L-band Digital Aeronautical Communications System (LDACS)

draft-ietf-raw-ldacs-07

Nils Mäurer, Thomas Gräupl, Corinna Schmitt

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- **By participating in the IETF, you agree to follow IETF processes and policies.**
- **If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.**
- **As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.**
- **Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.**
- **As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.**

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

BCP 9 (Internet Standards Process)

BCP 25 (Working Group processes)

BCP 25 (Anti-Harassment Procedures)

BCP 54 (Code of Conduct)

BCP 78 (Copyright)

BCP 79 (Patents, Participation)

https://www.ietf.org/privacy-policy/ (Privacy Policy)

RAW
Internet-Draft
Intended status: Informational
Expires: 21 August 2021

N. Maeurer, Ed.
T. Graeupl, Ed.
German Aerospace Center (DLR)
C. Schmitt, Ed.
Research Institute CODE, UniBwM

17 February 2021

L-band Digital Aeronautical Communications System (LDACS)
draft-ietf-raw-ldacs-07

Abstract

This document provides an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation. LDACS is a scheduled, reliable multi-application cellular broadband system with support for IPv6. LDACS SHALL provide a data link for IP network-based aircraft guidance. High reliability and availability for IP connectivity over LDACS are therefore essential.

draft-ietf-raw-05 (IETF 109)

Table of Contents

Changes

draft-ietf-raw-07 (IETF 110)

Chapter 10 – Security Considerations (1)

- Problem: Changing Threat-Landscape

- Historically Communication Navigation Surveillance (CNS) wireless technology emerged from military
- PHY layer security feasible for military due to financial and spectrum abundance
- But: Civil applications have significantly lower spectrum
- Today: Software Defined Radios and aeronautical open source software make CNS technologies relatively easily accessible

- Consequences:
  - Future digital aeronautical wireless communications require security features
  - Security features require sufficient bandwidth
  - Most important due to progress of digitalization

→ Strong cybersecurity measures are a **MUST** for LDACS ←

Chapter 10 – Security Considerations (2)

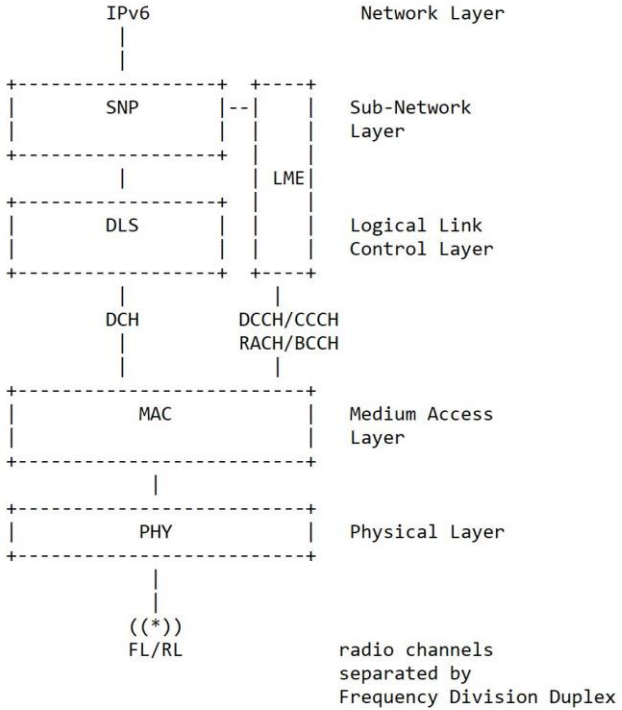
- LDACS's Security:
  - **SHALL** protect availability & continuity
  - **SHALL** protect the integrity of messages in transit
  - **SHALL** provide authenticity of messages in transit
  - **SHOULD** provide confidentiality of messages in transit
  - **SHOULD** provide non-repudiation for necessary messages in transit
  - **SHALL** provide mutual authentication
  - **SHALL** authorize the permitted actions of users & deny actions else
  - **SHALL** provide capability preventing the propagation of intrusions within LDACS domains & towards external domains

Chapter 10 – Security Considerations (3)

Scope of Security

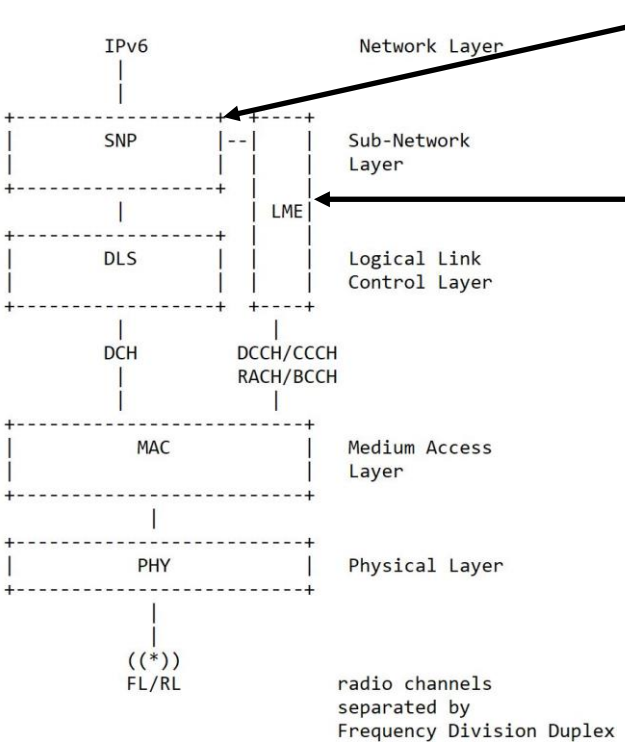
- LDACS security located on the Link Layer
- LDACS security secures connection between Aircraft Station (AS) and Ground Station (GS)

