Advancing the Security of LDACS

Nils Mäurer, Thomas Gräupl, Corinna Schmitt, Gabi Dreo Rodosek and Helmut Reiser

***Abstract*—The ”Single European Sky” air traffic management master plan foresees the introduction of several modern digital data links for aeronautical communications. The candidate for long-range continental communications is the L-band Digital Aeronautical Communications System (LDACS). LDACS is a cellular, ground-based digital communications system for flight guidance and communications related to safety and regularity of flight. Hence, the aeronautical standards, imposed by the International Civil Aviation Organization (ICAO), for cybersecurity of the link and network layer, apply. In previous works, threat- and risk analyses of LDACS were conducted, a draft for an LDACS cybersecurity architecture introduced, algorithms proposed, and the security of a Mutual Authentication and Key Establishment (MAKE) procedure of LDACS formally verified. However, options for cipher-suites and certificate management for LDACS were missing. Also, previous works hardly discussed the topic of post-quantum security for LDACS. This paper proposes a cell-attachment procedure, which establishes a secure LDACS communication channel between an aircraft and corresponding ground-station upon cell-entry of the aircraft. Via the design of a hybrid LDACS Public Key Infrastructure (PKI), the choice of a pre- or post-quantum Security Level (SL) is up to the communications participants. With that, this work introduces a full LDACS cell-attachment protocol based on a PKI, certificates, certificate revocation and cipher-suites including pre- and post-quantum options. Evaluations in the symbolic model show the procedure to fulfill LDACS security requirements and a communications performance evaluation demonstrates feasibility, matching requirements imposed by regulatory documents.**

***Index Terms*—Cybersecurity, Authentication, Key Establishment, LDACS, Post-Quantum Cryptography, Tamarin, FACTS2, Communications Performance**

I. Introduction

MODERN aircraft are connected to Air Traffic Control (ATC) and Aeronautical Operational Control (AOC) via voice and data communications in all phases of flight [1]. These communications between pilot, air traffic controller, airline and more stakeholders is generally referred to as Air Traffic Management (ATM). Most voice communications today is handled by High Frequency (HF), Very High Frequency (VHF) and satellite, while data communications mostly rely on narrow-band customized VHF or satellite based solutions. As segregation of data communications networks for the transmission of data relating to the safety and regularity of flight and for passenger communications, is mandated, an aircrew today must rely on narrow-band services, while the passengers have access to broadband communications. [1]

Increasing saturation of the VHF band around the world, especially in Europe [1], data links lacking digitalization, bandwidth and cybersecurity [2], are all obstacles for civil air traffic growth. While European air traffic was reduced by 55% due to COVID-19 [3], EUROCONTROL estimates European air traffic to recover by 2024 from 74% to 105%, compared to the air traffic level of 2019 [3]. Data traffic is even estimated to rise above previous levels, since many airlines used the COVID-19 pandemic to replace old aircraft with new ones, that produce more data [3]. Hence, previous shortcomings of the ATM remain and continue to hinder growth. The introduction of several modern digital data links for ATM communications is one pillar to overcome these restrictions [4]. The candidate for long-range terrestrial communications is the L-band Digital Aeronautical Communications System (LDACS). LDACS is a cellular, ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight [4], [5]. Internationally, LDACS is reflected in the International Civil Aviation Organization (ICAO) “Global Air Navigation Plan - GANP”, and is currently under standardization [6].

LDACS will be one of several link layer technologies transporting data in ICAO's Aeronautical Telecommunications Network (ATN)/IP-Protocol Suite (IPS) [7]. Hence relevant aeronautical standards for cybersecurity of the link layer, the network infrastructure, and relevant applications enabled by LDACS apply. Those are ICAO Doc 9896 [7], Radio Technical Commission for Aeronautics DO-379 [8] and ARINC 858 [9]. These documents define access control, options to protect user data in transit on link layer, and protection of the control plane of the radio access technology, as a requirement for incorporation into the ATN/IPS network. In previous works, threat- and risk analysis of LDACS were conducted [10], a draft for an LDACS cybersecurity architecture introduced [11], [12], algorithms were proposed [13], and the security of a Mutual Authentication and Key Establishment (MAKE) procedure of LDACS formally verified [12]. Thereby, the low data rates of aeronautical systems, which originate from limited dedicated spectrum for civil aviation, is considered. Hence, the rationale for the cell-attachment procedure is to reduce the overall amount of LDACS data security overhead [11], [13].

Previous works [11], [13] were missing options for cipher suites for LDACS, negotiation of security algorithms, LDACS Public Key Infrastructure (PKI) based certificates and the possibility to check for the validity of LDACS certificates.

N. Mäurer and T. Gräupl, Institute of Communications and Navigation, German Aerospace Center (DLR), Wessling, Germany (e-mail: {nils.maeurer, thomas.graeupl}@dlr.de).
C. Schmitt and G. Dreo Rodosek, Research Institute CODE, Universität der Bundeswehr München, Neubiberg, Germany (e-mail: {corinna.schmitt, gabi.dreo}@unibw.de).
H. Reiser, Leibniz-Supercomputing Center and the Ludwig-Maximilians-University (LMU) Munich, Garching, Germany (e-mail: reiser@lrz.de).

Furthermore, options to switch between pre- and post-quantum security algorithms were not investigated. Post-quantum security is especially important as safety-of-life aeronautical communications are many decades in service and updating the underlying aeronautical standards is a lengthy process, often taking years. Additionally, these changes need to pass ICAO-imposed safety exercises to prove that necessary security updates do not impact the safety or regularity of flight. Commercial cellular networks today, like 3G, 4G or 5G, on the other hand, receive frequent standards updates by 3GPP, are usually shorter in service and have lower reliability, availability and safety requirements due to their specific design for a non-safety-related use-case. Mainly due to the longevity of aeronautical communications, efficient quantum computers might be available during the life-cycle of LDACS, posing a serious risk for the underlying cryptography [14], [15]. As such, investigating post-quantum options for LDACS prior to the initial release of the LDACS manual is a necessity to ensure long-term LDACS safety and security. Previous MAKE procedures did not take these requirements into account, hence a remodelled, more efficient cell-attachment procedure, as well as security and performance evaluations are missing.

The objective of this paper is to propose a cell-attachment procedure with flexible underlying cryptographic measures, establishing a secure LDACS communication channel between an aircraft and corresponding ground-station upon cell-entry of that aircraft. This paper is an extension of [16]. Section II includes relevant technical background about LDACS and is completed with related work presented in Section III. Section IV sets the design goals of the envisioned protocols leading to the protocol specification (cf. Section V). Section VI provides a proof of the security properties of the cell-attachment procedure, as well as a performance evaluation. In Section VII implications from the evaluations, as well as further optimizations are discussed, before concluding the paper in Section VIII. [1]

II. Background on LDACS

LDACS is a ground-based digital bidirectional communications system for flight guidance and communications related to the safety and regularity of flight [4]. It has been developed in Europe and is currently under standardization in ICAO [6], [17]. It covers current Air Traffic Services (ATS), AOC data and also foresees future applications. A single LDACS cell can serve up to 512 Aircraft Station (AS) that communicate to an LDACS Ground Station (GS) in the Reverse Link (RL). The GS communicates to the AS in the Forward Link (FL). LDACS offers dynamic Coding and Modulation Scheme (CMS) depending on channel quality and enables 230.53 to 1428.27 kbps in the FL and 235.30 to 1390.40 kbps in the RL per LDACS cell, which is up to 90 times the net capacity than the currently used terrestrial links like the VHF data link mode 2 system [15], [17]. In addition to offering high data rates, LDACS introduces message priorities into this domain. Hence, more important messages, such as ATS data, can be scheduled with a higher priority, reaching its destination faster than low prioritized messages. This feature is very important for the introduced cell-attachment procedure, described in Section V. As the LDACS protocol highly relies on its logical channels, these are briefly introduced here: [18]

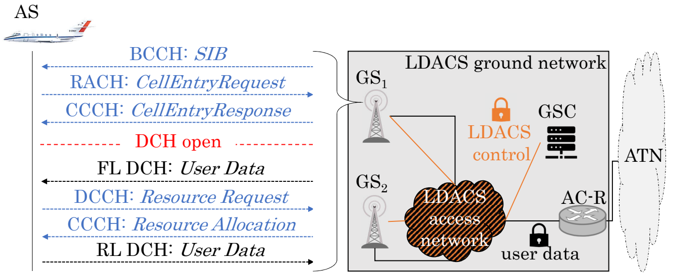


Fig. 1: LDACS *CellEntry* and network overview. Blue text refers to air gap specific LDACS control data (i.e., *CellEntry*), orange to ground specific LDACS control data (i.e., handover data between different GS) and black to user data.

As depicted in Figure 1, user data travels from the ATN via the Access-Router (AC-R) into the LDACS ground network. When this traffic is routed via the ATN/IPS, it is protected by Datagram Transport Layer Security (DTLS) on transport and by Internet Protocol Security (IPSec) on IP layer [9]. To follow the security in depth strategy envisioned by the ATN/IPS [9], data link security is added when data is transmitted over the air-gap, which is exactly where this work on LDACS security comes in. Within the LDACS ground network, there are the Ground Station Controller (GSC), which is responsible for handling LDACS related inter-GS control communications, and the LDACS access network, which connects GSC and AC-R to the last entity in the ground segment, the GS. Once that setup is complete, the GS starts sending a continuous stream of data in the FL, starting with the Broadcast Channel (BCCH), where the GS announces the existence of that LDACS cell via the "System Identification Broadcast (SIB)", the Common Control Channel (CCCH), where resources for sending user data are allocated to AS, and the FL Data Channel (DCH), where actual user data is transmitted. Every AS sends data in short bursts using resources allocated by the GS. The RL consists of the Random Access Channel (RACH), where the AS request access to an LDACS cell, the Dedicated Control Channel (DCCH) channel, where AS request resources that allow them to send user data on the RL DCH. Prior to being able to transmit user data, the AS has to undergo the *CellEntry* procedure. It begins with the AS becoming aware of the GS via reception of the system identification broadcast, then the actual request for cell access in the cell entry request and the GS replying with the cell entry response, which carries important parameters such as the LDACS specific address for that AS.

[1] Part of this work was published at the 1st IEEE Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS) in conjunction with IEEE Euro S&P 2021 [16]. This paper extends the previous work with the analysis of the LTE security design (Section III-C), an update of the LDACS PKI with a hybrid selection between pre- and post-quantum based certificates (Section IV), an update of the LDACS cell-attachment procedure (Section V-C), a detailed evaluation of the performance of the proposed cell-attachment procedure in extensive simulations (Section VI-B) and a discussion of these findings (Section VII).

III. Related Work

To understand the current state of link layer security in aeronautics, the security architectures of two aeronautical systems are discussed briefly in the following: Aeronautical Mobile Airport Communications System (AeroMACS) and ACARS Message Security (AMS).[2] Lastly, since LDACS is based in its design on LTE, security details of LTE are also shortly reviewed before closing with pointing out related work on network and service management.

