Chapter 1

Cybersecurity for the L-band Digital Aeronautical Communications System (LDACS)

Nils Mäurer[1] Thomas Gräupl[2] Corinna Schmitt[3]

Today's analog voice-based air–ground communication system for tactical aircraft guidance is suffering from the VHF band's increasing saturation in high-density areas. The air–ground communication infrastructure is therefore undergoing digitisation to ensure the sustainable growth of the air transportation system in the coming decades. As safety and security are strongly interrelated in aviation, strong cybersecurity is the foundation and enabler for digitalization in aviation. One of the new air-ground datalinks that shall enable this transformation is the L-band Digital Aeronautical Communication System (LDACS). It will be the primary long-range terrestrial datalink of the future IP-based aeronautical telecommunications network. In this chapter we describe the design process, draft, and the state-of-the-art cybersecurity architecture for LDACS.

[1] Institute of Communication and Navigation, German Aerospace Center (DLR)
[2] Institute of Communication and Navigation, German Aerospace Center (DLR)
[3] Research Institute CODE, Universität der Bundeswehr München

1.1 Introduction

Air Traffic Communications (ATC) is the backbone for safe and secure civil air traffic enabling aerial transport of 4.5 billion passengers and 61.3 million tonnes uplift in 2019 [1]. Up to 2020 civil air traffic has been growing constantly at a compound rate of 5.8% per year [2] and despite the severe impact of the COVID-19 pandemic, air traffic growth is expected to resume very quickly in post-pandemic times [1, 3]. With the growth of civil air traffic together with the increasing demand for data-requiring digital services for aircraft guidance and the business operation of airlines, communication increases as well. To cope with this growth, Air Traffic Management (ATM) systems must make more efficient use of its dedicated, limited spectrum making digitization of ATM services unavoidable [4].

The entire industry is currently undergoing such a digital transformation and one area that is mostly affected by this is Communication, Navigation and Surveillance (CNS). The Single European Sky ATM Research (SESAR)[4] program in the European Union (EU) and NextGEN[5] in the US have been tasked with the development of new technologies to create an aeronautical, digital Future Communications Infrastructure (FCI). Candidates in the FCI are Aeronautical Mobile Airport Communications System (AeroMACS) for airport communications (Airport (APT) and Terminal Maneuvering Area (TMA) domain), SatCOM for Oceanic Remote Polar (ORP)domains, and L-band Digital Aeronautical Communications System (LDACS) for long-range terrestrial aeronautical communications [5, 6]. LDACS will be the focus of this work. Fig. 1.1 shows the general structure for the FCI.

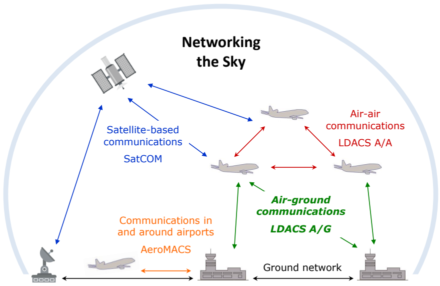

Networking the Sky
Satellite-based communications
SatCOM
Air-air communications
LDACS A/A
Air-ground communications
LDACS A/G
Communications in and around airports
AeroMACS
Ground network

Figure 1.1: The Future Communication Infrastructure (FCI) with new data links such as LDACS and AeroMACS [7, 8].

As safety and security are strongly interrelated in aviation, strong cybersecurity is the foundation and enabler for digitalization in aviation. The World Economic Forum, the International Civil Aviation Organization (ICAO), as well as the cybersecurity research community agree with that [9, 10, 11, 12]. Unfortunately cybersecurity for CNS is still not realized in most deployed systems [13, 14, 15, 16]. In part this is due to the requirements for aeronautical datalinks, (1) low latency and (2) low additional security data overhead [17].

Another part is the difficulty and cost of implementing cybersecurity in a system, once it has been designed, prototyped, released and possibly deployed. The further down in that chain, the less likely and the more expensive it is to integrate security measures. One excellent example is VHF Data Link mode 2 (VDLm2) [18]. VDLm2 is a digital datalink based on Very High Frequency (VHF). It was invented

[4] https://www.sesarju.eu/, Jan. 14, 2021

[5] https://www.faa.gov/nextgen/, Jan. 14, 2021

in the 1990ies and provides a data rate of 31.5 kbps by using Differential 8 Phase Shift Keying (D8PSK), Carrier Sense Multiple Access (CSMA) in the 118 MHz to 137 MHz band [19]. Despite being around for decades, the requirement documents [20, 21] or specifications [22, 19] of the datalinks VHF or VDLm2 do not fulfill any of the information security definitions of confidentiality, integrity, availability, authenticity, accountability, non-repudiation or reliability defined by RFC 4949 [23]. Even newer aeronautical information systems, such as Automatic Dependent Surveillance Broadcast (ADS-B), a Global Navigation Satellite System (GNSS) dependent surveillance technology used by aircraft to automatically broadcast their GNSS based position, which is mandatory since 2020, is mainly known of its insecurity [24, 25, 13, 26, 27] by information security standards. One of the few datalinks in the aeronautical ecosystem, which has a dedicated cybersecurity architecture is the FCI candidate for airport communications, AeroMACS. The system is majorly based on the IEEE 802.16 WiMAX standard [7], which has a security sub-layer integrated in its protocol stack. These selected examples show a clear picture: Information security or cybersecurity is still scarcely integrated into aeronautical communications.

In this chapter we describe the design process, draft and the state-of-the-art of the cybersecurity architecture for the ground-based digital communications system LDACS. LDACS has been designed with security in the mind, and shall introduce state-of-the-art cybersecurity to aeronautics.

In Section 1.2, we introduce LDACS, relevant technical details and previous work on the cybersecurity of LDACS. In Section 1.3, we list requirements and objectives for the cybersecurity architecture for LDACS, which we present in Section 1.4. For evaluation purposes, we evaluate the cybersecurity additions in a mathematical model, a software simulation of LDACS and real flight trials in Section 1.5 before concluding in Section 1.6.

1.2 Background on LDACS

LDACS is a ground-based digital communications system for flight guidance and communications related to safety and regularity of flight [5, 6]. It has mainly been developed in Europe and is currently under standardization by ICAO [28, 29].

1.2.1 System Characteristics

LDACS has its origin in merging parts of the B-VHF [30], B-AMC [31, 32], TIA-902 (P34) [33], and WiMAX IEEE 802.16e technologies [34]. In 2007 the spectrum for LDACS was allocated at the World Radio Conference (WRC), which is shown in picture 1.2.

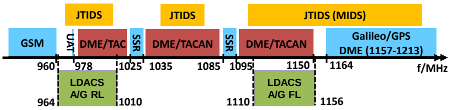


Figure 1.2: Frequency assignment for LDACS at WRC 2007, next to DME

It was decided to allocate the spectrum next to Distance Measuring Equipment (DME), resulting in an in-lay approach between the DME channels for LDACS as illustrated in Figure 1.3.

Furthermore, LDACS uses 4G technology to remain highly flexible and scalable and efficient in coding, supporting adaptive coding and modulation. Additionally, it applies Frequency Division Duplexing (FDD) because of the limited bandwidth available with the inlay approach. Besides all these, LDACS supports seamless handovers, data and voice transmissions, Quality of Service (QoS), has a navigation and surveillance extension, and an Air-to-Air (A2A) link is currently being developed.

1.2.2 Communication Functionality

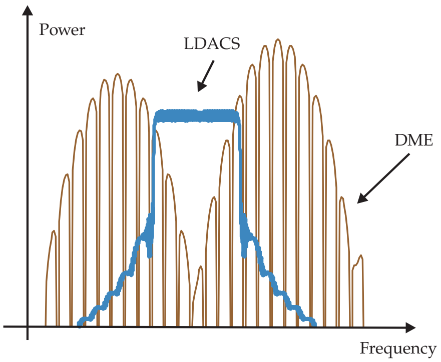


Figure 1.3: Inlay approach for LDACS in between the DME bursts

LDACS was especially designed for ATC and ATM applications like Controller–Pilot Data Link Communications (CPDLC), Automatic Dependent Surveillance-Contract (ADS-C), full 4D trajectories exchange and real-time weather information such as the Graphical Weather Service (WXGRAPH). It is envisioned that Ground Based Augmentation System (GBAS) functionality will be also be provided via LDACS in the future as well [35, 36]. The underlying enabler for all those applications are the main LDACS parameters listed in Table 1.1. Thus, LDACS covers current Air Traffic Services (ATS), Aeronautical Operational

Control (AOC) data and also future applications, enables new concepts (e.g., sectorless ATM) and has at least an order of magnitude more net capacity than the currently used terrestrial links like the VDLm2 system [29].

The latest extension of LDACS communications capabilities – A/A communication – is researched in the German national project IntAirNet [6]. The goal is to establish direct A/A communications between aircraft in communication range allowing infrastructure-less aeronautical network for ad-hoc networks between aircraft. However, this research is only at an early stage, thus we will focus solely on the LDACS A/G link.

Table 1.1: Main parameters for LDACS

Number of sub carriers	64 (50 used)
Bandwidth	625 / 488 kHz
Subcarrier spacing	9.765625 kHz
OFDM symbol duration	102.4 μ
Guard interval	(4.8 + 12.8) μ
Net data rate	470 kbits - 2.82 Mbit/s

1.2.3 LDACS Network Entities

Fig. 1.4 depicts involved components and communication links.

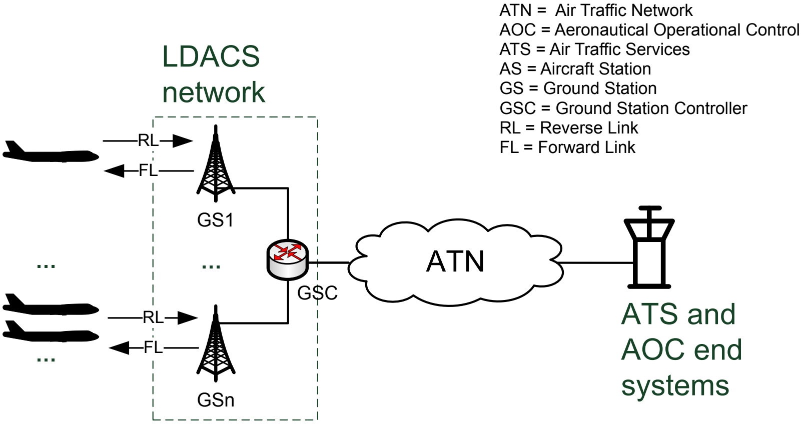


Figure 1.4: Network architecture of LDACS [37]

Up to 512 Aircraft Station (AS) communicate to an LDACS Ground Station (GS) in the Reverse Link (RL). GS communicate to AS in the Foward Link (FL). GSs are controlled by a Ground Station Controller (GSC). The GSC connects the LDACS sub-network to the global Aeronautical Telecommunications Network (ATN) to which the corresponding Air Traffic Services (ATS) and Aeronautical Operational Control (AOC) end systems are attached.

1.2.4 LDACS Protocol Stack

For AS and GS, we can identify different layers and entities in the LDACS protocol stack namely Physical Layer (PHY), Medium Access Layer (MAC), Data Link Service (DLS), LDACS Management Entity (LME), Voice Interface (VI) and Sub-Network Protocol (SNP) and for the GSC, we identify the LME, as illustrated in figure 1.5.

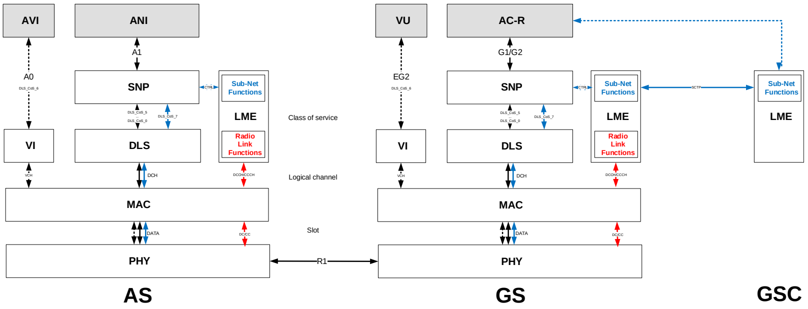


Figure 1.5: The LDACS sublayer is embedded in the FCI (IPv6, voice and control traffic) and consists of Physical layer (PHY), Medium Access Layer (MAC), Data Link Service layer (DLS) and Voice Interface (VI), both located in the logical link control sublayer and finally the Sub-Network Protocol layer (SNP). The LDACS Management Entity (LME) serves as a cross layer entity between MAC, DLS and SNP layer and is the single LDACS relevant entity in the GSC. Voice data is transmitted to higher layers via the Airborne Voice Interface (AVI) on AS side and Voice Unit (VU) on GS side. Data is passed to higher layers via the Airborne Network Interface (ANI) in the AS and via the Access-Router (AC-R) in the GS.

