A Combined Link Layer Security Solution for FCI Datalink Technologies

Nils Mäurer, Thomas Ewert, Thomas Gräupl
Institute of Communication and Navigation
German Aerospace Center (DLR)
Wessling, Germany
{nils.maeurer, thomas.ewert, thomas.graeupl}@dlr.de

Kazuyuki Morioka, Naoki Kanada
Electronic Navigation Research Institute (ENRI)
Tokyo, Japan
{morioka, kanada}@mpat.go.jp

Corinna Schmitt
Research Institute CODE
Universität der Bundeswehr München
Neubiberg, Germany
corinna.schmitt@unibw.de

***Abstract*—With the surge in global air travel demand, the aviation industry is facing significant challenges. The saturation of frequencies in Air Traffic Management (ATM) results in communication issues, necessitating the replacement of traditional analogue systems with digital alternatives. For that purpose several new datalinks are introduced as the Future Communications Infrastructure (FCI). This multilink system aims to ease communications, by allowing data to be routed via any datalink in the FCI, the aircraft is currently connected to. While some FCI datalinks, such as AeroMACS, LDACS, and partially SatCOM, have dedicated security concepts, others like VDLm2 lack such measures. This raises the question of how to securely and efficiently route traffic over any FCI datalink while ensuring the multilink itself remains secure at the link layer.**

The objective of this work is to propose an overall multilink security concept for FCI datalinks. We introduce an initial authentication and key establishment scheme, discuss various security concepts for aircraft authentication to ground endpoints, and propose multiple handover protocols for secure transitions between radios within the multilink. The proposed protocols are evaluated using the Tamarin symbolic model checker, considering their impact on the datalink and ground access network performance. Ultimately, we recommend two suitable concepts for ensuring multilink security at the link layer.

***Index Terms*—Cyber Security, Trust, FCI, LDACS, AeroMACS, VDLm2, Communication Performance**

I. Introduction

The rapid digitization of aviation has brought about significant advancements in aeronautical datalinks, such as the Aeronautical Mobile Airport Communications System (AeroMACS), the L-band Digital Aeronautical Communications System (LDACS), and safety SatCOM. These communications systems, along with older systems, such as the VHF Data Link mode 2 (VDLm2) or High Frequency Next (HFN) play a vital role in ensuring safe and efficient flight operations by enabling the exchange of critical information between aircraft and ground systems. However, a concerning issue persists across these datalinks - the lack of a common, unified datalink security solution [1].

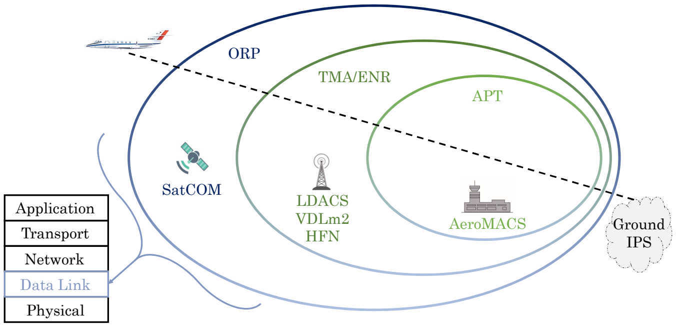

Fig. 1: Aeronautical datalinks with area of application: data is transported from ground IP-Protocol Suite (IPS) in the Airport (APT) domain via AeroMACS, in the Terminal Maneuvering Area (TMA)/En-Route (ENR) domain via LDACS, VDLm2 or HFN, and in the Oceanic, Remote, Polar (ORP) domain via SatCOM. All datalink technologies operate on link layer.

While VDLm2 and HFN lack any datalink security [1], AeroMACS [2], LDACS [3], [4] and safety SatCOM [5] have standardized their own unique solutions. This fact, however, makes handovers of security association in the Future Communications Infrastructure (FCI) multilink system difficult and cumbersome as non-standardized keys are negotiated or authentication procedures differ in their security claims. Thus, the absence of a standardized cybersecurity framework poses serious challenges and vulnerabilities to flight operations. Losing security claims in a handover can mean critical flight-related information, including Air Traffic Control (ATC) instructions, meteorological data, and aircraft performance data, becoming vulnerable to tampering or unauthorized disclosure.

Recognizing the pressing need for a common, unified datalink security solution, the objective of this paper is to present a comprehensive framework that addresses these cybersecurity challenges. By proposing a standardized security solution, this research aims to enhance the resilience, integrity, and confidentiality of aeronautical datalinks, ensuring the safe and efficient functioning of flight operations in the digital age.

The paper is structured as followed: Section II includes necessary information on VDLm2, Iridium SwiftBroadband (SB), Inmarsat Certus, LDACS, AeroMACS, and HFN. Important protocol details, as well as the overall security solution is presented in III. The solution is presented and evaluated in Section IV. Finally, the paper is concluded in Section VI.

II. Background

ARINC standard 858 [6] defines the supported FCI datalinks for the Aeronautical Telecommunications Network (ATN)/IPS. Each of them are presented in the following sections.

A. VHF Datalink Mode 2

VDLm2 is a terrestrial digital aeronautical datalink operating in the Very High Frequency (VHF) band introduced in the 1990s. The user-data payload has a data rate of approximately 10 kbps [7]. However, a large-scale SESAR study in 2015 [8] revealed that by 2025, VDLm2 would be inadequate in providing sufficient Air Traffic Management (ATM) services.

Regarding connection establishment, the three-way handshake defined by RTCA DO-281C [7] has the Ground Station (GS) broadcasting a Ground Station Information Frame (GSIF), the Aircraft Station (AS) responding with its ID and the GS confirming connection establishment. However, VDLm2 does not specify link layer security [7].

