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

Nils Mäurer
Institute of Communications and Navigation
German Aerospace Center (DLR)
Oberpfaffenhofen, Germany
nils.maeurer@dlr.de

Arne Bilzhause
Institute of IT-Security and Security Law
University of Passau
Passau, Germany
ab@sec.uni-passau.de

***Abstract*—With air transportation growing and current civil aeronautical communication systems reaching their capacity limit in high density areas, the need for new aeronautical communication technologies becomes apparent. The biggest challenge in recent years is the transition from analogue voice to digital data communication and the related trend towards an increased autonomous data processing. A promising candidate for the digital future communication infrastructure in continental areas is the terrestrial long-range L-band Digital Aeronautical Communications System (LDACS), which is currently in the process of being standardized by the International Civil Aviation Organization (ICAO). As safety and security are strongly intertwined in civil aviation, every installation of LDACS requires protection against cyber-attacks. This paper introduces a cybersecurity architecture for LDACS and proposes suitable security algorithm, which can achieve the security objectives on top of the architecture. Therefore we integrate new security functions within the existing protocol stack of LDACS. We provide an architecture for user data encryption, data integrity, authenticated key agreement, entity authentication, broadcast channel protection, and key and access management.**

***Index Terms*—LDACS, Cybersecurity, FCI, Security Architecture**

I. Introduction

Civil air traffic has been growing considerably in recent years and is expected to double by 2025 compared to 2008 [1]. With increased usage of airspace, Air Traffic Management (ATM) communication infrastructure needs to be modernized to cope with this growth [2]. Currently air traffic management communication relies on legacy systems using the VHF band which is becoming saturated in the high density areas of Europe and the US [3]. To identify relevant features and to evaluate whether an already existing system can meet the requirements of future communications the Federal Aviation Administration (FAA) and EUROCONTROL started a joint study called action plan 17. The outcome was that no current technology can fulfill all demands [4]. Action plan 17 sparked the development of new systems based on the identified necessities and desired features. To provide long term, scalable growth of air transportation and to enable new air traffic management services and technologies in the future, the introduction of computerized air traffic management applications and digital data communications is required [5], [6]. Hence, analogue systems have to be augmented by digital means as large parts of aeronautical communications of tomorrow will be running on IP-based networks [7].

In order to support the transition from analogue to digital systems in air traffic management, two projects were initiated: Single European Sky ATM Research (SESAR) [8] in Europe and Next Generation National Airspace System (NextGen) [9] in the United States. Within these projects, new broadband digital data link technologies for air traffic management are developed, standardized and will be part of an IP-based aeronautical telecommunications network, called the Future Communications Infrastructure (FCI) [7]. For airport communications a new short-range terrestrial system was developed, called AeroMACS [35]. Communication in the oceanic, remote, or polar domain will make use of Satellite Communications (SatCOM) [10]. Communication in the en-route domain shall use the terrestrial long-range L-band Digital Aeronautical Communications System (LDACS). All technologies are summarized in figure 1.
LDACS was developed in cooperation between the German Aerospace Center (DLR) [5], [11], Frequentis AG [12], and the University of Salzburg in Austria [13], [14] with its origins in merging parts of the B-VHF [15], B-AMC [16]–[18], TIA-902 (P34) [33], and WiMAX IEEE 802.16e technologies [19].

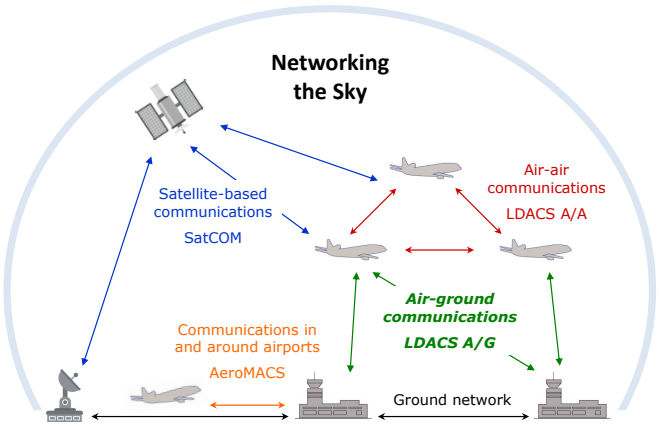

Fig. 1. Introducing an approach for future digital communication in aviation called "Networking the sky" with several new data links such as LDACS and AeroMACS [31], [32].

With the paradigm shift from analogue to digital wireless communications and the related trend towards an increased autonomous data processing, LDACS requires a thorough cybersecurity analysis and a proposal on how to properly protect the system against threats from the IT sector, as security and safety are strongly intertwined in aviation [7], [39]. A comprehensive and well-designed cybersecurity architecture for LDACS is therefore key to its final deployment and success. However, such an architecture has not yet been specified.

The contributions of this paper are an architecture design for a cybersecurity solution for LDACS and the proposal of algorithms that support its implementation.

II. Background on LDACS

LDACS is a broadband air-ground data link proposed to supplement the VHF communication infrastructure in the L-band [5]. It is designed to provide air-ground data communication with optional support for digital voice. It is a cellular broad-band system based on Orthogonal Frequency-Division Multiplexing (OFDM) technology [34] and supports quality-of-service taking the requirements of aeronautical services into account. It shares many technical features with 3G and 4G wireless communications systems. LDACS will be one of several wireless access networks connecting aircraft to the aeronautical telecommunications network. The LDACS access network contains several ground-stations, each of them providing one LDACS network (see figure 2).

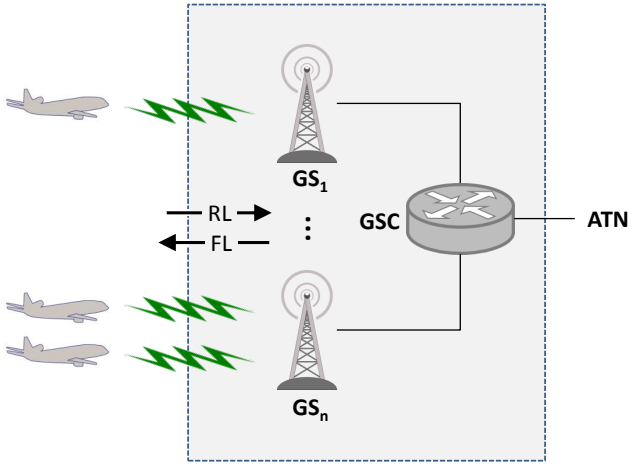

Fig. 2. An LDACS ground segment comprises several Ground-Stations (GS) controlled by one Ground-Station Controller (GSC). Aircraft, respectively Aircraft-Stations (AS) connect to GS wirelessly and transmit in the Forward Link (FL) and Reverse Link (RL). The GSC provides the gateway to the Aeronautical Telecommunications Network (ATN).

