, 122, 127)

ISO/IEC 9594-7:1993 | ITU-T Rec. X.521 (1993). Information Technology -- Open Systems Interconnection -- The Directory: Selected Object Classes.

ISO/IEC 9594-8:1997 | ITU-T Rec. X.509 (1997). Information Technology -- Open Systems Interconnection -- The Directory: Authentication Framework.

ISO/IEC 9595:1991. Information technology — Open Systems Interconnection — Common management information service definition.

ISO/IEC 9596-1:1991. Information technology — Open Systems Interconnection — Common management information protocol — Part 1: Specification.

ISO/IEC 9596-2:1993. Information technology — Open Systems Interconnection — Common management information protocol — Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

ISO/IEC 9646-1:1994. Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 1: General concepts.

ISO/IEC 9646-2:1994. Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 2: Abstract Test Suite specification.

ISO/IEC 9646-4:1994. Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 4: Test realization.

ISO/IEC 9646-5:1994. Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 5: Requirements on test laboratories and clients for the conformance assessment process.

ISO/IEC 9646-7:1995. Information technology — Open Systems Interconnection — Conformance testing methodology and framework — Part 7: Implementation Conformance Statements.

ISO/IEC 9834-1:1993. Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities — Part 1: General procedures.

ISO/IEC 9834-2:1993. Information Technology Open Systems Interconnection Procedures for specific OSI Registration Authorities — Part 2: Registration Procedures for OSI Document Types.

ISO/IEC 9834-6:1993. Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities — Part 6: Application processes and application entities.

ISO/IEC TR 10000-1:1995. Information technology — Framework and taxonomy of International Standardized Profiles — Part 1: General principles and documentation framework.

ISO/IEC TR 10000-2:1995. Information technology — Framework and taxonomy of International Standardized Profiles — Part 2: Principles and Taxonomy for OSI profiles.

ISO/IEC 10021-1:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 1: System and Service Overview.

ISO/IEC 10021-1/Amd.2:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 1: System and Service Overview.

ISO/IEC 10021-1:1999. Information Technology — Message Handling Systems (MHS) — Part 1: System and Service Overview.

ISO/IEC 10021-2:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture.

ISO/IEC 10021-2/Amd.1:1993. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture.

ISO/IEC 10021-2/Amd.2:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 2: Overall Architecture.

ISO/IEC 10021-2:1999. Information Technology — Message Handling Systems (MHS) — Part 2: Overall Architecture.

ISO/IEC 10021-3:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 3: Abstract Service Definition Conventions.

ISO/IEC 10021-4:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures.

ISO/IEC 10021-4/Amd. 1:1994. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures.

ISO/IEC 10021-4:1999. Information Technology — Message Handling Systems (MHS) — Part 4: Message Transfer System: Abstract Service Definition and Procedures.

ISO/IEC 10021-5:1990. Information Technology — Text Communication — Message-Oriented Text Interchange

System (MOTIS) — Part 5: Message Store: Abstract Service Definition.

ISO/IEC 10021-5/Amd. 1:Date. Message Store Extensions and Message Store Logs.

ISO/IEC 10021-5:1999. Information Technology — Message Handling Systems (MHS) — Part 5: Message Store: Abstract Service Definition.

ISO/IEC 10021-6:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 6: Protocol Specifications.

ISO/IEC 10021-6:1999. Information Technology — Message Handling Systems (MHS) — Part 6: Protocol Specifications.

ISO/IEC 10021-7:1990. Information Technology — Text Communication — Message-Oriented Text Interchange System (MOTIS) — Part 7: Interpersonal Messaging System.

ISO/IEC 10021-7:1999. Information Technology — Message Handling Systems (MHS) — Part 7: Interpersonal Messaging System.

ISO/IEC 10028:1993. Information technology — Telecommunications and information exchange between systems — Definition of the relaying functions of a Network layer intermediate system.

ISO/IEC 10035-1:1995. Information Technology Open Systems Interconnection Connectionless ACSE Protocol to Provide the Connectionless Mode ACSE Service.