B. Safety SatCOM

Currently, two safety SatCOM datalinks are used in aeronautical communications: Inmarsat SB and Iridium Certus [6].

In the aeronautical domain, Inmarsat Iris and JX systems are relevant. Inmarsat Iris is currently certified as class B (possibly evolving to class A) and supports IPv4 at speeds up to 432 kbps [9], [10]. The JX system offers higher QoS with speeds up to 50 Mbps (forward) and 5 Mbps (reverse) per beam. It ensures secure end-to-end connections, including mutual authentication, data integrity protection controls, and secure voice and data paths to the ground [10].

Iridium Certus, currently a class B system, has the potential for an upgrade to class A for IPv4 services. It employs the Iridium NEXT constellation and utilizes the IP Security (IPSec) suite with Internet Key Exchange (IKE) and an Iridium-based Public Key Infrastructure (PKI) for network security and secure communication [11].

C. L-band Digital Aeronautical Communications System

LDACS is a cellular, ground-based system that supports flight guidance and communications related to flight safety and regularity [12], [13]. In Europe, it is the foreseen successor for VDLm2 and enables 1.4 Mbps in both directions for user-data. Roll-out is foreseen starting 2026. LDACS cell-entry is a three way handshake between AS and GS. First, the GS broadcasts regularly a beacon, announcing its cell and ID. Then the AS requests access announcing its ID in a random access channel and lastly, the GS confirms the cell-entry [14]. After the following authentication and key establishment, payload can be securely exchanged. [14]–[16]

TABLE I: Cryptographic Symbols (I)

Symbol	m	c	t	ID	N	T
Meaning	Message	Ciphertext	MAC tag	Identifier	Nonce	Timestamp

TABLE II: Cryptographic Symbols (II)

Symbol	Meaning
K	Cryptographic key
z	Shared secret
g	Public common element (e.g., cyclic group generator)
(r, P)	Ephemeral public-/private-key pair with r denoting the private, P the public key
(S, V)	Long-term public-/private-key pair with S denoting the private, V the public key
$Cert_A$	Certificate of entity A
$OCSP_A$	Validity proof for certificate of entity A

TABLE III: Cryptographic Operations

Symbol	Meaning
$c \leftarrow \textsc{Encrypt}(K, m)$	Encryption
$m \leftarrow \textsc{Decrypt}(K^{-1}, c)$	Decryption
$(c, t) \leftarrow \text{AEAD\_}\textsc{Encrypt}(K, N, m)$	AEAD encryption
$m \leftarrow \text{AEAD\_}\textsc{Decrypt}(K^{-1}, N, (c, t))$	AEAD decryption
$t \leftarrow \textsc{Mac}(K, m)$	MAC tag construction
$\{0, 1\} \leftarrow \textsc{verify}(K, m, t)$	MAC tag verification
$\sigma \leftarrow \textsc{Sig}(S, m)$	Signature construction
$\{0, 1\} \leftarrow \textsc{verify}(V, m, \sigma)$	Signature verification

D. AeroMACS

AeroMACS, based on IEEE 802.16 WiMAX technology, operates in the APT domain, providing safety and non-safety services. It is deployed in over 40 airports globally and offers up to 7.2 Mbps in both directions for user-data [2], [17].

The link establishment process is a three-way message exchange, with the GS broadcasting a beacon containing its transmission parameters and ID. The AS then requests access and informs about its capabilities, which the GS confirms by responding with its own capabilities. Once the ground and aircraft radios are connected, the authentication and key establishment follow, securing the exchange of user-data [2].

E. HF Next

The HFN concept aims to enhance the aged High Frequency (HF) communications by introducing more spectrally efficient waveforms allowing for digital voice, 100 kbps user-data throughput while maintaining interoperability with legacy HF systems. Roll-out is foreseen starting in 2024. Similar to VDLm2, no link layer security is foreseen. [18]

III. FCI Security Solution Prerequisites

In this section, we identify overall security requirements for FCI link layer security, introduce a suitable initial authentication and key establishment method, and present possible air-ground link-layer security association handovers.

A. Notation

The symbols given in Tables I and II are used in this work, with operations defined in Table III. Note, if a symbol is given with $Symbol_A$, it means the symbol is of entity with ID A.

B. Common Security Requirements

ARINC standard 858 [6] defines security requirements for FCI datalinks. These are "[to establish] a secure channel between the airborne radio systems and the peer radio access endpoints on the ground [...] to ensure authentication and integrity of air-ground message exchanges" [6].

a) Authentication: Authentication protocols are responsible for verifying the *authenticity* of entities involved in communication, ensuring *message integrity*, *message authenticity* and proving *undeniability*. Entity authentication focuses on confirming the identity of the sender and receiver, while message authentication also includes maintaining the integrity of the message itself. The definition of "full agreement" by Lowe et al. [19] is utilized for entity authentication in this work. Message integrity and authentication are achieved through the use of Message Authentication Codes (MACs), and message signatures are employed when undeniability is additionally required [20].

b) Key Establishment: Key establishment is typically performed during the establishment of a secure communications channel, involving mutual entity authentication. This process results in the sharing of a common secret, often referred to as the *session key*. Boyd et al. [20] distinguishes between *key transport* and *key agreement* protocols, both of which encompass authentication and key establishment. In *key transport*, one party generates the session key and securely distributes it to all protocol users. In *key agreement*, all parties contribute inputs to derive the session key. Pre-quantum key establishment methods cover both types of protocols. However, in the post-quantum era, only one National Institute of Standards and Technology (NIST)-approved method, CRYSTALS-KYBER[1], is allowed [20]. It is a *key transport* protocol. Therefore, this work considers both types of protocols.

c) Data Integrity, Authentication and Encryption: Data integrity and authenticity can be achieved through symmetric keys and MACs, or asymmetric key pairs and signatures, which also provide the *undeniability* property.

