



ICAO

Doc 9896

Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocol

Second Edition, 2015



Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION **Documents**
AVA Document Sharing Hub



| ICAO

Doc 9896

Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocol

Second Edition, 2015

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION **Documents**
AVA Document Sharing Hub

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

**Doc 9896, *Manual on the Aeronautical Telecommunication Network (ATN)
using Internet Protocol Suite (IPS) Standards and Protocols***

ISBN 978-92-9249-876-4

© ICAO 2015

All rights reserved. No part of this publication may be reproduced, stored in a
retrieval system or transmitted in any form or by any means, without prior
permission in writing from the International Civil Aviation Organization.

AMENDMENTS

Amendments are announced in the supplements to the *Products and Services Catalogue*; the Catalogue and its supplements are available on the ICAO website at www.icao.int. The space below is provided to keep a record of such amendments.

RECORD OF AMENDMENTS AND CORRIGENDA

[illegible][illegible]

FOREWORD

This document defines the data communications protocols and services to be used for implementing the International Civil Aviation Organization (ICAO) aeronautical telecommunication network (ATN) using the Internet protocol suite (IPS). The material contained in this document supplements ICAO Standards and Recommended Practices (SARPs) as contained in Annex 10 — *Aeronautical Telecommunications*, Volume III, Part I, Chapter 3.

Editorial practices in this document are as follows:

The detailed technical specifications in this document that include the operative verb “shall” are essential for implementation to secure proper operation of the ATN.

The detailed technical specifications in this document that include the operative verb “should” are recommended for implementation in the ATN. However, particular implementations may not require this specification to be implemented.

The detailed technical specifications in this document that include the operative verb “may” are optional. The use or non-use of optional items shall not prevent interoperability between ATN/IPS nodes.

This manual is divided into the following parts:

Part I — Detailed Technical Specifications:

This part contains a general description of ATN/IPS. It covers the network, transport and security requirements for the ATN/IPS.

Part II — Internet Protocol Suite (IPS) Applications:

This part contains a description of applications supported by the ATN/IPS. It includes convergence mechanisms and application services that allow legacy ATN/open system interconnection (OSI) applications to operate over the ATN/IPS transport layer.

Part III — Guidance Material:

This part contains guidance material on ATN/IPS communications including information on architecture, as well as general information to support the implementation of ATN/IPS.

TABLE OF CONTENTS

	<i>Page</i>
GLOSSARY	
Abbreviations and Terms	(ix)
 PART I. DETAILED TECHNICAL SPECIFICATIONS	
Chapter 1. Introduction	I-1-1
1.1 General overview	I-1-1
Chapter 2. Requirements	I-2-1
2.1 ATN/IPS administration	I-2-1
2.2 Link layer requirements	I-2-2
2.3 Internet layer requirements	I-2-2
2.4 Transport layer requirements	I-2-4
2.5 Security requirements	I-2-5
2.6 Performance	I-2-7
Appendix to Part I. Autonomous system (AS) numbering plan	I-APP-1
 PART II. INTERNET PROTOCOL SUITE (IPS) APPLICATIONS	
Chapter 1. Legacy ATN applications	II-1-1
1.1 Introduction	II-1-1
1.2 Ground data applications	II-1-1
1.3 Air-ground data applications	II-1-2
1.4 Transport layer	II-1-22
1.5 IPS dialogue service (DS) state tables	II-1-28
Chapter 2. Internet protocol-based applications	II-2-1
2.1 Telephony (VoIP)	II-2-1
2.2 Air-Ground Radio (via VoIP)	II-2-1

PART III. GUIDANCE MATERIAL

Chapter 1. Introduction	III-1-1
1.1 General overview	III-1-1
1.2 Background	III-1-2
1.3 General guidance	III-1-2
1.4 Protocol stack	III-1-7
1.5 Quality of Service (QoS)	III-1-16
1.6 Mobility guidance	III-1-20
1.7 Security guidance	III-1-23
1.8 Voice-over Internet protocol (VoIP)	III-1-30
1.9 IPS implementations	III-1-31
 Appendix to Part III. Reference documents	 III-APP-1

GLOSSARY

ABBREVIATIONS AND TERMS

The abbreviations used in this manual are defined as follows:

AAC	Aeronautical administrative communications
ACSP	Air communications service provider
AF	Assured forwarding
AH	Authentication header
AIDC	ATS interfacility data communications
AINSC	Aeronautical industry service communication
AMHS	ATS message handling system
ANSP	Air navigation service provider
AOC	Aeronautical operational communications
AS	Autonomous system
ATC	Air traffic control
ATM	Air traffic management
ATN	Aeronautical telecommunication network
ATS	Air traffic services
ATSC	Air traffic services communication
ATSMHS	ATS message handling services
ATSU	ATS unit
BGP	Border gateway protocol
CN	Correspondent node
CRL	Certificate revocation list
DiffServ	Differentiated services
ECC	Elliptic curve cryptography
ECP	Encryption control protocol
EF	Expedited forwarding
ESP	Encapsulating security payload
FIR	Flight information region
FMTP	Flight management transfer protocol
HA	Home agent
HC	Handover control
HMAC	Hash message authentication code
IANA	Internet assigned numbers authority
ICMP	Internet control message protocol
ICV	Integrity check value
IETF	Internet Engineering Task Force
IKEv2	Internet key exchange version 2
IP	Internet protocol
IPS	Internet protocol suite
IPsec	Internet protocol security
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISO	International Organization for Standardization
LIR	Local Internet registry

LM	Location management
MM	Mobility management
MN	Mobile node
MoA	Memorandum of Agreement
MSP	Mobility service provider
MTU	Maximum transmission unit
OLDI	Online data interchange
OSI	Open system interconnection
PHB	Per-hop behaviour
PPP	Point-to-point protocol
QoS	Quality of Service
RFC	Request for comments
RIR	Regional Internet registry
ROHC	Robust header compression
RTP	Real time transport protocol
SARPs	Standards and Recommended Practices
TCP	Transmission control protocol
TLS	Transport layer security
TOS	Type of service
UDP	User datagram protocol

DEFINITIONS

The following definitions are consistent with Internet Engineering Task Force (IETF) terminology:

Access network. A network that is characterized by a specific access technology.

Administrative domain. An administrative entity in the ATN/IPS. An administrative domain can be an individual State, a group of States, an aeronautical industry organization (e.g. an air-ground service provider), or an air navigation service provider (ANSP) that manages ATN/IPS network resources and services. From a routing perspective, an administrative domain includes one or more autonomous systems.

ATN/IPS internetwork. The ATN/IPS internetwork consists of IPS nodes and networks operating in a multinational environment.

Autonomous system. A connected group of one or more IP prefixes, run by one or more network operators, which has a single, clearly defined routing policy.

Global mobility. Global mobility is mobility across access networks.

Handover control. The handover control (HC) function is used to provide the “session continuity” for the “on-going” session of the mobile node.

Host. A host is a node that is not a router. A host is a computer connected to the ATN/IPS that provides end users with services.

Host-based mobility management. A mobility management (MM) scheme in which MM signalling is performed by the mobile node.

Inter-domain routing (exterior routing protocol). Protocols for exchanging routing information between autonomous systems. In some cases, they may be used between routers within an autonomous system, but they primarily deal with exchanging information between autonomous systems.

Intra-domain routing (interior routing protocol). Protocols for exchanging routing information between routers within an autonomous system.

IPS mobile node. An IPS node that uses the services of one or more mobility service providers (MSPs).

Local mobility. Local mobility is network layer mobility within an access network.

Location management. The location management (LM) function is used to keep track of the movement of a mobile node and to locate the mobile node for data delivery.

Mobility service provider (MSP). A service provider that provides mobile IPv6 service (i.e. home agents), within the ATN/IPS. An MSP is an instance of an administrative domain (AD) which may be an air communications service provider (ACSP), air navigation service provider (ANSP), airline, airport authority, government organization, etc.

Network-based mobility management. A mobility management (MM) scheme in which the MM signalling is performed by the network entities on behalf of the mobile node.

Node. A device that implements IPv6.

Router. A router is a node that forwards Internet protocol (IP) packets not explicitly addressed to itself. A router manages the relaying and routing of data while in transit from an originating end system to a destination end system.

Part I

DETAILED TECHNICAL SPECIFICATIONS

Chapter 1

INTRODUCTION

1.1 GENERAL OVERVIEW

1.1.1 This manual contains the minimum communication standards and protocols that will enable implementation of an ICAO aeronautical telecommunication network (ATN) based on the Internet protocol suite (IPS), referred to as the ATN/IPS. The scope of this manual is on interoperability across administrative domains. This includes administrative domains participating in the global ATN/IPS internetwork as well as administrative domains directly connected via point-to-point connections. Implementation of the ATN/IPS, including the standards and protocols included in this manual, will take place on the basis of regional air navigation agreements between ICAO Contracting States in accordance with Annex 10, Volume III, Part I, Chapter 3, 3.3.2. Planning and Implementation Regional Groups (PIRGs) coordinate such agreements.

1.1.2 The ATN/IPS protocol architecture is illustrated in Figure I-1-1. The ATN/IPS has adopted the same four-layer model as defined in Internet Society (ISOC) Internet standard STD003.

Note.— STD003 is a combination of Internet Engineering Task Force (IETF) RFC 1122 and RFC 1123.