TABLE I: AMS Security Algorithms [21]

Feature	Implementation
Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) with (1) SHA-256 (256 b) or (2) SHA-1 (160 b)
Key Establishment	Elliptic Curve Diffie-Hellman (ECDH) unified static model per ANSI X9.63
Key Derivation	Key Derivation Function (KDF) per ANSI X9.63 with SHA-256 as underlying hash-function
Message Authentication Code (MAC)	Hash-based Message Authentication Code (HMAC) with SHA-256 truncated to 128, 64, 32 most significant bits
Confidentiality	Either NULL encryption algorithm or AES-128-CFB128

A. ACARS Message Security

AMS offers two secure session establishment protocols: (1) public/private keys [21] based and (2) pre-shared secret key based [22].

As LDACS is very likely to have its own PKI as part of the ATN/IPS, this analysis focuses on the first AMS secure session establishment protocol. In Table I the realized security implementations for different AMS security features are listed. Proposed protocols in [21], [22] are prone to attacks, as demonstrated by Blanchet et. al [23]. In this work, a *key compromise impersonation attack* was identified if the long-term key of an aircraft is compromised, due to session keys being derived taking the long-term keys as input. One possible solution is using ephemeral public/private Diffie-Hellman key pairs for that purpose.

Another issue are the limited cipher suites: (1) key establishment only foresees the ECDH unified static model, hence static keys from which session keys are derived; (2) it is allowed that user data is sent without confidentiality. If encryption is desired AES128-CFB128 is the only option; (3) it is allowed that user data is sent without message integrity and data origin-authenticity. If integrity and authenticity are desired, a HMAC-256 generated MAC, truncated to 32 b is the only option . Finally certificate revocation is handled poorly: while the GS requests signed Certificate Revocation List (CRL) records to check the validity of the aircraft's certificate, the AS never receives proof of the validity of the GS certificate. Smith et al. [24], found some Aircraft Communications Addressing and Reporting System (ACARS) messages to use proprietary, weak ciphers, that the authors could mostly decipher. However, these ciphers are not equivalent to AMS and the authors noticed no use of AMS during their study. One possible reason for the additional existence of proprietary ciphers in ACARS and the limited use of AMS is cost, as the aircraft operator is usually charged extra for AMS. To save that cost and create the feeling of a secure ACARS system, the additional proprietary ciphers were introduced [24].

TABLE II: AeroMACS Security Algorithms [25]

Feature	Implementation
Signature	RSA signature algorithm [27] with SHA-1 [28]
Key Establishment	GS chosen *pre-PAK* encapsulation via RSA and public key of AS → AK key derivation via *Dot16KDF* based on *EAP* or *RSA* or both → KEKs and $H/CMAC$ keys are derived from AK → TEK is generated by the GS and transmitted encrypted via AES and the KEK: Hence the TEK results from AES key wrap with 128-bit key.
Key Derivation	Dot16KDF
MAC	AES-128-CCM
Confidentiality	AES-128-CCM

The cryptographic shortcomings of AMS, as well as the deployment issues of AMS should be taken as a lesson for LDACS. First, the security solution must address and overcome the aforementioned weaknesses and second, security must be an official part of the LDACS standard which ensures that LDACS is deployed with sound security as required by the standard.

B. AeroMACS

AeroMACS Minimum Operational Performance Standards (MOPS) [25] mainly refer to the IEEE 802.16-2009 standard [26] for the implementation of security:

The key management protocol of AeroMACS relies either on Extensible Authentication Protocol (EAP) [29], a PKI with X.509 digital certificates [30] or a sequence of RSA authentication first, followed by EAP. The used key management protocol by AeroMACS is PKMv2 [25]. Here, the focus is on the certificate-based part. Every AS carries a unique X.509 v3 certificate issued by the AS manufacturer binding the AS MAC address to the RSA encryption key.

AeroMACS uses Security Association (SA), which are sets of security information a GS and one or more AS share to support secure communications across a network. The primary SA is obligatory and set up during the initial connection establishment between AS and GS during the authorization process. For that purpose, AeroMACS relies on PKMv02, which has two phases:

Phase 1 – Authentication and Authorization
First, the AS presents the certificate of its Certificate Authority (CA). In a second message, a 64 b random value, its certificate, a Security Association ID (SAID) and an RSA signature over all fields are sent [26], [31]. The GS replies with the third message, including the previous and a new random value, the pre-Primary Authorization Key (PAK) encrypted with the public key of the AS, the lifetime and sequence number of the PAK, its certificate and an RSA-based signature over all attributes in the message. At this point, AS and GS

[2] Note, we chose AMS over Controller–Pilot Data Link Communications (CPDLC) security, since CPDLC can use the Secure Dialogue service described in ICAO Doc 9705 and Doc 9880 [19], but only offers a weak procedural and no cryptographic authentication procedure itself [20].

are mutually authenticated and use the *Dot16KDF* to derive the PAK. Optionally, the EAP procedure may follow, before the authorization key is derived via *Dot16KDF*, PAK and previously exchanged input parameters.

Phase 2 – PKMv2 SA TEK 3-way handshake Cryptographic capabilities are exchanged between AS and GS: a cipher-suite is agreed upon and keys for either Cipher-based MAC (CMAC) or HMAC via *Dot16KDF* and the AK, the Key Encryption Key (KEK), are negotiated. The latter is used by the GS to encrypt the Traffic Encryption Key (TEK)used for user data protection. All three PKMv2 SA TEK 3-way messages are protected by either a CMAC or HMAC generated MACs. Table II includes the used implementations for the different features offered by the AeroMACS security algorithm.

Since both AeroMACS and LDACS are both Future Communications Infrastructure (FCI) technologies, the LDACS PKI is envisioned to be aligned with AeroMACS's. As such, the realization and deployment of AeroMACS PKI shall be discussed shortly here: three different PKI interoperability models, (1) cross-certification, (2) bridge-CA, (3) single root CA were considered and the single root CA architecture chosen [32], [33]. DigiCert, Inc. was selected as AeroMACS root CA host, while COMODO CA, Inc. was chosen for sub-CA, ground device, server and aircraft certificate provider and with Eonti, Inc. managing AeroMACS PKI certificates services on behalf of the WiMAX forum members [32], [33]. These companies need therefore to be trusted by all AeroMACS users.

Summarizing, AeroMACS foresees no ephemeral keys, it only supports one cipher suite option and has no immediate proof, if the used certificates are still valid. LDACS security needs to address these weaknesses and also tackle the issue of establishing worldwide trust in the LDACS PKI.

C. 3GPP Long Term Evolution

In LTE a long-term master-key K is shared between User Equipment (UE) and home subscriber service, more specifically within the authentication center [34]. Hence, other than the security of AMS or the certificate-based authentication procedure of AeroMACS, the entire security between mobile endpoint and LTE network relies on the secrecy of the long-term master-key K. LTE security relies on three layers:

1) **LTE Security Authentication Procedure** - Here, mutual authentication of user equipment and network and the agreement on a mutually shared secret key takes place.
2) **Non Access Stratum Security** - Here, a secure connection between user and network is established to securely (integrity and confidentiality) deliver control data that travels over LTE radio links at NAS level between the UE and the Mobility Management Entity (MME) in the core network.
3) **Access Stratum Security** - This term refers to securing (integrity and confidentiality) signalling/control data and user data (confidentiality) between the user and the LTE base station.

When an UE comes into the vicinity of an LTE cell, the *initial attachment procedure* takes place [35]. Within that procedure, the establishment of a secure connection between UE and LTE network takes place during the *Authentication/Security* step. Essentially, this procedure consists of three steps: (1) the UE presenting its ID of the core network, (2) the core network sending a challenge consisting of an authentication token, a random number and and a key identifier to the UE and (3) the UE providing a response to the core network. That way, UE and the core network have proven to each other to be in possession of the long-term key K and, via using K, having agreed on an intermediary key called K_{ASME}. Further keys are derived from K_{ASME}, used for ensuring NAS and finally AS security.

Known weaknesses of LTE are identity spoofing [36] or, literally, breaking LTE communications on layer 2 [37] forcing the UE to deliver different user-data than requested. A valuable lesson for the security of LDACS from LTE is to also provide protection mechanisms to its control channel plane and to use IDs that are cryptographically linked to a certificate, hence hardening against identity spoofing attacks.

D. Network and Service Management

One useful idea for enhancing the security of the LDACS ground network monitoring the network security compliance as laid out by Lorenz et al. [38]. Since aeronautical user-data flows from air traffic controllers via the AC-R as depicted in Figure 1 into the LDACS ground network via a multitude of hops, the concept of a stateless firewall rule set can help in decreasing overall ground latency times. Depending on the actual realization of the ground network infrastructure in hard- or software, malicious end host (AS, ground) detection in a Software Defined Network (SDN) such as proposed by Varadharajan et al. [39] can further increase ground security. On the same note, in case SDN are an option for certain network parts, the secure placement of a the SDN controller such as proposed by Yang et al. [40] again improves security. Since industrial control, Internet of Things (IoT), and aeronautical communications share the commonalities, that they all are restricted in network and bandwidth resources, ideas from the work by Upadhyay et al. [41] on industrial control system security can also be found throughout this work.

IV. Design Goals

The LDACS cell-attachment security design matches requirements established in previous work [10], [12], [16] and standard protocols and well-established approaches for embedding cryptography are re-used wherever possible.

Previous security analysis of LDACS identified **requirements of the cell-attachment procedure** [11]–[13]: *Mutual Authentication*, *Perfect Forward Secrecy* and *Secure Key Establishment*. This requires the key establishment method to be based on ephemeral keys, or at least on both parties contributing to the final shared secrets. Also, the inputs need to be freshly chosen for every protocol run. LDACS can be used for multiple purposes and depending on its use, different Security Level (SL) are desired. This requires multiple options

This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2022.3189736

TABLE III: Deviating LDACS AS specific certificate content

Field	Value
Validity Period	notBefore: set by Issuing CA, time of certificate creation notAfter: set by Issuing CA, notBefore + 3 year

Subject Distinguished Name	`ID = <UA>`
	`C = <COUNTRY>`
	`O = <PKI Operating Organization>`
	`OU = < "ICAO airline three-letter designator" >`
	`CN = < "air device subject CN" >`

for cipher suites, authentication and key establishment. Additionally, validity of certificates based on a mutually trusted entity, such as a CA, has to be proven during the cell-attachment procedure. As explained in Section II, the LDACS data plane is split into user- and control-data. The user-data data plane must provide integrity and message origin-authentication and can optionally provide confidentiality [7], [10]. To protect the control plane of LDACS, specifically the CCCH, where resource allocations take place, a concept for Group Key Management (GKM) was introduced [42].

To ensure **robustness**, mechanisms of existing protocols are re-used to integrate security into the LDACS cell-attachment process. That way, the protocol depicted in Section V will bear some similarities to the SIGMA [43], the Internet Key Exchange version 2 (IKEv2) [44] and the elliptic curve 3-pass Station-to-Station (STS) protocol [45].

Different LDACS SLs require multiple **cipher-suites** and also the option to incorporate post-quantum options. One reason for defining post-quantum SLs, is the lifetime of digital aeronautical communications systems, with legacy systems, such as VHF Digital Link Mode 2 (VDLm2) existing since the 1990s [15]. First, at pre-quantum SLs, LDACS needs to provide options for different Diffie-Hellman Key Exchange (DHKE) together with public DHKE parameter. Following the work done in [13] ECDH is preferable, due to small overall key sizes in elliptic curves. Quantum-resistant candidates for higher SLs, such as Supersingular Isogeny Key Encapsulation (SIKE) [46], on the other hand provide a key encapsulation mechanism only, hence a separate, fresh input from the other party is necessary. Secondly, different SLs must be reflected in the used cryptography of the accepted certificate, hence the certificate type and version must be communicated, as well as the signature- and hash-algorithm.