In cases where confidentiality is required in addition to data integrity and authenticity, Authenticated Encryption with Associated Data (AEAD) encryption schemes can be utilized. These schemes generate a pair of ciphertext and tag: $(c, t) \leftarrow AEAD_{Encrypt}(k, N, m)$. If no additional data integrity and authenticity are needed, a simpler encryption scheme can be used: $c \leftarrow Encrypt(k, m)$.

It is important to distinguish between symmetric and asymmetric encryption. Key encapsulation schemes involve asymmetric encryption (key encapsulation and key decapsulation). In symmetric schemes, both parties use the same key k for encryption and decryption. Asymmetric schemes utilize public-private key pairs (S, V). When encrypting a message, the public key of the recipient is employed, ensuring that only the intended recipient can decrypt the message.

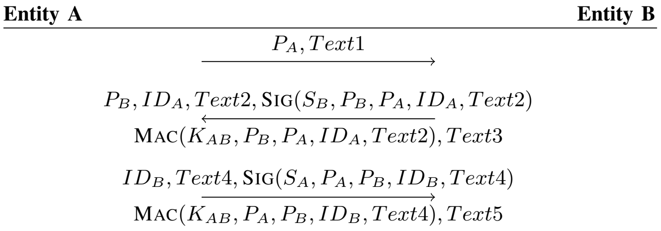
Entity A
Entity B
$P_A, Text1$
$P_B, ID_A, Text2, \textsc{Sig}(S_B, P_B, P_A, ID_A, Text2)$
$\textsc{Mac}(K_{AB}, P_B, P_A, ID_A, Text2), Text3$
$ID_B, Text4, \textsc{Sig}(S_A, P_A, P_B, ID_B, Text4)$
$\textsc{Mac}(K_{AB}, P_A, P_B, ID_B, Text4), Text5$

Fig. 2: Key Agreement Mechanism 7

C. Initial Authentication and Key Establishment

After establishing a link between an aircraft and the ground, the subsequent step involves initial authentication and key establishment to verify identities and negotiate symmetric keys for data protection. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard 11770-3:2021 [21] provides several key agreement schemes for this purpose. To minimize the payload and time required for the authentication sequence, we selected the most suitable candidate, which meets the requirements specified by ARINC 858 [6]. This candidate is the Key Agreement Mechanism (KAM)-7 scheme.

a) Prerequisites: Before any protocol run, the following prerequisites must be met:

1) Each entity A has an asymmetric signature system (S_A, V_A). In an asymmetric signature system, the public key V_A defines the verification transformation.
2) Each entity has access to an authenticated copy of the public key (i.e., V_A or V_B) of the respective other entity.
3) Entities have agreed on a common keyed-MAC function.
4) In case elliptic curve signatures, i.e., Elliptic Curve Digital Signature Algorithm (ECDSA), and key agreement methods are used, i.e., Elliptic Curve Diffie-Hellman (ECDH), both entities have agreed upon a common elliptic curve and hash function.

b) Key Agreement Mechanism 7: This key agreement mechanism is a three-pass scheme that establishes a shared secret between entities A and B with mutual authentication.

Additionally, it provides *key confirmation* (also called *consistency*), *explicit key authentication*, *perfect forward secrecy* upon a fresh selection of shared key parts on each protocol run, *resilience to key compromise impersonation attacks*, *resilience to unknown key share attacks* and even adheres to the highest definition of mutual authentication in Lowe's scale of authentication schemes, called *full agreement* [19]–[21].

The key agreement mechanism 7 is summarized as follows:

1) Entity A randomly and secretly generates r_A and computes P_A via g. Then it sends message 1 in Figure 2.
2) Entity B randomly and secretly generates r_B and computes P_B via g. Then it computes the shared secret key K_{AB} via P_A, r_B, g and builds the message DB_1 via $P_B, P_A, ID_A, Text2$. DB_1 is signed $\textsc{Sig}(S_B, DB_1)$ and a MAC tag $\textsc{Mac}(K_{AB}, DB_1)$ is built for key confirmation. It then sends message 2 in Figure 2.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 (accessed July 16, 2023)