1.1.3 This model has four abstraction layers called the link layer, the Internet or Internet protocol (IP) layer, the transport layer and the application layer.

1.1.4 As depicted in Figure I-1-1, this manual does not adopt any specific link layer protocol as this is a local or bilateral issue which does not affect overall interoperability.

1.1.5 This manual adopts the Internet protocol version 6 (IPv6) for Internet layer interoperability. Implementation of IPv4 in ground networks, for transition to IPv6 (or as a permanent network) is not addressed in this manual. IPv6 is to be implemented in air-ground networks. The border gateway protocol — 4 (BGP-4) with extensions is adopted for inter-domain routing.

1.1.6 The transmission control protocol (TCP) and user datagram protocol (UDP) are adopted for connection-oriented and connectionless services at the transport layer.

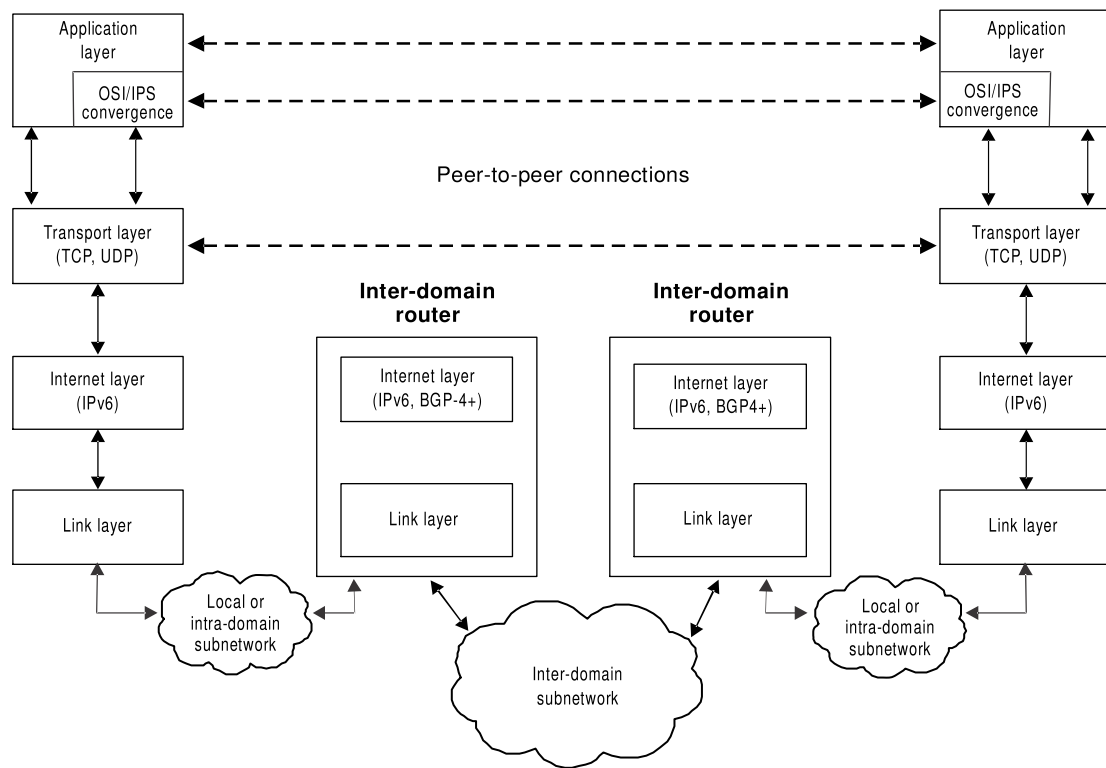


Figure I-1-1. ATN/IPS protocol architecture

Chapter 2

REQUIREMENTS

2.1 ATN/IPS ADMINISTRATION

The ATN/IPS

2.1.1 The ATN/IPS internetwork consists of IPS nodes and networks operating in a multinational environment in support of air traffic services communication (ATSC) as well as aeronautical industry service communication (AINSC), such as aeronautical administrative communications (AAC) and aeronautical operational communications (AOC).

2.1.2 In this manual, an IPS node is a device that implements IPv6. There are two types of IPS nodes:

- an IPS router is an IPS node that forwards Internet protocol (IP) packets not explicitly addressed to itself; and
- an IPS host is an IPS node that is not a router.

2.1.3 From an administrative perspective, the ATN/IPS internetwork consists of a number of interconnected administrative domains. An administrative domain can be an individual State, a group of States (e.g. an ICAO region), an air communications service provider (ACSP), an air navigation service provider (ANSP), or any other organizational entity that manages ATN/IPS network resources and services.

2.1.4 Each administrative domain participating in the ATN/IPS internetwork shall operate one or more IPS routers which execute the inter-domain routing protocol specified in this manual.