The LDACS air interface is a cellular data link with a star-topology connecting aircraft to ground-stations with a full duplex radio link. Each ground-station is the centralized instance controlling all air-ground communications within its radio cell. The LDACS core protocol stack defines two distinct layers, the physical layer and the data link layer. In the rest of the section, we point out all LDACS relevant entities and show the underlying protocol layers for each entity, with a corresponding description of its functionality. Afterwards we describe the state of the art of LDACS cybersecurity, prior to this work.

A. LDACS Network Entities

An LDACS network has three main entities: Aircraft Station (AS), Ground Station (GS) and Ground Station Controller (GSC). Up to 512 aircraft can connect to one ground-station. The GS is responsible to maintain a continuous data stream in the Forward Link (FL), while the Reverse Link (RL) consists of individual bursts of data from each aircraft. GS connect to one GSC, which connects the GS to the Aeronautical Telecommunications Network (ATN), thus enabling the direct data transfer between air traffic control and aircraft [11].

B. LDACS Protocol Layer in the Aircraft and Ground-station

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 Layer (DLS), Link Management Entity (LME), Voice Interface (VI) and Sub-Network Protocol Layer (SNP) as illustrated in figure 3.

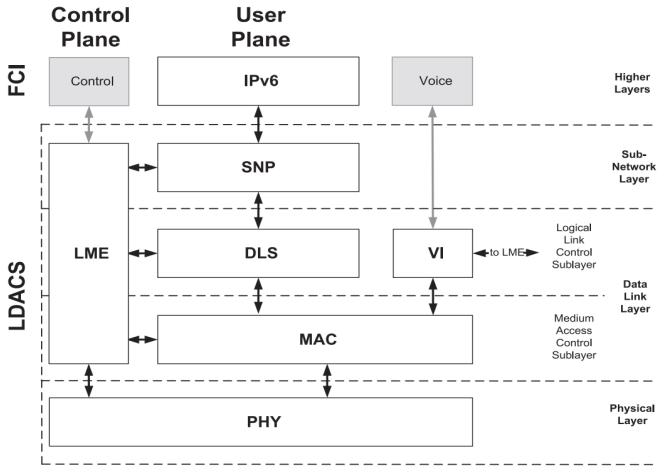

Fig. 3. The LDACS sublayer is embedded in the FCI (IPv6, voice and control traffic) and consists of Physical layer (PHY), Medium Access Layer (MAC), Data Link Service layer (DLS) and Voice Interface (VI), both located in the logical link control sublayer and finally the Sub-Network Protocol layer (SNP). The Link Management Entity (LME) serves as a cross layer entity between MAC, DLS and SNP layer.

For further considerations, only PHY, MAC, DLS, LME and SNP will play a major role, as the goal of this work is to secure the data link, not the voice component.

The physical layer provides the means to transfer data over the radio channel. 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 Frequency-Division Duplex (FDD). Forward link and reverse link use a 500 kHz channel each. The ground-station transmits a continuous

stream of 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 [6]. 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 medium access sub-layer and the logical link control sub-layer. The medium access 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 *Link Management Entity (LME)* and the *Sub-Network Protocol (SNP)*.

The main task of the link management entity is to perform configuration, resource management and mobility management of LDACS. The mobility management service in the link management entity 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). The sub-network protocol 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.

C. LDACS Protocol Layer in the Ground-Station Controller

The GSC consists of *Sub-Network Protocol (SNP)* and *Network Management Entity (NME)*. The sub-network protocol of the GSC has the same task as within the AS and GS protocol stack, whereas the network management entity has similar tasks as the link management entity in the aircraft and the ground-station. Namely it performs mobility management, which manages unique addressing of aircraft within the sub-network and is responsible for conducting aircraft handovers between connected GS. Thus the NME of the GSC manages several GS and knows which GS is currently suited to be the next GS for an AS requesting cell handover.

III. Previous Work

The current LDACS specification [11] includes no authentication and authorization of participants of the communication, no encryption or integrity proof for data and also no proof of integrity for the system. Here we present the current state of the art of previous LDACS cybersecurity considerations.

There are many standards in the industry describing the aims of a successful cybersecurity architecture, such as the Common Criteria process [21], the ISO norm 27001 [22] or the IEC norm 62443 [23]. Furthermore, we had a closer look at several cybersecurity frameworks like the ISACA COBIT 5.0 [42], the German IT-Grundschutz (*baseline security*) [43] and the framework of the National Institute of Standard and Technology (NIST) for improving critical infrastructure security [44]. In general, cybersecurity aims to achieve *confidentiality* of data, *integrity* of data, systems and assets, *availability* of data, system and assets, *authenticity* of participating entities of communication and *non-repudiation* to prove the occurrence of a claimed event or action and to link it evidently to its originating entity. Next, we define which of those properties are relevant for LDACS and how to achieve them.

A. LDACS Security Objectives

LDACS will majorly be used to provide Air Traffic Services (ATS), Aeronautical Operational Control (AOC), while maintaining the link via Network Management (NM) services. Previous threat and risk analyses [24], [25], [37] have identified several safety critical applications, particular those supporting air traffic services and safety related aeronautical operational control communications. To provide these services, a stable and secure network connection is required, thus leaving us with five objectives for securing LDACS. These were first pointed out by Bilzhause et al. [6]:

Objective 1 The operation of the LDACS system security functions shall not diminish the ability of the LDACS system to operate safely and effectively.

Objective 2 The LDACS system shall support reliability and robustness to mitigate denial of service attacks.

Objective 3 The LDACS system shall support message authentication and integrity to prevent message alteration attacks.

Objective 4 The LDACS system should support confidentiality to mitigate eavesdropping.

Objective 5 The LDACS system shall support entity authentication to mitigate impersonation attacks.

