

# Use of IPsec in the ATN IPS

## ICNS Conference 2007

May 1 - 3, 2007

Hilton Washington Dulles Airport

Herndon, Virginia

*Vic Patel*

FAA/ATO-P Security Engineering Team

William J. Hughes FAA Technical Center

Atlantic City International Airport

Atlantic City, NJ 08405

USA



Federal Aviation  
Administration



# ATN Service Infrastructures

The ATN consists of two categories:

- **Networks**
  - Air to Ground (A/G) Router Network and
  - Ground to Ground (G/G) Router Network
- **Applications**
  - Air Traffic Service (ATS) Inter-facility Data Communication (AIDC)
  - ATS Message Handling System (AMHS)
  - AMHS and Aeronautical Fixed Telecommunications Network (AMHS/AFTN) Gateway
  - Controller Pilot Data Link Communication (CPDLC)
  - Directory Service



# IPv6 in the ATN/IPS

- **The ICAO Aeronautical Communications Panel (ACP) Working Group N is developing technical provisions for using the Internet Protocol Suite (IPS) as the basis for the next generation Aeronautical Telecommunications Network (ATN). Referred to as the ATN IPS**
- **The ATN IPS will be based on the Internet Protocol Version 6 (IPv6)**
- **So far, only the Ground-Ground Technical Provisions have been specified.**
- **ACP Subgroup N1 (Internetworking) is developing the communications requirements for the ATN IPS**
- **ACP Subgroup N4 (Security) is developing the security requirements (in the Technical Manual\*) and security guidance for the ATN IPS**

\* ICAO Manual of Detailed Technical Specification for Internet Protocol Suite (IPS) – available at ICAO website (<http://www.icao.int/anb/Panels/ACP/indexp.html>) under the latest Subgroup N1 Meeting Report



# IPsec in the ATN/IPS

- **Network layer security in the ATN IPS will be based on the Internet Protocol Security (IPsec)**
- **However, support for security is not specifically mandated.**
  - “Support for security is to be based on a system threat and vulnerability analysis.”
- **And so the security requirements in the Technical Manual are conditioned**
  - “IPS Nodes in the ATN which support network layer security shall...”