To ensure interoperability between different SLs, a **hybrid, pre- and post-quantum combined LDACS PKI** is assumed. This allows one communication partner to choose, e.g., LDACS SL 2 pre-quantum, and all cryptographic primitives further used in the security chain reflect that choice. Following the ideas of Bindel et al. [47], it is suggested to use multiple certificates reflecting all SLs in the proposed advanced security strategy of LDACS. This also means, that the LDACS PKI has to support four different chains of trust, depending on the SL and each entity within the PKI, (i.e., CA, sub-CA or end-entity) has stored four different certificates, one for each SL. Thirdly, using the idea of Authenticated Encryption with Associated Data (AEAD), introduced in TLS 1.3 [48], respective algorithms protecting user data must be agreed upon, as well as underlying hash-algorithms required by AEAD.

Certificate revocations can be tracked by an entity within a PKI via a CRL [30] or the Online Certificate Status Protocol (OCSP) [49]. Here, OCSP is chosen over CRL due to three reasons: (i) bandwidth limitations on the air gap are a major concern for LDACS and OCSP requires less network bandwidth, (ii) the ground-connection from a GS to a Certificate Distribution Center (CDS) has several magnitudes more throughput than the wireless LDACS connection, hence regular updates enable near real-time status checks via OCSP, and (iii) since AS and GS both rely on trust derived from a CA higher up in their chain of trust, they both trust a CA signed OCSP message, guaranteeing the validity of a certificate of a communication partner at a certain point in time. Please note: Due to the hybrid pre-/post-quantum security scheme, OCSP responses have to be available for all SLs, as well.

V. Secure LDACS Cell-Attachment: Protocol

Here the secure LDACS cell-attachment procedure is introduced and described in detail.

A. Certificates and Certificate Handling

Following the recommendations for network nodes in the ATN/IPS from ICAO Doc 9896 [7], RTCA DO-379 [8] and ARINC P-858 [9], the content of LDACS GS certificates is set as depicted in Table IV with the differences in AS and GS certificate depicted in Table III.

Two strategies are combined to save the bandwidth for transmitting certificate data during flight: (1) end-entity certificates, together with the certificate chain up to its root of trust shall be stored securely in local storage [7] and (2) all relevant GS certificates, identified by the intended use of the aircraft or flight plan, shall be installed prior to flight, during maintenance. Please note, for every SL an end-entity supports, the respective certificate of this SL must be installed along with the matching certificate chain-of-trust.

LDACS AS and GS are part of the same LDACS PKI, hence they share a trusted CA. As an end-entity certificate compromise is more likely, compared to a sub-CA takeover, due to the CAs being better protected and using stronger cryptography than end-nodes, it is assumed that CAs in the chain of trust remain trustworthy during the time of flight. Hence, a trusted CA signed OCSP response of the validity of one end-entity certificate, is assumed to be trustworthy during flight. ICAO Doc 9896 [7] defines validity check update rates for offline CAs every 45 days and for online CAs every 48h. The update rates for validity checks of respective end-entity certificates are defined at every new LDACS cell-attachment attempt for both, the AS and GS certificate. With that, the GS requests the update status of AS and GS certificate from a CDS via a secure ground connection every time, an AS attempts to join an LDACS cell. Finally, the validity proof of the GS certificate must also be part of the LDACS cell-attachment procedure depicted in Figures 2 and 3. As mentioned in Section III-B, practical deployment of an LDACS PKI is challenging since it has to reflect the geopolitical realities of aviation. These are, that few states, with limited

TABLE IV: Content of LDACS GS certificates

Field	Value
Version	Positive integer
Serial Number	Positive integer generated by issuing CA
Issuer Signature Algorithm	SL 1 pre-q: ECDSA, SHA-256 [50] SL 2 pre-q: ECDSA, SHA-384 [50] SL 1 post-q: Falcon512 [51] SL 2 post-q: Falcon1024 [51]
Issuer Signature Value	Bit string calculated by Issuing CA on ASN.1 DER-encoded tbsCertificate [30]

Issuer Distinguished Name	`ID = <UA>`
	`C = <COUNTRY>`
	`O = <PKI Operating Organization>`
	`CN = <PKI Operating Organization>`

Validity Period	notBefore: set by Issuing CA, time of certificate creation notAfter: set by Issuing CA, notBefore + 1 year

Subject Distinguished Name	`ID = <UA>`
	`C = <COUNTRY>`
	`O = <PKI Operating Organization>`
	`CN = <GS Operating Organization>`

Subject Public Key Information	SL 1 pre-q: algorithmIdentifier: ID-EC256PublicKey parameter: P-256/brainpoolP256r1 [50], [52] SL 2 pre-q: algorithmIdentifier: ID-EC384PublicKey parameter: P-384/brainpoolP384r1 [50], [52] SL 1 post-q: algorithmIdentifier: ID-Falcon512PublicKey [51] SL 2 post-q: algorithmIdentifier: ID-Falcon1024PublicKey [51]
Issuer's Signature	SL 1 pre-q: ECDSA, SHA-256 [50] SL 2 pre-q: ECDSA, SHA-384 [50] SL 1 post-q: Falcon512 [51] SL 2 post-q: Falcon1024 [51]

TABLE V: LDACS `CCLDACS` Security Algorithms

Feature	Implementation
GKM	SL 1-2 pre-q/post-q: One-way Function Tree (OFT) [53] or GKM [54]
Key Encapsulation	SL 1 pre-q/post-q: AES-128-CCM [55] SL 2 pre-q/post-q: AES-256-CCM [55]
CCCH data protection	SL 1 pre-q/post-q: 96 bit tag, 128 bit key, AES-128-CMAC [56] SL 2 pre-q/post-q: 128 bit tag, 256 bit key, AES-256-CMAC [56]
DCCH data protection	SL 1 pre-q/post-q: 64 bit tag, 128 bit key, AES-128-CMAC [56] SL 2 pre-q/post-q: 64 bit tag, 256 bit key, AES-256-CMAC [56]
Key Derivation	SL 1-2 pre-q/post-q: HMAC Key Derivation Function (HKDF) [57]

trust towards each other, have the technical capabilities of securing critical infrastructure, while ICAO tries to enable access to safe and reliable air transport to every country worldwide, true to its motto ”No Country Left Behind” [20]. As such, trust and technical capabilities are limiting factors in a successful deployment of the PKI. Because of these reasons we recommend a gradual implementation approach via the cross-signing PKI strategy, hence one country setting up the PKI and all countries' root CAs cross-signing to each other. As such, countries with the technical capabilities would benefit from a secure data transport as of today, while other countries can gradually set up their respective PKIs and join the global network via CA cross-signing.

TABLE VI: LDACS `EPLDACS` Security Algorithms

Feature	Implementation
Signature	SL 1 pre-q: ECDSA, SHA-256, P-256/brainpoolP256r1 [50], [52] SL 2 pre-q: ECDSA, SHA-384, P-384/brainpoolP384r1 [50], [52] SL 1 post-q: Falcon512 [51] SL 2 post-q: Falcon1024 [51]
Key Establishment	SL 1 pre-q: ECDH, P-256/brainpoolP256r1 [50], [52] SL 2 pre-q: ECDH, P-384/brainpoolP384r1 [50], [52] SL 1 post-q: SIKEp434_c [46] SL 2 post-q: SIKEp751_c [46]
Key Derivation	SL 1-2 pre-q/post-q: HKDF [57]
MAC (only)	SL 1 pre-q/post-q: 128 bit tag, 128 bit key, AES-128-CMAC [56] SL 2 pre-q/post-q: 128 bit tag, 256 bit key, AES-256-CMAC [56]
Please note: Choice of *MAC (only)* or *AEAD* are mutually exclusive.	
AEAD	SL 1 pre-q/post-q: 128 bit tag, 128 bit key, AES-128-CCM [55] SL 2 pre-q/post-q: 128 bit tag, 256 bit key, AES-256-CCM [55]

B. Cipher Suites

Overall, four SLs are defined, two pre- and two post-quantum, with the possibility to add additional ones in the future. The SL are called LDACS SL 1-2 pre-quantum (pre-q) and LDACS SL 1-2 post-quantum (post-q), reflecting the pre- and post-quantum choice of algorithms and key lengths of a 128 bit key at pre- and post-quantum SL 1 and 256 bit key at pre- and post-quantum SL 2. LDACS supports two kinds of algorithm lists: The first `EPLDACS` represents choices regarding MAKE and either user data integrity and authenticity protection only, or user data AEAD protection. The second, `CCLDACS`, represents choices for GKM protocols and MAC generation for control data protection. Please note, details of LDACS control channel protection are out of scope for this work and the `CCLDACS` is discussed here.

AEAD or MACs only are applied onto LDACS user-data sub-network packet-data units [11], [17], which are 128 Byte to 1536 Byte long [17] and may therefore limit the choice of cryptographic algorithms. The AES-CMAC [56] algorithm is proposed for integrity and authenticity only protection of LDACS user messages, as truncation of the output MAC is explicitly allowed by RFC 4493 [56] and exact security bounds have been evaluated for that scheme [58]. As AEAD scheme, AES-CCM [55] is proposed, due to its simple implementation and non-reliance on initialization vectors. Both schemes, AES-CMAC and AES-CCM, have also the advantage to resist the possible threat of quantum computers [14]. Hence, only key establishment and signature algorithms for LDACS SL 1-2 post-q have to be updated to post-quantum cryptography [14]. To save bandwidth, the use of efficient Elliptic Curve Cryptography (ECC) based signature schemes (here: ECDSA) for SLs 1-2 pre-q with *P-256/brainpoolP256r1* at SL 1 and *P-384/brainpoolP384r1* curves at SL 2 are specified.