B. LDACS Security Functions

From the objectives we can now define security functions that should be integrated in the LDACS cybersecurity architecture. Here we give the formal definition by the Internet Engineering Task Force (IETF) [45] of the terminology, printed in cursive characters, and put the definitions in an LDACS context by using [6], [37]:

Authentication *Authentication is the process of verifying a claim that a system entity or system resource has a certain attribute value. An authentication process consists of two basic steps: (1) Identification step: Presenting the claimed attribute value to the authentication subsystem. (2) Verification step: Presenting or generating authentication information that acts as evidence to prove the binding between the attribute and that for which it is claimed.*

Authorization *Authorization is defined as an approval that is granted to a system entity to access a system resource.*

Confidentiality *Confidentiality describes the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].*

Integrity The general term "Integrity" can be split up in several specifications such as data integrity and system integrity.

System Integrity *An attribute or quality "that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.* Thus integrity here refers to the correct and intended functioning of systems.

Data Integrity *The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.* This is related to mechanisms for data origin authentication, inter-entity user data integrity protection during transmission, and replay detection by making use of cryptographic primitives.

Safety *The property of a system being free from risk of causing harm (especially physical harm) to its system entities.* For us, safety measures include self-tests, functions for information flow control according to previously specified information flow control policies and approaches for general availability protection.

Robustness Robustness can be defined in different levels: *A characterization of (1) the strength of a security function, mechanism, service, or solution and (2) the assurance (or confidence) that it is implemented and functioning.* So starting in the physical layer, protection against physical tampering and interference is crucial for achieving a reliable and robust system, followed by clear policies and implemented mechanisms on the software layers above.

Key Management *Key management is the process of handling keying material during its life cycle in a cryptographic system; and the supervision and control of that process.* Thus secure cryptographic key management, i.e. key generation, key distribution, key access and key revocation as well as making use of the keys in cryptographic operations like encryption, decryption, generation or verification of cryptographic checksums for integrity and so forth, is an essential requirement for the success of the security functions defined above.

C. Approaches for Implementing LDACS Security

In figure 4 we summarize the data flow between entities and the communication between LDACS devices. In accordance to previous work [6], we argue that placing protection mechanisms in the link management entity and sub-network protocol of the LDACS protocol stack will be most efficient in securing LDACS. The data link service is thereby the intermediate entity in distributing security data between the link management entity and the sub-network protocol.

LDACS cybersecurity will be managed by the network management entity of the ground-station controller with the sub-network protocol service applying only cryptographic measures as configured by the network management entity.

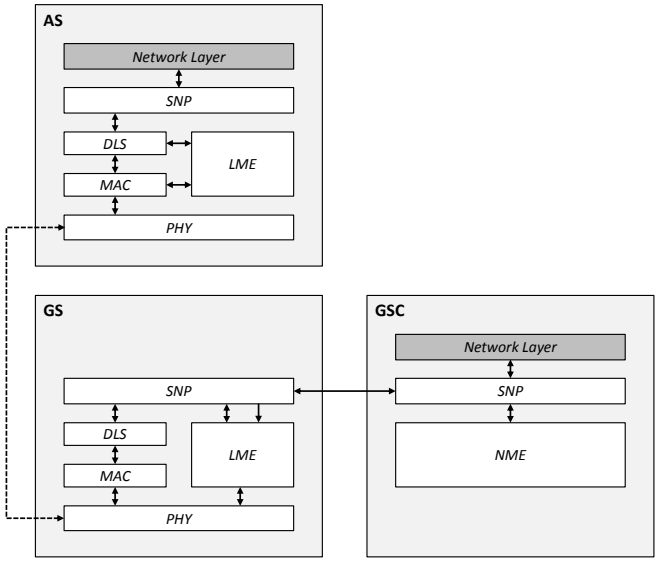

Fig. 4. Communication overview with protocol stacks of AS, GS and GSC. The link between AS-GS is wireless (dashed lines), while the GSC-GS link is wired (solid line).

Thus the network management entity of the ground-station controller will receive a new, additional functionality namely the security service, performing authentication of aircraft and ground-station and providing the configuration parameters for secure communication to the sub-network protocol. With these measures we can achieve end-to-end encryption from ground-station controller to aircraft, provide entity authentication among all parties and introduce a key negotiation between relevant parties.

IV. LDACS Cybersecurity Architecture

When designing the LDACS cybersecurity architecture there are two major requirements: we need (1) low latency and (2) low additional security data overhead [6]. Those two constraints appear in all solution approaches in this section.

A. Defining the Endpoints of Security

As ground-station controller, ground-station and aircraft will all be equipped with LDACS transceivers, those will be defined as endpoints of security in a device-to-device approach.

B. Entity Authentication

We need to make sure that only legitimate entities can participate in the communication system. Therefore, we need ways for entities to authenticate to each other so that trust between parties can be established.

We propose to fulfill this goal via introducing a Public Key Infrastructure (PKI) and install certificates on all necessary entities, forming a chain-of-trust. To enable this, we propose the use of X.509 certificates, which are distributed via pre-installation within the entity or via certificates sent ad hoc. These tasks take exclusively place within the link management entity or in the network management entity respectively. As

AeroMACS already has a PKI solution [40], [41], we want to align the LDACS approach. The AeroMACS PKI consists of the global root Certificate Authority (CA) which defines the security requirements for the AeroMACS digital certificates. Below the root CA there are several online Sub-CAs operating on their Certification Practice Statement (CPS) ensuring compliance to the Certificate Policy (CP). After several of those layers we reach the end-entity certificates managed in lifecycles and ensuring compliance to the certificate policy again [40]. We envision a similar LDACS PKI related or intertwined with the AeroMACS PKI by adapting the concept of an offline root CA managed by the International Civil Aviation Organization (ICAO) and the tiers below managed by respective country Sub-CAs, such as a German Sub-CA and so forth.

However, there is also a trust "bridge" certification approach, suggested by the Federal Aviation Administration (FAA) in 2018 with the ICAO providing only a bridge CA to establish trust among various Sub-CAs [38]. The selection of the final approach is subject to future work.