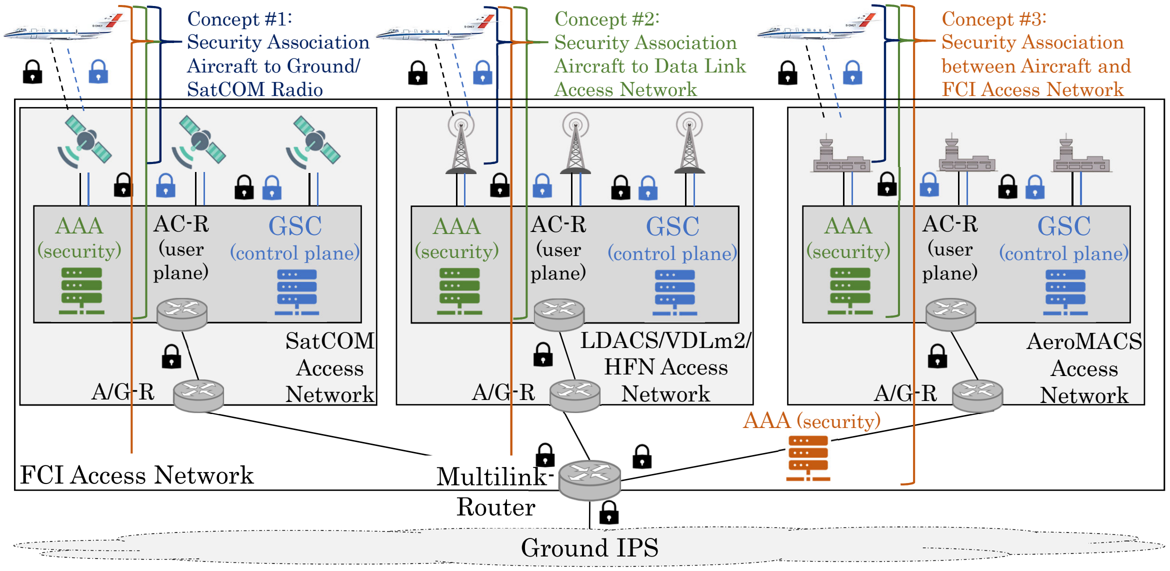

Fig. 3: The FCI link layer security association concepts are applicable to all datalinks. *Concept #1* (dark blue) establishes the datalink security association between the aircraft and a single ground/SatCOM radio. *Concept #2* (dark green) involves the datalink security association with an Authentication, Authorization and Accounting (AAA) server in the datalink access network. *Concept #3* (dark orange) pertains to the datalink security association with an AAA server in the FCI access network. The ATN/IPS data (black) originates from the ground IPS, passes through the multilink router, and is directed to the specific datalink associated with the aircraft. It is then transmitted via the Air/Ground-Router (AG-R) and Access-Router (AC-R) to the connected ground/SatCOM radio for delivery to the aircraft. Link maintenance control data is managed by the Ground Station Controller (GSC) (blue). Control data is secured within the datalink network, while the ATN/IPS data is secured at least at the transport layer until it reaches the AC-R.

3) Entity A verifies B's signature using B's public verification key V_B and verifies A's ID and value P_A sent in the first step. If the checks pass, A constructs the secret key via K_{AB} via r_A, P_B, g. Using K_{AB}, $\text{MAC}(K_{AB}, DB_1)$ can be verified. Then it builds its own signature and MAC tag via the message DB_2, which consists of $P_A, P_B, ID_B, Text4$. It then sends message 3 in Figure 2.
4) At last, entity B verifies A's signature using A's public verification key V_A and verifies B's ID and that values P_A, P_B sent in the previous steps match. If all checks pass, B verifies the $\text{MAC}(K_{AB}DB_2)$.

Please note, key confirmation is explicitly provided in both directions via $\text{MAC}(K_{AB}, DB_1)$ and $\text{MAC}(K_{AB}DB_2)$. Also note, if the data fields $Text1/Text3, Text5/Text3$ contain the public key certificates of entities A and B, respectively, then the second prerequisite can be relaxed to the requirement that all entities are in possession of an authenticated copy of the CA's public verification key. Key confirmation can also be achieved by using K_{AB} to encrypt the signatures instead of transmitting the MACs. In this case prerequisite three changes to "both entities need to have agreed on a common encryption function". [21]

D. Observations on the Handover of Security Associations

Figure 3 shows three security association concepts along with the assumed network topology. While an initial authentication and key establishment given in Section III-C is necessary in all cases, the question remains to which endpoint the aircraft establishes a security association. Each of the three concepts shown in Figure 3 has their distinct advantages and disadvantages and a major impact on how security associations are handed over in the FCI multilink. Since this work focuses on security solutions for FCI datalinks, we assumes that communications entities in the datalink access network or the multilink access network have established a secure communications channel among each other, prior to any aircraft attempting to authenticate.

a) Concept #1: Embedding link layer AAA functionality in the ground/SatCOM radio offers a significant advantage. The security association can remain within the link layer, ensuring high security standards without the need for exporting keys over the ground access network. Keys stored in the radio's Trusted Processing Module (TPM) enable fast and secure initial authentication and key establishment. However, the aircraft needs to re-authenticate when switching between ground/SatCOM radios. Secure communications channels in the datalink access network between entities provide two benefits: first, established keys between aircraft and ground/SatCOM radio can be utilized for seamless secure handover protocols to new radios, keeping the keys within the radio's TPM; second, the trust relationship between an aircraft and a ground/SatCOM radio can extend to other radios in the same datalink access network due to the pre-established trust in that access network.

b) Concept #2: The aircraft performs initial authentication and key establishment with a AAA server located in the datalink access network through the ground/SatCOM radio. This allows the security association to be transferred via the secure ground datalink access network to the intended ground/SatCOM radio during transitions. However, session keys are established between the aircraft and AAA server and securely transported to the connected ground/SatCOM radio. Consequently, this scenario operates beyond the link layer, and keys cannot be securely stored in a single TPM.

c) Concept #3: In the third concept, the aircraft performs initial authentication and key establishment with a AAA server in the multilink access network. The advantage is that the security association can be transferred via the secure ground multilink access network to any datalink ground/SatCOM radio during transitions. When the ground/SatCOM radio informs the GSC about the handover, the multilink AAA server can seamlessly transfer the security association to the specific radio device. Additionally, new keys can be derived from the established key hierarchy between the aircraft and multilink AAA server, with aircraft and AAA server maintaining the master keys.

These concepts demand different solutions, presented in Section IV.

IV. FCI Datalink Security Solution

Here we present the ISO/IEC 11770-3 KAM-7 FCI instatiation and give different HO protocol options.