SL 1 post-q and above requires quantum-resistant schemes. Since current “National Institute of Standards and Technology (NIST) round-4” and “PQC Selected Algorithms 2022” sig-

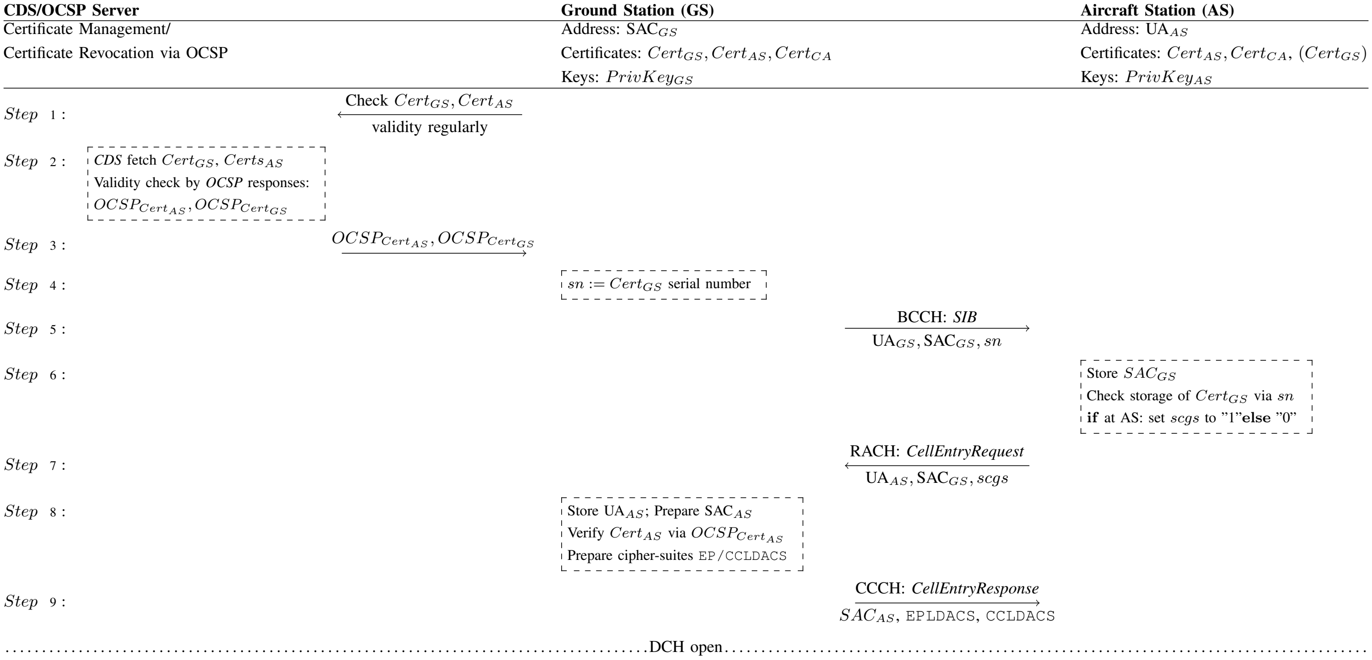

CDS/OCSP Server
Certificate Management/
Certificate Revocation via OCSP
Ground Station (GS)
Address: SAC$_{GS}$
Certificates: $Cert_{GS}, Cert_{AS}, Cert_{CA}$
Keys: $PrivKey_{GS}$
Aircraft Station (AS)
Address: UA$_{AS}$
Certificates: $Cert_{AS}, Cert_{CA}$, $(Cert_{GS})$
Keys: $PrivKey_{AS}$
Step 1 :
Check $Cert_{GS}, Cert_{AS}$
validity regularly
Step 2 :
CDS fetch $Cert_{GS}$, $Certs_{AS}$
Validity check by OCSP responses:
$OCSP_{Cert_{AS}}, OCSP_{Cert_{GS}}$
Step 3 :
$OCSP_{Cert_{AS}}, OCSP_{Cert_{GS}}$
Step 4 :
$sn := Cert_{GS}$ serial number
Step 5 :
BCCH: SIB
UA$_{GS}$, SAC$_{GS}$, sn
Step 6 :
Store SAC_{GS}
Check storage of $Cert_{GS}$ via sn
if at AS: set $scgs$ to "1"else "0"
Step 7 :
RACH: CellEntryRequest
UA$_{AS}$, SAC$_{GS}$, $scgs$
Step 8 :
Store UA$_{AS}$; Prepare SAC$_{AS}$
Verify $Cert_{AS}$ via $OCSP_{Cert_{AS}}$
Prepare cipher-suites EP/CCLDACS
Step 9 :
CCCH: CellEntryResponse
SAC_{AS}, EPLDACS, CCLDACS
DCH open

Fig. 2: 4-pass LDACS cell-attachment procedure (1/2)

nature and key establishment schemes are considered secure to date [3] [4], only the LDACS evaluation criteria of network, computational and storage overhead are considered for the algorithm choice here. Following the argumentation of Ewert et al. [42], the network security data overhead is the most important selection criteria. Hence, the isogeny based Key Encapsulation Mechanism (KEM) SIKE, and the post-quantum signature scheme *Falcon*, with corresponding public parameters, are used for this purpose, as they have the smallest ciphertext and public key size of all current KEMs and smallest signature and public key size of all current post-quantum signature schemes.

At SL 1 post-q, *Falcon512* is used, as its 666 Byte signature[5] is almost four times smaller as the other final-round candidate Dilithium with 2420 Byte[6]. Also public key sizes of *Falcon512*, with 897 Byte, are considerably smaller than the only other post-quantum candidate Rainbow-I, that offers a smaller signature size of 528 Byte but at the cost of a much larger public key size of 157.8 kB [59]. At SL 2 post-q *Falcon1024* is used. Finally, the KEM SIKE, respectively *SIKEp434_c* at level SL 1 post-q and *SIKEp751_c* at SL 2 post-q are chosen as post-quantum key establishment algorithms because of their relatively small public key sizes of 197 Byte and 315 Byte respectively [46]. All proposed security algorithms in EPLDACS and CCLDACS are listed in Tables VI and V.

Following the notations of TLS 1.3 [48], the choice of LDACS_ECDHE_ECDSA_WITH_AES_128_CCM_SHA256 _P256 denotes the algorithmic choice for LDACS SL 1 pre-q with AEAD in place.

C. The LDACS Cell-Attachment Procedure

With cipher suite options for LDACS being defined, the LDACS cell-attachment procedure is formulated and depicted in Figure 2 and 3. Please note, the MAKE procedure is entirely performed in the DCH, as LDACS control channels are small and fixed in size. The LDACS DCH is flexible in size, as briefly described in Section II, supports changes in the underlying cryptography and transports much more data. Please also note, that for all security related data, the highest priority of LDACS messages is foreseen. This allows timely delivery of security related messages, even in a full LDACS cell, with a high data load, as the scheduler prioritizes these above all other messages, except emergency calls. Furthermore, this concept implies a limitation of security related messages per participant, to counter the risk of starving out lower prioritized data traffic, as already mentioned in [13]. Hence, the cell-attachment can be retried three times only, before that participant is locked out by the GS for a predefined time. After that timer has run out, cell-attachment can be retried with that participant again. Basic entities of communication are the CDS together with OCSP server, the GS and the AS. Moreover, the protocol supports both, pre-quantum ECDH key establishment and post-quantum SIKE key encapsulation, interchangeably. If X is an ephemeral secret key, then $\mathrm{P} \leftarrow \textsc{Encaps}(\mathrm{X})$ is the ephemeral public key. On the other hand, $\mathrm{Z} \leftarrow \textsc{Decaps}(\mathrm{P}', \mathrm{X})$ is a shared secret computed from public key P' and a secret X. $\textsc{Enc}_K$ denotes the encryption under key K. In the following the resulting steps, referring to the numbering used in Figure 2 and 3, are briefly described:

[3] https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions, accessed 07/06/2022

[4] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022,accessed07/06/2022

[5] https://falcon-sign.info/, accessed 10/17/2021

[6] https://pq-crystals.org/dilithium/index.shtml, accessed 10/21/2021

Steps 1-3: The GS checks the validity of locally stored certificates $Cert_{GS}$ and $Cert_{AS}$ regularly with the CDS and via OCSP.

Steps 4-9: In the BCCH, the GS announces its existence with the system identification broadcast message, including its unique identifier UA_{GS}, local address, the Sub-net Access Code (SAC) (SAC_{GS}), and its current certificate serial number sn. The approaching AS receives this beacon, stores the GS identifiers and checks whether the GS certificate is stored locally or not. The $scgs = Status_{Cert_{GS}}$ flag is set to "1" else to "0", respectively. The AS replies in the RACH revealing its identifier UA_{AS}. The GS checks whether the AS certificate is stored locally and valid and assigns the LDACS specific address SAC_{AS} to the AS. The SAC_{AS}, all supported cipher-suites for MAKE and user-data protection in $\texttt{EPLDACS}$ and the GS choice of control channel protection algorithms in $\texttt{CCLDACS}$ is sent to the AS. With that, the cell entry procedure of LDACS is done and the MAKE protocol (detailed in step 10-19) begins via the opened DCH channel.

Steps 10-11: The AS chooses algorithms from the provided options and stores that choice in the *algo* parameter. It also stores the received address SAC_{AS}, and the $\texttt{CCLDACS}$ cipher-suite. Depending on the selected algorithms, a private key x_{AS} is chosen, the public key P_{AS} (either a public DHKE key or the public key of the KEM) is computed, and a nonce N_{AS} generated. The public parameters are sent to the GS in the first MAKE message.

Steps 12-13: The GS stores N_{AS} and P_{AS}, generates its nonce N_{GS}, chooses its own private key x_{GS}, calculates P_{GS} (either a public DHKE key or a chosen secret wrapped in P_{AS} representing the ciphertext of the KEM) and responds with the $Cert_{GS}$ (if requested by the AS within *scgs*), N_{GS}, P_{GS} and its $Cert_{GS}$ OCSP validity proof. Then it calculates the shared ephemeral secret z (either via its own private DH key and the public DH key from the AS or by using its generated secret for the KEM, together with the N_{AS} as input for the agreed hash-function $\mathcal{H}$), from which it derives three keys via the set KDF with $\mathrm{z}, N_{AS}, N_{GS}$ as input: (1) the session key $K_{AS,GS}$, (2) the MAC protocol key K_M and (3) the encryption protocol key K_E, of which (2,3) are only used in the MAKE phase.

Steps 14-15: The AS verifies the validity of the $Cert_{GS}$. It further calculates the shared secret z (either via its own private DH key and the public DH key from the GS or by using its generated secret for the KEM, together with the N_{AS} as input for the agreed hash-function $\mathcal{H}$), from which it also derives three keys via the set KDF with $\mathrm{z}, N_{AS}, N_{GS}$ as input: (1) the session key $K_{AS,GS}$, (2) the MAC key K_M and (3) the encryption key K_E, of which (2,3) are only used in the MAKE phase. Using K_M and the keyed-MAC function agreed upon via $\texttt{EPLDACS}$ and $algo$, a MAC m_{AS} over all identifiers is calculated and signed together with *algo*, t_{AS}, N_{AS}, N_{GS} within the signature σ_{AS}. Please note: the MAC m_{AS} is necessary in the signature for identity binding purposes. Finally σ_{AS} is encrypted with K_E and sent to the GS. Please note: the AS uses the algorithms from *algo*. In case no confidentiality option was negotiated and the MAC part in $\texttt{EPLDACS}$ does not contain an encryption option (i.e., AES-CMAC), then AES-128-CCM is used as minimum default.

Steps 16-18: Now the message $\textsc{Enc}_{K_E}(\sigma_{AS})$ is decrypted, m_{AS} generated, and the signature σ_{AS} verified. Upon success, the AS is authentic and the GS builds a MAC of its own with using the identifiers in the order GS, then AS, m_{GS}, and builds its signature σ_{GS} with $\texttt{EPLDACS}$, $\texttt{CCLDACS}$, P_{GS}, P_{AS}, N_{GS}, N_{AS} and m_{GS}. Please note: the MAC m_{GS} is necessary in the signature for identity binding purposes. Finally σ_{GS} is encrypted with K_E and sent to the AS.

Step 19: The AS decrypts $\textsc{Enc}_{K_E}(\sigma_{GS})$, builds m_{GS} and verifies σ_{GS}. Upon success, the GS is authentic, both share the session key $K_{AS,GS}$ and have already reached key confirmation via having successfully used K_M and K_E.