ISO/IEC 10035-1:1995/Amd.1:1997. Information Technology - Open Systems Interconnection - Connectionless Protocol for the Association Control Service Element : Protocol Specification Amendment 1 : Incorporation of Extensibility Markers and Authentication Parameters.

ISO/IEC 10035-2:1995. Information technology — Open Systems Interconnection — Connectionless ACSE protocol to provide the Connectionless-Mode ACSE service — Part 2: Protocol implementation conformance statement (PICS) proforma.

ISO/IEC 10040 : 1992|CCITT Recommendation X.701 (1992). Information technology – Open Systems Interconnection – Systems management overview

ISO/IEC 10164-4 : 1992|CCITT Recommendation X.733 (1992). Information technology – Open Systems Interconnection – Systems management: Alarm reporting function

ISO/IEC 10164-5 : 1993|CCITT Recommendation X.734 (1992). Information technology – Open Systems Interconnection – Systems management: Event report management function

ISO/IEC 10164-6 : 1993|CCITT Recommendation X.735 (1992). Information technology – Open Systems Interconnection – Systems management: Log control function

ISO/IEC 10164-7 : 1992|CCITT Recommendation X.736 (1992). Information technology – Open Systems Interconnection – Systems management: Security alarm reporting function

ISO/IEC 10165-1 : 1992|CCITT Recommendation X.720 (1992). Information technology – Open Systems Interconnection – Structure of management information: Management information model

ISO/IEC 10165-2 : 1992|CCITT Recommendation X.721 (1992). Information technology – Open Systems Interconnection – Structure of management information: Definition of management information

ISO/IEC 10165-4 : 1992|CCITT Recommendation X.722 (1992). Information technology – Open Systems Interconnection – Structure of management information: Guidelines for the definition of managed objects

ISO/IEC 10165-5 : 1994|CCITT Recommendation X.723 (1993). Information technology – Open Systems Interconnection – Structure of management information: Generic management information

ISO/IEC 10165-6 : 1997|CCITT Recommendation X.724 (1996). Information technology – Open Systems Interconnection – Structure of management information: Requirements and guidelines for implementation conformance statement proformas associated with OSI management

ISO/IEC 10169-1:1991. Information technology — Open Systems Interconnection — Conformance test suite for the ACSE protocol — Part 1: Test suite structure and test purposes.

ISO/IEC 10181-1:1996. Information Technology - Security Frameworks in Open Systems - Frameworks Overview.

ISO/IEC 10181-2:1996. Information Technology - Security Frameworks in Open Systems - Authentication Framework.

ISO/IEC 10181-3:1996. Information Technology - Security Frameworks in Open Systems - Access Control Framework.

ISO/IEC 10181-6:1996. Information Technology - Security Frameworks in Open Systems - Integrity Framework.

ISO/IEC 10589:1992. Information technology — Telecommunications and information exchange between systems — Intermediate system to intermediate system intra-domain-routing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO/IEC 8473).

ISO/IEC ISP 10611-1:1994. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 1: MHS Service Support.

ISO/IEC ISP 10611-2:1994. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by MHS.

ISO/IEC ISP 10611-3:1994. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 3: AMH11-Message Transfer (P1).

ISO/IEC ISP 10611-4:1994. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 4: AMH12-MTS Access (P3).

ISO/IEC ISP 10611-4:1999. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 4: AMH12 and AMH14 - MTS Access (P3) and MTS 94 Access (P3). (Edition 3)

ISO/IEC ISP 10611-5:1994. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 5: AMH13-MS Access (P7).

ISO/IEC ISP 10611-5:1999. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 5: AMH13-MS Access (P7). (Edition 3)

ISO/IEC ISP 10611-6:1999. Information technology — International Standardized Profiles AMH1n — Message Handling Systems — Common Messaging — Part 6: AMH15-MS 94 Access (P7). (Edition 2)

ISO/IEC TR 10730:1993. Information technology — Open systems Interconnection Tutorial on naming and addressing.