The physical layer provides the means to transfer data over the radio channel (R1 interface). The LDACS ground-station supports bidirectional links to multiple aircraft under its control. The forward link direction (ground-to-air) and the reverse link direction (air-to-ground) are separated by FDD. Forward link and reverse link use a 500 kHz channel each. The ground-station transmits a continuous stream of Orthogonal Frequency-Division Multiplexing (OFDM) symbols on the forward link. In the reverse link different aircraft are separated in time and frequency using a combination of Orthogonal Frequency-Division Multiple Access (OFDMA) and Time Division Multiple Access (TDMA). Aircraft thus transmit discontinuously on the reverse link with radio bursts sent in precisely defined transmission opportunities allocated by the ground-station [17].

The data-link layer provides the necessary protocols to facilitate concurrent and reliable data transfer for multiple users. The LDACS data link layer is organized in two sub-layers: The MAC sub-layer and the Logical Link Control (LLC) sub-layer. The MAC sub-layer manages the organization of transmission opportunities in slots of time and frequency. The logical link control sub-layer provides reliable and acknowledged point-to-point logical channels between the aircraft and the ground-station using an automatic repeat request protocol.

Within the LDACS data link layer two entities are of special interest to us: The *LDACS Management Entity (LME)* and the *Sub-Network Protocol (SNP)*.

The main task of the LME is to perform configuration, resource management and mobility management of LDACS. The mobility management service in the LME provides support for registration and de-registration (cell entry and cell exit of aircraft), scanning channels of neighboring cells and handover between cells. It also manages the addressing of aircraft within cells. The resource management service is responsible for link maintenance (power, frequency and time adjustments). In Fig. 1.5, we see that that these functionalities are provided from within the LME via the ”Radio Link Function”, while user data and communications to the SNP is managed via the ”Sub-Net Functions”. The SNP glues the LDACS network together and works as a connector to the network layer. It provides end-to-end user plane and control connectivity between the aircraft, ground-station and ground-station controller within the LDACS sub-network.

1.2.5 Interfaces, Data Flow and Logical Channels

LDACS internal control data is exchanged between AS and GS over the radio link (R1) and up within the protocol stacks via Common Control (CC) and Dedicated Control (DC) slots between PHY and MAC, Common Control Channel (CCCH) and Dedicated Control Channel (DCCH) logical control channels between MAC and LME. Thus all critical LDACS control functions are handled by the LME.

User data is depicted in black in Fig. 1.5 and travels from ground based Aeronautical Network Service Provider (ANSP) or airline servers via the AC-R over the G1/G2 link into the SNP. The DLS offers different Classes of Service (CoS), depending on the priority of the user packet and via these (DLS_CoS_0...5) into the DLS. Between DLS and MAC, the Data Channel (DCH) logical channels transports user data to the lower layer and via the DATA interface on slot level, user data is handed down from the MAC to PHY layer. Between AS and GS, user data is transmitted then via the radio link (R1), before it is received and handed up between the different protocol layers in the AS, before being handed up to the ANI via the A1 interface. In Fig. 1.6, we see the corresponding control channels, with a deeper description of user (DCH) and control channels (RACH, BCCH, CCCH, DCCH) following below:

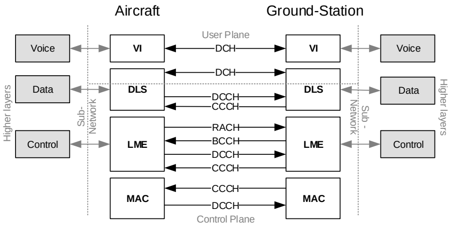


Figure 1.6: Overview of LDACS logical channels for user data (DCH) and control data (BCCH, RACH, CCCH, DCCH) [29]

FL Data Channel (DCH) As the FL channel is held in continuous OFDM transmission, dedicated for the deliverance of user data, the GS locally allocates FL channel resources (i.e. FL PHY-SDUs) within slots and manages the access priorities.

RL Data Channel (DCH) In contrast to the FL DCH, RL DCH uses a bandwidth on demand scheme. Each AS has to request channel resources (RL PHY-SDUs) from the GS before they can send any user or control data in the RL data channel.

Data Control Channel (DCCH) The DCCH is used in RL only, by any AS to convey MAC/Logical Link Layer (LLC) control messages to the GS, while each AS has its own DCCH so that none other than this specific aircraft can send on that channel.

Common Control Channel (CCCH) The CCCH is used in FL only and only by one GS in order to announce e.g. the MAC slot layout and to perform resource allocation in the FL/RL to the AS. Also the GS may send control messages on this channel.

Random Access Channel (RACH) The RACH's purpose is predominantly for AS to make cell entry requests. Only AS may use it.

Broadcast Control Channel (BCCH) As in the name, cell configuration information and mobility management commands are sent to the AS via broadcast messages. Only the GS can use it and it reaches all aircraft listening to the same broadcast Subscriber Access Code (SAC).

1.2.6 LDACS Frame Structure

In the FL direction, each Super Frame (SF) starts with a Broadcast Channel (BC) slot, where the GS announces its existence to the AS and sends physical parameters for link establishment. The rest of the FL SF is split into four Multi Frame (MF), each containing nine OFDM frames and each frame comprises three FL Physical Layer-Service Data Unit (PHY-SDU). Every FL PHY-SDU can be used to transmit FL user data or CC data, in which GS can allocate resources to an AS. Details about the LDACS frame structure are depicted in Fig. 1.7.

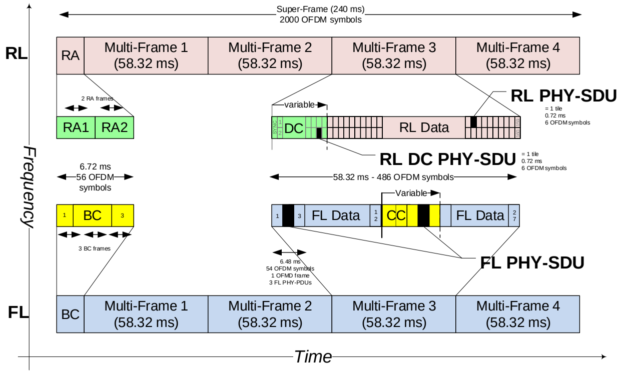


Figure 1.7: Frame structure of LDACS [29]

In the RL, a SF starts with a Random Access (RA) slot, where AS can request access to an LDACS cell, and continues with four MFs. Each RL MF is constructed from 162 RL PHY-SDU equivalent to OFDMA tiles. They are used for two purposes, namely (1) to transmit DC data, which are used by an AS to request the allocation for resources allowing them to send on the RL and (2) to transmit RL user data.

1.2.7 LDACS Cell Entry Procedure

Once a GS is securely connected to the aeronautical ground network via the GSC, it starts sending a broadcast message, the System Identificaiton Broadcast (SIB) message, containing relevant information such as network identification, physical parameters such as channel frequencies and more. When an AS enters the cell served by a GS, it receives the SIB and sends a CELL_RQST message in reply. The CELL_RQST message contains a ”unique address identifying the LDACS radio” [29]. When the GS receives the CELL_RQST message, a CELL_RESP message is sent back to the AS, informing the AS about its System Area Code (SAC). The SAC is a local and temporary address for the AS in the cell. After this exchange of control channel messages, both communication parties are informed about LDACS specific addresses, timing, frequency, and power values and can start the user data communication.

1.2.8 LDACS Data Rate

Data is transported in the DCH via different FL PHY-SDUs and RL PHY-SDUs of different sizes. Depending on coding and modulation, thus the channel quality, the FL PHY-SDUs sizes range from 728 to 3296 Bit, and the RL PHY-SDUs range from 112 to 528 Bit. With 27 frames per MF in total and one to eight FL PHY-SDUs being reserved on the Flight Level (FL) for the Common Control messages, this leaves 19 to 26 FL PHY-SDUs per MF for data transport. The minimum amount of Bit per MF can thus be calculated with $19 * 728 = 13,832$ Bit and the maximum Bit per MF with $26 * 3296 = 85,696$ Bit. On the reverse link, the RL PHY-SDUs are separated into 162 tiles. The first two tiles are sync tiles, followed by a minimum of two DC and a maximum of 32 DC tiles, which limits the minimum usable user data per MF to $(162 - 2 - 32) * 112 = 14,336$ Bit and allows a maximum of $(162 - 2 - 2) * 528 = 83,424$ Bit per MF [29].

This is equivalent to a minimum data rate of 230.5 kbit/s on the FL and 238.9 kbit/s on the RL, with maximum control channel use. Respectively, the maximum data rate is 1428.3 kbit/s on the FL and 1390 kbit/s on the RL, with minimum control channel use.

1.3 Security Requirements, Objectives and Functions

In previous works [38, 17, 37], several threat and risk analysis were performed resulting in the identification of assets, threats and corresponding security requirements, objectives and functions. LDACS must follow the same protection goals as any other aeronautical datalink within the FCI. These are [39, 11]:

Safety The system must sufficiently mitigate attacks, which contribute to safety hazards.

Flight regularity The system must sufficiently mitigate attacks, which contribute to delays, diversions, or cancellations of flights.

Protection of business interests The system must sufficiently mitigate attacks which result in financial loss, reputation damage, disclosure of sensitive proprietary information, or disclosure of personal information.

The next step was to identify assets and objectives: Anything that someone places value upon is regarded as asset. For LDACS five assets were identified: (1) hardware, (2) software, (3) link, (4) data, and (5) services [11].

LDACS Hardware It is responsible for the execution of LDACS software, providing relevant functionality (i.e., supporting any of LDACS possible CNS services). Furthermore LDACS relevant information is stored on it. LDACS hardware refers to AS, GS, and GSC but also to an Authentication, Authorization and Accounting (AAA) server, e.g., integrated within the GSC, Access Routers, the links between entities and the respective LDACS specific internal and shared network and routers.

LDACS Software It enables LDACS CNS capabilities. Thus, we need to make sure that a software component of the devices or sub system is not corrupt, has no errors or other defects. Also we have to prevent wrong installation or configuration of the software components.

LDACS Radio Link All required radio links, accurate time synchronization along with LDACS control data and radio communications connections enabling LDACS to transmit send and receive data via that link are assets. Most important here is preventing unauthorized access, altered hardware, eavesdropping, jamming and spoofing. However, we will not introduce hardware protection mechanisms, such as regular quality checks, access limitations to special hardware and control of personal working on that hardware, or physical layer robustness mechanisms, such as frequency hopping, pilot symbol scrambling, but rather focus on providing protocol based security from the MAC layer up.

LDACS Data All data, relevant for an error-free execution of LDACS services are an asset. These include (but are not limited to) (1) identities of communication entities, (2) LDACS control data, (3) user data, (4) confidential data, only accessible for legitimate users and entities only, (5) any cryptographic material, (6) configuration data or (7) data relevant for navigation services.

LDACS Services Several services, such as system management, announcement and routing, mobility and authentication service are required for an operational baseline for LDACS. As use case, at least 21 high critical ATS user data services and 14 high critical AOC data services [38, 37] were identified to be provided by LDACS. As new functions in ATS and AOC services can be introduced on a frequent basis, this work can only contribute to highlighting already existing safety relevant services in regard to LDACS. Examples of them are the ATC Clearance (ACL), Data Link Logon (DLL), Flight Plan Consistency (FLIPCY), Flight Plan Data (FLTPLAN), Network Connection NETCONN or Network Keep Alive NETKEEP service.

This analysis lead to the identification of five security objectives for LDACS in [17], which were extended to nine objectives in the official LDACS Standards and Recommended Practices (SARPS) [40]. These are (1) to protect availability and continuity of service, to protect (2) integrity, (3) authenticity for user and control plane messages in transit, (4) provide non-repudiation of origin, (5) confidentiality for user plane messages in transit, (6) mutual entity authentication, (7) authorize explicitly permitted actions of users or entities, (8) prevent the propagation of intrusions within LDACS domains and towards external domains and (9) protect against service attacks to a level consistent with the application service requirements.

With these guidelines and objectives in mind, security functions were defined in [41, 11], following the definitions from RFC 4949 [23].

Entity Authentication We need to integrate functions for mutual *entity identification*, *authentication authorization* and *accounting* for every participant within the LDACS sub-net, thus preventing any un-authorized access or use of LDACS.

Key Management LDACS shall include functions for secure *key generation*, *key agreement*, *key derivation*, *key access* and *key destruction*.

(User) Data Confidentiality We suggest using strong *symmetric encryption* for user data encryption, due to low computational overhead and fast operation times. After a master key has been negotiated between each communicating party and an encryption key derived from it, incoming user messages from the air traffic network can be encrypted.