VI. Evaluation

TABLE VII: Tamarin verification results

Lemma	Scope	Result	Steps
Executable (AS has Cert)	Exists-trace	✔Verified	38
Executable (AS needs Cert)	Exists-trace	✔Verified	37
Mutual Authentication	All-traces	✔Verified	92
Secure Key Establishment	All-traces	✔Verified	1042
Perfect Forward Secrecy	All-traces	✔Verified	104

The evaluation of the proposed cell-attachment procedure of LDACS is performed in two ways here: first a formal, symbolic proof is conducted via the symbolic model checking tool Tamarin [60], to demonstrate the fulfillment of the envisioned security properties. In a second step, the security additions are simulated within the LDACS simulation via the Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2) framework [61] and relevant metrics such as added latency and security data overhead measured.

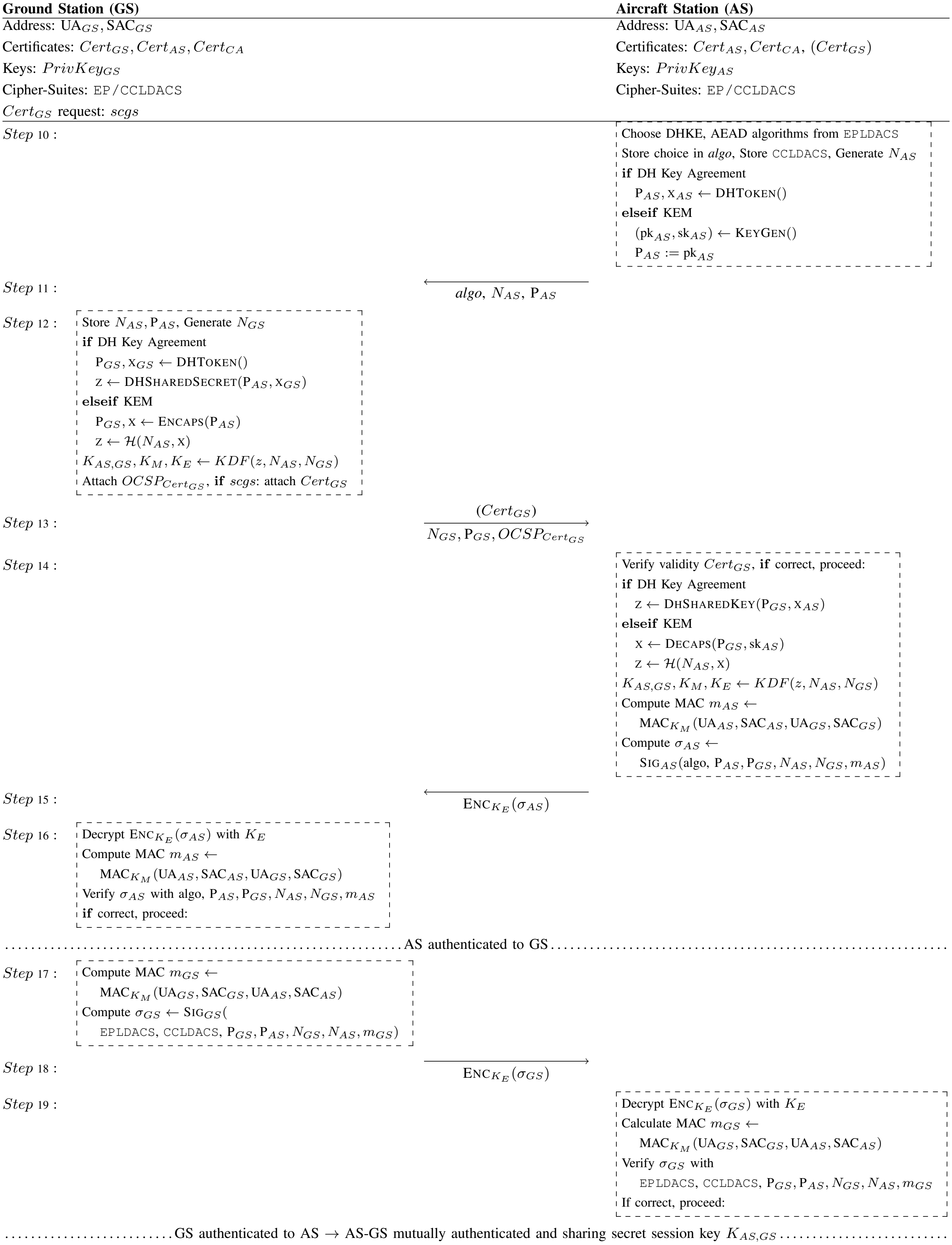
A. Symbolic Model

The details of the symbolic model of the LDACS cell attachment procedure are discussed in [16]. Only the relevant results are therefore repeated here.

The Tamarin prover version 1.6.0 was used in automatic mode to prove the five lemmata presented in [16]. The verification took 2 m 10 s on a Ubuntu 18.04 Laptop with an Intel(R) Core(TM) i7-8650U CPU and 16GB of RAM. All five lemmata could be verified without interaction, as depicted in Table VII.

The source code of the Tamarin model is available for download at GitHub[7]. The "scope" column states which type of proof has been done: 'exists-trace'-proofs verify, that the given property or lemma holds at least for one trace of the protocol; 'all-traces'-proofs respectively verify that the property holds for all traces. The last column displays the number of verification steps that were executed by Tamarin to verify the lemma. As all lemmata have been proven to hold, all required security controls of the LDACS cell-attachment procedure also hold in the symbolic model.

[7] https://github.com/kr4ck-com/LDACSCellAttProof, accessed 06/04/2022



Ground Station (GS)	**Aircraft Station (AS)**
Address: UA$_{GS}$, SAC$_{GS}$	Address: UA$_{AS}$, SAC$_{AS}$
Certificates: $Cert_{GS}, Cert_{AS}, Cert_{CA}$	Certificates: $Cert_{AS}, Cert_{CA}$, $(Cert_{GS})$
Keys: $PrivKey_{GS}$	Keys: $PrivKey_{AS}$
Cipher-Suites: `EP/CCLDACS`	Cipher-Suites: `EP/CCLDACS`
$Cert_{GS}$ request: $scgs$	

Step 10 : (AS)

```
Choose DHKE, AEAD algorithms from EPLDACS
Store choice in algo, Store CCLDACS, Generate $N_{AS}$
if DH Key Agreement
    $P_{AS}, x_{AS} \leftarrow$ DHToken()
elseif KEM
    $(pk_{AS}, sk_{AS}) \leftarrow$ KeyGen()
    $P_{AS} := pk_{AS}$
```

Step 11 : $\xleftarrow[algo,\ N_{AS},\ P_{AS}]{}$

Step 12 : (GS)

```
Store $N_{AS}, P_{AS}$, Generate $N_{GS}$
if DH Key Agreement
    $P_{GS}, x_{GS} \leftarrow$ DHToken()
    $z \leftarrow$ DHSharedSecret($P_{AS}, x_{GS}$)
elseif KEM
    $P_{GS}, x \leftarrow$ Encaps($P_{AS}$)
    $z \leftarrow \mathcal{H}(N_{AS}, x)$
$K_{AS,GS}, K_M, K_E \leftarrow KDF(z, N_{AS}, N_{GS})$
Attach $OCSP_{Cert_{GS}}$, if scgs: attach $Cert_{GS}$
```

Step 13 : $\xrightarrow[N_{GS}, P_{GS}, OCSP_{Cert_{GS}}]{(Cert_{GS})}$

Step 14 : (AS)

```
Verify validity $Cert_{GS}$, if correct, proceed:
if DH Key Agreement
    $z \leftarrow$ DhSharedKey($P_{GS}, x_{AS}$)
elseif KEM
    $x \leftarrow$ Decaps($P_{GS}, sk_{AS}$)
    $z \leftarrow \mathcal{H}(N_{AS}, x)$
$K_{AS,GS}, K_M, K_E \leftarrow KDF(z, N_{AS}, N_{GS})$
Compute MAC $m_{AS} \leftarrow$
    MAC$_{K_M}$(UA$_{AS}$, SAC$_{AS}$, UA$_{GS}$, SAC$_{GS}$)
Compute $\sigma_{AS} \leftarrow$
    Sig$_{AS}$(algo, $P_{AS}, P_{GS}, N_{AS}, N_{GS}, m_{AS}$)
```

Step 15 : $\xleftarrow[\text{Enc}_{K_E}(\sigma_{AS})]{}$

Step 16 : (GS)

```
Decrypt Enc$_{K_E}(\sigma_{AS})$ with $K_E$
Compute MAC $m_{AS} \leftarrow$
    MAC$_{K_M}$(UA$_{AS}$, SAC$_{AS}$, UA$_{GS}$, SAC$_{GS}$)
Verify $\sigma_{AS}$ with algo, $P_{AS}, P_{GS}, N_{AS}, N_{GS}, m_{AS}$
if correct, proceed:
```

....AS authenticated to GS..

Step 17 : (GS)

```
Compute MAC $m_{GS} \leftarrow$
    MAC$_{K_M}$(UA$_{GS}$, SAC$_{GS}$, UA$_{AS}$, SAC$_{AS}$)
Compute $\sigma_{GS} \leftarrow$ Sig$_{GS}$(
    EPLDACS, CCLDACS, $P_{GS}, P_{AS}, N_{GS}, N_{AS}, m_{GS}$)
```

Step 18 : $\xrightarrow[\text{Enc}_{K_E}(\sigma_{GS})]{}$

Step 19 : (AS)

```
Decrypt Enc$_{K_E}(\sigma_{GS})$ with $K_E$
Calculate MAC $m_{GS} \leftarrow$
    MAC$_{K_M}$(UA$_{GS}$, SAC$_{GS}$, UA$_{AS}$, SAC$_{AS}$)
Verify $\sigma_{GS}$ with
    EPLDACS, CCLDACS, $P_{GS}, P_{AS}, N_{GS}, N_{AS}, m_{GS}$
If correct, proceed:
```

..........................GS authenticated to AS → AS-GS mutually authenticated and sharing secret session key $K_{AS,GS}$..........................

Fig. 3: 4-pass LDACS cell-attachment procedure (2/2)

TABLE VIII: Sizes for cryptographic additions in the LDACS cell attachment procedure, *B* is Bytes, *b* is bit

SL	Symbols										
	$OCSP_{Cert_{AS}}$ $OCSP_{Cert_{GS}}$	sn	$scgs$	N_{GS} N_{AS}	`EP-LDACS`	`CC-LDACS`	$algo$	P_{AS}	P_{GS}	$Cert_{GS}$	σ_{AS}/σ_{GS}
1 pre-q	174 *b*	256 *b*	1 *b*	96 *b*	192 *b*	8 *b*	16 *b*	257 *b*	257 *b*	348 *B*	512 *b*
2 pre-q	206 *B*	256 *b*	1 *b*	128 *b*	192 *b*	8 *b*	16 *b*	385 *b*	385 *b*	396 *B*	768 *b*
1 post-q	776 *B*	256 *b*	1 *b*	128 *b*	192 *b*	8 *b*	16 *b*	197 *B*	236 *B*	1814 *B*	666 *B*
2 post-q	1390 *B*	256 *b*	1 *b*	256 *b*	192 *b*	8 *b*	16 *b*	335 *B*	410 *B*	3324 *B*	1280 *B*

B. Computer Simulation

FACTS2 is a simulation framework based on service-oriented software architecture [61]. It allows for rapid prototyping of aeronautical communications systems via powerful tools, allowing for the simulation of real air traffic and air traffic data patterns, as well as the simulation of the data links responsible transmitting that data. LDACS emulations [62], as well as actual LDACS flight trials in 2019 [5] confirmed the correctness and precision of the LDACS implementation within FACTS2.