2.1.5 From a routing perspective, inter-domain routing protocols are used to exchange routing information between autonomous systems (AS), where an AS is a connected group of one or more IP address prefixes. The routing information exchanged includes IP address prefixes of differing lengths. For example, an IP address prefix exchanged between ICAO regions may have a shorter length than an IP address prefix exchanged between individual States within a particular region.

2.1.6 Administrative domains should coordinate their policy for carrying transit traffic with their counterparts.

ATN/IPS mobility

2.1.7 ATN/IPS mobility is based on IPv6 mobility standards, operated by mobility service providers (MSP).

Note.— An MSP in the ATN/IPS is an instance of an administrative domain which may be an ACSP, ANSP, airline, airport authority, government or other aviation organization.

2.1.8 ATN/IPS MSPs shall operate one or more home agents (HAs).

2.2 LINK LAYER REQUIREMENTS

The specification of the link layer characteristics for an IPS node is a local issue.

2.3 INTERNET LAYER REQUIREMENTS

General IPv6 internetworking

- 2.3.1 IPS nodes shall implement IPv6 as specified in RFC 2460.
- 2.3.2 IPS nodes shall implement IPv6 maximum transmission unit (MTU) path discovery as specified in RFC 1981.
- 2.3.3 IPS nodes shall set the flow label field of the IPv6 header to zero, as it is not used in the ATN/IPS.

Mobile IPv6

- 2.3.4 IPS mobile nodes (MNs) shall implement mobile IPv6 as specified in RFC 3775.
- 2.3.5 IPS HAs shall implement mobile IPv6 as specified in RFC 3775.
- 2.3.6 IPS MNs and HAs may implement extensions to mobile IPv6 to enable support for network mobility as specified in RFC 3963 and enhancements to MIPv6 listed in Part III, Chapter 1, 1.6.9, 1.6.10 and 1.6.11.
- 2.3.7 IPS nodes that implement mobile IPv6 route optimization should allow route optimization to be administratively enabled or disabled, with the default being disabled.

Note.— The use of mobile IPv6 route optimization is not mandated by this specification until further requests for comments (RFCs) on standards have been developed by the IETF.

Network addressing

- 2.3.8 IPS nodes shall implement IPv6 addressing architecture as specified in RFC 4291.
- 2.3.9 IPS nodes shall use globally scoped IPv6 addresses when communicating over the ATN/IPS.
- 2.3.10 Administrative domains shall obtain IPv6 address prefix assignments from their local Internet registry (LIR) or regional Internet registry (RIR).
- 2.3.11 MSPs shall obtain a /32 IPv6 address prefix assignment for the exclusive use of IPS mobile nodes or mobile networks.

2.3.12 MSPs should use the IPv6 address structure for aircraft assignments (see Figure I-2-1).

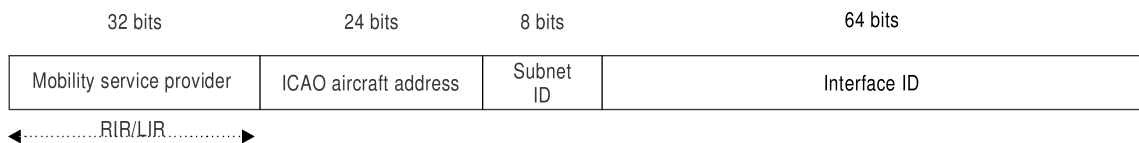


Figure I-2-1. Autonomous system number plan

Note 1.— Under this structure, each aircraft constitutes a /56 IPv6 end-site, which is based on the ICAO 24-bit aircraft address as defined in Annex 10, Volume III, Part I, Appendix to Chapter 9.

Note 2.— For on-board services (ATS, AOC, AAC, etc.), an aircraft may have either multiple subnets interconnected to a mobile router, multiple MSPs or a combination of both.

2.3.13 MSPs shall advertise their /32 aggregate prefix to the ATN/IPS.

Inter-domain routing

Note 1.— Inter-domain routing protocols are used to exchange routing information among AS.

Note 2.— For routing purposes, an AS has a unique identifier called an AS number.

Note 3.— A single administrative domain may be responsible for the management of several AS.

Note 4.— The routing protocol within an AS is a local matter determined by the managing organization.

2.3.14 IPS routers shall implement the Border Gateway Protocol (BGP-4) as specified in RFC 4271 for inter-domain routing across administrative domains.

2.3.15 IPS routers which support inter-domain dynamic routing shall implement the BGP-4 multiprotocol extensions as specified in RFC 2858.

2.3.16 Administrative domains shall use AS numbers for ATN/IPS routers that implement BGP-4.

2.3.17 IPS routers that implement the Border Gateway Protocol (BGP-4) for inter-domain routing across administrative domains shall follow the AS numbering plan.