Data Integrity As several threat-and-risk analysis for LDACS revealed, data-in-transit integrity is one of the most important security property for wireless communications systems [38, 17, 37], as due to the wireless nature of the communication medium, it is inherently easy to eavesdrop on messages, modify or delete them.

Data Origin Authentication Some data on the link, such as entity authentication related data, shall include a *data origin proof*.

System Integrity *Self-checks* and checks at startup of systems/devices of LDACS shall detect manipulation or errors in behavior of the security mechanisms.

Robustness LDACS shall support functions ensuring *reliability* and *robustness* to mitigate jamming, spoofing, interference or DoS attacks.

Secure Logging Mechanisms for security and non-security relevant logging, together with regular checks and possibly including the digital signature of the logging device, ensures secure logging of actions within the LDACS radio devices.

Physical Access LDACS shall provide physical security commensurate to the data it contains. This includes zeroing out keys and other secret data in emergency cases.

1.4 A comprehensive Cybersecurity Architecture for LDACS

In this chapter, we combine the inner workings of LDACS from Section 1.2 and cybersecurity requirements and functions from Section 1.3 together to present a comprehensive cybersecurity architecture for LDACS.

1.4.1 Placements of Security Functionality in Protocol Stack

In [17, 37, 41] suitable placement of security functionality within the LDACS protocol stack was discussed.

We argue that placing protection mechanisms in the LME and SNP entities within the protocol stack will be most efficient in securing LDACS. MAC and DLS will also receive new tasks (e.g., measures for control channel protection). Security endpoints for secure user data communication and primary entity authentication are the AS and GSC, while the control data plane will be protected between GS and AS. Lastly, GSC and GS will establish a secure connection, prior to any aircraft being able to successfully connecting to the LDACS network. With these measures we can achieve user plane end-to-end security from GSC to AS, provide entity authentication among all parties and introduce key negotiation and derivation functions between relevant parties.

1.4.2 Trust

The LDACS security concept requires all entities in an LDACS network to authenticate to each other to ascertain that only trusted participants can use the system. To establish trust within the network, there are multiple ways to achieve this:

Public Key Infrastructure (PKI)

The general idea of a PKI is the attempt to solve the problem of having to trust a communication's partner identity claim.

A PKI can solve this problem via involving a trusted third party who verifies the identities of the parties who wish to engage in communication via issuing a digital certificate.

The most commonly used digital certificates are X.509 [42] certificates, which contain (1) the issuing Certificate Authority (CA), the (2) CA digital signature, (3) version number, (4) serial number, (5) owner, (6) owner's public key, (7) validity period, (8) certificate usage and (9) signature algorithm. As aviation operates worldwide, a hierarchical PKI will have to be deployed with several sub-CAs being distributed over the world.

Basically there are two proposals on how to achieve worldwide trust coverage [43]:

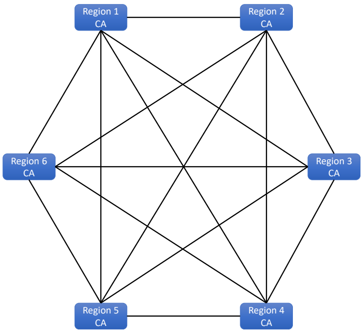


Figure 1.8: Worldwide aeronautical PKI - cross certification [7, 8]

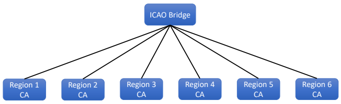


Figure 1.9: Worldwide aeronautical PKI - ICAO trust bridge

One root CA is installed per geographic region and then it performs cross-certification with distributed root-CAs of all other geographic regions around the world. Subdomains can exist within ATM organisations. Here trust emerges from the assured trustworthiness of each regional root CA cross-certifying other and being cross-certified by other regional CAs. This approach is depicted in Fig 1.8.

The other idea is to have one worldwide (probably offline) root CA, hosted by a trusted worldwide entity, such as ICAO, with several regions sub-CAs distributed around the world. That way, the ICAO hosted root CA serves as trust bridge, as seen in Fig 1.9. However, a PKI comes with some drawbacks for digital aeronautical communications:

1. Massive rollout, management, and revocation of certificates are required.
2. A root of trust has to be declared and accepted by state actors worldwide potentially requiring secure cross certification among all countries worldwide respecting political situations and regulations in aviation. Thus, the infrastructure must map to the political reality of aviation which is, that a small number of state actors capable of securing critical infrastructure with limited trust towards the outside. All this makes a PKI possibly not the best solution for a aeronautical trust framework.

With the two drawbacks mentioned PKI may be a challenging solution for an aeronautical trust framework. But keeping in mind that digital data links for civil aeronautical traffic (i.e. AeroMACS) use a PKI as their trust solution [44], it looks promising to use PKI also for LDACS.

The advantage of this way forward is the possible alignment of the LDACS PKI concept with the AeroMACS PKI [44], which is already realised and operational. Furthermore all entities within the FCI should remain interoperable, providing a seamless multi-link concept for aeronautical data, which makes the PKI based trust solutions the most likely one.

Physical Unclonable Function (PUF) Challenge-Response Pair (CRP)

The concept of Physical Unclonable Function (PUF) based trust lies within the property of unclonability of PUFs and thus the uniqueness of PUFs. Hence, a PUF can be interpreted as a unique device's fingerprint, an enabler to create a unique set of CR pairs and a strong random number generator. With a secure database on ground where Challenge Response Pairs (CRP) are stored (and possibly unique per authentication round) a MAKE scheme can be established and trust incorporated into the system based on the trust placed unto the first transmission of CRP and secrecy of CRP. However, the PUFs would have to be installed within the radio hardware during a secure manufacturing process.

1.4.3 Mutual Authentication and Key Exchange (MAKE)

Depending on the method how trust is incorporated into the system there are different approaches for Mutual Authentication and Key Exchange (MAKE) procedures. Overall all procedures need to fulfill the following three objectives:

Mutual Authentication: Both parties can be sure of the identity of the other and that both actually participated in this interaction.

Secure Key Agreement: Both parties have established a shared session key, which means both parties know this key and know that they can use it for a secure communication with the other party for the duration of this session. The key must have never been used before in a session and only the two parties can know it.

Perfect Forward Secrecy: The established session key remains secret, even when the private signing keys of the involved parties have been compromised after this session.

1.4.3.1 Station-to-Station (STS)-MAKE

The origin of LDACS mutual authentication and key exchange protocol, first mentioned in [41], is a variation of the STS protocol [45]. Since the publication of [41], we investigated different STS variants and protocol 5.25 ”Modified STS protocol” in [45] proves to be more secure and concise than that mentioned in [41]. It prevents the possibility of a Man-in-the-Middle attack during the exchange of the key material by signing the respective material with the help of exchanged or pre-stored public key certificates of the respective communication partner. However, in order to ensure trust in public keys from the respective communication partner, a PKI is required [41]. With a PKI and certificates in place, the modified STS protocol becomes a good candidate for mutual authentication and key agreement for LDACS.

STS-MAKE Protocol Run

The LDACS STS-MAKE protocol is illustrated in figure 1.10 and discussed in detail below. The protocol has 5 steps:

Step 1 – Start of STS: After cell entry is done, and the DCH of LDACS is open for authentication purposes, the GSC chooses a secret x and calculates its Diffie-Hellman public key $t_{GSC} = g^x$.

Step 2 – Server Hello Key Exchange: The GSC sends the *ServerHelloKeyExchange* message to the AS. The AS chooses a secret y and calculates its Diffie-Hellman public key t_{AS}. It then calculates the static Diffie-Hellman shared key $S_{AS,GSC} = (g^x)^y \mod p$ and the shared session key $K_{AS,GSC} = KDF(S_{AS,GSC})$ via a predefined Key Derivation Function (KDF) and creates its own signature $Sig_{AS}(t_{AS}, t_{GSC}, ID_{AS}, ID_{GSC})$.

Step 3 – Client Hello Key Exchange: The AS sends now its Diffie-Hellman public key t_{AS} and its signature to the GSC in the *ClientHelloKeyExchange* message. The GSC verifies the AS signature $Sig_{AS}(t_{AS}, t_{GSC}, ID_{AS}, ID_{GSC})$. If that verification passes, at this point the AS is authenticated to the GSC. The GSC proceeds to generate $S_{AS,GSC} = (g^y)^y \mod p$ and $K_{AS,GSC} = KDF(S_{AS,GSC})$ via a predefined KDF.