One system requirement for the LDACS security design is set by RTCA DO-350A. It defines a limit for the cell-attachment time of 10s for Required Communications Performance (RCP) 130/A1 messages [63]. Cell-attachment latency and security data overhead at different LDACS Bit Error Rates (BERs) and CMSs are therefore key performance indicators for the evaluation.

For the implementation of the proposed cell-attachment mechanism into the FACTS2 implementation of LDACS, first the sizes of cryptographic primitives have to be defined. Table VIII depicts all necessary additions for the cell-attachment procedure during the cell-entry. The rationale for these sizes is as follows: (a) signatures sizes are assumed without encoding overhead (i.e., the signature of *ECDSA-SHA-256 on P-256* is represented as two coordinates on the P-256 curve, hence 512 bit), (b) a minimum OCSP response has 110 Byte without the corresponding signature [49], (c) the serial number sn of an LDACS certificate, (d) the existence of the $Cert_{GS}$ at the AS ($scgs$) is indicated via 1 bit, (e) `EPLDACS` is encoded within two bytes and with currently 12 different cipher suites that is 192 bit, (f) the GS chooses the `CCLDACS`, encodes its decision in one byte and tells the AS, which algorithm to use, (g, h) the public DHKE keys of AS and GS have the same size of compressed public elliptic-curve keys [64], while for *SIKE*, P_{AS} actually represents the public *SIKE* key and P_{GS} the ciphertext in which the shared secret in encapsulated into, (i) a X.509 v03 `tbsCertificate` without signature and public key is of minimum length 251 Byte [30], hence the sizes result when adding these two values of the corresponding SL, (j) signatures sizes are assumed without encoding overhead.

a) Establishing a baseline:
To start out with a baseline, hence to find out the minimum communications latency times for the LDACS cell-attachment procedure, an LDACS implementation without security addition was chosen and the total data transported and the latency of the cell-entry procedure measured. For that experiment, the following parameters were chosen, to simulate an optimal environment: (1) The highest LDACS CMS of 8, (2) a BER of 0, (3) one AS entering an otherwise empty LDACS cell, (4) no data traffic within the cell. This resulted in a total amount of exchanged data of 206 bit and took a total of 273 ms. Performing the same experiment, hence the cell-entry procedure with security additions, resulted in a data overhead of (SL 1 pre-q) 758 bit, (SL 2 pre-q, SL 1 post-q) 790 bit, (SL 2 post-q) 918 bit and the same latency of 273 ms for all SLs.

The next question is to find out a baseline for the total cell-attachment latency and security data overhead introduced by each SL of MAKE, with and without the $Cert_{GS}$ stored at AS. The latency and security data overhead values for the LDACS cell-attachment procedure, simulated with one AS in an otherwise empty LDACS cell, with and without $Cert_{GS}$ stored at AS, are given in Table IX.

TABLE IX: Latency and security data overhead

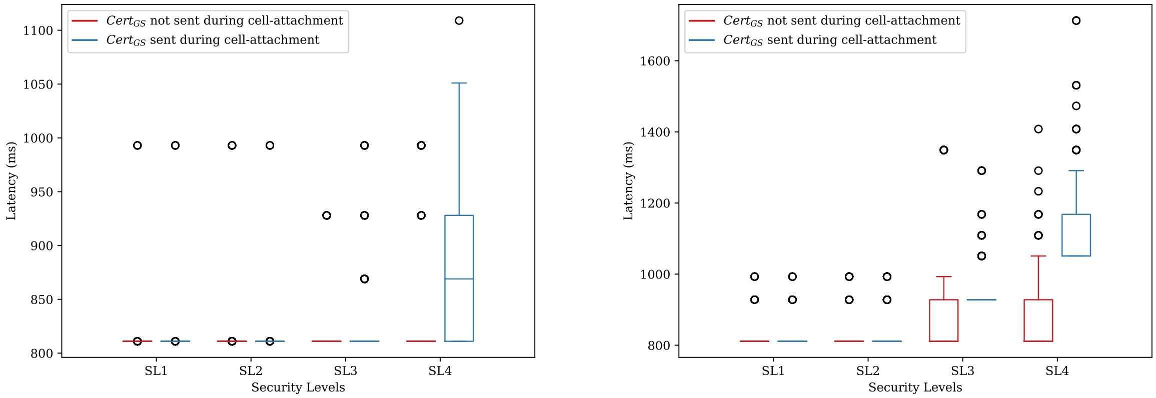
SL	$Cert_{GS}$ at AS		$Cert_{GS}$ not at AS	
	latency	data	latency	data
1 pre-q	811 *ms*	3,594 *bit*	811 *ms*	6,378 *bit*
2 pre-q	811 *ms*	4,682 *bit*	811 *ms*	7,850 *bit*
1 post-q	811 *ms*	21,056 *bit*	811 *ms*	35,568 *bit*
2 post-q	811 *ms*	38,544 *bit*	811 *ms*	65,136 *bit*

As seen in Table IX, the baseline latency remains the same for every configuration resulting in a total latency of 811ms. At a BER of 0, no retransmissions occur and at all SLs, the exchanged security data fits into the scheduled LDACS user-data sub-network packet data units.

Hence, different BER and CMS, representing the scenario of the radio channel quality getting worse, and how that affects the LDACS cell attachment procedure, have to be explored to get a more realistic picture.

b) Changing BER and LDACS CMS:
As a next step, BER, CMS, $scgs$, as well as SLs were set as follows: $BER \in \{0.0, 10^{-6}, 10^{-5}\}$, reflecting the best case of zero bit errors on the data link, the expected working point and the worst case scenario for LDACS operations [17], $CMS \in \{1, 2, 3, 4, 5, 6, 7, 8\}$, reflecting all supported CMS schemes of LDACS from most-robust to most data-efficient data transmission options, $scgs \in \{0, 1\}$ reflecting the option for the $Cert_{GS}$ to be locally stored at the AS and $SL \in \{1 \text{ (pre-q/post-q)}, 2 \text{ (pre-q/post-q)}\}$ representing the four SLs. Overall this resulted in 192 different simulation scenarios.

At $BER = 0$ and for all CMS, the latency for SL 1 pre-q and SL 2 pre-q, with and without $Cert_{GS}$ stored at the AS, remains always at 811ms. The same applies for alle CM for SL 1 post-q, and SL 2 post-q with $Cert_{GS}$ not being transmitted during cell-attachment. However, with the $Cert_{GS}$ being transmitted during the cell-attachment, latency increases slightly to 869ms for SL 1 post-q@$CMS = 1$ and for SL 2 post-q@$CMS \in \{4, 5\}$ and even more for SL 2 post-q



(a) LDACS cell-attachment latencies for $BER = 10^{-6}$

(b) LDACS cell-attachment latencies for $BER = 10^{-5}$

Fig. 4: Comparison of cell-attachment latencies against the design goal of LDACS ($BER = 10^{-6}$) and the worst case ($BER = 10^{-5}$) for LDACS.

@$CMS \in \{1, 2, 3\}$, to 928ms. Otherwise, the CMS has little impact on the overall latency for $BER = 0$.

For $BER \in \{10^{-6}, 10^{-5}\}$, the simulation was repeated 100 times per scenario to receive reliable results. While results from $BER = 10^{-6}$ were close to the ones at $BER = 0$, the three most important findings should be mentioned here: (1) The actual SL does not impact latencies and data overhead much, hence all SLs can be recommended for the LDACS use case; (2) Latencies for all SLs remained below 994ms in the 95-percentile with the maximum latency being at 1110ms for SL 2 post-q with no $Cert_{GS}$ at the AS @$CMS \in \{3, 5\}$; (3) Data overhead remained at a maximum of 6,322 bit at SL1, 7,794 bit at SL2, 35,512 bit at SL 1 post-q, and at SL 2 post-q the 95-percentile remained below 65,081 bit with the maximum being at 136,760 bit. These results and findings are also explicitly shown in Figure 4a. Here the box represents the *interquartile range (IQR)* between qartile 1 (Q1) and quartile 3 (Q3), with the middle line being the median. The upper horizontal line represents the inclusion of all values below $Q3 + 1.5 \times IQR$, while single dots represent *outliers* with a value larger than $Q3 + 1.5 \times IQR$. The most important result here is, even the maximum latency measured at the worst case BER, remains at 1710 ms, hence five times below the requirements set by RTCA DO-350A of 10s [63].

At $BER = 10^{-5}$, the overall cell-attachment latency and data overhead increases due to necessary retransmissions. This is depicted in Figure 4b with the same legends for the boxes as mentioned before fore Figure 4a. Here, For pre-quantum security the amount of transmitted data remains at $BER = 10^{-6}$ level and the 95-percentile latencies below 929 ms, with the maximum detected latency values being at 993 ms. At SL 1 post-q, the amount of transmitted data remains at $BER = 10^{-6}$ level and the 95-percentile latencies increase, but remain below 1111 ms, with maximum value at 1350 ms. At SL 2 post-q, retransmissions of security related data occur, due to the large key and signature sizes. Hence the 95-percentile of transmitted data remains below 89,690 b, with the maximum amount being at 310,840 b. The 95-percentile latency remains below 1351ms with the maximum latency being at 1710 ms.

Overall, these findings clearly demonstrate the viability of the 4-pass cell-attachment procedure for LDACS, as it always remains far below the required 10 s threshold imposed by RTCA DO-350A [63].

VII. Discussions

As demonstrated by the evaluations via Tamarin in Section VI-A, the proposed 4-pass cell-attachment procedure fulfills the LDACS requirements and the evaluations via FACTS2 in Section VI-B reveal the procedure also to match the timing requirements imposed by regulatory documents.

However, certificate distribution, as well as current considerations at ICAO, pose some room for optimizations. First, with ICAO currently being in the process of designing the ATN/IPS, current updates on the ATN/IPS certificates could be applied to LDACS as well: the changes especially affect the lifetime of ground certificates, as these are foreseen to be assigned a lifetime of just one day [65]. The reasoning is, that ground infrastructure has large bandwidth available and the daily update of certificates is most likely cheaper than maintaining a CRL or OCSP infrastructure for ground certificates. For LDACS the change in $Cert_{GS}$ lifetime from one year to one day validity would have the advantage of an overall lower management effort, however coming at the potential cost of increasing the necessary amount of security data on the LDACS datalink [66]. Independent of the final decision on ground certificate lifetimes, an OCSP or CRL service is still necessary for the assurance of validity of the AS certificate, as their lifetime will remain at three years. Hence, the CDS and OCSP services should be separated, e.g., provided by different companies.

Another important finding, concerning certificate lifetime, is, that the lifetime of all $Cert_{AS}$/$Cert_{GS}$ should never start and end at the same time, as this would mean a high load at once, e.g, when the majority of AS certificate need to be renewed. For a better load distribution, the issuing time of certificates should differ in time such that new certificates have to be issued at different points of time. This is especially true, in case the ground certificates actually receive a short, one day lifetime.