ISO/IEC 10731:1994. Information technology — Open Systems Interconnection — Conventions for the definition of OSI services. Reference: ITU-T Rec. X.210 (1993).

ISO/IEC 10747:1994. Information technology — Telecommunications and information exchange between systems — Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO/IEC 8473 PDUs.

ISO/IEC ISP 11183-1:1992. Information technology — International Standardized Profiles AOM1n OSI Management — Management Communications — Part 1: Specification of ACSE, presentation and session protocols for the use by ROSE and CMISE.

ISO/IEC ISP 11183-2:1992. Information technology — International Standardized Profiles AOM1n OSI Management — Management Communications — Part 2: CMISE/ROSE for AOM12 — Enhanced Management Communications.

ISO/IEC ISP 11183-3:1992. Information technology — International Standardized Profiles AOM1n OSI Management — Management Communications — Part 3: CMISE/ROSE for AOM11 — Basic Management Communications.

ISO/IEC ISP 11188-1:1995. Information Technology — International Standardized Profile — Common upper layer requirements — Part 1: Basic connection oriented requirements.

ISO/IEC ISP 11189. Information Technology – International Standardized Profiles – FDI2 – MHS use of the Directory.

ISO/IEC 11588-8:1997. Information technology - Message handling systems (MHS) management: Message Transfer Agent management

ISO/IEC 11570:1992. Information technology — Telecommunications and information exchange between systems — Open Systems Interconnection — Transport protocol identification mechanism.

ISO/IEC ISP 12060-1:1995. Information technology - International standardised profiles - OSI management - Management functions - Part 1: AOM211 - General management capability

ISO/IEC ISP 12060-4:1995. Information technology - International standardised profiles - OSI management - Management functions - Part 4: AOM221 - General event report management

ISO/IEC ISP 12060-5:1995. Information technology - International standardised profiles - OSI management - Management functions - Part 5: AOM231 - General log control

ISO/IEC DISP 12060-9:1997. Information technology – International standardised profiles - OSI management – Management functions – Part 9: AOM2432n – Access control

ISO/IEC ISP 12062-1:1995. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 1: IPM MHS Service Support.

ISO/IEC ISP 12062-1:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 1: IPM MHS Service Support. (Edition 3)

ISO/IEC ISP 12062-2:1995. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 2: AMH21 — IPM Content.

ISO/IEC ISP 12062-2:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 2: AMH21 — IPM Content. (Edition 3)

ISO/IEC ISP 12062-3:1995. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 3: AMH22 — IPM Requirements for Message Transfer (P1).

ISO/IEC ISP 12062-3:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 3: AMH22 — IPM Requirements for Message Transfer (P1). (Edition 3)

ISO/IEC ISP 12062-4:1995. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 4: AMH23 — IPM Requirements for MTS Access (P3).

ISO/IEC ISP 12062-4:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 4: AMH23 and AMH25 — IPM Requirements for MTS Access (P3) and MTS 94 Access (P3). (Edition 3)

ISO/IEC ISP 12062-5:1995. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 5: AMH24 — IPM Requirements for Enhanced MS Access (P7).

ISO/IEC ISP 12062-5:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 5: AMH24 — IPM Requirements for Enhanced MS Access (P7). (Edition 3)

ISO/IEC ISP 12062-6:1999. Information technology — International Standardized Profiles AMH2n — Message Handling Systems — Interpersonal Messaging — Part 5: AMH26 — IPM Requirements for Enhanced MS 94 Access (P7). (Edition 2)

ISO/IEC ISP 15125-1. Information Technology - International Standardized Profiles – ADY11 – DUA Support of Directory Access Protocol.

ISO/IEC ISP 15125-2. Information Technology - International Standardized Profiles – ADY12 – DUA Support of Distributed Operations.

ISO/IEC ISP 15125-3. Information Technology - International Standardized Profiles – ADY21 – DSA Support of Directory Access Protocol.

ISO/IEC ISP 15125-4. Information Technology - International Standardized Profiles – ADY22 – DSA Support of Distributed Operations.