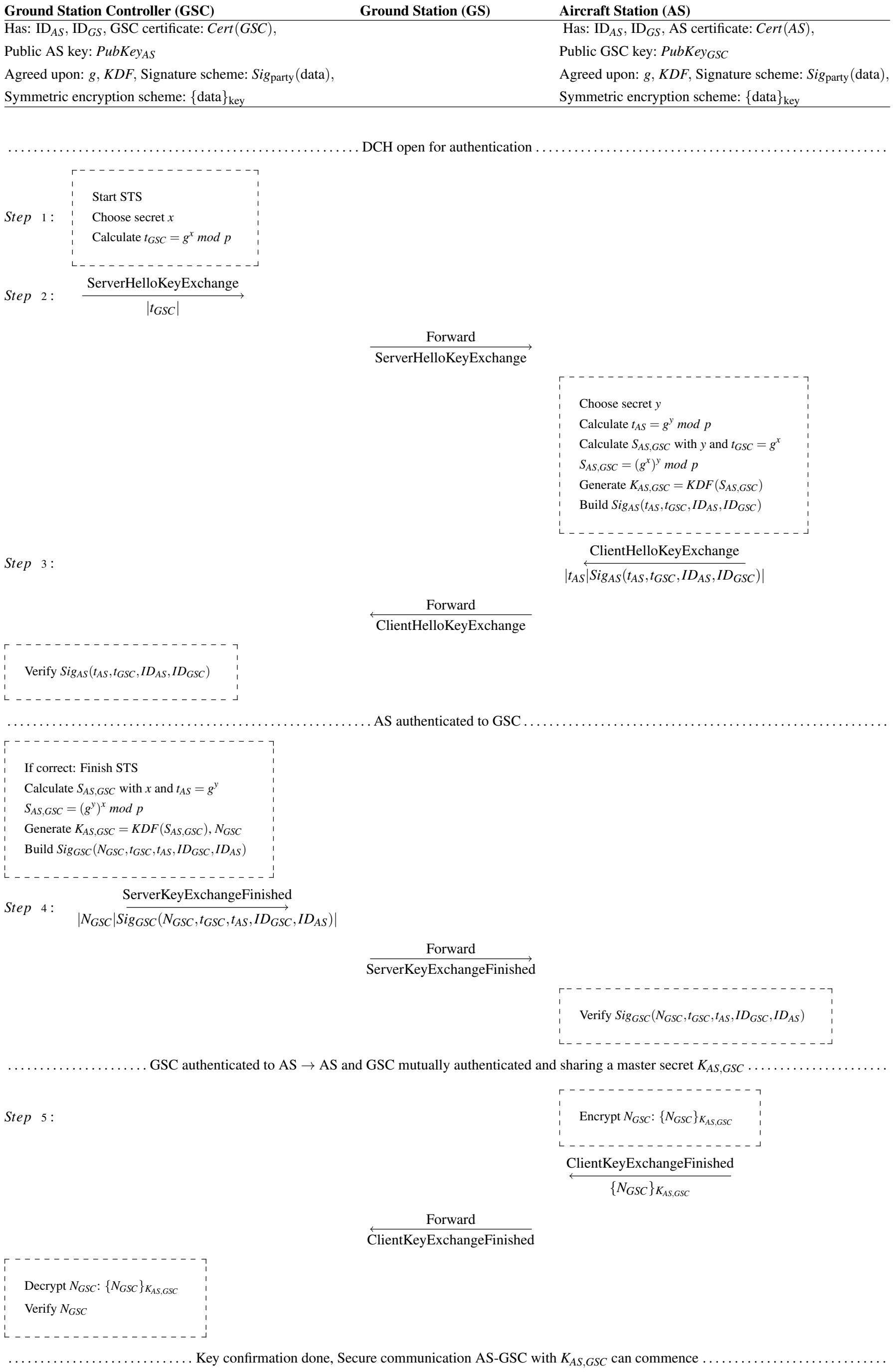

Ground Station Controller (GSC)
Ground Station (GS)
Aircraft Station (AS)
Has: ID_{AS}, ID_{GS}, GSC certificate: $Cert(GSC)$,
Public AS key: $PubKey_{AS}$
Agreed upon: g, KDF, Signature scheme: $Sig_{\text{party}}(\text{data})$,
Symmetric encryption scheme: $\{\text{data}\}_{\text{key}}$
Has: ID_{AS}, ID_{GS}, AS certificate: $Cert(AS)$,
Public GSC key: $PubKey_{GSC}$
Agreed upon: g, KDF, Signature scheme: $Sig_{\text{party}}(\text{data})$,
Symmetric encryption scheme: $\{\text{data}\}_{\text{key}}$
DCH open for authentication
Step 1 :
Start STS
Choose secret x
Calculate $t_{GSC} = g^x \ mod \ p$
Step 2 :
ServerHelloKeyExchange
$|t_{GSC}|$
Forward
ServerHelloKeyExchange
Choose secret y
Calculate $t_{AS} = g^y \ mod \ p$
Calculate $S_{AS,GSC}$ with y and $t_{GSC} = g^x$
$S_{AS,GSC} = (g^x)^y \ mod \ p$
Generate $K_{AS,GSC} = KDF(S_{AS,GSC})$
Build $Sig_{AS}(t_{AS}, t_{GSC}, ID_{AS}, ID_{GSC})$
Step 3 :
ClientHelloKeyExchange
$|t_{AS}|Sig_{AS}(t_{AS}, t_{GSC}, ID_{AS}, ID_{GSC})|$
Forward
ClientHelloKeyExchange
Verify $Sig_{AS}(t_{AS}, t_{GSC}, ID_{AS}, ID_{GSC})$
AS authenticated to GSC
If correct: Finish STS
Calculate $S_{AS,GSC}$ with x and $t_{AS} = g^y$
$S_{AS,GSC} = (g^y)^x \ mod \ p$
Generate $K_{AS,GSC} = KDF(S_{AS,GSC})$, N_{GSC}
Build $Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})$
Step 4 :
ServerKeyExchangeFinished
$|N_{GSC}|Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})|$
Forward
ServerKeyExchangeFinished
Verify $Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})$
GSC authenticated to AS → AS and GSC mutually authenticated and sharing a master secret $K_{AS,GSC}$
Step 5 :
Encrypt N_{GSC}: $\{N_{GSC}\}_{K_{AS,GSC}}$
ClientKeyExchangeFinished
$\{N_{GSC}\}_{K_{AS,GSC}}$
Forward
ClientKeyExchangeFinished
Decrypt N_{GSC}: $\{N_{GSC}\}_{K_{AS,GSC}}$
Verify N_{GSC}
Key confirmation done, Secure communication AS-GSC with $K_{AS,GSC}$ can commence

Figure 1.10: LDACS STS-MAKE Protocol [46]

Now both parties have a shared session key $K_{AS,GSC}$. It then builds another signature tag $Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})$.

Step 4 – Server Key Exchange Finished: The GSC sends its nonce N_{GSC} and signature $Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})$ in the *ServerKeyExchangeFinished* message to the AS. There the AS verifies the GSC signature $Sig_{GSC}(N_{GSC}, t_{GSC}, t_{AS}, ID_{GSC}, ID_{AS})$. If that verification passes, at this point the GSC is authenticated to the AS.

Step 5 – Client Key Exchange Finished: To attain key confirmation, the AS encrypts the nonce N_{GSC}, $\{N_{GSC}\}_{K_{AS,GSC}}$ and sends that in the *ClientKeyExchangeFinished* message to the GSC. At the GSC, the N_{GSC} nonce is decrypted and verified. If that verification step is successful, key confirmation of the key $K_{AS,GSC}$ is achieved.

Choice of Diffie-Hellman Key Exchange (DHKE) Type and Message Sizes
Currently, three different DHKE approaches are considered for the STS-MAKE procedure: Classic, ephemeral DHKE, Elliptic Curve Diffie-Hellmann (ECDH) and Supersingular Isogeny Diffie–Hellman (SIDH). The original DHKE was first published in 1976 and is based on the discrete logarithm or Diffie-Hellman problem [47]. Given a cyclic group G of prime order n, a generator g of G and elements $g^x, g^y \in G$, find g^{xy}. Due to the possibility of Man-in-the-Middle attacks [48], authenticated DHKE schemes (e.g., STS, Internet Key Exchange (IKEv2) and IKE version 2 (IKEv2) protocols [45] were invented.

Elliptic curve cryptography [49] enabled smaller key sizes, resulting in the the ECDH protocol [50]. Based on the conjectured difficulty of finding isogenies between supersingular elliptic curves [51], SIDH finally represents a post-quantum robust version of the DHKE [52, 53].

We define data sizes for the authentication and key agreement messages here for the STS for LDACS protocol. For signatures lengths, we assume a total length of 64 Byte for a message signature, produced by current signature procedures such as EdDSA-Ed25519 [54] or even post-quantum procedures such as rainbow [55].

All messages have a header consisting of $TYPE$, ID, UA and $PRIO$ fields. $TYPE$ is a 4 Bit long field and clarifies the message type, ID is 12 Bit long and denotes the ID of that message, UA is the 28 Bit long Unique Address field, containing the LDACS specific addresses of AS and GS and finally the 4 Bit long $PRIO$ field signifies the priority this particular message has. We collect all these fields into the *header* resulting in a 48 Bit length. A nonce N is of length 96 Bit. t_{GSC} and t_{AS} are the Diffie-Hellman public keys of the respective entities and have different sizes, depending on the choice of the Diffie-Hellman procedure. The sizes for the Diffie-Hellman public key of the GSC t_{GSC} are: $\{DHKE = 3072|ECDH = 256|SIDH = 2624\}$. The sizes for the Diffie-Hellman public key of the AS t_{AS} are: $\{DHKE = 3072|ECDH = 256|SIDH = 2640\}$.

The *ServerHelloKeyExchange* message, responsible to initiate the STS protocol between AS and GSC consists of the *header* and the Diffie-Hellman public key of the GSC t_{GSC}. Depending on the size of the public keys, the sizes for the *ServerHelloKeyExchange* are $\{3120, 304, 2672\}$ Bit. The key exchange message AS to GSC is denoted as *ClientHelloKeyExchange* and consists of the *header*, the Diffie-

Hellman public key of the AS t_{AS} and an AS signature Sig_{AS}. Depending on the size of the Diffie-Hellman public keys, the sizes for *ClientHelloKeyExchange* are $\{3632, 816, 3200\}$ Bit.

Table 1.2: Message sizes for STS-MAKE in *bit*

Message	STS-DHKE	STS-ECDH	STS-SIDH
Step 2	3120	304	2672
Step 3	3632	816	3200
Step 4	656	656	656
Step 5	144	144	144
Total	7552	1920	6672

The *ServerKey ExchangeFinished* consists of the *header*, a nonce N_{GSC}, and a GSC signature Sig_{GSC}, totalling in 652 Bit. Finally the *ClientKeyExchangeFinished* finishes the protocol and simply contains a header and the encrypted nonce N_GSC, resulting in 144 Bit. Overall this leads to a total amount of authentication bits shown in Table 1.2.

Please note, the STS-MAKE for LDACS was proven to fulfill the three objectives for LDACS MAKE protocols, mentioned at the beginning of the chapter, using the model checker Tamarin [56].

1.4.3.2 Physical Unclonable Function based Mutual Authentication and Key Exchange (PMAKE)

As mentioned in Section 1.4.2, due to several reasons, PKI based MAKE protocols might hold several disadvantages due to the political reality in aviation, that is, a small number of dominant state actors are capable of securing critical infrastructure and have limited trust towards others.

To address this problem, we proposed the use PUFs within LDACS radios to generate device unique CRPs, used in PMAKE for mutual authentication. PUFs use device unique random patterns, which are introduced in the manufacturing process to differentiate chips and make them uniquely identifiable. In other words, a PUF can be interpreted as a unique device's fingerprint, an enabler to create a unique set of cr pairs and a strong random number generator.

PMAKE Protocol Run

Instead of the establishment of a PKI, (1) very mobile node (aircraft) has to be equipped with a PUF during the construction process of the specific LDACS radio device and (2) an initial CRP has to be exchanged between aircraft and ground based secure verification database in a secure environment. At the end of this initial exchange, the secure database within the GSC securely stores the CRP $< C_{AS_0}, R_{AS_0} >$ and the AS stores $< C_{AS_0} >$. The main part of the protocol is depicted in Fig. 1.11.

Step 1: The AS, upon receiving such a beacon, generates a random number r_{AS} and depending on the respectively chosen DHKE procedure, it calculates t_{AS} and $\alpha = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$. It then responds with $|t_{AS} \oplus C_{AS_0}|\alpha|\mathrm{ID}_{AS}|$.

Step 2: Once the GS receives the response to the beacon message, it appends its ID to the message and forwards $|t_{AS} \oplus C_{AS_0}|\alpha|\mathrm{ID}_{AS}|\mathrm{ID}_{GS}|$ to the GSC.

Table 1.3 Notations used in the PMAKE scheme

Notation	**Definition**
msg1 $\oplus$ msg2	XOR operation on msg1 with msg2
msg1 | msg2	Concatenation operation on msg1 with msg2
PUF_A	Physical Unclonable Function of entity A
$\text{HMAC}_K(msg)$	Hash-based Message Authentication Code with key K and input data *msg*
$\text{HKDF}(K)$	HMAC Key Derivation Function (HKDF) with input K
C_{A_i}	i-th Challenge for PUF from entity A
R_{A_i}	i-th Response from PUF from entity A
ID_A	Identifier of entity A
r_A	Random integers of entity A ”Ephemeral private key”
t_A	Ephemeral public key of entity A
g	Public Diffie-Hellman parameters
$S_{AS,GSC}$	Static Diffie-Hellman key shared between AS and GSC
$K_{AS,GSC}$	Session key for AS-GSC communications
$\{msg\}_K$	Symmetric encryption of data *msg* with key K
N_A	Nonce of entitiy A

Step 3: With the help of the previously stored tuple $< C_{AS_0}, R_{AS_0} >$, the GSC can compute the Diffie-Hellman public key of the AS $t_{AS} = t_{AS} \oplus C_{AS_0} \oplus C_{AS_0}$ and $\alpha' = HMAC_{R_{AS_0}}(\text{ID}_{AS}, \text{ID}_{GS}, t_{AS})$. It then checks whether $\alpha' == \alpha$ match. If that is the case, the AS has authenticated to the GSC. Then the GSC generates a random number r_{GSC} of its own and again in dependence on the previously agreed DHKE procedure, calculates t_{GSC}. Now the shared AS-GSC key $S_{AS,GSC}$ can be calculated via the secret of the GSC r_{GSC} and the Diffie-Hellman public key of the AS t_{AS}. With that, the GSC calculates the session key $K_{AS,GSC}$ via the HKDF and $S_{AS,GSC}$. Finally a new challenge C_{AS_1} is chosen by the GSC and two new MAC tags are calculated. β is used to conceal C_{AS_1}, while γ serves as authenticity proof about the GSC for the AS. It finally sends $|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|\text{ID}_{GSC}|$ to the GS.

Step 4: The GS forwards that message to the AS.

Step 5: First the AS calculates the Diffie-Hellman public key of the GSC via $t_{GSC} = t_{GSC} \oplus t_{AS} \oplus t_{AS}$. To be able to decipher C_{AS_1}, β' is calculated by the AS by reconstructing R_{AS_0} and using previously established values t_{GSC}, t_{AS}, ID_{GSC}, ID_{GS}, ID_{AS}. As $C_{AS_1} = \beta \oplus C_{AS_1} \oplus \beta'$ the AS successfully received the new challenge C_{AS_1}. It then calculates its own value for $\gamma' = HMAC_{R_{AS_0}}(C_{AS_1})$ and compares $\gamma' = \gamma$. If they match, the GSC has authenticated to the AS. Furthermore the verifiable integrity and return of t_{AS} proves to the AS, that the GSC actually participated in the protocol. Now the AS calculates the shared key $S_{AS,GSC}$ with r_{AS} and t_{GSC} and derives the session key $K_{AS,GSC} = HKDF(S_{AS,GSC})$. Via the AS PUF a new response R_{AS_1} is