Eventually, we have the key material i.e. public and private key and according certificates specifically for each LDACS device (AS, GS or GSC). These end-entity certificates can be uploaded onto AS, GS or GSC e.g. via a specified secure communication channel or on dedicated maintenance events by authorized staff. Secure certificate distribution is thus solved, when we have established secure communication channels between entities and layers of the PKI and can exchange certificates via those channels. For certificate revocation we propose to use segmented, protected, secure Certificate Revocation Lists (CRL) distributed over all layers and entities of the PKI. We propose this approach as it has been shown to be scalable and efficient with seamless delivery [47]. When all participants of communication have received their end-entity certificate, allowing for global interoperability, and are integrated into the LDACS PKI, they have knowledge of relevant key material in order to mutually authenticate to each other.

C. Authenticated Key Agreement

Together with the first messages between new communication participants, verifying their identity, we can include ways of authenticated key agreement (e.g. for symmetric session keys) such as proposed in the authenticated ephemeral Diffie-Hellman scheme. With that approach, we get two things done with little additional security data overhead in our communication channel: (1) entities can mutually authenticate each other using the same messages used for (2) key negotiation and key agreement. This process can be rerun (at any time) to generate new key material. AeroMACS offers a similar approach to renew key material [38]. In table I we sum up the required symmetric keys for secure inter-entity communication in LDACS.

The procedure also takes place exclusively in the link management entity. After a key has been negotiated, we need a key derivation function on both sides to derive different keys for e.g. encryption, generation of Message Authentication Codes (MAC), Initialization Vectors (IV) and so on.

TABLE I
OVERVIEW OF SYMMETRIC KEYS FOR LDACS COMMUNICATING ENTITIES

Entity #1	Entity #2	Purpose of Key
GSC	GS	Between ground-station controller, the most trusted entity, and the ground-station a key must be negotiated for secure transmission of link management data and to collect data from several ground-stations. Those are connected to one ground-station controller, which enables plausibility checks on the incoming data traffic. The key derivation function makes sure to derive sufficiently enough keys for each task for each entity in the GSC i.e. encryption, generation and verification of Message Authentication Codes (MAC).
GSC	AS	Between ground-station controller and aircraft end-to-end authenticated encryption must be built so messages can be transmitted securely. If that encryption key can be shared with the air traffic surveillance institution, even air traffic management traffic can be transmitted in an encrypted way, as long as the controlling instance (e.g. the German Flight Control (DFS)), has access to the key and can also follow the communication of air traffic management traffic. There will be no explicit key for encryption between ground-station and aircraft, thus the ground-station will only forward encrypted traffic between ground-station controller and aircraft.

D. Key Derivation

As we now have a single master key negotiated between relevant entities, we need several keys to secure the session. If we can assume that the negotiated master key is uniformly distributed, we can use a Key Derivation Function (KDF). Our proposal for such a technique is the HKDF [46], 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 is taken (here we call it Master Key MK) and a fixed-length Pseudo Random Key PRK is extracted. The extract phase is especially important, if our master key MK is not sufficiently uniform (e.g. the key is uniform only in a subset of the original key space). Here we extract a pseudo random key PRK from the master key MK by adding a salt value, which can be any fixed non-secret string chosen at random. In the process the pseudo random key K 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 [46]. The following two formulas summarize the first step:

$$HKDF - Extract(salt, MK) \rightarrow PRK \quad (1)$$

$$PRK = HMAC(salt, MK) \quad (2)$$

Secondly the key PRK is expanded, resulting in multiple additional pseudorandom keys as output of the KDF. Therefore, we need PRK, an optional context string CTX describing the application we use the key for and a value L which is the length of the output keying material in octets to receive the Output Keying Material OKM of L octets.

$$HKDF - Expand(PRK, CTX, L) \rightarrow OKM \quad (3)$$

We can write the output of OKM as $K(1)||K(2)||...||K(t)$ with $t = \lceil \frac{L}{k} \rceil$ and k denoting the output and key length of the hash function used with HMAC. Thus we get [26]:

$$HKDF(PRK, CTX, L) = K(1)||K(2)||...||K(t) \quad (4)$$

$$K(1) = HMAC(PRK, CTX||0) \quad (5)$$

$$K(i+1) = HMAC(PRK, K(i)||CTX||i), 1 \leq i < t \quad (6)$$

In the end the value of $K(t)$ is truncated to its first $d = L \; mod \; k$ bits and the counter i is of given fixed size e.g. one byte. As the values of $K(i)$ are usually not mapped as individual keys but concatenated to produce an arbitrary amount of key bits [26], we can use HKDF as a KDF to derive sufficient keys for all entities and services with required key lengths.

E. Confidentiality Protection

We suggest using symmetric approaches for 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 messages from the air traffic network can be encrypted. This happens in the sub-network protocol layer at the respective entity and the message can be decrypted at the other end of communication, also in the sub-network protocol of that entity.

We propose to establish end-to-end encryption for e.g. Aeronautical Operational Control (AOC) data between GSC and AS, thus requiring encryption keys for protecting this part of the communication channel. A suitable algorithm to symmetrically encrypt the data traffic between AS and GSC can be AES [28].

F. Message Integrity Protection

For message integrity protection, we suggest to use a designated derived session key from the KDF to form a message authentication code with the help of symmetric key material. This means that non-repudiation of messages, sent from an entity is not given, however it can be cryptographically proven that a message secured with that specific message authentication code must come from either one of the two entities sharing the same encryption key, hence achieving data origin authentication. This task takes place in the sub-network protocol.

G. Availability Protection

The topic of availability protection in wireless communications is wide ranging as we have to protect against jamming, interfering, message bursts, rogue base stations, bandwidth limitations and so on. Research is currently done to protect the availability of LDACS in the physical layer. Here we want to add a protection against Denial of Service (DoS) attacks on higher layers [20], [36]. We propose to use packet filters at each of the entities, controlling the amount of packets traveling from and to a communication partner. Also the use of load balancers at central communication nodes such as the GSC is recommended to rebalance the load or distribute it to other entities, in case the network receives too much traffic. When aeronautical telecommunications network, GSC, GS and AS are verified by each other, no unauthorized entity should be able to successfully participate in the LDACS system. However, that does not yet prevent jamming or interfering in the same frequency and is subject to future research, currently done at the German Aerospace Center (DLR) [20], [36].