Note.— Administrative domains that require additional private AS numbers should coordinate through ICAO.

2.3.18 IPS routers which support inter-domain dynamic routing should authenticate routing information exchanges as specified in RFC 2385.

Error detection and reporting

2.3.19 IPS nodes shall implement Internet Control Message Protocol (ICMPv6) as specified in RFC 4443.

Quality of Service (QoS)

2.3.20 Administrative domains shall make use of differentiated services (DiffServ) as specified in RFC 2475 as a means to provide Quality of Service (QoS) to ATN/IPS applications and services.

2.3.21 Administrative domains shall enable ATN/IPS DiffServ class of service to meet the operational and application requirements.

2.3.22 Administrative domains supporting voice-over IP services shall assign those services to the expedited forwarding (EF) per-hop behaviour (PHB) as specified in RFC 3246.

2.3.23 Administrative domains shall assign ATN application traffic to the assured forwarding (AF) PHB as specified in RFC 2597.

Note.— Assured forwarding allows the ATN/IPS operator to provide assurance of delivery as long as the traffic does not exceed the subscribed rate. Excess traffic has a higher probability of being dropped if congestion occurs.

2.3.24 Administrative domains that apply measures of priority to the AF PHBs shall assign relative measures based on the ATN mapping of priorities defined in Annex 10, Volume III, Part I, Chapter 3, Table 3-1.

IP version transition

2.3.25 Administrative domains should use the dual IP layer mechanism for IPv6 to IPv4 compatibility as described in RFC 4213.

Note.— This provision ensures that ATN/IPS hosts also support IPv4 for backward compatibility with local IPv4 applications.

2.4 TRANSPORT LAYER REQUIREMENTS

Transmission control protocol (TCP)

2.4.1 IPS hosts requiring connection-oriented transport service shall implement the transmission control protocol (TCP) as specified in RFC 793.

2.4.2 IPS nodes may implement TCP extensions for high performance as specified in RFC 1323.

User datagram protocol (UDP)

2.4.3 IPS hosts requiring connectionless transport service shall implement the user data gram protocol (UDP) as specified in RFC 768.

Transport protocol port numbers

2.4.4 IPS nodes shall support and make use of the TCP and/or UDP port numbers defined in Part II, 1.5.4 and Part III, 1.4.28, of this document.

2.5 SECURITY REQUIREMENTS

Note.— The use of the following security requirements for communications in the ATN/IPS should be based on a system threat and vulnerability analysis.

2.5.1 This section defines IPS node security requirements and capabilities but does not impose their use for communications in the ATN/IPS.

Ground-ground security

Note.— IP layer security in the ground-ground ATN/IPS internetwork is implemented using Internet protocol security (IPsec) and the Internet key exchange version 2 (IKEv2) protocol.

Ground-ground IPsec/IKEv2

2.5.2 IPS nodes in the ground-ground environment shall comply with the security architecture for the Internet protocol as specified in RFC 4301.

2.5.3 IPS nodes in the ground-ground environment shall implement the IP encapsulating security payload (ESP) protocol as specified in RFC 4303.

2.5.4 IPS nodes in the ground-ground environment may implement the IP authentication header (AH) protocol as specified in RFC 4302.

2.5.5 IPS nodes in the ground-ground environment shall implement the Internet key exchange version (IKEv2) protocol as specified in RFC 4306.

2.5.6 IPS nodes in the ground-ground environment shall implement the cryptographic algorithm implementation requirements for the ESP and AH, if AH is implemented as specified in RFC 4835.

2.5.7 IPS nodes in the ground-ground environment shall implement the null encryption algorithm as specified in RFC 4835, but not the null authentication algorithm, when establishing Internet protocol security (IPsec) associations.

2.5.8 IPS nodes in the ground-ground environment shall implement the cryptographic algorithms for use in the IKEv2 as specified in RFC 4307, when negotiating algorithms for key exchange.

2.5.9 IPS nodes in the ground-ground environment should use the Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile as specified in RFC 5280, when digital signatures are used as the IKEv2 authentication method.

2.5.10 IPS nodes in the ground-ground environment should use the Internet X.509 public key infrastructure certificate policy and certificate practices framework as specified in RFC 3647, when digital signatures are used as the IKEv2 authentication method.

Note.— The Air Transport Association (ATA) Digital Security Working Group (DSWG) has developed a certificate policy (ATA Specification 42) for use in the aviation community. ATA Specification 42 includes certificate and CRL profiles that are suitable for aeronautical applications and interoperability with an aerospace industry public key infrastructure (PKI) bridge. These profiles provide greater specificity than, but do not conflict with, RFC 5280.