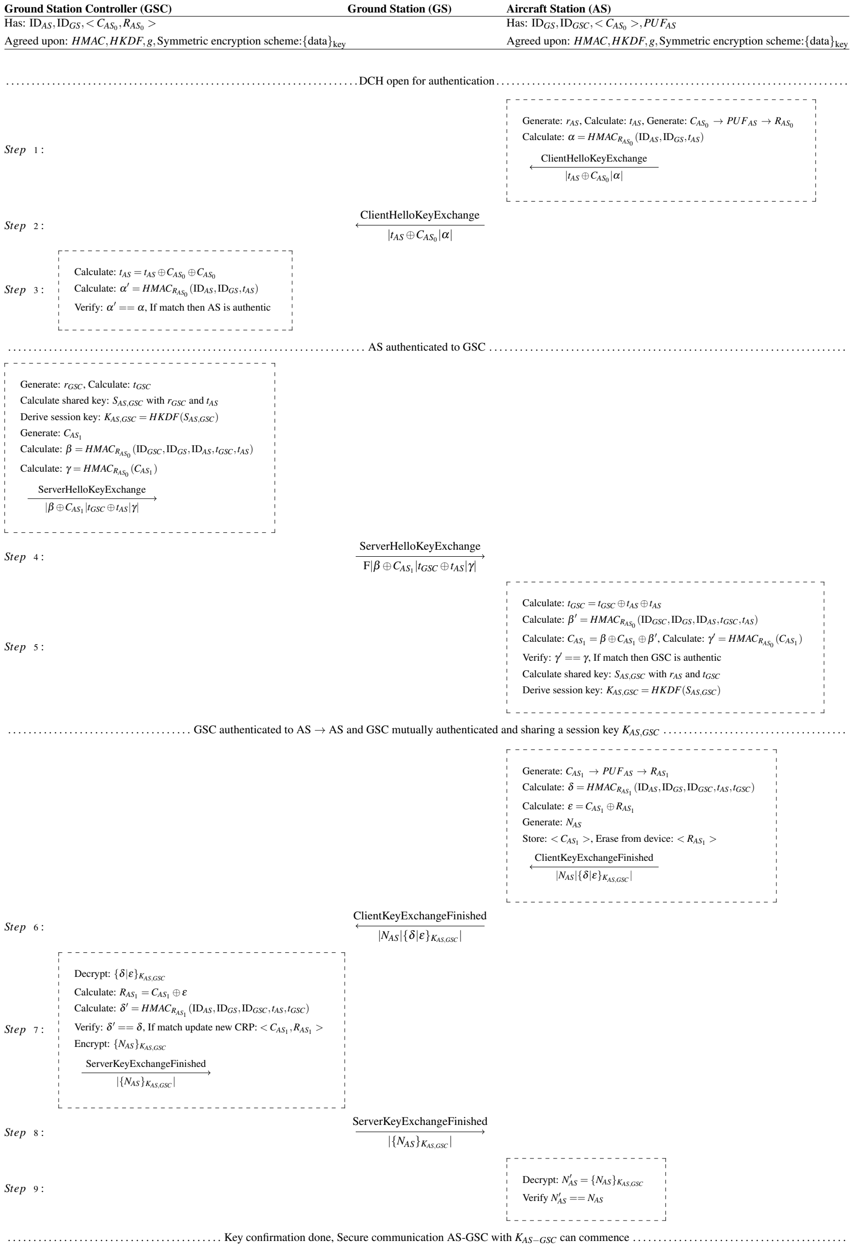

Ground Station Controller (GSC)
Ground Station (GS)
Aircraft Station (AS)
Has: $\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, < C_{AS_0}, R_{AS_0} >$
Has: $\mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, < C_{AS_0} >, PUF_{AS}$
Agreed upon: $HMAC, HKDF, g,$ Symmetric encryption scheme: $\{\mathrm{data}\}_{\mathrm{key}}$
Agreed upon: $HMAC, HKDF, g,$ Symmetric encryption scheme: $\{\mathrm{data}\}_{\mathrm{key}}$
DCH open for authentication
Step 1 :
Generate: r_{AS}, Calculate: t_{AS}, Generate: $C_{AS_0} \rightarrow PUF_{AS} \rightarrow R_{AS_0}$
Calculate: $\alpha = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$
ClientHelloKeyExchange
$|t_{AS} \oplus C_{AS_0}|\alpha|$
Step 2 :
ClientHelloKeyExchange
$|t_{AS} \oplus C_{AS_0}|\alpha|$
Step 3 :
Calculate: $t_{AS} = t_{AS} \oplus C_{AS_0} \oplus C_{AS_0}$
Calculate: $\alpha' = HMAC_{R_{AS_0}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, t_{AS})$
Verify: $\alpha' == \alpha$, If match then AS is authentic
AS authenticated to GSC
Generate: r_{GSC}, Calculate: t_{GSC}
Calculate shared key: $S_{AS,GSC}$ with r_{GSC} and t_{AS}
Derive session key: $K_{AS,GSC} = HKDF(S_{AS,GSC})$
Generate: C_{AS_1}
Calculate: $\beta = HMAC_{R_{AS_0}}(\mathrm{ID}_{GSC}, \mathrm{ID}_{GS}, \mathrm{ID}_{AS}, t_{GSC}, t_{AS})$
Calculate: $\gamma = HMAC_{R_{AS_0}}(C_{AS_1})$
ServerHelloKeyExchange
$|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|$
Step 4 :
ServerHelloKeyExchange
$\mathrm{F}|\beta \oplus C_{AS_1}|t_{GSC} \oplus t_{AS}|\gamma|$
Step 5 :
Calculate: $t_{GSC} = t_{GSC} \oplus t_{AS} \oplus t_{AS}$
Calculate: $\beta' = HMAC_{R_{AS_0}}(\mathrm{ID}_{GSC}, \mathrm{ID}_{GS}, \mathrm{ID}_{AS}, t_{GSC}, t_{AS})$
Calculate: $C_{AS_1} = \beta \oplus C_{AS_1} \oplus \beta'$, Calculate: $\gamma' = HMAC_{R_{AS_0}}(C_{AS_1})$
Verify: $\gamma' == \gamma$, If match then GSC is authentic
Calculate shared key: $S_{AS,GSC}$ with r_{AS} and t_{GSC}
Derive session key: $K_{AS,GSC} = HKDF(S_{AS,GSC})$
GSC authenticated to AS → AS and GSC mutually authenticated and sharing a session key $K_{AS,GSC}$
Generate: $C_{AS_1} \rightarrow PUF_{AS} \rightarrow R_{AS_1}$
Calculate: $\delta = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$
Calculate: $\varepsilon = C_{AS_1} \oplus R_{AS_1}$
Generate: N_{AS}
Store: $< C_{AS_1} >$, Erase from device: $< R_{AS_1} >$
ClientKeyExchangeFinished
$|N_{AS}|\{\delta|\varepsilon\}_{K_{AS,GSC}}|$
Step 6 :
ClientKeyExchangeFinished
$|N_{AS}|\{\delta|\varepsilon\}_{K_{AS,GSC}}|$
Step 7 :
Decrypt: $\{\delta|\varepsilon\}_{K_{AS,GSC}}$
Calculate: $R_{AS_1} = C_{AS_1} \oplus \varepsilon$
Calculate: $\delta' = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$
Verify: $\delta' == \delta$, If match update new CRP: $< C_{AS_1}, R_{AS_1} >$
Encrypt: $\{N_{AS}\}_{K_{AS,GSC}}$
ServerKeyExchangeFinished
$|\{N_{AS}\}_{K_{AS,GSC}}|$
Step 8 :
ServerKeyExchangeFinished
$|\{N_{AS}\}_{K_{AS,GSC}}|$
Step 9 :
Decrypt: $N'_{AS} = \{N_{AS}\}_{K_{AS,GSC}}$
Verify $N'_{AS} == N_{AS}$
Key confirmation done, Secure communication AS-GSC with K_{AS-GSC} can commence

Figure 1.11: PMAKE protocol [57]

generated to the new challenge C_{AS_1} via $C_{AS_1} \rightarrow PUF_{AS} \rightarrow R_{AS_1}$. It then calculates $\delta = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$ that will be used by the GSC as proof for the authenticity and correctness of the new response R_{AS_1}. $\varepsilon = C_{AS_1} \oplus R_{AS_1}$ is used to conceal the response R_{AS_1} during transport. For key confirmation purposes, the AS generates a nonce N_{AS}. At this point, the AS securely stores C_{AS_1} and erases R_{AS_1} from memory. As AS and GSC have previously agreed upon suitable encryption algorithms, the AS sends N_{AS} in the clear and δ and ε encrypted with $K_{AS,GSC}$ back to the GSC.

Step 6: The GS forwards that message to the GSC.

Step 7: The GSC decrypts the message with the agreed upon encryption algorithm and key $K_{AS,GSC}$. It then computes $R_{AS_1} = C_{AS_1} \oplus \varepsilon$. It then calculates $\delta' = HMAC_{R_{AS_1}}(\mathrm{ID}_{AS}, \mathrm{ID}_{GS}, \mathrm{ID}_{GSC}, t_{AS}, t_{GSC})$ and checks whether $\delta' == \delta$. If that is the case, the GSC can be sure of the authenticity of the response R_{AS_1} and the participation of AS in the protocol. It updates the current tuple for that AS to $< C_{AS_1}, R_{AS_1} >$. It then encrypts N_{AS} and sends it back to the AS.

Step 8: The GS forwards that message to the AS.

Step 9: Finally the AS decrypts $N'_{AS} = \{N_{AS}\}_{K_{AS,GSC}}$ and compares $N'_{AS} == N_{AS}$. If they match, AS is assured that GSC also holds the shared key, key confirmation was successful and user data communication can commence.

PMAKE Data Overhead

Again, in analogy to the previous description of message sizes for STS-MAKE, we assign amounts of bits to the different messages.

Table 1.4 Message sizes for PMAKE in bit

Message	**PMAKE-DHKE**	**PMAKE-ECDH**	**PMAKE-SIDH**
Step 1	3276	460	2844
Step 3	3404	588	2956
Step 5	400	400	400
Step 7	144	144	144
Total	7224	1592	6344

We assume the same sizes as before, so *header* = 48 Bit, all IDs = 28 Bit, nonces $N_{AS} = 96$ Bit, MAC tag (c.f., $\alpha, \beta, \gamma, \delta, \varepsilon$)= 128 Bit, Diffie-Hellman public key sizes for t_{GSC}: $\{DHKE = 3072|ECDH = 256|SIDH = 2624\}$, Diffie-Hellman public key sizes for t_{AS}: $\{DHKE = 3072|ECDH = 256|SIDH = 2640\}$. We show all PMAKE message sizes in Table 1.4.

1.4.4 Key Derivation

One all parties within the network have successfully authenticated to each other, key derivation is necessary to generate different keys for different purposes. For example, we need keys for user data protection and keys for control data protection.

HKDF
As shown in Fig. 1.10 and Fig.1.11, we use the HKDF, a KDF built from Hash-based Message Authentication Codes (HMAC). It uses the ”extract-then-expand” paradigm, meaning that it consists of two main phases.

First the input keying material (here: master key/static Diffie Hellman shared key) is taken and a fixed-length pseudo-random key is extracted. The extract phase is especially important, if the master key is not sufficiently uniform (e.g. the key is uniform only in a subset of the original key space). In that case, we extract a pseudo random key from the master key by adding a salt value, which can be any fixed non-secret string chosen at random. In the process the pseudo random key becomes indistinguishable from a uniform distribution of bits. In general, HKDF can be used with or without salt value, both variations work, however the use of salt significantly increase the strength of HKDF. Salt ensures independence between different uses of the hash function, supports ”source-independent” extraction, and strengthens the analytical results that back the HKDF design [58].

User Data Protection Keys
Also depending on the algorithm choice for securing user data on the datalink, we need either one symmetric key (e.g., for AES-GCM [59], which allows integrity and confidentiality protection) or two symmetric keys for integrity and confidentiality protection.

Control Data Protection Keys
As discussed before in Section 1.2.6, securing the control plane of LDACS proves more difficult than its user plane. The underlying problems are very small chunks of data (e.g., RL DCCH: 83 Bit) and the need that every aicraft within one LDACS cell can read the entire control data plane of LDACS. Thus using individual AS specific keys for securing the CCCH, DCCH channels is not possible. We do not put additional cryptographic protection on the Random Access Control Channel (RACH) or bçch, as if any spoofer or attacker sending information within those data links is detected and filtered out during the MAKE procedure of LDACS. As the data on the DCCH is mainly responsible to enable an AS to request data allocations, such that it can send user data and the CCCH being the logical channel, via which those resources are granted, integrity protection of these is most important to prevent any attacker redistributing LDACS resources.

The only possible way to meet all these requirements, is via introducing group key mechanisms for LDACS. We are currently investigating and comparing the suitability of the Group-IKEv2 [60], Chinese Remainder Group Key (CRGK) [61], Central Authorized Key Extension (CAKE) [62] and Logical Key Hierarchy (LKH) protocol [63] for LDACS. This process is ongoing work and has not concluded yet.

1.4.5 User Data Security

After the MAKE procedure and with the key derivation of user keys, the user data plane of LDACS can be secured.

We propose to secure LDACS SN-PDUs, thus Packet Data Uni (PDU)s on the SNP, as their size can vary from 128 to 1536 Byte [29], which makes them possibly the largest PDUs within LDACS. This helps minimizing security data overhead, in case a Message Authentication Code (MAC) tag is attached to the SN-PDU.