ISO/IEC ISP 15125-5. Information Technology - International Standardized Profiles – ADY41 – DUA Authentication as DAP Initiator.

ISO/IEC ISP 15125-6. Information Technology - International Standardized Profiles – ADY42 – DSA Authentication as DAP Responder.

ISO/IEC ISP 15125-7. Information Technology - International Standardized Profiles – ADY43 – DSA to DSA Authentication.

ISO/IEC ISP 15126-1. Information Technology - International Standardized Profiles – FDY11 – Common Directory Use.

ISO/IEC ISP 15126-2. Information Technology - International Standardized Profiles – FDY12 – Directory System Schema.

ISO/IEC 15946-2:1999. Cryptographic techniques based on elliptic curves – Part 1: General, Draft.

ISO/IEC 15946-2:1999. Cryptographic techniques based on elliptic curves – Part 2: Signatures, Draft.

ISO/IEC 15946-3:1999. Cryptographic techniques based on elliptic curves – Part 2: Key establishment, Draft

ITU-T Rec X.25 (1996). Interface between DTE and DCE terminals Operating in Packet Mode.

ITU-T Rec. X.215 Addendum 1 (1995). Information processing systems — Open Systems Interconnection — Service Definition for Session Layer Efficiency Enhancements.

ITU-T Rec. X.216 Addendum 1 (1995). Information processing systems — Open Systems Interconnection — Service Definition for Presentation Layer Efficiency Enhancements.

ITU-T Rec. X.225 Addendum 1 (1995). Information processing systems — Open Systems Interconnection — Protocol Specification for Session Layer Efficiency Enhancements.

ITU-T Rec. X.226 Addendum 1 (1995). Information processing systems — Open Systems Interconnection — Protocol Specification for Presentation Layer Efficiency Enhancements.

ITU-T Recommendation X.500 (1993)|ISO/IEC 9594: 1993. Information Technology - Open Systems Interconnection -The Directory: Overview of Concepts, Models and Services.

ITU-T Recommendation X.509 (1997)|ISO/IEC 9594-8: 1997. Information Technology - Open Systems Interconnection -The Directory: Authentication framework.

ITU-T Rec X.666 (1995). Procedures for registration of international and multinational organization names.

ITU-T Rec. X.680 (1994)|ISO/IEC 8824-1:(1994). Information Technology -- Open Systems Interconnection -- Abstract Syntax Notation One (ASN.1): Specification of basic notation

ITU-T Rec. X.681 (1994)|ISO/IEC 8824-2:(1994). Information Technology -- Open Systems Interconnection -- Abstract Syntax Notation One (ASN.1): Information object specification

ITU-T Rec. X.682 (1994)|ISO/IEC 8824-3:(1994). Information Technology -- Open Systems Interconnection -- Abstract Syntax Notation One (ASN.1):Constraint specification

ITU-T Rec. X.683 (1994)|ISO/IEC 8824-4:(1994). Information Technology -- Open Systems Interconnection -- Abstract Syntax Notation One (ASN.1):Parameterization of ASN.1 specifications

ITU-T Rec. X.690 (1994) | ISO/IEC 8825-1:(1994). Information Technology -- Open Systems Interconnection -- Specification of ASN.1 encoding rules: Basic, Canonical and Distinguished Encoding Rules

ITU-T Recommendation X.803 (1994)|ISO/IEC 10745:1995. *Information technology – Open Systems Interconnection – Upper layers security model*.

ITU-T Recommendation X.830 (1995)|ISO/IEC 11586-1: 1996, Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Overview, Models and Notation.