H. Secure Logging

A big advantage of using asymmetric cryptography is that logs can be signed and encrypted at the same time, thus allowing no change after a certain point of time. So we suggest adding a signature of the respective entity when something is added to the log, proving that only the respective entity has accessed the security log. Furthermore secure timestamps are required and to prevent too much overhead, events can be gathered in blocks which are then written securely in the log in pre-defined time intervals. The security log in the link management entity should specifically hold reports about failed authentication, unknown signatures, certificates, malformed messages, incoming messages with lower priority and so on. The log in the sub-network protocol holds information about encryption, decryption and creation and verification of message authentication codes. Thus, most importantly it should log events of undecryptable messages, incoming message types, unverifiable MACs (failed integrity checks), thus events that diverge from a normal protocol run.

I. Broadcast Control Channel Protection

To exchange system relevant data between entities and layers, LDACS uses four logical control channels. The Broadcast Control Channel (BCCH) in the forward link is used by the ground-station to announce cell configuration information and to issue mobility management commands to aircraft. It provides enough space to put in "beacons" from the GS allowing an aircraft to verify if they start communication with a valid communication partner on the ground. Beacons can be signatures of cells, verifiable by the link management entity of the aircraft.

Overall we have enough space to add an additional signature in one of the broadcast messages. Without much data overhead involved, this gives incoming aircraft a chance to authenticate the ground-station with each signed beacon, which is sent every 240ms. To further protect against replay attack, the

TESLA broadcast authentication protocol with a suitable key-chain and time synchronization to ensure a stable protocol run might be used [27].

J. Algorithms and Protocols

Table II lists a suggestion of algorithms that we estimate currently suitable for the respective operations. In all considerations, it must be noted that we have to operate with the least latency possible and we have to keep the amount of security data in the A/G data link at a minimum. Also in general algorithms could and should be exchanged in time depending on their guaranteed security level during the next years.

K. Key and Access Management

a) Entity Authentication: Regarding the aforementioned public key infrastructure we suggest to place one certificate authority either serving as root or bridge CA, at the International Civil Aviation Organization (ICAO), and then use Sub-CAs meaning that there will be a European, American and Asian Sub-CA. These will then sign country Sub-CAs and so forth, with finally reaching the end-entity certificates in the devices. The sub domains will be split up among countries and rely on the Air Traffic Management (ATM) organizations of a specific country (e.g. the German Flight Control (DFS) in Germany). It is important to note that communication participants only receive the public keys for necessary communication partners. With that approach we keep the storage requirements low. We suggest placing the required certificates onto the LDACS transceiver hardware. That way, whenever a key is compromised, key revocation can take place during the daily maintenance of the aircraft via the aforementioned segmented certificate revocation lists. It is assumed that the GS and especially the GSC are physically protected, so only selected personnel has access to the ground LDACS transceivers or the gateway, i.e. to nodes directly connected to the air traffic network.

b) Master Keys: After the link management entity has securely negotiated a master key, session keys for the GSC-AS or GSC-GS communication can be derived. The master key remains valid, as long as the aircraft stays in range of the same GSC, which will broadly be the scope of ten to twenty ground-stations. After leaving the range of that GSC, a new master key will be negotiated for the next GSC via the link management entity. The old master key will be deleted from sub-network protocol and link management entity and finally a new session key, derived from a new master key will be handed to the sub-network protocol.

V. Overview of entire Cybersecurity Architecture

In the following we describe the three phases of initial interaction that take place during an implementation of all prior described security measures. Phase 1 takes place between GSC and GS, phase 2 between GS and AS, and phase 3 between AS and GSC via GS. The overview of the phases can be seen in figure 5

TABLE II
Suggested algorithms for the cybersecurity architecture

Security Functions	Algorithm	Explanation
Confidentiality	AES-GCM	Galois Counter Mode (GCM) is a mode of operation on symmetric key block ciphers utilizing AES. It provides authenticated encryption/decryption and can be used for integrity and confidentiality protection at the same time [28] thus saving us computational effort and bandwidth.
Integrity	HMAC, GMAC	As HMAC combined with a strong hash function like the SHA3 cryptographic hash family is among the most used MAC procedures, we suggest using HMAC for message integrity and keeping the used hash function updated. Alternatively AES-GCM provides authenticated encryption, thus requiring no additional hash function and implementations for integrity protection [29]. For digital signatures, the Digital Signature Algorithm (DSA) in its latest revision by NIST [48] could be used.
Availability	Packet Filtering, Rate Limiting	We recommend to analyze the origin and amount of packets originated by a single entity to apply rate limiting if appropriate. Also incoming packets to the aeronautical telecommunications network, thus traveling through the ground-station controller, must be closely inspected after their decryption to avoid malicious packets.
Entity Authentication	STS	Based on the authenticated Diffie-Hellman key exchange, the Station to Station (STS) protocol provides key agreement and mutual entity authentication by assuming that the parties have signature keys to sign messages providing security against man-in-the-middle attacks. Also it provides perfect forward secrecy and two-way explicit key confirmation [30] with comparatively little message overhead.
Key Negotiation	STS	As described above, STS provides key agreement and mutual entity authentication at the same time, with just four messages, the key confirmation included, thus being a suitable protocol for our resource limited LDACS scenario.
Key Derivation	HKDF	We need a key derivation function to derive different cryptographically strong secret keys to be able to protect different services in system. Therefore we negotiate an initial keying material, i.e. a shared master secret via STS, that is normally not uniformly distributed and use the KDF to derive one or more now uniformly distributed cryptographically strong secret keys. The HKDF, following the "extract-then-expand" approach, is suitable to be used here as it builds a synergy with the integrity protection which also uses HMAC.