Confidentiality Protection
We suggest using symmetric approaches for data encryption, due to low computational overhead and fast operation times. We propose to establish end-to-end encryption for e.g., Aeronautical Operational Control (AOC) data between GSC and AS. After extensive discussion with representatives of ATC instances, it became apparent, that ATS data will probably not be encrypted, as every air traffic controller operating in the area should be able to read that data for safety reasons. Thus, between layer 3 and the LDACS sublayer, some notification of the content of the packet will be necessary. As encryption algorithm, we recommend AES-256-GCM [59] with Galois Counter Mode (GCM) being a mode of operation on symmetric key block. It provides authenticated encryption and decryption operations and it proves robust against currently known quantum-computer-based algorithms [64]. The last property is important, as due to the long service life of aeronautical communications, this rising threat might become dangerous during its life cycle.

Integrity Protection
All user data, sent via LDACS, requires some kind of integrity protection mechanism. We propose two mutually exclusive strategies:

AES-GCM Galois Counter Mode is a mode of operation for symmetric key cryptographic block ciphers (i.e., here: AES). It supports two operations: authenticated encryption and decryption. If only message authentication is required, the variation Galois Message Authentication Code (GMAC) can be used. After the application of this operation mode, we are left with a ciphertext C of exactly the same length as the plaintext P and an authentication tag T of 128 Bit length. However [65] defines tag sizes of 128, 120, 112, 104, or 96, 64 and 32 Bit length, with a clear recommendation to use 96 Bit or more.

HMAC Here, the idea is to combine the Keyed-Hash Message Authentication Code (HMAC) message authentication mechanism [66] and combine it with hash-functions from the SHA-3 hash-family [67]. We propose HMAC-SHA3-128, that way, we are left with a plaintext P and a message tag T of 128 Bit length.

1.4.6 Control Data Security

As described in depth in Section 1.4.4, securing the control data plane of LDACS proves to be far more complicated than its user plane. Reasons for this are far smaller message sizes (c.f., DC: 83 Bit, CC: 728 Bit), the need, that every participant within an LDACS cell need to be able to (1) read its contents and (2) be assured of their authenticity.

That way, it is clear, that we need control data integrity and not necessarily confidentiality. This leaves us with the problem, that a simple message tag simply does not fit in the small control messages. Even if we shrink the tag size to e.g., 32 Bit, radically reducing the security level, the capacity of LDACS would be also reduced drastically, as fewer resources could be requested and allocated, due to the reduced configuration data space left within the messages.

Securing FL control plane data is easier than its RL counterpart, as the GS can send a continuous stream of OFDM symbols on the FL and is thus the only entity putting data on the CCCH. Assuming a group key has been negotiated within the group of one GS and all AS within that particular LDACS cell, that key can be used by the GS to add a small message tag to a CC-PDU. Assuming a 64 Bit tag to be sufficiently secure, this still results in a $64/728 = 8,8\%$ overhead.

On the other direction, every AS requests resources on the DCCH, thus every aircraft contributes DC-PDUs and every one is 83 Bit long. With that size, and given that only 8 Bit are currently reserved for padding [29], applying a message tag per DC-PDU is impossible.

This topic, altogether with the investigation of group key procedure for LDACS is currently ongoing and will have to be solved before the LDACS security architecture can be finalized.

1.4.7 Changes within the LDACS Protocol Stack

At the beginning of that chapter, we discussed placement of security functionality within the LDACS protocol stack. After having described the entire process of how trust is handled, options for entity authentication and key exchange, key derivation, user data and control data protection, we want to assign all these tasks to certain entities within the LDACS protocol stack.

In Fig. 1.12, we have added security relevant states and functionality, marked in red, within the LDACS protocol stack. As said at the beginning of this chapter, LME and SNP are the two most important, security related entities. The LME handles the entire connection establishment and now MAKE procedure, together with key negotiation, derivation, handover and secure logging. It is also responsible for protecting control channel data. The SNP, after the MAKE procedure is over and it has received the user data session key from the LME handles user data protection.

Also one important factor are the CoS of LDACS: After initial connection establishment and during the MAKE procedure, the DLS and SNP only allow packets of the highest priority (i.e., CoS=7) to pass through to the LME for authentication purposes. No other data packet is able to pass through, before the LME has not successfully completed the entire MAKE procedure, with session keys being deployed at LME for control data protection and SNP for user data protection.

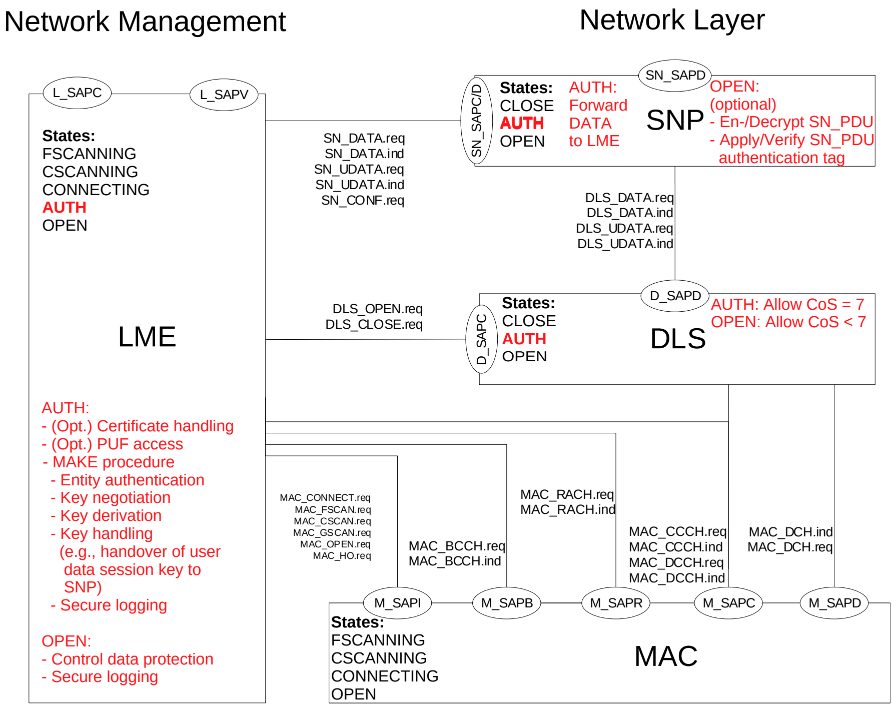


Figure 1.12: Security related changes within the LDACS protocol stack

1.5 Evaluation of the LDACS Cybersecurity Architecture

The cybersecurity measures of LDACS were evaluated in [11, 68, 46, 57]. Here we want to present evaluations (1) in a theoretical model for LDACS security data and latency overhead, (2) modelled in an event based simulation framework Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS) and (3) actual flight trials.

1.5.1 Theoretical Model for LDACS Security Latency Overhead

In 2015, Gräupl et al. [69] presented a full methodology on how to emulate latencies for user data in the forward and reverse link of LDACS depending on the Bit Error Rate (BER) and message size.

Taking re-transmissions into account, the FL latency can be calculated with

$$L_{FL}(t) = m_{FL}(t) + (1 + \delta_{RX}(1+n)) \times d_{MF} \tag{1.1}$$

and the RL latency with

$$L_{RL}(t) = m_{RL}(t) + (2 + \delta_{RX}(N+3)) \times d_{MF}. \tag{1.2}$$

Table 1.5 Parameter values for latency timing for the LDACS MAC protocol [46]

Forward Link Model (Eq. 1.1)		**Reverse Link Model (Eq. 1.2)**	
Parameters	**Values**	**Parameters**	**Values**
d_{MF}	60ms	d_{MF}	60ms
$m_{FL}(t)$	Time until start of next FL MF: Every 1 to 60ms modelled by $U(1,60)$	$m_{RL}(t)$	Average time until start of next MAC cycle: $\#AS/32 \times d_{MF} + wait$ $wait$ modelled by $U(1,60)$
n	Average amount of MF after transmission until next DC slot is scheduled for AS in MAC-cycle: $n = \#AS/32$	N	Average amount of MFs after transmission until next DC slot is scheduled for AS: $N = (\#AS/32 - 3) \mod \#AS/32$
BER	$10^{-6}, 10^{-5}$		
P	$P(\{\text{no error in packet}\}) = (1 - BER)^l$ $P(\{\text{error in packet}\}) = 1 - ((1 - BER)^l)$		

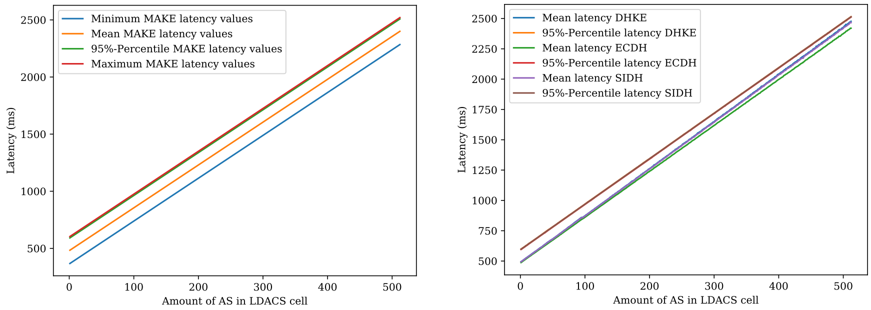
In Equation 1.1, we use $m_{FL}(t)$ to classify the time until the start of the next CC frame, $\delta_{RX} \in \{0,1\}$ to indicate a re-transmission, d_{MF} denotes the length of a MF and n is derived from the length of the reverse link medium access cycle from forward link perspective.

In Equation 1.2, we use $m_{RL}(t)$ to denote the time until the start of next DC slot, $\delta_{RX} \in \{0,1\}$ to indicate a re-transmission, d_{MF} denotes the length of a MF and N is derived from the length of the reverse link medium access cycle from reverse link perspective.

We model $\delta_{RX} \in \{0,1\}$ as stochastic process, based on the packet error rate. Given a BER, we can calculate the packet error rate based on the length of a packet l: $P(\{\text{no error in packet}\}) = (1 - BER)^l$. Thus the opposite event, that a packet indeed contains an error is: $P(\{\text{error in packet}\}) = 1 - ((1 - BER)^l)$. These two probability decide the value of δ_{RX}, whether a re-transmission is necessary and, thus, an error appeared in the packet, or not.

For more details on the model, please refer to [69] and [46].

With these equations, we calculate LDACS authentication latencies based on the amount of AS within an LDACS cell. We see these results in Fig. 1.13.



(a) Authentication latency at $BER = 0$

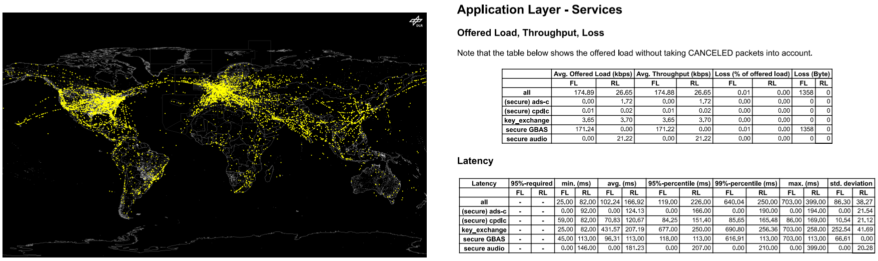
(b) Authentication latency at $BER = 10^{-5}$

Figure 1.13: Authentication baseline latency at $BER = 0$ vs. authentication latency at worst case scenario of $BER = 10^{-5}$.

Please note that due to the similar message sizes, PMAKE and STS-MAKE have almost equal authentication latencies. Both authentication procedures finish quicker with smaller message sizes at higher BER, thus ECDH finishes faster than SIDH, which in turn finishes faster than DHKE. The requirements document DO-350A imposes a $RCTP_{CSP} = 10s$ threshold for RCP 130/A1 message types [70], meaning that all authentication and connection establishment must be completed below the 10s threshold [29]. As we clearly see in Fig. 1.13, we always remain below this threshold, even when an LDACS cell is full.

1.5.2 Model within FACTS2 Simulation Framework

Another important way of evaluating changes within the LDACS protocol is rapid prototyping with software based simulations. FACTS [71] is a simulation framework based on modern, service-oriented software architecture: Simulation services organized in a parallelized toolchain of loosely coupled software services split by the separation of concerns. It allows for the simulation of infrastructure, generation of aeronautical data traffic, simulation of flight patterns or parsing of real-world flight patterns, simulation of arbitrary aeronautical data links and protocols and more. Every tool is tasked with one task (e.g., simulating the LDACS datalink) and multiple tools can be piped together, using Unix pipes on the command line. In Fig. 1.14, we see first worldwide air traffic movement, then FACTS simulates realistic air traffic data, simulates LDACS as underlying datalink and outputs a report on the performance of the datalink.



Application Layer - Services

Offered Load, Throughput, Loss

Note that the table below shows the offered load without taking CANCELED packets into account.