LDACS Protocol Stack



Chapter 10 – Security Considerations (4)

Security Functionality in Protocol Stack



- Handles User Plane Security (DCH) (Confidentiality + Integrity Protection)
- Manages Certificates
- Handles Mutual Authentication and Key Agreement
  - Entity Authentication
  - Key Negotiation
  - Key Derivation
  - Key Management
- Security Logging
- Control Channel (BCCH/CCCH/DCCH) Protection

Chapter 10 – Security Considerations (5)

Trust

- All entities in an LDACS network must authenticate to each other
- LDACS will follow AeroMACS lead and also use an FCI specific PKI [RFC5280]
- LDACS will use X.509 certificates for each end-entity

Mutual Authentication and Key Agreement

Prerequisites: Unique identities at AS/GS and digital certificates pre-deployed during maintenance at the respective end-entities

1. Identity-based Station-to-Station (STS) protocol
2. Identity-based SIGn and Mac (SIGMA) protocol

Chapter 10 – Security Considerations (6)

DHKE Choice

- Considered ephemeral DHKE with 3072bit keys
- Elliptic Curve DHKE with 256bit keys
- Supersingular Isogeny DHKE with 2640bit keys

→ Current choice: ECDH with 256bit keys

Key Derivation

- KDF: Hash-based Message Authentication Code (HMAC) (KDF) – HKDF [RFC5869]

Chapter 10 – Security Considerations (7)

User Data Security

- AES-128-GCM, AES-256-GCM [RFC5288] for confidentiality/integrity protection
- HMAC-SHA3-128 for integrity protection only
- Key $K_{AS,GS}$ agreed upon via STS/SIGMA and derived via HKDF

Control Data Security

- Challenges:
  - Control channels of LDACS very small
  - Control channels must be accessible and verifiable by all members in an LDACS cell

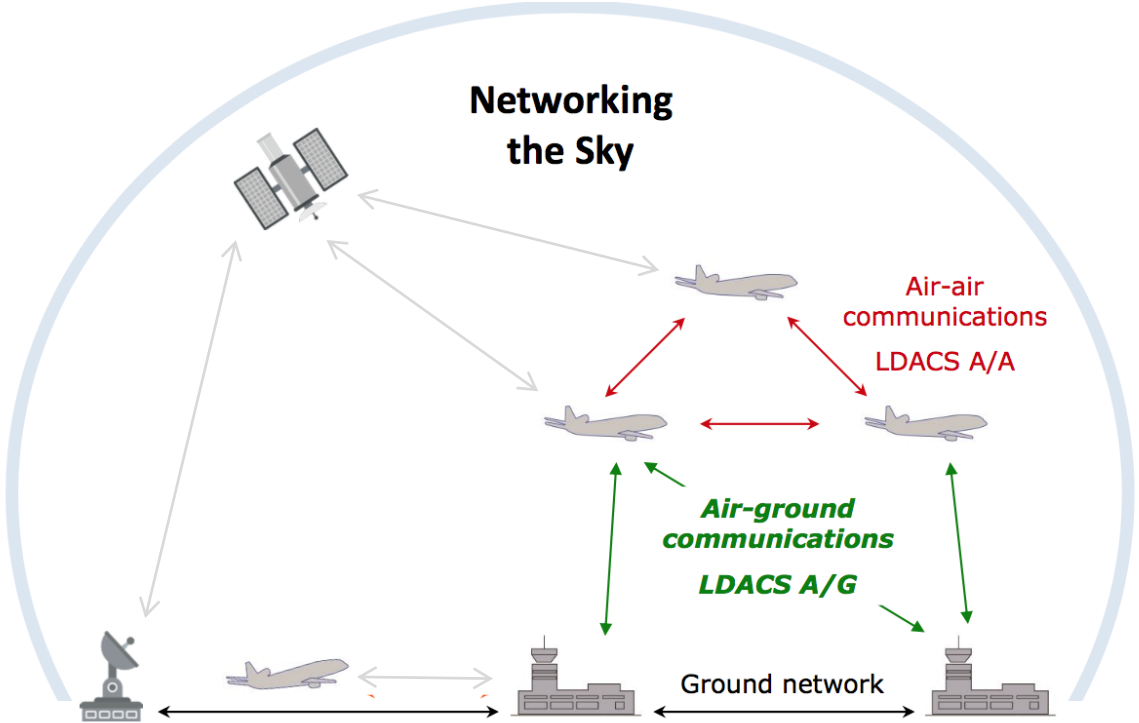
→ Solution: LDACS Cell Group Keys via One-Way Function Trees (OFT)

→ Time-bound Signature in BCCH

→ CRC+MAC in CCCH

→ Encryption+CRC+MAC in DCCH

Thanks


Networking
the Sky
Air-air
communications
LDACS A/A
Air-ground
communications
LDACS A/G
Ground network