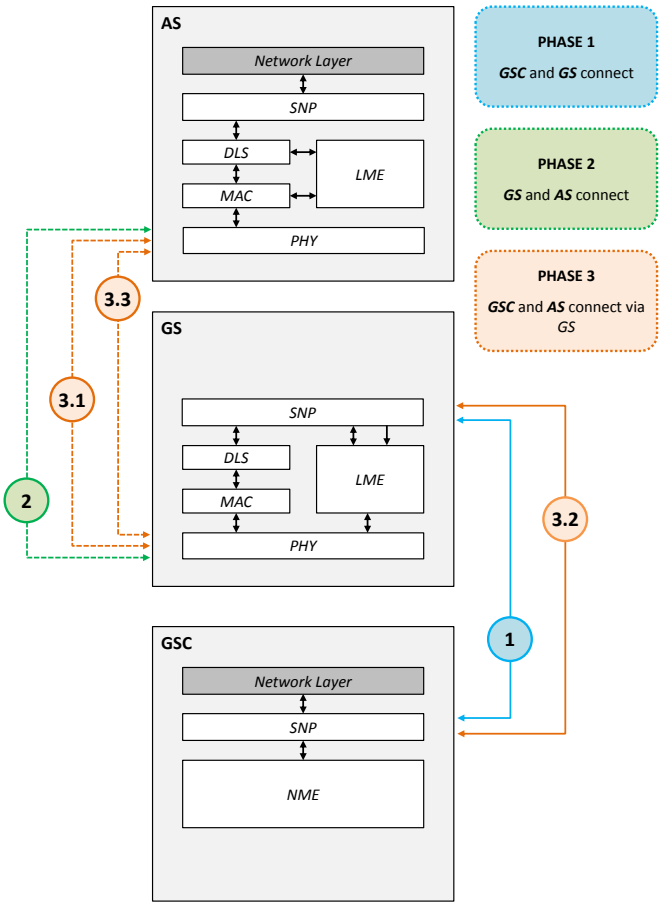

Fig. 5. Overview of the three initial communication phases of the LDACS cybersecurity architecture.

A. Phase 1 - GSC and GS (Figure 6)

- GSC and GS connect.
- Key negotiation and entity authentication take place between GSC and GS.
- After successful mutual authentication, the key negotiation can end with a key confirmation message. Now the GS link management entity and data link service can receive incoming messages from the GSC, as both parties are mutually authenticated. At the GSC the network management entity is also ready for messages from the respective GS. Furthermore, maintenance messages can be securely (encrypted and authenticated) transmitted between the GS link management entity and GSC network management entity.

B. Phase 2 - GS and AS (Figure 7)

- After the GSC and GS are mutually authenticated (phase 1), the GS can start sending signed broadcast messages in the Broadcast Control Channel, thus announcing its existence to aircraft. The broadcast messages have a GS specific signature attached to it, allowing recipient AS to verify the identity of the GS.
- The AS link management entity receives the GS broadcast message and allocates a usable channel.
- Now the AS link management entity can verify the signature and thus verify the identity of the GS.
- If a correct and known GS broadcasts the signal, the AS link management entity responds with a Cell Entry Request.
- The GS responds to that cell entry request via a cell entry response, enabling data communication between the new AS and GS. This is done by sending parameters like frequency, transmission power or slot number to the AS.

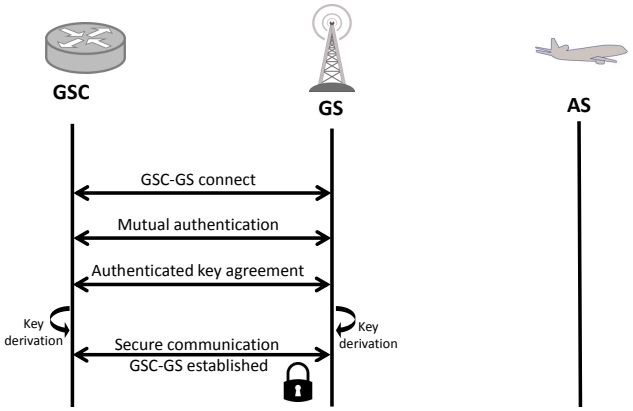

Fig. 6. Message exchange during phase 1 - GSC and GS connect.

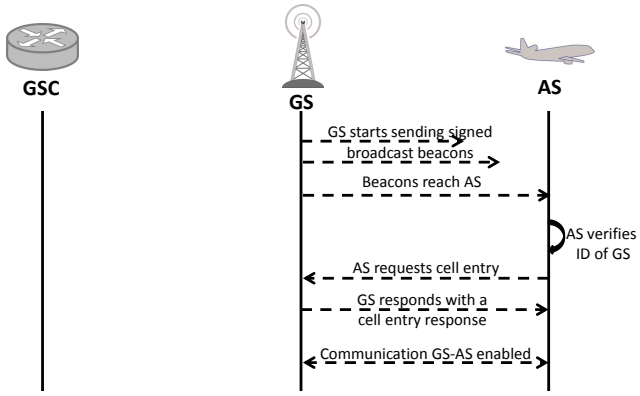

Fig. 7. Message exchange during phase 2 - GS and AS connect.

C. Phase 3 - GSC, GS and AS (Figure 8)

3.1)
- The GSC does not yet know of the existence of a new AS.
- The AS transmits its own signature as the first message allowing the GS to verify the identity of the AS.
- If the GS verifies the AS as a valid communication participant, it forwards the AS signature via the

secure channel GSC-GS to the GSC, which is finally informed about the existence of the AS.

3.2)
- The GSC verifies the identity of the AS.
- It then replies with its own GSC signature, encrypts the message and sends it via the GS to the AS.
- The AS can now verify the identity of the GSC and finish the authentication and key negotiation phase.

3.3)
- Finally the GSC network management entity derives required key material based on the master key and forwards the derived key to its own sub-network protocol, while the AS link management entity does the same for its sub-network protocol, allowing secure data communication between GSC and AS, forwarded by the GS.

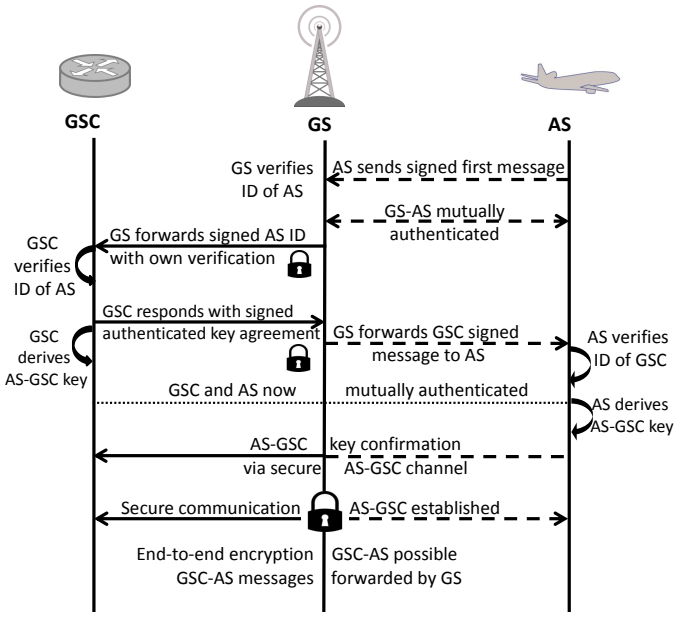

Fig. 8. Message exchange during phase 3 - GSC, GS and AS establish secure communication link.