Air-ground security

Air-ground access network security

2.5.11 IPS mobile nodes shall implement the security provisions of the access network to enable access network security.

Note.— For example, the WiMAX, 3GPP, and 3GPP2 access networks have authentication and authorization provisions.

Air-ground IPsec/IKEv2

2.5.12 IPS nodes in the air-ground environment shall comply with the security architecture for the Internet protocol as specified in RFC 4301.

2.5.13 IPS nodes in the air-ground environment shall implement the IP ESP protocol as specified in RFC 4303.

2.5.14 IPS nodes in the air-ground environment shall implement AUTH_HMAC_SHA2_256-128 as the integrity algorithm for ESP authentication as specified in RFC 4868, when establishing IPsec security associations.

2.5.15 IPS nodes in the air-ground environment which implement encryption shall implement AES-GCM with an 8 octet integrity check value (ICV) and with a key length attribute of 128 bits for ESP encryption and authentication as specified in RFC 4106.

2.5.16 IPS nodes in the air-ground environment shall implement the IKEv2 protocol as specified in RFC 4306.

2.5.17 IPS nodes in the air-ground environment shall implement IKEv2 with the following transforms:

- a) PRF_HMAC_SHA_256 as the pseudo-random function as specified in RFC 4868.
- b) 256-bit random encryption control protocol (ECP) group for Diffie-Hellman key exchange values as specified in RFC 4753.
- c) ECDSA with SHA-256 on the P-256 curve as the authentication method as specified in RFC 4754.
- d) AES-CBC with 128-bit keys as the IKEv2 encryption transforms as specified in RFC 3602.
- e) HMAC_SHA_256-128 as the IKEv2 integrity transform as specified in RFC 4868.

2.5.18 IPS nodes in the air-ground environment should use the Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile as specified in RFC 5280, when digital signatures are used as the IKEv2 authentication method.

2.5.19 IPS nodes in the air-ground environment should use the Internet X.509 public key infrastructure certificate policy and certificate practices framework as specified in RFC 3647, when digital signatures are used as the IKEv2 authentication method.

Note.— The Air Transport Association (ATA) Digital Security Working Group (DSWG) has developed a certificate policy (ATA Specification 42) for use in the aviation community. ATA Specification 42 includes certificate and CRL profiles that are suitable for aeronautical applications and interoperability with an aerospace industry PKI bridge. These profiles provide greater specificity than, but do not conflict with, RFC 5280.

2.5.20 IPS nodes in the air-ground environment, shall implement mobile IPv6 operation with IKEv2 and the revised IPsec architecture as specified in RFC 4877.

Air-ground transport layer security

2.5.21 IPS mobile nodes and correspondent nodes may implement the transport layer security (TLS) protocol as specified in RFC 5246.

2.5.22 IPS mobile nodes and correspondent nodes shall implement the cipher suite :

TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA as specified in RFC 4492 when making use of TLS.

Air-ground application layer security

2.5.23 IPS mobile nodes and correspondent nodes may implement application layer security at the IPS dialogue service boundary, which is specified in Part III, 1.7.20, of this document.

2.5.24 IPS mobile nodes and correspondent nodes shall append a keyed hashed message authentication code (HMAC) as specified in RFC 2104 using SHA-256 as the cryptographic hash function, when application layer security is used.

2.5.25 An HMAC tag truncated to 32 bits shall be computed over the user data concatenated with a 32-bit send sequence number for replay protection, when application layer security is used.

2.5.26 IKEv2 shall be used for key establishment as specified in 2.5.12 to 2.5.20, when application layer security is used.

2.6 PERFORMANCE

2.6.1 IPS nodes may implement RFC 2488 in order to improve performance over satellite links.

2.6.2 IPS nodes may implement the ROHC header compression (ROHC) framework as specified in RFC 4995 in order to optimize bandwidth utilization.

2.6.3 If ROHC is supported, then the following ROHC profiles shall be supported as applicable:

- a) the ROHC profile for TCP/IP specified in RFC 4996;
- b) the ROHC profile for real time transport protocol (RTP)/UDP/ESP specified in RFC 3095;
- c) the IP-only ROHC profile specified in RFC 4843; and
- d) the ROHC over point-to-point protocol (PPP) profile specified in RFC 3241.

Appendix to Part I

AUTONOMOUS SYSTEM (AS) NUMBERING PLAN

Note.— This numbering plan covers ICAO Contracting States, non-Contracting States and Territories.