A system is always designed for the expected working case, in the case of LDACS for an expected BER of 10^{-6}. At this level of BER, the evaluations of Section VI-B have demonstrated, that a pre-stored $Cert_{GS}$ at the AS does not reduce authentication and key establishment latencies by much for SL 1-2 pre-q and SL 1 post-q. Only at SL 2 post-q, with large post-quantum signatures and public key sizes, the difference in latency between pre-stored and not pre-stored $Cert_{GS}$ was about 300 ms. This is a clear indication that the possible short $Cert_{GS}$ lifetime would be viable. Further, with the design of always sending the $Cert_{GS}$, this also means that the OCSP response for the ground certificate can be omitted, hence saving even more security data overhead and possibly latency.

Lastly, only in the worst case of $BER = 10^{-5}$, the inclusion of $Cert_{GS}$ at every cell-attachment procedure has a much bigger impact. As seen in Section VI-B, at SL 1 post-q, the latency difference is about 200ms and at SL 2 post-q reaches even 800ms. However, as the expected working point of LDACS is set at $BER = 10^{-6}$, that is a design decision that has to be weight against each other depending on the choice of the infrastructure and environment, where LDACS is deployed. If LDACS is deployed within Europe with a tight network of ground stations, then the expected BER will hardly ever be below 10^{-6}. However, if LDACS will further be deployed, e.g., in the northern part of Canada with a vast area to cover with fewer GS, then the expected BER could be lower than 10^{-6} and then pre-installed $Cert_{GS}$ with longer lifetimes could become interesting. However, for now, as LDACS is foreseen to be deployed in Europe first with a high amount of GS (i.e., 84 GS over Europe [67]), the former choice of shorter $Cert_{GS}$ could save latency and security data overhead in the long run.

Overall, the results presented in this work will be taken as input for the standardization efforts of the LDACS cybersecurity architecture at ICAO and within the Internet Engineering Task Force (IETF) [18].

VIII. Conclusion

Throughout this work, a full LDACS cell-attachment procedure, together with AS, GS certificates, possible cipher suites with pre- and post-quantum cryptographic choices, and options for certificate revocations and validity checks was presented. The cell-attachment procedure was carefully designed to work correctly and fulfill the necessary security properties under pre- and post-quantum cryptographic primitives. Looking at two aeronautical communications systems, namely AMS and AeroMACS, and LTE, pros- and cons of their relative security design were discussed. This resulted in identifying key establishment with fresh input parameters from both sides, multiple cipher suites and regular validity checks for certificates as design goals for the LDACS cell-attachment procedure. As LDACS will have its own dedicated PKI, the content of end-entity AS and GS certificates, together with pre- (*ECDSA*) and post-quantum (*Falcon*) signature options was discussed. Then, cipher suite options for user-data AEAD, MAKE algorithms and control-data protection algorithms were listed. Finally the entire LDACS cell-attachment procedure was introduced, spanning the original LDACS cell entry procedure, extending it with a 4-pass MAKE protocol. The design of that procedure was formally verified with Tamarin, passing all tests *Mutual Authentication*, *Secure Key Establishment* and *Perfect Forward Secrecy*. Simulations in FACTS2 proved that the cell-attachment procedure under all four SLs fulfills the 10s connection establishment threshold imposed by RTCA DO-350A. Future work pursues different aspects on LDACS security: (1) finalizing LDACS control channel protection (2) establishing clear guidelines on algorithmic choices in the LDACS cipher-suites, including when and how to upgrade to post-quantum security levels, (3) specifying a secure LDACS ground cell-handover procedure and (4) integrating the LDACS security architecture into the overall ATN/IPS security-in-depth approach.

Appendix

ACARS	Aircraft Communications Addressing and Reporting System
AC-R	Access-Router
AEAD	Authenticated Encryption with Associated Data
AeroMACS	Aeronautical Mobile Airport Communications System
AMS	ACARS Message Security
AOC	Aeronautical Operational Control
AS	Aircraft Station
ATC	Air Traffic Control
ATN	Aeronautical Telecommunications Network
ATM	Air Traffic Management
ATS	Air Traffic Services
BCCH	Broadcast Channel
BER	Bit Error Rate
CA	Certificate Authority
CCCH	Common Control Channel
CDS	Certificate Distribution Center
CMAC	Cipher-based MAC
CMS	Coding and Modulation Scheme
CPDLC	Controller–Pilot Data Link Communications
CRL	Certificate Revocation List
DCCH	Dedicated Control Channel
DCH	Data Channel
DHKE	Diffie-Hellman Key Exchange
EAP	Extensible Authentication Protocol
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FACTS2	Framework for Aeronautical Communications and Traffic Simulations 2
FL	Forward Link
GKM	Group Key Management
GS	Ground Station
GSC	Ground Station Controller
HF	High Frequency
HKDF	HMAC Key Derivation Function

HMAC	Hash-based Message Authentication Code
ICAO	International Civil Aviation Organization
IPS	IP-Protocol Suite
KDF	Key Derivation Function
KEK	Key Encryption Key
KEM	Key Encapsulation Mechanism
LDACS	L-band Digital Aeronautical Communications System
MAC	Message Authentication Code
MAKE	Mutual Authentication and Key Establishment
OCSP	Online Certificate Status Protocol
PAK	Primary Authorization Key
PKI	Public Key Infrastructure
RACH	Random Access Channel
RL	Reverse Link
SA	Security Association
SDN	Software Defined Network
SIKE	Supersingular Isogeny Key Encapsulation
SL	Security Level
TEK	Traffic Encryption Key
UE	User Equipment
VHF	Very High Frequency

REFERENCES

[1] ICAO, "Handbook On Radio Frequency Spectrum Requirements For Civil Aviation, Volume I, ICAO Spectrum strategy, Policy Statements And Related Information," https://standards.globalspec.com/std/10402555/ICAO9718VOLUMEI, accessed 06/04/2022, International Civil Aviation Organization (ICAO), Doc 9718, 01 2018.

[2] M. S. Ben Mahmoud, A. Pirovano, and N. Larrieu, "Aeronautical communication transition from analog to digital data: A network security survey," *Computer Science Review*, vol. 11-12, pp. 1–29, 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013714000021

[3] EUROCONTROL, "EUROCONTROL Forecast Update 2021-2024," https://www.eurocontrol.int/sites/default/files/2021-05/eurocontrol-four-year-forecast-2021-2024-full-report.pdf, accessed 06/04/2022, EUROCONTROL, Tech. Rep., 05 2021.

[4] M. Schnell, U. Epple, D. Shutin, and N. Schneckenburger, "LDACS: Future Aeronautical Communications for Air-Traffic Management," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 104–110, 2014.

[5] M. A. Bellido-Manganell, T. Gräupl, O. Heirich, N. Mäurer, A. Filip-Dhaubhadel, D. M. Mielke, L. M. Schalk, D. Becker, N. Schneckenburger, and M. Schnell, "LDACS Flight Trials: Demonstration and Performance Analysis of the Future Aeronautical Communications System," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 1, pp. 615–634, 2022.

[6] International Civil Aviation Organization (ICAO), "CHAPTER 13 L-Band Digital Aeronautical Communications System (LDACS)," https://portal.icao.int/CP-DCIWG/ACPWGF/DCIWGPT-TMeetingNo19/PT-T19_WP03.1-PfA-LDACS_SARPs.docx, accessed 05/25/2022, International Civil Aviation Organization (ICAO), Montreal, Canada, Tech. Rep., May 2022.

[7] ICAO, "Manual On The Aeronautical Telecommunication Network (ATN) Using Internet Protocol Suite (IPS) Standards and Protocols," https://standards.globalspec.com/std/10026940/icao-9896, accessed 06/04/2022, International Civil Aviation Organization (ICAO), Doc 9896, 01 2015.

[8] RTCA, "Internet Protocol Suite Profiles," https://www.rtca.org/products/do-379/, accessed 06/04/2022, Radio Technical Commission for Aeronautics (RTCA), DO-379, 12 2019.

[9] ARINC, "INTERNET PROTOCOL SUITE (IPS) FOR AERONAUTICAL SAFETY SERVICES PART 1 AIRBORNE IPS SYSTEM TECHNICAL REQUIREMENTS," https://standards.globalspec.com/std/14391274/858p1, accessed 06/04/2022, Aeronautical Radio, Incorporated (ARINC), ARINC SPECIFICATION 858P1, 06 2021.

[10] A. Bilzhause, B. Belgacem, M. Mostafa, and T. Gräupl, "Datalink security in the L-band digital aeronautical communications system (LDACS) for air traffic management," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 11, pp. 22–33, 2017.

[11] N. Mäurer and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018, pp. 1–10.

[12] N. Mäurer, C. Gentsch, T. Gräupl, and C. Schmitt, "Formal Security Verification Of The Station-to-Station Based Cell-Attachment Procedure Of LDACS," in *18th International Conference on Security and Cryptography*. SCITEPRESS Digital Library, 2021, pp. 1–8.

[13] N. Mäurer, T. Gräupl, C. Gentsch, and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS," in *2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, 2020, pp. 1–10.

[14] D. Bernstein and T. Lange, "Post-Quantum Cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[15] RTCA, "Minimum Operational Performance Standards (MOPS) for Aircraft VDL Mode 2 Physical Link and Network Layer," https://www.rtca.org/products/do-281c-electronic/, accessed 06/04/2022, Radio Technical Commission for Aeronautics (RTCA), DO-281C, 09 2018.

[16] N. Mäurer, T. Gräupl, C. Gentsch, T. Guggemos, M. Tiepelt, C. Schmitt, and G. D. Rodosek, "A Secure Cell-Attachment Procedure of LDACS," in *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 2021, pp. 113–122.

[17] T. Gräupl, C. Rihacek, and B. Haindl, "LDACS A/G Specification," https://www.ldacs.com/wp-content/uploads/2013/12/SESAR2020_PJ14-W2-60_D3_1_210_Initial_LDACS_AG_Specification_00_01_00-1_0_updated.pdf, accessed 06/04/2022, German Aerospace Center (DLR), SESAR2020 PJ14-02-01 D3.3.030, 12 2020.

[18] N. Mäurer, T. Gräupl, and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)," Internet Engineering Task Force, Internet-Draft draft-ietf-raw-ldacs-10, 03 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-raw-ldacs-10

[19] ICAO, "Doc 9880 — Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part I-IV," https://standards.globalspec.com/std/10183529/icao-9880-part-i, accessed 02/12/2022, International Civil Aviation Organization (ICAO), Doc 9880, 01 2016.

[20] ICAO, "Doc 10037 - Global Operational Data Link Document (GOLD)," https://www.skybrary.aero/bookshelf/books/4134.pdf, accessed 02/12/2022, International Civil Aviation Organization (ICAO), Doc 10037, 06 2017.

[21] ARINC, "Datalink Security Part 1 - ACARS Message Security," https://standards.globalspec.com/std/1039315/ARINC823P1, accessed 06/04/2022, Aeronautical Radio, Incorporated (ARINC), ARINC SPECIFICATION 823P1, 12 2007.

[22] ARINC, "Datalink Securoity Part 2 - Key Management," https://standards.globalspec.com/std/1086688/arinc-823p2, accessed 06/04/2022, Aeronautical Radio, Incorporated (ARINC), ARINC SPECIFICATION 823P2, 03 2008.

[23] B. Blanchet, "Symbolic and Computational Mechanized Verification of the ARINC823 Avionic Protocols," in *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*, 2017, pp. 68–82.

[24] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS," in *Financial Cryptography and Data Security*, A. Kiayias, Ed. Cham: Springer International Publishing, 2017, pp. 285–301.