	Avg. Offered Load (kbps)		Avg. Throughput (kbps)		Loss (% of offered load)		Loss (Byte)	
	FL	RL	FL	RL	FL	RL	FL	RL
all	174.89	26.65	174.88	26.65	0.01	0.00	1358	0
(secure) ads-c	0.00	1.72	0.00	1.72	0.00	0.00	0	0
(secure) cpdlc	0.01	0.02	0.01	0.02	0.00	0.00	0	0
key_exchange	3.65	3.70	3.65	3.70	0.00	0.00	0	0
secure GBAS	171.24	0.00	171.22	0.00	0.01	0.00	1358	0
secure audio	0.00	21.22	0.00	21.22	0.00	0.00	0	0

Latency

Latency	95%-required		min. (ms)		avg. (ms)		95%-percentile (ms)		99%-percentile (ms)		max. (ms)		std. deviation	
	FL	RL	FL	RL	FL	RL	FL	RL	FL	RL	FL	RL	FL	RL
all	-	-	25.00	82.00	102.24	166.92	119.00	226.00	640.04	250.00	703.00	399.00	86.30	38.27
(secure) ads-c	-	-	0.00	92.00	0.00	124.13	0.00	166.00	0.00	190.00	0.00	194.00	0.00	21.54
(secure) cpdlc	-	-	59.00	82.00	70.83	120.67	84.25	151.40	85.65	165.48	86.00	169.00	10.54	21.12
key_exchange	-	-	25.00	82.00	431.57	207.19	677.00	250.00	690.80	256.36	703.00	258.00	252.54	41.69
secure GBAS	-	-	45.00	113.00	96.31	113.00	118.00	113.00	616.91	113.00	703.00	113.00	66.61	0.00
secure audio	-	-	0.00	146.00	0.00	181.23	0.00	207.00	0.00	210.00	0.00	399.00	0.00	20.28

(a) Graphical output of worldwide air traffic

(b) Output of LDACS measurement report

Figure 1.14: Two important capabilities of FACTS: (1) visual output of air traffic movement (2) measurement reports on the performance of tested datalinks [71]

In [68], we used FACTS to demonstrate a proof of concept of the user data security architectural concept of LDACS. Results proved, that the implementation concept with the "auth" state within protocol entities and different classes of service, with the highest priority class reserved for authentication purposes, works as intended. Thus authentication, key exchange, derivation and handover were performed and SN-PDUs could be secured via the AES-256-GCM algorithm and the negotiated, shared session keys as described in Section 1.4.7.

1.5.3 Real World Demonstration of LDACS Security Features

Lastly, during the German national project Migration towards COm/NAV capabilities of LDACS (MICONAV) in March/April 2019, we could demonstrate some security features of LDACS in the worldwide first LDACS flight trials. Fig. 1.15 shows the research aircraft used in the flight trials, a Falcon 20-E5, together with the position of the L-band antenna.

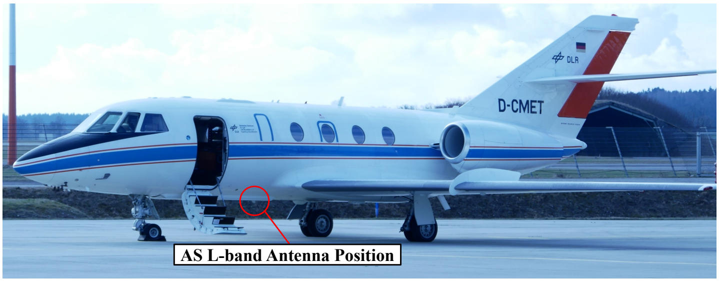
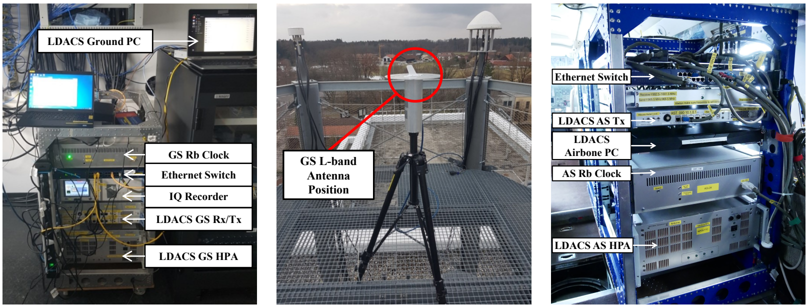


Figure 1.15: DLR's research aircraft Falcon 20-E5 (D-CMET) [36]

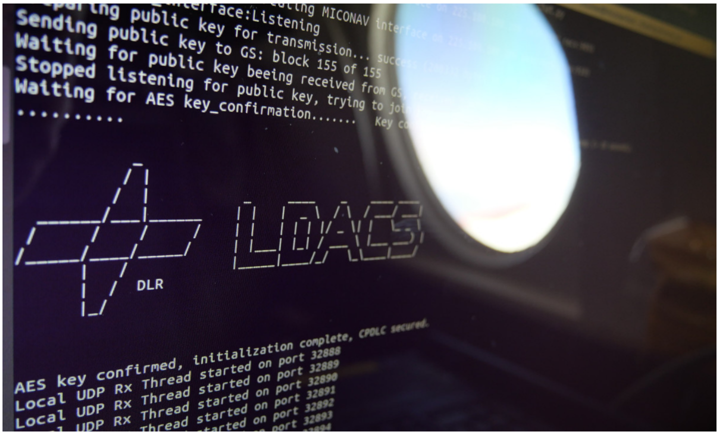
In Fig.1.16a and in Fig. 1.16b, we show the LDACS GS demonstration setup and in Fig. 1.16c the AS LDACS demonstration equivalent.



(a) LDACS ground station (b) LDACS antenna (c) Airborne equipment

Figure 1.16: Overview of airborne and ground LDACS equipment [36]

With pre-installed certificates at the AS and GS, we demonstrated a key encapsulation procedure based on the post-quantum robust public-key cryptosystem McEliece [72]. Using this negotiated session key as a result, we encrypted any actual data, such as text messages, CPDLC messages, ADS-C messages for AS positioning with the aforementioned AES-256-GCM symmetric cryptosystem. With data gained during the actual flight, we can confirm, that the chosen MAKE procedure itself remained below the required $RCTP_{CSP} = 10s$ threshold for RCP 130/A1 message types [70]. Overall we performed 19 key exchanges and observed a mean key exchange time of 508.15 ms and a 95-percentile of 513.13 ms. This matches the values presented in Fig. 1.13 with just one AS in an LDACS cell very well and is a strong indicator for the accuracy of the theoretical model and the FACTS simulation.



```
...ing public ...erface:Listening ...ing MICONAV interface
Sending public key for transmission... success
Waiting for public key to GS: block 155 of 155
Stopped listening for public key beeing received from GS
Waiting for AES key_confirmation.......  Key co
..........
```

```
AES key confirmed, initialization complete, CPDLC secured.
Local UDP Rx Thread started on port 32888
Local UDP Rx Thread started on port 32889
Local UDP Rx Thread started on port 32890
      UDP Rx Thread started on port 32891
              started on port 32892
                              32893
                              32894
```

Figure 1.17: Console output during after successful key exchange. All further communication afterwards was secured using AES-256-GCM.

In Fig. 1.17, we see the console output of a successful key exchange and with secured communications channel opened, aboard the Falcon 20-E5 during MICONAV.

1.6 Conclusion

This work presents a summary of the design of the LDACS cybersecurity concept. We introduce the FCI and the current state of cybersecurity in digital aeronautical communications, which is that especially on legacy datalinks (i.e., ADS-B, VDLm2) there is no information security based on the definitions from the internet security glossary RFC 4949. We continue with a presentation of relevant technical details about LDACS and then with a threat- and risk analysis, defining security requirements, objectives and functions. We start the section on the LDACS cybersecurity architecture with different trust approaches, a PKI and a PUF CRP based, then continue with two MAKE procedure based on these trust solutions. We propose the use of AES-GCM for user data protection, and state out reasons, why integrity is more important than confidentiality. On the security for control plane data, we are investigating the use of group-key procedure, however this is still a work in progress. Finally we finish with a compete integration of the security additions within the LDACS protocol stack. In the evaluation, we show, that both MAKE procedures finish far below the required latency threshold and only put up to 1 kB of additional security data on the link. Also via analytical evaluation, a software event-based simulation, and flight trials, we present a first proof-of-concept of LDACS cybersecurity.

Future work aims to solve the open problem of control channel security of LDACS by investigating different group key procedures and different approaches on guaranteeing integrity of control data. Also proving the semantic correctness and soundness of LDACS protocol security with model checkers such as Tamarin, Scyther or ProVerif is an important step in the validation of LDACS cybersecurity features. Finally, further flight trials are planned for 2022, where the entire cybersecurity concept can be validated in flight trials on more advanced LDACS prototype hardware.

All candidates within the FCI require strong cybersecurity features. We agree with this requirement as we strongly believe, cybersecurity is the enabler in the future automation of civil air traffic. As LDACS is the worldwide first truly integrated CNS system, and thus an important part of the digitization process, this work on cybersecurity for LDACS is an essential pillar for the final standardization and deployment of LDACS.

Abbreviations

A2A Air-to-Air
AC-R Access-Router
ADS-B Automatic Dependent Surveillance Broadcast
ADS-C Automatic Dependent Surveillance-Contract
AeroMACS Aeronautical Mobile Airport Communications System
ANI Airborne Network Interface
ANSP Aeronautical Network Service Provider
AOC Aeronautical Operational Control
APT Airport
AS Aircraft Station
ATC Air Traffic Communications
ATM Air Traffic Management
ATN Aeronautical Telecommunications Network
ATS Air Traffic Services
AVI Airborne Voice Interface

BC Broadcast Channel
BER Bit Error Rate

CA Certificate Authority
CC Common Control
CCCH Common Control Channel
CNS Communication, Navigation and Surveillance
CoS Classes of Service
CPDLC Controller–Pilot Data Link Communications
CRP Challenge-Response Pair
CSMA Carrier Sense Multiple Access

D8PSK Differential 8 Phase Shift Keying
DC Dedicated Control
DCCH Dedicated Control Channel
DCH Data Channel
DHKE Diffie-Hellman Key Exchange
DLS Data Link Service
DME Distance Measuring Equipment

ECDH Elliptic Curve Diffie-Hellmann

FACTS Framework for Aeronautical Communications and Traffic Simulations 2
FCI Future Communications Infrastructure
FDD Frequency Division Duplexing
FL Flight Level
FL Foward Link

GBAS Ground Based Augmentation System
GNSS Global Navigation Satellite System
GS Ground Station
GSC Ground Station Controller

HKDF HMAC Key Derivation Function
HMAC Keyed-Hash Message Authentication Code

ICAO International Civil Aviation Organization
IKEv2 Internet Key Exchange

KDF Key Derivation Function

LDACS L-band Digital Aeronautical Communications System
LLC Logical Link Control
LME LDACS Management Entity

MAC Medium Access Layer
MAKE Mutual Authentication and Key Exchange
MF Multi Frame
MICONAV Migration towards COm/NAV capabilities of LDACS

OFDM Orthogonal Frequency-Division Multiplexing
OFDMA Orthogonal Frequency-Division Multiple Access
ORP Oceanic Remote Polar

PDU Packet Data Uni
PHY Physical Layer
PHY-SDU Physical Layer-Service Data Unit
PKI Public Key Infrastructure
PMAKE Physical Unclonable Function based Mutual Authentication and Key Exchange
PUF Physical Unclonable Function

QoS Quality of Service

RA Random Access
RACH Random Access Control Channel
RL Reverse Link

SAC System Area Code
SARPS Standards and Recommended Practices
SESAR Single European Sky ATM Research
SF Super Frame
SIB System Identificaiton Broadcast
SIDH Supersingular Isogeny Diffie–Hellman
SNP Sub-Network Protocol
STS Station-to-Station

TDMA Time Division Multiple Access
TMA Terminal Maneuvering Area

VDLm2 VHF Data Link mode 2
VHF Very High Frequency
VI Voice Interface
VU Voice Unit

References

[1] IATA. Economic Performance of the Airline Industry. International Air Transport Association (IATA); 2020. [Online]. Available: https://www.iata.org/en/iata-repository/publications/economic-reports/airline-industry-economic-performance—november-2020—report/.

[2] ACI. Economic Performance of the Airline Industry. Airports Council International (ACI); 2019. [Online]. Available: https://store.aci.aero/product/annual-world-airport-traffic-report-2019/.

[3] Iacus SM, Natale F, Santamaria C, et al. Estimating and projecting air passenger traffic during the COVID-19 coronavirus outbreak and its socio-economic impact. Safety Science. 2020 September;129:104791. Available from: http://www.sciencedirect.com/science/article/pii/S0925753520301880.