A. A Note on Trust

Prerequisites in Section III-C require that parties A and B have access to an authenticated copy of the respective other party's public key. This problem is commonly tackled using a PKI, where the public key is stored in an entity's certificate, which is then signed by the entity higher up in the trust chain, i.e., the sub-CA or even the root-CA. Section II already stated that Iridium's SatCOM constellations, AeroMACS and LDACS rely on a dedicated PKI. Hence, for the following Sections IV-B and IV-C a PKI is assumed as well. This includes authentic copies of the entities long-term public keys in the form of certificates $Cert_A$ and possibly the validity proof of those certificates in the form of Online Certificate Status Protocol (OCSP) responses or a current Certificate Revocation List (CRL).

B. Initial Mutual Authentication and Key Agreement

Prerequisites and properties here are the same as given in Section III-C. Background on each FCI datalink given in Section II revealed that every connection establishment process exchanges control-data before user-data can be transmitted. Since the FCI trust infrastructure is PKI based, it is unclear whether an aircraft has an authenticated copy of the ground/SatCOM radio long-term public key locally stored. However, the aircraft can signal ground/SatCOM whether it has stored the certificate in question locally, given that during connection establishment identifiers are already exchanged and that these identifiers are also used in the entity's certificate for identification purposes. Via this approach, unnecessary transmission of the ground/SatCOM radio certificate can be avoided and security data overhead reduced. The instantiated protocol is given in Figure 4.

Entity A			**Entity B**
Step 1 :		$\xrightarrow{P_A, list}$	
Step 2 :	(	$\xleftarrow{ChangeCipherSpec, algo}$	)
Step 3 :	(	$\xleftarrow{P'_A}$	)
Step 4 :		$\xleftarrow{P_B, ID_A, (algo)}$ $\textsc{Sig}(S_B, P_B, P_A, ID_A, (ChangeCipherSpec), algo)$ $\textsc{Mac}(K_{AB}, P_B, P_A, ID_A, (ChangeCipherSpec), algo)$	
Step 5 :		$\xrightarrow{ID_B, (c_{k_{set}}, t_{k_{set}}, OCSP_{Cert_A}, Cert_A)}$ $\textsc{Sig}(S_A, P_A, P_B, ID_B, (c_{k_{set}}, t_{k_{set}}, OCSP_{Cert_A}, Cert_A))$ $\textsc{Mac}(K_{AB}, P_A, P_B, ID_B, (c_{k_{set}}, t_{k_{set}}, OCSP_{Cert_A}, Cert_A))$	

Fig. 4: ISO/IEC 11770-3 KAM-7 FCI instantiation

Please note the protocol shown in Figure 4 assumes A as the ground/SatCOM radio or the datalink/multilink AAA server (provided a secure connection in the respective ground access network) and B as the aircraft radio. The following explains changes from Figure 2 to Figure 4.

Step 1: $Text1$ was replaced by $list$, where entity A lets B know which cipher-suits it supports.

Step 2 and 3: In case P_A is based on elliptic curves that entity B does not support (i.e., a scenario where an American radio uses NIST P- curves for ECDSA, but a German radio only supports brainpool curves [22], [23]), B can communicate that towards A via the $ChangeCipherSpec$ and additionally tells A its choice of algorithms in $algo$. A then replies with a cipher-suite conform public (ephemeral) key P'_A.

Step 4: $Text2$ is replaced by $algo$ (only if steps 2 and 3 were not necessary) and $ChangeCipherSpec$ is additionally included as the $Text2$ field within the $\textsc{Mac}$ and $\textsc{Sig}$ if a change in cipher-suite was necessary in steps 2 and 3. In case A wishes to have a current validity proof of B's certificate (i.e., B's long-term public key S_B), it can request an OCSP response or current CRL from the datalink/multilink AAA or Certificate Distribution Server (CDS).

Step 5: In case group keys are necessary to be distributed to the aircraft, A can AEAD encrypt them in $c_{k_{set}}, t_{k_{set}}$. In case a validity proof of A's long-term public key is necessary, A can add $OCSP_{Cert_A}$. Lastly, if during connection establishment the aircraft did not have $A's$ certificate stored locally, it can send it in the last message in $Text4$. All optional values here for $Text4$ are included in the $\textsc{Mac}$ and $\textsc{Sig}$ operation.

Additionally, the key K_{AB} need not be the session key. We recommend that A and B arrive at the shared secret z (i.e., via r_A, P_B, g or P_A, r_B, g), and then use a, e.g., the HMAC Key Derivation Function (HKDF), to derive all necessary keys [24]. We recommend to derive at least one key for the protocol operations, i.e., K_M for $t_B \leftarrow \textsc{Mac}(K_M, DB_1)$ and $t_A \leftarrow \textsc{Mac}(K_M, DB_2)$ (cf. Section III-C) computations, and one session key, i.e., K_{AB}.

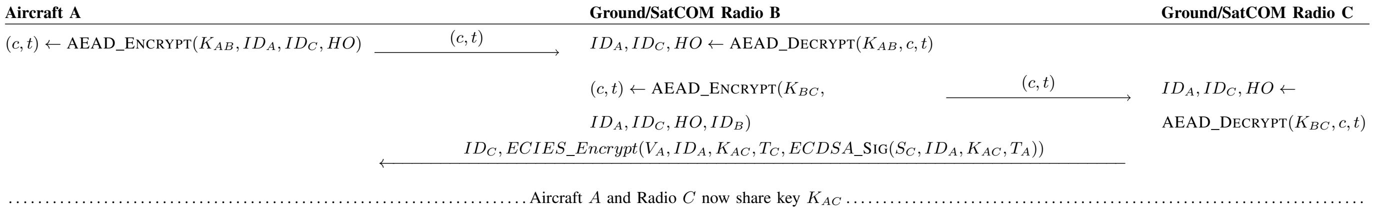
Aircraft A
Ground/SatCOM Radio B
Ground/SatCOM Radio C
$(c,t) \leftarrow$ AEAD_ENCRYPT(K_{AB}, ID_A, ID_C, HO)
(c,t)
$ID_A, ID_C, HO \leftarrow$ AEAD_DECRYPT(K_{AB}, c, t)
$(c,t) \leftarrow$ AEAD_ENCRYPT$(K_{BC},$
$ID_A, ID_C, HO, ID_B)$
(c,t)
$ID_A, ID_C, HO \leftarrow$
AEAD_DECRYPT(K_{BC}, c, t)
$ID_C, ECIES_Encrypt(V_A, ID_A, K_{AC}, T_C, ECDSA_SIG(S_C, ID_A, K_{AC}, T_A))$
Aircraft A and Radio C now share key K_{AC}