D. Summary

At the end of the three phases we have a secure (confidentiality and integrity protected) channel between GS-GSC and between AS-GSC, while secure AS-GSC messages are forwarded by the GS. All entities are mutually authenticated, either by using the STS protocol and by that, also negotiating a master key (AS-GSC, GS-GSC), or by verifying signed messages sent by the respective entity (AS-GS). Thus the data channel AS-GSC is end-to-end secured and no unauthenticated entity can participate in the LDACS communication. Furthermore, benign ASs are securely connected to the ATN via the GSC gateway.

VI. Conclusion

The contributions of the paper are the draft of a cybersecurity architecture for LDACS and the proposal of a first set of algorithms for its implementation. We identified the Link Management Entity, Sub-Network Entity and the Network Management Entity in the respective protocol stacks to be the layers where the security functionality should be implemented. Based on this, we introduced means for user data end-to-end encryption, data integrity, authenticated key agreement, entity authentication, broadcast control channel protection and also discussed options for key and access management. The proposed architecture can achieve confidentiality by implementing symmetric encryption using AES-GCM, and integrity protection by using HMAC with the SHA3 hash family. Entity authentication and authenticated key negotiation are realized by utilizing the Station to Station (STS) protocol and a suitable Key Derivation Function (KDF), i.e HKDF, providing sufficient session keys in the right format. Trust relations between LDACS entities are based on a Public Key Infrastructure (PKI) approach. Finally, we finish our security architecture design by extending the functionality and the role of the Ground Station Controller to become a central security entity between multiple Ground Stations. Hence, the Ground Station Controller will also be the endpoint of the secure channel (i.e. confidentiality and integrity protected communication) to Aircraft Stations. As a result the LDACS cybersecurity architecture provides protection against potential cyber-attacks, and at the same time enables a secure connection of benign aircraft, via the Ground Station Controller gateway, to the ATN.

The next steps are to design a thorough protocol sequence including detailed parts of the involved messages during the establishment of secure LDACS communication. And based on this, the security of the resulting protocol has to be proven formally. Moreover, while general conditions of the LDACS environment (i.e narrow frequency ranges and limited bandwidth) have been respected in the design of the security architecture and the selection of algorithms, it is crucial to further asses the performance of the overall security approach (e.g. by simulations). I.a., not only the provided security functionality, but also a reasonable low overhead of security data, will be key for further progress towards LDACS security specification and standardization.

References

[1] EUROCONTROL, "EUROCONTROL's Challenges of Growth 2008 Study Report", 2008.

[2] JPDO, "Concept of Operations for the Next Generation Air Transportation System (Version 3.2)", Washington, DC, JPDO., 2010.

[3] B. Kamali, "An overview of VHF civil radio network and the resolution of spectrum depletion", In Proc. of the 2010 Integrated Communications, Navigation, and Surveillance Conference, 2010.

[4] EUROCONTROL/FAA, "Action Plan 17 Future Communications Study - Final Conclusions and Recommendations", 2007.

[5] M. Schnell, U. Epple, D. Shutin and N. Schneckenburger, "LDACS: Future aeronautical communications for air-traffic management", IEEE Communications Magazine, 52(5):104-110, 2014.

[6] A. Bilzhause, B. Belgacem, M. Mostafa, T. Gräupl, "Datalink Security in the L-Band Digital Aeronautical Communications System (LDACS) for Air Traffic Management", IEEE Aerospace and Electronic Systems Magazine, 2017.

[7] M. Mahmoud, A.Pirovano, N. Larrieu. "Aeronautical communication transition from analog to digital data: A network security survey", Computer Science Review, 11:1-29, 2014.

[8] T. Keaveney, C. Stewart, "Single European Sky ATM Research Joint Undertaking", SESAR homepage: https://www.sesarju.eu/, Last accessed May, 22nd 2018.

[9] U.S. Department of Transportation, Federal Aviation Administration, "Next Generation Air Transportation System", NextGen homepage: https://www.faa.gov/nextgen/, Last accessed May, 22nd 2018.

[10] C. Morlet, F. Vanin, R. Florou, N. Lan, "Satellite communications for air traffic management", In Proc. of the 19th Ka and Broadband Communications, Navigation and Earth Observation Conference, Florence, Italy, 2013.

[11] T. Gräupl. C. Rihacek, B. Haindl, "LDACS A/G Specification", SESAR2020 PJ14-02-01 D3.3.010, 2017.

[12] M. Sajatovic, B. Haindl, U. Epple, T. Gräupl, C. Rihacek, M. Schnell, N. Fistas, J.-U. Koch, H.-W. Kim, E. Le-Ho, "Updated LDACS1 System Specification", SESAR JU, Brussels, Belgium, report EWA04-1-T2-D1, 2011.

[13] T. Gräupl, M. Ehammer, "L-DACS1 Data Link Layer Evolution of ATN/IPS", in Proc. 30th Digital Avionics Systems Conf., Seattle, WA, 2011.

[14] T. Gräupl, M. Ehammer, C.-H. Rokitansky, "L-DACS 1 Data Link Layer Design and Performance", in Proc. Integrated Communications Navigation and Surveillance Conf., Arlington, VA, 2009.

[15] S. Brandes, M. Schnell, C.H. Rokitansky , M. Ehammer, T. Gräupl, H. Steendam, M. Guenach, C. Rihacek, B. Haindl, "B-VHF - Selected Simulation Results and Final Assessment", in Proc. 25th Digital Avionics Systems Conf., Port-land, OR, 2006.

[16] C. H. Rokitansky, M. Ehammer, T. Gräupl, M. Schnell, S. Brandes, S. Gligorevic, C. Rihacek, M. Sajatovic, "B-AMC A system for future Broadband Aeronautical Multi-Carrier communications in the L-Band", in Proc. 26th Digital Avionics Systems Conf., Dallas, TX, pp. 4.D.2-1 - 4.D.2-13, 2007.