[4] Slim M, Mahmoud B, Pirovano A, et al. Aeronautical Communication Transition From Analog to Digital Data: A Network Security Survey. Computer Science Review. 2014 May;11-12:1–29.

[5] Schnell M, Epple U, Shutin D, et al. LDACS: Future Aeronautical Communications for Air-Traffic Management. IEEE Communication Magazine. 2014 May;52(5):104–110.

[6] Schnell M. Update on LDACS - The FCI Terrestrial Data Link. In: 19th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2019. p. 1–10.

[7] Kamali B. AeroMACS: An IEEE 802.16 Standard-based Technology for the Next Generation of Air Transportation Systems. John Wiley & Sons; 2018.

[8] Gräupl T, Rihacek C, Haindl B. LDACS A/G Specification. Oberpfaffenhofen, Germany: German Aerospace Center (DLR); 2019.

[9] Strohmeier M, Schäfer M, Pinheiro R, et al. On perception and reality in wireless air traffic communication security. IEEE transactions on intelligent transportation systems. 2016;18(6):1338–1357.

[10] Bernsmed K, Fr C, Meland PH, et al. Security requirements for SATCOM datalink systems for future air traffic management. In: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC). IEEE; 2017. p. 1–10.

[11] Mäurer N, Schmitt C. Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis. In: 19th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2019. p. 1A2/1–1A2–13.

[12] Hall A, Wingfield J, De Moura G, et al. Advancing Cyber Resilience in Aviation: An Industry Analysis. World Economic Forum; 2020.

[13] Costin A, Francillon A; EURECOM. Ghost in the Air(Traffic): On Insecurity of ADS-B protocol and Practical Attacks onADS-B Devices. Black Hat USA. 2012 August;p. 1–10.

[14] Strohmeier M, Lenders V, Martinovic I. On the security of the automatic dependent surveillance-broadcast protocol. IEEE Communications Surveys & Tutorials. 2014;17(2):1066–1087.

[15] Stelkens-Kobsch TH, Hasselberg A, Mühlhausen T, et al. Towards a more secure ATC voice communications system. In: 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC). IEEE; 2015. p. 4C1–1.

[16] Harison E, Zaidenberg N. Survey of Cyber Threats in Air Traffic Control and Aircraft Communications Systems. In: Cyber Security: Power and Technology. Springer; 2018. p. 199–217.

[17] Bilzhause A, Belgacem B, Mostafa M, et al. Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management. Aerospace and Electronic Systems Magazine. 2017 November;32(11):22–33.

[18] ICAO. LDACS White Paper–A Roll-out Scenario. International Civil Aviation Organization (ICAO); 2019.

[19] ICAO. Doc 9776 - Manual on VHF Digital Link (VDL) Mode 2. International Civil Aviation Organization (ICAO); 2015. [Online]. Available: http://www.icscc.org.cn/upload/file/20190102/Doc.9776-EN Manual on VHF Digital Link (VDL) Mode 2.pdf.

[20] RTCA. DO-225, VHF Air-Ground Communications System Improvements Alternatives Study and Selection of Proposals for Future Action. Radio Technical Commission for Aeronautics (RTCA); 1994.

[21] RTCA. DO-281C - Minimum Operational Performance Standards (MOPS) for Aircraft VDL Mode 2 Physical Link and Network Layer. Radio Technical Commission for Aeronautics (RTCA); 2018.

[22] ICAO. Annex 10 - Aeronautical Telecommunications - Volume III - Communication Systems. International Civil Aviation Organization (ICAO); 2007. [Online]. Available: https://store.icao.int/en/annex-10-aeronautical-telecommunications-volume-iii-communication-systems.

[23] Shirey R. Internet Security Glossary, Version 2. RFC Editor; 2007. 4949. Available from: https://www.rfc-editor.org/rfc/rfc4949.txt.

[24] Kunkel R. Village DA, editor. Air Traffic Control: Insecurity and ADS-B [YouTube, Date video uploaded: 16.01.2011, [Video file]]. DEFCON 28; 2011. [Online]. Available: https://www.youtube.com/watch?v=aU8NpyYf9wY [Accessed: January 07, 2020].

[25] McCallie D, Butts J, Mills R. Security analysis of the ADS-B implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection. 2011;4(2):78–87.

[26] Strohmeier M, Schäfer M, Lenders V, et al. Realities and challenges of nextgen air traffic management: the case of ADS-B. IEEE Communications Magazine. 2014;52(5):111–118.

[27] Wu Z, Shang T, Guo A. Security Issues in Automatic Dependent Surveillance-Broadcast (ADS-B): A Survey. IEEE Access. 2020;8:122147–122167.

[28] (ICAO) ICAO. Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix. Montreal, Canada: ICAO; 2018.

[29] Gräupl T, Mäurer N, Schmitt C. FACTS2: Framework for Aeronautical Communications and Traffic Simulations 2. In: Proceedings of the 16th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks; 2019. p. 63–66.

[30] Brandes S, Schnell M, Rokitansky CH, et al. B-VHF - Selected Simulation Results and Final Assessment. In: 25th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2006. p. 3A4/1–3A4/12.

[31] Rokitansky CH, Ehammer M, Gräupl T, et al. B-AMC A System for Future Broadband Aeronautical Multi-Carrier Communications in the L-Band. In: 36th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2007. p. 4D2/1–4D2/13.

[32] Schnell M, Brandes S, Gligorevic S, et al. B-AMC - Broadband Aeronautical Multi-carrier Communications. In: 8th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2008. p. 4D2/1–4D2/13.

[33] Haindl B, Rihacek C, Sajatovic M, et al. Improvement of L-DACS1 Design by Combining B-AMC with P34 and WiMAX Technologies. In: 9th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2009. p. 1–8.

[34] Ehammer M, Gräupl T. AeroMACS - An Airport Communications System. In: 30th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2011. p. 4C1/1–4C1/16.

[35] Felux M, Gräupl T, Mäurer N, et al. Transmitting GBAS messages via LDACS. In: 2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC). IEEE; 2018. p. 1–7.

[36] Mäurer N, Gräupl T, Bellido-Manganell MA, et al. Flight Trial Demonstration of Secure GBAS via theL-band Digital Aeronautical Communica-

tionSystem (LDACS). IEEE Aerospace and Electronic Systems Magazine. 2021;p. 1–19.

[37] Mäurer N, Bilzhause A. Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis. In: 18th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2018. p. 1A2/1–1A2–11.

[38] Zelkin N, Henriksen S. L-Band Digital Aeronautical Communications System Engineering - Initial Safety and Security Risk Assessment and Mitigation. Cleveland, OH, USA: National Aeronautics andSpace Administration, TT Corporation Advanced Engineering & Sciences Division; 2011 (accessed July 5, 2019).

[39] Mäurer N, Gräupl T, Schmitt C. L-band Digital Aeronautical Communications System (LDACS). Internet Engineering Task Force; 2020. draft-ietf-raw-ldacs-05. Work in Progress. Available from: https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-05.

[40] International Civil Aviation Organization (ICAO). Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix. Montreal, Canada: International Civil Aviation Organization (ICAO); 2018.

[41] Mäurer, N and Bilzhause, A . A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS). In: 37th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2018. p. 1–10.

[42] Cooper D, Santesson S, Farrell S, et al. Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC Editor; 2008. 5280. Available from: https://www.rfc-editor.org/rfc/rfc5280.txt.

[43] R S. Cybersecurity for global Aviation - A Trust Framework enabling global secure aviation interoperability. In: ICNS Conference 2018 Plenary Panel I, Integrated Communications Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2016. p. 1–19.

[44] Crowe B. Proposed AeroMACS PKI Specification is a Model for Global and National Aeronautical PKI Deployments. In: WiMAX Forum at 16th Integrated Communications, Navigation and Surveillance Conference (ICNS). New York, NY, USA: IEEE; 2016. p. 1–19.

[45] Boyd C, Mathuria A, Stebila D. Protocols for Authentication and Key Establishment. Heidelberg, Germany: Springer; 2020.

[46] Mäurer, N , Gräupl, T and Schmitt, C . Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS. In: 39th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2020. p. 1–10.

[47] Diffie W, Hellman M. New Directions in Cryptography. IEEE Transactions on Information Theory. 1976 Nov;22(6):644–654.

[48] Blake-Wilson S, Menezes A. Authenticated Diffe-Hellman Key Agreement Protocols. In: International Workshop on Selected Areas in Cryptography. Heidelberg, Germany: Springer; 1998. p. 339–361.

[49] Koblitz N. Elliptic Curve Cryptosystems. Mathematics of computation. 1987 January;48(177):203–209.

[50] Baumslag G, Fine B, Kreuzer M, et al. A Course in Mathematical Cryptography. Berlin, Germany: Walter de Gruyter GmbH & Co KG; 2015.

[51] Rostovtsev A, Stolbunov A. Public-Key Cryptosystem Based on Isogenies. IACR Cryptology ePrint Archive. 2006 May;p. 1–19.

[52] Jao D, De Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: 4th International Workshop on Post-Quantum Cryptography. Heidelberg, Germany: Springer; 2011. p. 19–34.

[53] Jao D. Jao D, editor. Supersingular Isogeny Key Encapsulation. SIKE - Supersingular Isogeny Key Encapsulation; 2020 (accessed May 09, 2020). https://sike.org/files/SIDH-spec.pdf.

[54] Josefsson S, Liusvaara I. Edwards-Curve Digital Signature Algorithm (EdDSA). RFC Editor; 2017. 8032. Available from: https://www.rfc-editor.org/rfc/rfc8032.txt.

[55] Ding J, Schmidt D. Rainbow, a New Multivariable Polynomial Signature Scheme. In: 3rd International Conference on Applied Cryptography and Network Security. Heidelberg, Germany: Springer; 2005. p. 164–175.

[56] Schmidt B, Meier S, Cremers CJF, et al. Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties. In: Chong S, editor. 25th IEEE Computer Security Foundations Symposium, CSF 2012, Cambridge, MA, USA, June 25-27, 2012. IEEE Computer Society; 2012. p. 78–94. Available from: https://doi.org/10.1109/CSF.2012.25.

[57] Mäurer N, Gräupl T, Schmitt C, et al. PMAKE: Physical Unclonable Function-basedMutual Authentication Key Exchange Scheme forDigital Aeronautical Communications. In: 2021 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE; 2021. p. TODO.

[58] Krawczyk H, Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC Editor; 2010. 5869. Available from: https://www.rfc-editor.org/rfc/rfc5869.txt.

[59] Salowey J, Choudhury A, McGrew D. AES Galois Counter Mode (GCM) cipher suites for TLS. RFC Editor; 2008. 5288. Available from: https://www.rfc-editor.org/rfc/rfc5288.txt.

[60] Weis B, Smyslov V. Group Key Management using IKEv2 - draft-yeung-g-ikev2-16. RFC Editor; 2020. -. Available from: https://tools.ietf.org/html/draft-yeung-g-ikev2-16.

[61] Zheng X, Huang CT, Matthews M. Chinese remainder theorem based group key management. In: Proceedings of the 45th annual southeast regional conference; 2007. p. 266–271.

[62] Guggemos T, Streit K, Knüpfer M, et al. No Cookies, just CAKE: CRT based Key Hierarchy for Efficient Key Management in Dynamic Groups. In: International Conference for Internet Technology and Secured Transactions; 2018. p. 25–32.

[63] Sakamoto N. An efficient structure for LKH key tree on secure multicast communications. In: 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE; 2014. p. 1–7.

[64] Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;549(7671):188–194.

[65] Dworkin MJ. SP 800-38D -Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC. National Institute of Standards & Technology; 2007.

[66] Krawczyk H, Bellare M, Canetti R. HMAC: Keyed-Hashing for Message Authentication . RFC Editor; 1997. 2104. Available from: https://www.rfc-editor.org/rfc/rfc2104.txt.

[67] Pritzker P, Gallagher PD. SHA-3 standard: permutation-based hash and extendable-output functions. Information Tech Laboratory National Institute of Standards and Technology. 2014;p. 1–35.

[68] Mäurer N, Gräupl T, Schmitt C. Evaluation of the LDACS Cybersecurity Implementation. In: 38th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2019. p. 1–10.

[69] Gräupl T, Mayr M. Method to Emulate the L-band Digital Aeronautical Communication System for SESAR Evaluation and Verification. In: 34th Digital Avionics Systems Conference (DASC). New York, NY, USA: IEEE; 2015. p. 1–18.

[70] RTCA/EUROCAE. Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard). Washington, DC / Malakoff, France: RTCA/EUROCAE; 2016.

[71] Gräupl T, Mäurer N, Schmitt C. FACTS2: Framework for Aeronautical Communications and Traffic Simulations 2. In: Proceedings of the 16th ACM International Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks; 2019. p. 63–66.

[72] McEliece RJ. A public-key cryptosystem based on algebraic. Coding Thv. 1978;4244:114–116.