Fig. 5: ISO/IEC 11770-3 SKTM-3, with ECIES and ECDSA, FCI instantiated Handover (HO) protocol, setting new key K_{AC}

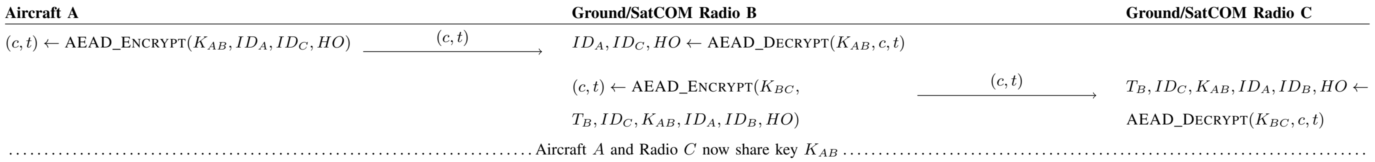
Aircraft A
Ground/SatCOM Radio B
Ground/SatCOM Radio C
$(c,t) \leftarrow$ AEAD_ENCRYPT(K_{AB}, ID_A, ID_C, HO)
(c,t)
$ID_A, ID_C, HO \leftarrow$ AEAD_DECRYPT(K_{AB}, c, t)
$(c,t) \leftarrow$ AEAD_ENCRYPT$(K_{BC},$
$T_B, ID_C, K_{AB}, ID_A, ID_B, HO)$
(c,t)
$T_B, ID_C, K_{AB}, ID_A, ID_B, HO \leftarrow$
AEAD_DECRYPT(K_{BC}, c, t)
Aircraft A and Radio C now share key K_{AB}

Fig. 6: ISO/IEC 11770-2 KEM-3 FCI instantiated HO protocol, reusing A-B established key K_{AB}

If the aircraft authentication counterpart was a datalink/-multilink AAA server, denoted, establishing and using a key hierarchy can further ease later handovers. Let's assume that the aircraft and AAA server have established K_{AB} as a master key. For better readability, we refer to a master key as K_{MK}. From that master key K_{MK}, an aircraft-ground/SatCOM radio session key can be derived on aircraft and AAA server side and then securely transported from AAA server to ground/SatCOM radio. This idea is extended upon in Section IV-C when discussing *Concepts #2/#3* from Section III-D.

C. Lightweight Handover Protocols

Here protocols for all three concepts discussed in Section III-D and shown in Figure 3 are introduced.

a) Concept 1: In case the negotiated keys remain in the respective radios TPMs, a new key with the new ground/SatCOM radio must be agreed upon. With the aircraft already authenticated towards one ground/SatCOM radio, and the ground/SatCOM radios in the datalink access network being securely connected to each other the ISO/IEC 11770-3 Secret Key Transport Mechanism (SKTM)-3 [21], combined with Elliptic Curve Integrated Encryption Scheme (ECIES) and ECDSA can be used. ECIES is standardized in [25] and IND-CCA2 secure. The protocol is given in Figure 5.

It ensures entity authentication of entity C to entity A, implicit key authentication from entity A to entity C, key confirmation from entity C to entity A and A can be sure that it shares the correct key K_{AC} with C, but entity C can only be sure that entity A has indeed received the key after it has obtained a positive reply from entity A encrypted using key K_{AC}. This should be the case once data communications commences.

In case the negotiated keys can be securely exported from respective radios TPMs, the existing security association can be forwarded to the new ground/SatCOM radio. ISO/IEC 11770-2 Key Establishment Mechanism (KEM)-3 [26] can be applied between ground/SatCOM radio B (the one the aircraft is attached to at the moment) and C (the one the aircraft wants to attach to next) when B and C have established a secure communications channel and share a key K_{BC} prior to the handover. Additionally, A, B and C must have agreed upon an AEAD function, e.g., AES-CCM or AES-GCM-SIV. This mechanism provides unilateral authentication C to B, and provides key confirmation and explicit key authentication from B to C. An instantiated version with the aircraft requesting a handover to ground/SatCOM radio C is shown in Figure 6.

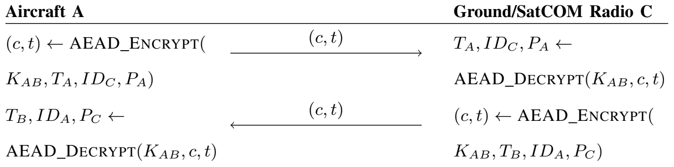
Aircraft A
Ground/SatCOM Radio C
$(c,t) \leftarrow$ AEAD_ENCRYPT$($
$K_{AB}, T_A, ID_C, P_A)$
(c,t)
$T_A, ID_C, P_A \leftarrow$
AEAD_DECRYPT(K_{AB}, c, t)
$T_B, ID_A, P_C \leftarrow$
AEAD_DECRYPT(K_{AB}, c, t)
(c,t)
$(c,t) \leftarrow$ AEAD_ENCRYPT$($
$K_{AB}, T_B, ID_A, P_C)$

Fig. 7: ISO/IEC 11770-2 KEM-5 FCI instantiated HO protocol

Using K_{AB} as a new master key, the aircraft A and ground/SatCOM radio C could then even run the two-pass ISO/IEC 11770-2 KEM-5 [26], which provides A and C with mutual authentication and key confirmation and explicit key authentication from C to A. That way, even upon compromise of key K_{AB} the new connection A-C remains secure. The protocol run is shown in Figure 7.