<i>ICAO region</i>	<i>Country/organization/location</i>	<i>AS number</i>
APAC	Afghanistan	64512
APAC	American Samoa (United States)	64513
ESAF	Angola	64514
NACC	Anguilla (United Kingdom)	64515
NACC	Antigua and Barbuda	64516
SAM	Argentina	64517
NACC	Aruba (Netherlands)	64518
WACAF	Ascension and St. Helena (United Kingdom)	64519
APAC	Australia	64520
NACC	Bahamas	64521
APAC	Bangladesh	64522
NACC	Barbados	64523
NACC	Belize	64524
WACAF	Benin	64525
NACC	Bermuda (United Kingdom)	64526
APAC	Bhutan	64527
SAM	Venezuela	64528
SAM	Bolivia	64529
ESAF	Botswana	64530
SAM	Brazil	64531
ESAF	British Indian Ocean Territory	64532
APAC	Brunei Darussalam	64533
WACAF	Burkina Faso	64534
ESAF	Burundi	64535
APAC	Cambodia	64536
WACAF	Cameroon	64537

<i>ICAO region</i>	<i>Country/organization/location</i>	<i>AS number</i>
NACC	Canada	64538
WACAF	Cabo Verde	64539
NACC	Cayman Islands (United Kingdom)	64540
WACAF	Central African Republic	64541
WACAF	Chad	64542
SAM	Chile	64543
APAC	China	64544
SAM	Colombia	64545
WACAF	Congo	64546
APAC	Cook Islands	64547
NACC	Costa Rica	64548
WACAF	Côte d'Ivoire	64549
NACC	Cuba	64550
APAC	Democratic People's Republic of Korea	64551
WACAF	Democratic Republic of the Congo	64552
APAC	Timor-Leste	64553
ESAF	Djibouti	64554
NACC	Dominica	64555
NACC	Dominican Republic	64556
APAC	Easter Island (Chile)	64557
SAM	Ecuador	64558
MID	Egypt	64559
NACC	El Salvador	64560
WACAF	Equatorial Guinea	64561
ESAF	Eritrea	64562
ESAF	Ethiopia	64563
SAM	Falklands Islands (United Kingdom)	64564
NACC	French Antilles	64565
WACAF	Gabon	64566
WACAF	Gambia	64567
WACAF	Ghana	64568
NACC	Grenada	64569
APAC	Guam (United States)	64570

ICAO region	Country/organization/location	AS number
NACC	Guatemala	64571
WACAF	Guinea	64572
WACAF	Guinea-Bissau	64573
SAM	Guyana	64574
SAM	French Guiana	64575
NACC	Haiti	64576
NACC	Honduras	64577
APAC	Hong Kong, China	64578
APAC	Wallis and Futuna Islands (France)	64579
APAC	India	64580
APAC	Indonesia	64581
MID	Iran, Islamic Republic of	64582
MID	Iraq	64583
EUR/NAT	Israel	64584
NACC	Jamaica	64585
APAC	Japan	64586
APAC	Johnston Island (United States)	64587
MID	Jordan	64588
ESAF	Kenya	64589
MID	Bahrain	64590
APAC	Kingman Reef (United States)	64591
APAC	Kiribati	64592
MID	Kuwait	64593
ESAF	Réunion (France)	64594
APAC	Lao People's Democratic Republic	64595
MID	Lebanon	64596
ESAF	Lesotho	64597
WACAF	Liberia	64598
MID	Libya	64599
APAC	Macao, China	64600
ESAF	Madagascar	64601
ESAF	Malawi	64602
APAC	Malaysia	64603

<i>ICAO region</i>	<i>Country/organization/location</i>	<i>AS number</i>
APAC	Maldives	64604
WACAF	Mali	64605
APAC	Mariana Islands (United States)	64606
APAC	Marshall Islands	64607
EUR/NAT	Albania	64608
EUR/NAT	Armenia	64612
EUR/NAT	Austria	64616
EUR/NAT	Azerbaijan	64620
EUR/NAT	Belarus	64624
EUR/NAT	Belgium	64628
EUR/NAT	Bosnia and Herzegovina	64632
EUR/NAT	Bulgaria	64636
EUR/NAT	Croatia	64640
MID	Cyprus	64644
EUR/NAT	Czech Republic	64648
EUR/NAT	Denmark	64652
EUR/NAT	Estonia	64656
EUR/NAT	Finland	64660
EUR/NAT	France	64664
EUR/NAT	Georgia	64668
EUR/NAT	Germany	64672
EUR/NAT	Greece	64676
EUR/NAT	Hungary	64680
EUR/NAT	Iceland	64684
EUR/NAT	Ireland	64688
EUR/NAT	Italy	64692
EUR/NAT	Kazakhstan	64696
EUR/NAT	Kyrgyzstan	64700
EUR/NAT	Latvia	64704
EUR/NAT	Liechtenstein	64706
EUR/NAT	Lithuania	64708
EUR/NAT	Luxembourg	64712
EUR/NAT	The former Yugoslav Republic of Macedonia	64716