[25] RTCA, "Minimum Operational Performance Standards (MOPS) for the Aeronautical Mobile Airport Communication System (AeroMACS," https://www.rtca.org/products/do-346-electronic/, accessed 06/04/2022, Radio Technical Commission for Aeronautics (RTCA), DO-346, 02 2014.

[26] IEEE, "IEEE Standard For Local And Metropolitan Area Networks Part 16: Air Interface For Broadband Wireless Access Systems," https://standards.ieee.org/standard/802_16-2009.html, accessed 06/04/2022, Institute of Electrical and Electronics Engineers (IEEE), IEEE Std 802.16-2009, 03 2009.

[27] J. Jonsson and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1," RFC 3447, 02 2003. [Online]. Available: https://www.rfc-editor.org/info/rfc3447

[28] NIST, "Secure Hash Standard (SHS)," https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf, accessed 06/04/2022, National Institute of Standards and Technology (NIST), FIPS 180-4, 08 2015.

[29] J. Vollbrecht, J. D. Carlson, L. Blunk, D. B. D. Aboba, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748, 06 2004. [Online]. Available: https://www.rfc-editor.org/info/rfc3748

[30] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," RFC 5280, 05 2008. [Online]. Available: https://www.rfc-editor.org/info/rfc5280

[31] F. Yang, "Comparative Analysis on TEK Exchange between PKMv1 and PKMV2 for WiMAX," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, 2011, pp. 1–4.

[32] O. Marcia, "AeroMACS PKI," in *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*, 2018, pp. 1–15.

[33] B. Kamali, *AeroMACS: An IEEE 802.16 Standard-based Technology for the Next Generation of Air Transportation Systems*. John Wiley & Sons, 09 2018.

[34] 3GPP, "3GPP System Architecture Evolution (SAE); Security Architecture," https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-h10.zip, accessed 06/04/2022, 3rd Generation Partnership Project (3GPP), 33.401, 03 2022.

[35] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 17.2)," https://www.3gpp.org/ftp/Specs/archive/23_series/23.401/23401-h40.zip, accessed 06/04/2022, 3rd Generation Partnership Project (3GPP), 23.401, 03 2022.

[36] T. Fei and W. Wang, "LTE Is Vulnerable: Implementing Identity Spoofing and Denial-of-Service Attacks in LTE Networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[37] D. Rupprecht, K. Kohls, T. Holz, and C. Pöpper, "Breaking LTE on Layer Two," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1121–1136.

[38] C. Lorenz, V. Clemens, M. Schrötter, and B. Schnor, "Continuous Verification of Network Security Compliance," *IEEE Transactions on Network and Service Management*, pp. 1–17, 11 2021.

[39] V. Varadharajan and U. Tupakula, "Counteracting Attacks From Malicious End Hosts in Software Defined Networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 160–174, 03 2020.

[40] S. Yang, L. Cui, Z. Chen, and W. Xiao, "An Efficient Approach to Robust SDN Controller Placement for Security," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1669–1682, 05 2020.

[41] D. Upadhyay, M. Zaman, R. Joshi, and S. Sampalli, "An Efficient Key Management and Multi-layered Security Framework for SCADA Systems," *IEEE Transactions on Network and Service Management*, pp. 1–19, 08 2021.

[42] T. Ewert, N. Mäurer, and T. Gräupl, "Group Key Distribution Procedures for the L-Band Digital Aeronautical Communications System (LDACS)," in *2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, 2021, pp. 1–10.

[43] H. Krawczyk, "SIGMA: The 'SIGn-and-MAc' Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols," in *Advances in Cryptology - CRYPTO 2003*, D. Boneh, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 400–425.

[44] C. Kaufman, P. E. Hoffman, Y. Nir, P. Eronen, and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)," RFC 7296, 10 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7296

[45] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2004.

[46] D. Jao, "Supersingular Isogeny Key Encapsulation," https://sike.org/files/SIDH-spec.pdf, accessed 06/04/2022, National Institute of Standards and Technology (NIST), Tech. Rep., 10 2020.

[47] N. Bindel, U. Herath, M. McKague, and D. Stebila, "Transitioning to a Quantum-Resistant Public Key Infrastructure," in *Post-Quantum Cryptography*, T. Lange and T. Takagi, Eds. Cham: Springer International Publishing, 2017, pp. 384–405.

[48] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, 08 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8446

[49] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and D. C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC 6960, 06 2013. [Online]. Available: https://www.rfc-editor.org/info/rfc6960

[50] E. Barker, "Digital Signature Standard (DSS)," https://doi.org/10.6028/NIST.FIPS.186-4, accessed 06/04/2022, National Institute of Standards and Technology (NIST), FIPS.186-4, 07 2013.

[51] D. Soni, K. Basu, M. Nabeel, N. Aaraj, M. Manzano, and R. Karri, *FALCON*. Cham: Springer International Publishing, 2021, pp. 31–41. [Online]. Available: https://doi.org/10.1007/978-3-030-57682-0_3

[52] J. Merkle and M. Lochter, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation," RFC 5639, 03 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5639

[53] Y. Sun, M. Chen, A. Bacchus, and X. Lin, "Towards Collusion-Attack-Resilient Group Key Management Using One-Way Function Tree," *Comput. Netw.*, vol. 104, no. C, p. 16–26, jul 2016. [Online]. Available: https://doi.org/10.1016/j.comnet.2016.04.014

[54] C. F. Muckenhirn and H. Harney, "Group Key Management Protocol (GKMP) Architecture," RFC 2094, 07 1997. [Online]. Available: https://www.rfc-editor.org/info/rfc2094

[55] D. McGrew, D. Bailey, M. Campagna, and R. Dugal, "AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS," RFC 7251, 06 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7251

[56] T. Iwata, J. Song, J. Lee, and R. Poovendran, "The AES-CMAC Algorithm," RFC 4493, 06 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4493

[57] D. H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," RFC 5869, 05 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc5869

[58] M. Nandi, "Improved security analysis for OMAC as a pseudorandom function," *Journal of Mathematical Cryptology*, vol. 3, no. 2, pp. 133–148, 2009. [Online]. Available: https://doi.org/10.1515/JMC.2009.006

[59] M. Raavi, S. Wuthier, P. Chandramouli, Y. Balytskyi, X. Zhou, and S.-Y. Chang, "Security Comparisons and Performance Analyses of Post-quantum Signature Algorithms," in *Applied Cryptography and Network Security*, K. Sako and N. O. Tippenhauer, Eds. Cham: Springer International Publishing, 2021, pp. 424–447.

[60] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The TAMARIN Prover for the Symbolic Analysis of Security Protocols," in *Computer Aided Verification*, N. Sharygina and H. Veith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 696–701.

[61] T. Gräupl, N. Mäurer, and C. Schmitt, "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*, ser. PE-WASUN '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 63–66. [Online]. Available: https://doi.org/10.1145/3345860.3365111

[62] T. Gräupl and M. Mayr, "Method to emulate the L-band digital aeronautical communication system for SESAR evaluation and verification," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, 2015, pp. 2D1–1–2D1–11.

[63] RTCA/EUROCAE, "Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)," RTCA/EUROCAE, Washington, DC / Malakoff, France, DO-350, 03 2016.

[64] G. Seroussi, "ANSI X9.62-2005 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)," https://standards.globalspec.com/std/1955141/ANSIX9.62, access 06/04/2022, Federal Office for Information Security Germany, Tech. Rep., 11 2005.

[65] P. Patterson and V. Maiolla, "ATN IPS Certificate Profiles updated," https://portal.icao.int/CP-DCIWG/testdocument/IPSSecDoc10095EditorialTeamwebmeetingNo9/ATN-IPS-Certificate-Profiles-updated.docx, accessed 10/23/2021, International Civil Aviation Organization (ICAO), Tech. Rep., 05 2021.

[66] T. Ewert, N. Mäurer, and T. Gräupl, "Improving usable ldacs data rate via certificate validity optimization," in *2022 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, 2022, pp. 1–9.

[67] M. Mostafa, M. A. Bellido-Manganell, and T. Gräupl, "Feasibility of Cell Planning for the ¡italic¿L¡/italic¿-Band Digital Aeronautical Communications System Under the Constraint of Secondary Spectrum Usage," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 10, pp. 9721–9733, 2018.

BIOGRAPHIES

Nils Mäurer has been working as a scientist at the Institute of Communications and Navigation for the German Aerospace Center (DLR) since 2017. There he works on cybersecurity in the field of digital aeronautical communication systems. He is researching the cybersecurity design of the L-band Digital Aeronautical Communications System (LDACS), the Future Communications Infrastructure (FCI) candidate for future terrestrial aviation communications. In MICONAV, the maiden flight campaign for LDACS Nils Mäurer was directly responsible for the worldwide first demonstration of Post-Quantum secured communications in civil aviation. Also, he was directly responsible for demonstrating the worldwide first secure transmission of the Ground Based Augmentation System (GBAS) data via the LDACS data link. He is currently finishing his PhD at the Bundeswehr University Munich.

Thomas Gräupl received the Ph.D. degree in computer science and the M.Sc degree in mathematics from the University of Salzburg, Austria in 2011 and 2004, respectively. He is a senior researcher with the institute of communications and navigation of the German Aerospace Center DLR. He was a researcher with the University of Salzburg. His current research interests include wireless digital communication systems and the performance evaluation of communication systems through computer simulations.

Corinna Schmitt received her diploma for Informatics (Bioinformatics) from the Eberhard-Karls Universität Tübingen (Germany). She continued with a Ph.D. in computer science with research in the area of the Internet of Things at the Technische Universität München (Germany) and followed up on it with a habilitation receiving the Venia Legendi in 2021 from the University of Zurich (Switzerland). This was also accepted by the Universität der Bundeswehr München (Germany) where she is employed at the moment as Head of Secure IoT investigating security issues in the connected world on air and ground applications. Additionally, she investigates socio-economic factors related to current IoT applications enhancing the acceptance of new technology in manifold areas as well as rising awareness for security and resilience at the same time.

Gabi Dreo Rodosek is Professor for Communication Systems and Network Security at the Bundeswehr University Munich. She is the Coordinator of the EU H2020 project CONCORDIA and holds several supervisory and advisory mandates in industry. Besides, she is member of the Digital Council of the German Ministry of Defence, member of the World Economic Forum's Global Future Council on Cybersecurity, member of the Board of the Security Network Munich etc. Professor Dreo studied computer science at the University of Maribor, Slovenia and got her PhD and habilitation from the Ludwig-Maximilians-University in Munich. Her research interests include AI-based network security, Software-Defined Networks, 5G/6G, Moving Target Defence.

Helmut Reiser is the deputy director at the Leibniz-Supercomputing Center (Leibniz-Rechenzentrum, LRZ) in Garching near Munich and Professor of computer science at the Ludwig-Maximilians-University (LMU) Munich. The LRZ, as an Institute of the Bavarian Academy of Sciences and Humanities, is the computing center for the Munich Universities of excellence: LMU as well as the Technical University Munich (TUM). Helmut Reiser's research areas as a professor at the LMU chair of Communication Systems and System Programming focus on communication systems and internet-based services, distributed systems, internet-applications, design and operation of IT infrastructures, concepts in IT- and IT service management, system programming and operating systems, as well as IT security.