The shared secret z is derived via r_A, P_C, g on A's side and via r_C, P_A, g on C's side. Key derivation may follow similar as in Section IV-B, however this time strictly following [26], with $z, P_A, P_C, T_A, T_C, ID_A, ID_C$ as IKM to arrive at K_{AC}.

b) Concept 2: As discussed in Section IV-B, when an aircraft initially establishes a security association to an AAA server located in the datalink access network, those entities can agree on a master key from which further keys, e.g., to secure the communications from aircraft to following ground/SatCOM radios in that datalink access network, can be derived. Using ideas from 4G/5G key hierarchy [27], [28], and AAA server and aircraft having initially agreed (cf. Section IV-B) on a master key K_{MK}, we arrive at the following key hierarchy and secret key transport mechanism inspired by the ISO/IEC

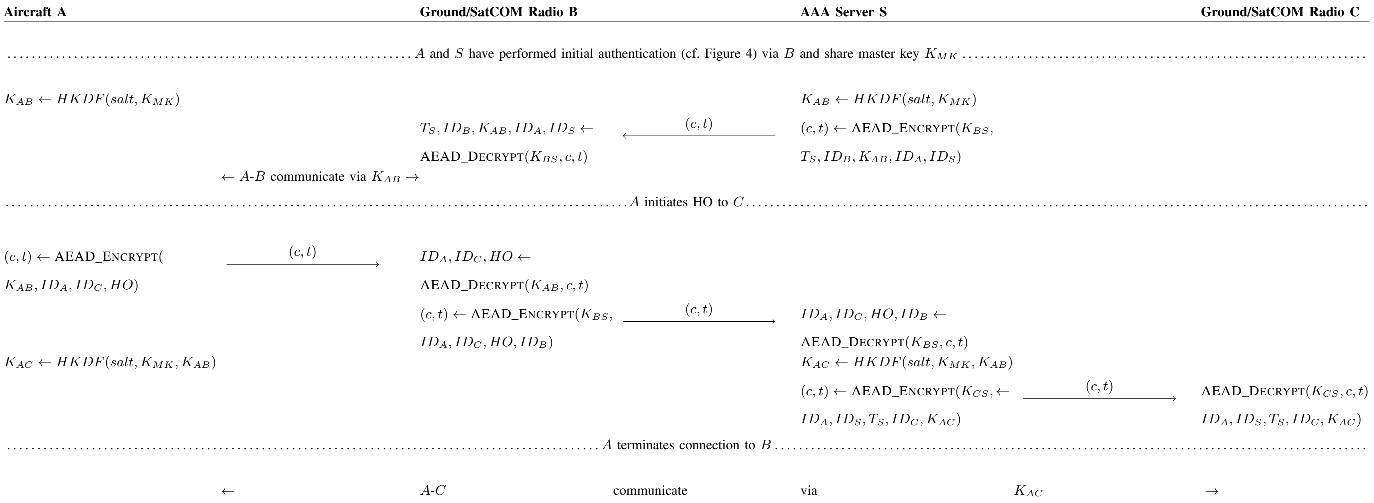
Aircraft A
Ground/SatCOM Radio B
AAA Server S
Ground/SatCOM Radio C
A and S have performed initial authentication (cf. Figure 4) via B and share master key K_{MK}
$K_{AB} \leftarrow HKDF(salt, K_{MK})$
$K_{AB} \leftarrow HKDF(salt, K_{MK})$
$T_S, ID_B, K_{AB}, ID_A, ID_S \leftarrow$ AEAD_DECRYPT(K_{BS}, c, t)
(c,t)
$(c,t) \leftarrow$ AEAD_ENCRYPT$(K_{BS}, T_S, ID_B, K_{AB}, ID_A, ID_S)$
$\leftarrow$ A-B communicate via K_{AB} $\rightarrow$
A initiates HO to C
$(c,t) \leftarrow$ AEAD_ENCRYPT(K_{AB}, ID_A, ID_C, HO)
(c,t)
$ID_A, ID_C, HO \leftarrow$ AEAD_DECRYPT(K_{AB}, c, t)
$(c,t) \leftarrow$ AEAD_ENCRYPT$(K_{BS}, ID_A, ID_C, HO, ID_B)$
(c,t)
$ID_A, ID_C, HO, ID_B \leftarrow$ AEAD_DECRYPT(K_{BS}, c, t)
$K_{AC} \leftarrow HKDF(salt, K_{MK}, K_{AB})$
$K_{AC} \leftarrow HKDF(salt, K_{MK}, K_{AB})$
$(c,t) \leftarrow$ AEAD_ENCRYPT$(K_{CS}, \leftarrow ID_A, ID_S, T_S, ID_C, K_{AC})$
(c,t)
AEAD_DECRYPT(K_{CS}, c, t) $ID_A, ID_S, T_S, ID_C, K_{AC})$
A terminates connection to B
$\leftarrow$ A-C communicate via K_{AC} $\rightarrow$

Fig. 8: ISO/IEC 11770-2 KEM-3 FCI instantiated HO protocol, with Master Key (MK) based Key Derivation Function (KDF)

11770-3 Secret Key Transport Mechanism 3 [26] using HKDF [24]. The protocol is shown in Figure 8 and described below.