ICAO region	Country/organization/location	AS number
EUR/NAT	Malta	64720
EUR/NAT	Republic of Moldova	64724
EUR/NAT	Monaco	64728
EUR/NAT	Netherlands	64732
EUR/NAT	Norway	64736
EUR/NAT	Poland	64740
EUR/NAT	Portugal	64744
EUR/NAT	Romania	64748
EUR/NAT	Russian Federation	64752
EUR/NAT	Serbia	64756
EUR/NAT	Slovakia	64760
EUR/NAT	Slovenia	64764
EUR/NAT	Spain	64768
EUR/NAT	Sweden	64772
EUR/NAT	Tajikistan	64776
EUR/NAT	Switzerland	64780
EUR/NAT	The Holy See	64782
EUR/NAT	Turkey	64784
EUR/NAT	Turkmenistan	64788
EUR/NAT	Ukraine	64792
EUR/NAT	United Kingdom	64796
EUR/NAT	Uzbekistan	64800
EUR/NAT	Algeria	64804
EUR/NAT	Andorra	64808
EUR/NAT	Gibraltar (United Kingdom)	64812
EUR/NAT	Greenland (Denmark)	64816
EUR/NAT	Montenegro	64820
EUR/NAT	Morocco	64824
EUR/NAT	San Marino	64828
EUR/NAT	Tunisia	64832
EUR/NAT	Regional - Europe	65108
EUR/NAT	Regional - Europe	65112
EUR/NAT	EUROCONTROL	65208

<i>ICAO region</i>	<i>Country/organization/location</i>	<i>AS number</i>
EUR/NAT	EUROCONTROL	65212
EUR/NAT	EUROCONTROL	65216
EUR/NAT	EUROCONTROL	65220
EUR/NAT	EUROCONTROL	65224
EUR/NAT	EUROCONTROL	65228
EUR/NAT	EUROCONTROL	65232
EUR/NAT	EUROCONTROL	65236
WACAF	Mauritania	65237
ESAF	Mauritius	65238
NACC	Mexico	65239
APAC	Micronesia, Federated States of	65240
APAC	Midway (United States)	65241
APAC	Mongolia	65242
NACC	Montserrat (United Kingdom)	65243
ESAF	Mozambique	65244
APAC	Myanmar	65245
ESAF	Namibia	65246
APAC	Nauru	65247
APAC	Nepal	65248
NACC	Netherlands Antilles	65249
APAC	New Caledonia (France)	65250
APAC	New Zealand	65251
NACC	Nicaragua	65252
WACAF	Niger	65253
WACAF	Nigeria	65254
APAC	Niue (New Zealand)	65255
MID	Oman	65256
APAC	Pakistan	65257
APAC	Palau	65258
	Palestinian Territory, occupied	65259
APAC	Palmyra (United States)	65260
SAM	Panama	65261
APAC	Papua New Guinea	65262

ICAO region	Country/organization/location	AS number
SAM	Paraguay	65263
SAM	Peru	65264
APAC	Philippines	65265
APAC	Pitcairn Island (United Kingdom)	65266
APAC	French Polynesia	65267
NACC	Puerto Rico (United States)	65268
MID	Qatar	65269
APAC	Republic of Korea	65270
APAC	Fiji	65271
ESAF	Rwanda	65272
NACC	Saint Kitts and Nevis	65273
NACC	Saint Lucia	65274
NACC	Saint Vincent and the Grenadine	65275
APAC	Samoa	65276
WACAF	Sao Tome and Principe	65277
MID	Saudi Arabia	65278
WACAF	Senegal	65279
ESAF	Seychelles	65280
WACAF	Sierra Leone	65281
APAC	Singapore	65282
APAC	Solomon Islands	65283
ESAF	Somalia	65284
ESAF	South Africa	65285
APAC	Sri Lanka	65286
MID	Sudan	65287
SAM	Suriname	65288
ESAF	Swaziland	65289
MID	Syrian Arab Republic	65290
APAC	Thailand	65291
WACAF	Togo	65292
APAC	Tonga	65293
NACC	Trinidad and Tobago	65294
NACC	Turks and Caicos Islands (United Kingdom)	65295

<i>ICAO region</i>	<i>Country/organization/location</i>	<i>AS number</i>
APAC	Tuvalu	65296
ESAF	Uganda	65297
ESAF	Comoros	65298
MID	United Arab Emirates	65299
ESAF	United Republic of Tanzania	65300
NACC	United States	65301
SAM	Uruguay	65302
APAC	Vanuatu	65303
APAC	Viet Nam	65304
NACC	British Virgin Islands (United Kingdom)	65305
NACC	Virgin Islands (United States)	65306
APAC	Wake Island (United States)	65307
	Western Sahara	65308
MID	Yemen	65309
ESAF	Zambia	65310
ESAF	Zimbabwe	65311