ITU-T Recommendation X.831 (1995)|ISO/IEC 11586-2:1996. Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element(SESE) service definition

ITU-T Recommendation X.832 (1995)|ISO/IEC 11586-3:1996. Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) protocol specification

ITU-T Recommendation X.834 (1996)|ISO/IEC 11586-5:1997. Information technology – Open systems interconnection – Generic upper layers security: Security exchange service element (SESE) protocol implementation conformance statement (PICS) proforma

ITU-T Rec. X.880 (1994)|ISO/IEC 13712-1:(1994). Information Technology -- Open Systems Interconnection -- Remote Operations: Concepts models and notation

ITU-T Rec. X.881 (1994)|ISO/IEC 13712-2:(1994). Information Technology -- Open Systems Interconnection -- OSI Realizations – Remote Operations Service Element (ROSE) service definition

ITU-T Rec. X.882 (1994)|ISO/IEC 13712-3:(1994). Information Technology -- Open Systems Interconnection -- OSI Realizations – Remote Operations Service Element (ROSE) protocol specification

National Institute of Standards and Technology (U.S.), 1999. Recommended elliptic curves for federal government use

Standards for Efficient Cryptography Group, 1999. SEC1, Elliptic curve cryptography

1.2 GENERAL

1.2.1 The aeronautical telecommunication network (ATN) shall provide data communication services and application entities in support of:

a) the delivery of air traffic services (ATS) to aircraft;

b) the exchange of ATS information between ATS units; and

c) other applications such as aeronautical operational control (AOC) and aeronautical administrative communication (AAC).

Note 1.— The conceptual model of the ATN is as shown in Figure 1.2.

Note 2.—Provisions have been made to accommodate the exchange of information between aircraft operator ground based systems and ATS units, such as weather, flight plans, notices to airmen and dynamic real time air traffic flow management.

Note 3.—Provisions have also been made to accommodate aeronautical passenger communication (APC).

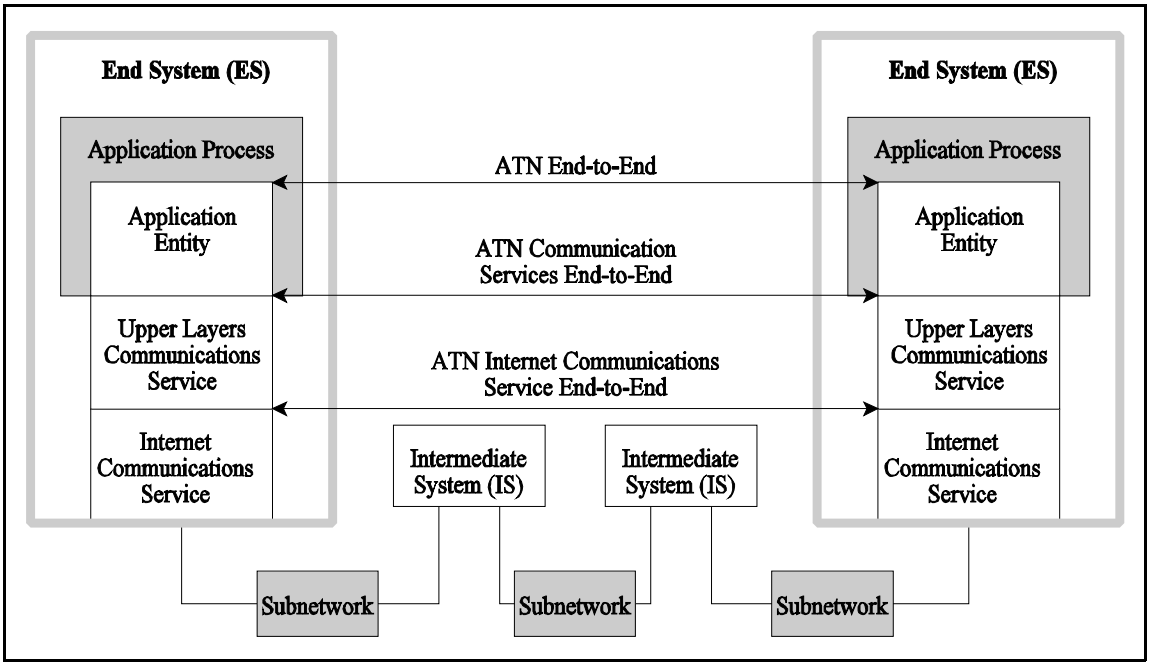
1.2.2 When the aeronautical telecommunication network is used in support of air traffic services, it shall conform with the provisions of this document.