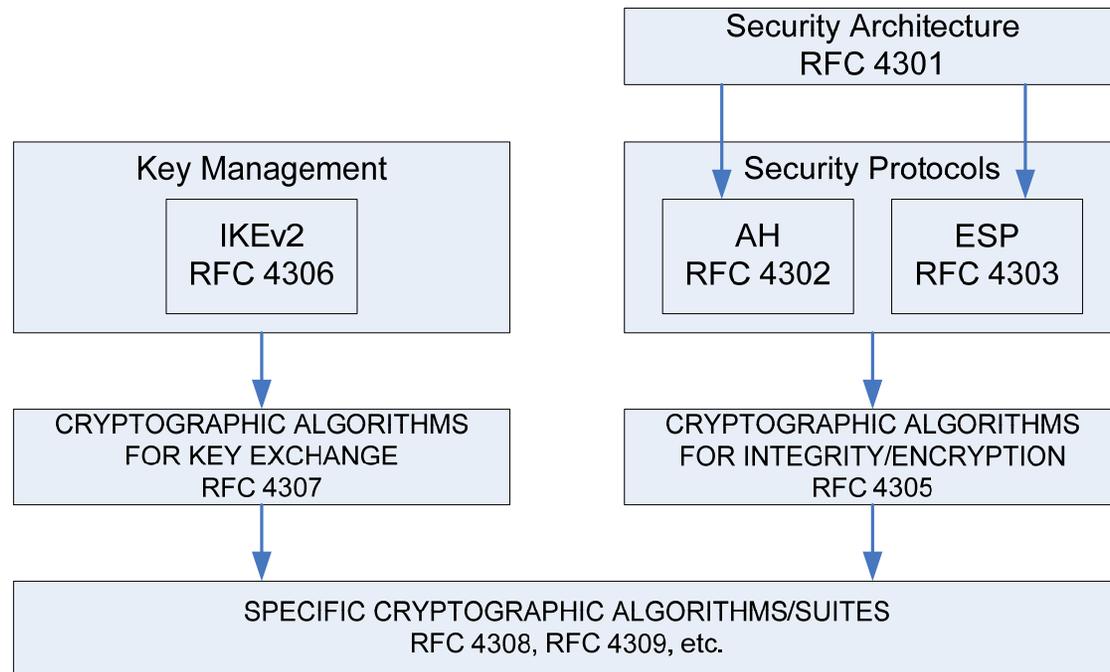


# IPsec Overview

- **Security Architecture – RFC 4301 explains the architecture and components of IPsec and their interactions**
- **Security Protocols – RFCs 4302 and 4303 describing the AH and ESP protocols**
- **Automated Key Management – RFC 4306 defining IKEv2**
- **Cryptographic Algorithms for Integrity and Encryption – RFC 4305 defines the mandatory, default algorithms for use with AH and ESP**
- **Cryptographic Algorithms for Key Exchange – RFC 4307 defines the mandatory algorithms for use with IKEv2**



# IPsec Documentation Roadmap



# Which Version of IPsec

- **There are two versions of IPsec**
- **IPsec-v2 is specified in:**
  - RFC-2401 Security Architecture for the Internet Protocol
  - RFC-2402 IP Authentication Header
  - RFC-2406 IP Encapsulating Security Payload (ESP)
- **IPsec-v3 is specified in:**
  - RFC-4301 Security Architecture for the Internet Protocol
  - RFC-4302 IP Authentication Header
  - RFC-4303 IP Encapsulating Security Payload (ESP)
- **The ATN IPS specifies IPsec-v3**
  - Although IPsec-v2 is currently the most commonly available version, it is anticipated that IPsec-v3 will eventually be widely supported
  - The Tech Manual's publication will be 2008 with initial implementations using IPv6 for Interregional Connections



# AH or ESP

- **The two IPsec over-the-wire security protocols are the Authentication Header (AH) protocol and the Encapsulating Security Protocol (ESP)**
  - Both protocols provide integrity, authentication, and replay protection
  - ESP may provide confidentiality (encryption) also
- **The ATN IPS Technical Manual requires ESP and makes AH optional**
- **The ATN IPS Technical Manual requires authentication with ESP and makes encryption optional**



# Key Management

- **The ATN IPS Technical Manual requires support for manual key management**
  - Manual configuration of the security key and Security Parameters Index is required
  - It is recognized that this does not scale well and IPsec's replay protection mechanisms are not available
- **The ATN IPS Technical Manual recommends support for the Internet Key Exchange (IKEv2) protocol**
  - Recommendations on the use of IKEv2 will be in Guidance Material
    - Main mode or aggressive mode, use of digital signatures, etc.
    - Use of shared secrets with IKEv2 over manual key management

# Transforms and Algorithms

- **The ATN IPS Technical Manual requires support for Cryptographic Algorithm Implementation Requirements for ESP and AH as specified in RFC 4305**
  - Null Encryption Algorithm is required but not the Null Authentication Algorithm
- **The ATN IPS Technical Manual requires support for Cryptographic Algorithms for Use in the Internet Key Exchange (IKEv2) as specified in RFC 4307**



# Expected Use of IPsec in Ground-Ground ATN IPS

- **It is expected that IPsec will be used for Virtual Private Networks (VPN) within an Administrative Domain, i.e., within a Region or State**
  - In this environment locally-issued certificates may be employed
- **IPsec may be used Inter-regionally between BGP-4 Routers**
  - Current common practice however is to use TCP/MD5 “signatures”
  - IPsec will scale better but PKI use needs to be developed
    - Industry initiatives like CertiPath\* may help here
- **The ATN IPS Technical Manual simply recommends authentication between Routers**

\* CertiPath is a joint venture among ARINC, SITA, and Exostar, LLC to provide certificates to the aerospace and defense industries