[17] C.H. Rokitansky, M. Ehammer, T. Gräupl, S. Brandes, S. Gligorevic, M. Schnell, C. Rihacek, M. Sajatovic, "B-AMC Aeronautical Broadband Communication in the L- band", in Proc. 1st CEAS European Air and Space Conference, Berlin, Germany, pp. 487-496, 2007.

[18] M. Schnell, S. Brandes, S. Gligorevic, C.-H. Rokitansky, M. Ehammer, T. Gräupl, C. Rihacek, M. Sajatovic, "B-AMC Broadband Aeronautical Multi-carrier Communications", in Proc. Integrated Communications Navigation and Surveillance Conf., Bethesta, MD, 2008.

[19] M. Ehammer, T. Gräupl, "AeroMACS An Airport Communications System", in Proc. 30th Digital Avionics Systems Conf., Seattle, WA, pp.4C1-1,4C1-16, 2011.

[20] O. Osechas, M. Mostafa, T. Gräupl, M. Meurer, "Addressing vulnerabilities of the CNS infrastructure to targeted radio interference", in IEEE Aerospace and Electronic Systems Magazine, vol. 32, no. 11, pp. 34-42, doi: 10.1109/MAES.2017.170020, 2017.

[21] TCCR Agreement. "Common criteria for information technology security evaluation part 1-3: Revision 4", NIST, page 93, 2012.

[22] G. Disterer. "ISO/IEC 27000, 27001 and 27002 for information security management", Last accessed July 29 2017, 2013.

[23] T. Phinney. "IEC 62443: Industrial network and system security", Last accessed July 29 2017, 2013.

[24] SRMGSA FINAL. "Safety Risk Management Guidance For System Acquisitions", 2007.

[25] N. Zelkin, S. Henriksen, "L-band digital aeronautical communications system engineering-initial safety and security risk assessment and mitigation", NASA, 2011.

[26] H. Krawczyk, P. Eronen, "Hmac-based extract-and-expand key derivation function (hkdf)", 2010.

[27] A. Perrig, R. Canetti, J. D. Tygar, D. Song, "The TESLA broadcast authentication protocol", Rsa Cryptobytes, 5, 2005.

[28] E. Käsper, and P. Schwabe, "Faster and timing-attack resistant AES-GCM", In Cryptographic Hardware and Embedded Systems-CHES 2009 (pp. 1-17). Springer, Berlin, Heidelberg, 2009.

[29] H. Krawczyk, R. Canetti, M. Bellare, "HMAC: Keyed-hashing for message authentication", 1997.

[30] Y. Desmedt, "Station-to-station protocol." Encyclopedia of Cryptography and Security. Springer US, 1256-1256, 2011.

[31] T. Gräupl, M. Ehammer, and C.-H. Rokitansky, Simulation Results and Assessment of the NEWSKY Concept for Integrated IP-Based Aeronautical Networking, in Proc. 28th Digital Avionics Systems Conf., Orlando, FL, 2009, pp.4.A.2-1,4.A.2-15.

[32] T. Gräupl, and M. Ehammer, Simulation Results and Final Recommendations of the SANDRA Concept for Integrated IP-Based Aeronautical Networking, in Proc. Integrated Communications Navigation and Surveillance Conf., Herndon, VA, 2013.

[33] B. Haindl, C. Rihacek, M. Sajatovic, B. Phillips, J. Budinger, M. Schnell, D. Lamiano, W. Wilson, "Improvement of L-DACS1 Design by Combining B-AMC with P34 and WiMAX Technologies", Integrated Communications Navigation and Surveillance Conference (ICNS 2009), Arlington, VA, USA, May 2009.

[34] S. Brandes, U. Epple, S. Gligorevic, M. Schnell, B. Haindl, M. Sajatovic, "Physical layer specification of the L-band Digital Aeronautical Communications System (L-DACS1)", in Proc. of the 2009 Integrated Communications, Navigation and Surveillance Conference, ICNS 2009, 2009.

[35] S. Wilson, "The network security architecture and possible safety benefits of the AeroMACS network." Integrated Communications, Navigation and Surveillance Conference (ICNS), 2011. IEEE, 2011.

[36] M. Bellido-Manganell, "Impact assessment of LDACS on JTIDS.", Integrated Communications, Navigation and Surveillance Conference (ICNS), 2017. IEEE, 2017.

[37] N. Mäurer, A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis", Integrated Communications, Navigation and Surveillance Conference (ICNS), Washington D.C, US, 2018.

[38] R. Segers, "Cybersecurity for global Aviation - A Trust Framework enabling global secure aviation interoperability", ICNS Conference 2018 Plenary Panel I, Integrated Communications Navigation and Surveillance Conference (ICNS 2018), 2018.

[39] M. Standar, "Next Generation of CNS Services and the enabling infrastructure", ICNS Conference 2018 Plenary Panel III, Integrated Communications Navigation and Surveillance Conference (ICNS 2018), 2018.

[40] B. Crowe, "Proposed AeroMACS PKI Specification is a Model for Global and National Aeronautical PKI Deployments", WiMAX Forum, Integrated Communications Navigation and Surveillance Conference (ICNS 2016), 2016.

[41] Byrne, D. "AeroMACS At Glance ... Moving Towards the Airport 3.0", WiMAX FORUM, 2018.

[42] ISACA, "COBIT 5: A business framework for the governance and management of enterprise IT." Isaca, 2012.

[43] BSI, "BSI-Standard 200-X - Information Security Management Systems (ISMS), Methodology, Risk Analysis." BSI, 2017.

[44] NIST, "Framework for Improving Critical Infrastructure Cybersecurity - Version 1.1", NIST, 2018.

[45] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, https://www.rfc-editor.org/info/rfc4949.

[46] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, https://www.rfc-editor.org/info/rfc5869.

[47] P. P. Papadimitratos, G. Mezzour, and J.-P. Hubaux. "Certificate revocation list distribution in vehicular communication systems." Proc. of the fifth ACM international workshop on VehiculAr Inter-NETworking. ACM, 2008.

[48] NIST, "FIPS PUB 186-4 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - Digital Signature Standard (DSS)", Information Technology Laboratory, National Institute of Standards and Technology, July 2013, http://dx.doi.org/10.6028/NIST.FIPS.186-4.

[49] Committee on National Security Systems (U.S. Government), "National Information Assurance (IA) Glossary", CNSS Instruction No. 4009, 2006.