1.2.2.1 Conformance to this edition of this document shall include support for the technical provisions for ATN Security Services and ATN Systems Management.

Note.— When the provisions for ATN Security Services and for ATN Systems Management services are herein qualified by such statements as "when ATN security services are supported" this is intended to accommodate implementations conformant to prior editions of this document. Implementations claiming conformance to this edition of this document are expected to support these enhanced capabilities.

1.2.3 Requirements for use of the ATN shall be made on the basis of regional air navigation agreements.

1.2.4 **Recommendation.—** *Civil aviation authorities should co-ordinate, with national authorities and aeronautical industry, those implementation aspects of the ATN which will permit its world-wide safety, interoperability and efficient use, as appropriate.*



Note 1.— Shading indicates elements outside the scope of these SARPs. User requirements define the interface between the application entity and the user and ensure the functionality and interoperability of the ATN.

Note 2.— The figure represents a simplified model of the ATN and does not depict all of its capabilities (e.g. the store and forward capability which is provided for ATS message handling service).

Note 3.— Various end-to-end points have been defined within the ATN to specify certain end-to-end performance requirements. It may be necessary, however, to define different end-to-end points to facilitate the qualification of implementations to those performance requirements. In such cases, the end-to-end points should be clearly defined and correlated with the end-to-end points shown in the figure.

Note 4. — An IS is a conceptual representation of functionality and does not correspond precisely to a router. A router which implements the System Management Application requires the protocols of an end-system and when using the System Management application is also acting as an end-system.

Figure 1.2 Conceptual model of the ATN

1.3 SYSTEM LEVEL REQUIREMENTS

Note.—The system level requirements are high-level technical requirements that have been derived from operational requirements, technological constraints and regulatory constraints (administrative and institutional). These system level requirements are the basis for the functional requirements and lower-level requirements.

1.3.1 The ATN shall use International Organization for Standardization (ISO) communication standards for open systems interconnection (OSI).

1.3.2 The ATN shall provide a means to facilitate migration to future versions of application entities and/or the communication services.

Note.—It is an objective that the evolution towards future versions facilitates the backward compatibility with previous versions.

1.3.3 The ATN shall enable the transition of existing AFTN/CIDIN users and systems into the ATN architecture.

1.3.4 The ATN shall make provisions whereby only the controlling ATS unit may provide ATC instructions to aircraft operating in its airspace.

Note.—This is achieved through the current and next data authority aspects of the controller-pilot data link communications (CPDLC) application entity.

1.3.5 The ATN shall accommodate routing based on a pre-defined routing policy.

1.3.6 The ATN shall provide means to define data communications that can be carried only over authorized paths for the traffic type and category specified by the user.

1.3.7 The ATN shall offer ATSC classes in accordance with the criteria in Table 1-1.

Table 1-1 Transit Delays for ATSC Classes

Maximum one-way ATN end-to-end transit delay at 95% probability (seconds)	*ATSC Class*
Reserved	A
4.5	B
7.2	C
13.5	D
18	E
27	F
50	G
100	H
No value specified	no preference
Note 1.— The value for the ATN end-to-end transit delay represents approximately 90% of the value for the total end-to-end transit delay between the ultimate users of the system. *Note 2.— The 95% probability is based on the availability of a route conforming to the requested ATSC class.*	

Note 1.— When an ATSC class is specified by an ATN application, packets will be forwarded in the ATN internet communications service on a best effort basis. Best effort basis means that when a route is available of the requested ATSC class, the packet is forwarded on that route. When no such route is available, the packet will be forwarded on the first known route of the ATSC class higher than that requested, or if there is no such route, first known route of the ATSC class lower than that requested.

Note 2.— The ATN communications service will not inform application entities if the requested ATSC class was not achieved. It is the responsibility of the application entity to determine the actual transit delay achieved by local means such as time stamping.

1.3.8 The ATN shall operate in accordance with the communication priorities defined in Table 1-2 and Table 1-3.

Table 1-2. Mapping of ATN communication priorities

Message categories	*ATN application*	*Corresponding protocol priority*	
		Transport layer priority	*Network layer priority*
Network/systems management	SM	0	14
Distress communications		1	13
Urgent communications		2	12
High-priority flight safety messages	CPDLC, ADS	3	11
Normal-priority flight safety messages	ATIS, AIDC	4	10
Meteorological communications	METAR	5	9
Flight regularity communications	CM, ATSMHS	6	8
Aeronautical information service messages	METAR, ATIS	7	7
Network/systems administration	SM, DIR	8	6
Aeronautical administrative messages		9	5
<unassigned>		10	4
Urgent-priority administrative and U.N. Charter communications		11	3
High-priority administrative and State/Government communications		12	2
Normal-priority administrative communications		13	1
Low-priority administrative communications and APC		14	0
Note.— The network layer priorities shown in the table apply only to connectionless network priority and do not apply to subnetwork priority.			

Table 1-3. Mapping of ATN network priority to mobile subnetwork priority

Message categories	*ATN network layer priority*	*Corresponding mobile subnetwork priority (see Note 5)*			
		AMSS-1 (see Note 4)	*VDL Mode 2*	*SSR Mode S*	*HFDL*
Network/systems management	14	14	see Note 1	high	14
Distress communications	13	14	see Note 1	high	14
Urgent communications	12	14	see Note 1	high	14
High-priority flight safety messages	11	11	see Note 1	high	11
Normal-priority flight safety messages	10	11	see Note 1	high	11
Meteorological communications	9	8	see Note 1	low	8
Flight regularity communications	8	7	see Note 1	low	7
Aeronautical information service messages	7	6	see Note 1	low	6
Network/systems administration	6	5	see Note 1	low	5
Aeronautical administrative messages	5	4	not allowed	not allowed	not allowed
<unassigned>	4	not assigned	not allowed	not allowed	not allowed
Urgent-priority administrative and U.N. Charter communications	3	3	not allowed	not allowed	not allowed
High-priority administrative and State/Government communications	2	2	not allowed	not allowed	not allowed
Normal-priority administrative communications	1	1	not allowed	not allowed	not allowed
Low-priority administrative communications & Aeronautical Passenger Communications	0	0	not allowed	not allowed	not allowed

Note 1.— VDL Mode 2 has no specific subnetwork priority mechanisms.

Note 2.— The AMSS SARPs specify mapping of message categories to subnetwork priority without explicitly referencing ATN network layer priority.

Note 3.— The term "not allowed" means that only communications related to safety and regularity of flight are authorized to pass over this subnetwork as defined in the subnetwork SARPs.

Note 4. — The term AMSS-1 refers to the first generation Aeronautical Mobile Satellite Service.

Note 5. — Only those mobile subnetworks are listed for which subnetwork SARPs exist and for which explicit support is provided by the ATN Boundary Intermediate System technical provisions.

1.3.9 The ATN shall enable exchange of application information when one or more authorized paths exist.

1.3.10 The ATN shall notify the appropriate application processes when no authorized path exists.

1.3.11 The ATN shall provide means to unambiguously address all ATN end and intermediate systems.

1.3.12 The ATN shall enable the recipient of a message to identify the originator of that message.

1.3.13 The ATN addressing and naming plans shall allow States and organizations to assign addresses and names within their own administrative domains.

1.3.14 The ATN shall support data communications to fixed and mobile systems.

1.3.15 The ATN shall accommodate ATN mobile subnetworks as defined in this Annex.

1.3.16 The ATN shall make provisions for the efficient use of limited bandwidth subnetworks.

1.3.17 The ATN shall enable an aircraft intermediate system to be connected to a ground intermediate system via concurrent mobile subnetworks.

1.3.18 The ATN shall enable an aircraft intermediate system to be connected to multiple ground intermediate systems.

1.3.19 The ATN shall enable the exchange of address information between application entities.

1.3.20 The ATN shall support the context management (CM) application when any of the other air-ground applications are supported.

1.3.21 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the context management (CM) application.

1.3.22 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the automatic dependent surveillance (ADS) application.

1.3.23 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the controller-pilot data link communications (CPDLC) application.

1.3.24 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the automatic terminal information service (ATIS) application.

1.3.25 The ATN shall be capable of establishing, maintaining, releasing and aborting application associations for the ATS message handling services (ATSMHS) application.

1.3.26 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the ATS interfacility data communication (AIDC) application.

1.3.27 Where the absolute time of day is used within the ATN, it shall be accurate to within 1 second of coordinated universal time (UTC).

Note.—A time accuracy value may result in synchronization errors of up to 2 times the stated accuracy value.

1.3.28 The end system shall make provisions to ensure that the probability of not detecting a 255-octet

message being mis-delivered, non-delivered or corrupted by the internet communication service is less than or equal to 10^{-8} per message.

Note.— It is assumed that ATN subnetworks will ensure data integrity consistent with this system level requirement.

1.3.29 ATN end systems supporting ATN security services shall be capable of authenticating the identity of peer end systems, authenticating the source of application messages and ensuring the data integrity of the application messages.

Note.— Application messages in this context include messages related to ATS, systems management and directory services.

1.3.30 ATN ground and air-ground boundary intermediate systems supporting ATN security services shall be capable of authenticating the identity of peer boundary intermediate systems,authenticating the source of routing information and ensuring the data integrity of routing information.

1.3.31 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the exchange of directory information.

1.3.32 ATN systems supporting ATN systems management shall facilitate enhanced continuity of ATN operations, including the monitoring and maintenance of the quality of the communications service.

1.3.33 The ATN shall be capable of establishing, maintaining, releasing, and aborting peer to peer application associations for the Systems Management (SM) application.

1.3.34 The ATN shall be capable of establishing, maintaining, releasing and aborting peer-to-peer application associations for the aviation routine weather report service (METAR) application.

APPENDIX A - Change Control

A1. A change control process is used for tracking the editions of the ATN technical provisions, the version of the ATN specific protocols and the version of ATN applications.

Note. — This document is maintained under edition control. An edition of this document indicates the collection of technical provisions as of a specific publication date. The ATN technical provisions define a version number for ATN specific protocols and ATN applications. A version number is changed only if the ATN protocol/application will not interoperate with the prior version of the protocol/application. Later versions always subsume earlier versions The history of the document editions and the related protocol/application versions is indicated in the Table A-1.

Table A-1. Document edition and protocol/application version tracking

ATN Element	**Protocol/Application Version History**	**Doc 9705 Edition History**
CM	Version 1 – CM Version 2 – CM Server, security	Edition 1&2 Edition 3
ADS	Version 1 – ADS Version 2 – ADS Emergency status, Security	Edition 1&2 Edition 3
ARF	Version 1– ARF Version 2 – ADS Emergency status, Security	Edition 1&2 Edition 3
CPDLC	Version 1 – CPDLC Version 2 – Security	Edition 1&2 Edition 3
FIS	Version 1 – ATIS Version 2 – METAR, security	Edition 1&2 Edition 3
ATSMHS	– Basic ATSMHS – Extended ATSMHS, security	Edition 1&2 Edition 3
ICC	– AIDC	Edition 1&2&3
Upper Layers	– ULCS – Security	Edition 1&2 Edition 3
Mobile SNDCF	Version 1 – SNDCF Version 2 – SNDCF negotiation extension	Edition 1&2 Edition 3
Router to Router	– IDRP – IDRP Security	Edition 1&2 Edition 3
Router to End System	– ES-IS	Edition 1&2&3
Internetworking	– CLNP	Edition 1&2&3
Transport	– COTS/CLTS	Edition 1&2&3
Systems Management	– CMIP	Edition 3
Directory	– DSP	Edition 3