After initial authentication and key establishment (cf. Section IV-B) AAA server and aircraft perform the following steps, to arrive at a session key for aircraft A and ground/SatCOM B: For a 128-bit key, set IKM to K_{MK}, $info$ to the purpose of the key, e.g., "Aircraft A-Ground/SatCOM B User-Data AEAD Key", $salt$ to SHA256$(ID_A, ID_B, KC = 0)$, with "KC" referring to "key counter" and counting up the amount of established sessions between aircraft and ground/SatCOM radios - thus KC is set to 0 here. Lastly, set $Hash$ to SHA-256 and L to 16. Then AAA server and aircraft perform $PRK = HMAC_$SHA256$(salt, IKM)$ and $OKM \leftarrow HKDF\_Expand(PRK, info, L)$ with OKM being the resulting aircraft-ground/SatCOM radio session key K_{AB}. For a 256-bit key, the hash-function could be SHA-512 and L must be 32. Finally K_{AB} is securely transported from AAA server to ground/SatCOM radio B.

When a handover from ground/SatCOM radio B to ground/SatCOM radio C is requested by the aircraft A or, initialized from ground via the GSC, AAA server and aircraft perform the following steps, to arrive at a session key for aircraft A and ground/SatCOM C: For a 128-bit key, set IKM to K_{MK}, K_{AB}, $info$ to the purpose of the key, e.g., "Aircraft A-Ground/SatCOM C User-Data AEAD Key", $salt$ to SHA256$(ID_A, ID_B, KC{=}1)$ with KC being set to 1 here since there already was one previous aircraft to ground/SatCOM connection. Lastly, set $Hash$ to SHA-256 and L to 16. Then AAA server and aircraft perform $PRK = HMAC_$SHA256$(salt, IKM)$ and $OKM \leftarrow HKDF\_Expand(PRK, info, L)$ with OKM being the resulting aircraft-ground/SatCOM radio session key K_{AB}. For a 256-bit key, the hash-function could be SHA-512 and L must be 32. Finally K_{AC} is securely transported from AAA server to ground/SatCOM radio C. Please note, how the aircraft key K_{AB} from the previous session is additionally used in IKM and how KC is incremented by 1. For the next handover from ground/SatCOM radio C to ground/SatCOM radio D, IKM is set to K_{MK}, K_{AC}, KC to 2, and so forth. Thus, the respective next session key takes the session key from the previous session as one of its inputs and the counter prevents arriving at the same session key in case the aircraft switches directly between the exact same two ground/SatCOM cells.

Since *Concept #2* assumes the AAA server inside the datalink access network, there are two possible cases when the aircraft switches datalinks. Either, the aircraft undergoes the initial authentication and key agreement (cf. Section IV-B) with the new datalink access network AAA server to establish a new master key. Or, the original master key is hand over to a different data link access network, e.g., from AeroMACS to LDACS, via the secure multilink connection (cf. Figure 3). The first case would also work if only individual access networks are secured internally, without having any secure connections towards other datalinks access network over the multilink access network. The security of the second case entirely relies on a sound secure connection among all FCI candidates within the multilink access network.

c) Concept 3: Here, the same protocol as shown in Figure 8 can be utilized. There are two differences to *Concept #2*: (1) now the ground/SatCOM radio to which the aircraft wishes to transfer to can now be any datalink and (2) neither initial authentication and key agreement (cf. Section IV-B) with a new datalink nor handover of the security association between datalink access networks is necessary anymore.

V. Evaluation

In Section V-A we evaluate the security properties of the proposed security protocols in Figures 4 to 8 in the symbolic model via the symbolic model checker Tamarin [29]. In Section V-B we compare the security data overhead for each and protocol on the datalink and the ground access network.

A. Security Proofs

Tamarin employs a language based on multiset rewriting rules to define protocols and adversaries comprehensively. These rules establish a labeled transition system where the

TABLE IV: Tamarin proof of ARINC 858 [6] specified necessary datalink security properties

Lemma	Scope	Protocol					
		KAM-7	KAM-7 +CCS	SKTM-3	KEM-3	KEM-3 + KEM-5	KEM-3 MK KDF
Session Exists	Exists	✔	✔	✔	✔	✔	✔
2 Sessions Exist	Exists	✔	✔	✔	✔	✔	✔
Authentication A to B	All	✔	✔	✔	✘	✔	(✔)
Authentication B to A	All	✔	✔	✘	✔	✔	(✔)
Session Uniqueness A to B	All	✔	✔	✔	✘	✔	✔
Session Uniqueness B to A	All	✔	✔	✘	✘	✔	✔
Secrecy	All	✔	✔	✔	✔	✔	✔
PFS Secrecy	All	✔	✔	✘	✔	✔	✔
Key Consistency A to B	All	✔	✔	✔	✔	(✔)	(✔)
Key Consistency B to A	All	✔	✔	(✔)	✘	✔	(✔)

state encompasses the symbolic representation of the adversary's knowledge, network messages, freshly generated values, and the protocol's state. Through updating network messages and generating new ones, the adversary and the protocol engage in interactions. The adversary, following the Dolev-Yao model, wields control over the network and possesses the ability to delete, inject, modify, and intercept messages. Essentially, if a security property is valid in the symbolic model, the protocol is guaranteed to uphold that property in all scenarios. Hence, a correctly implemented protocol demonstrates the specified property as proven by this approach. [29]

We proof that one and multiple *sessions exist*, hence confirming the model is executable and allowing the attacker access to primitives of previous protocol runs. We proof *authentication* in both directions via the "full agreement" property [19], hence also *session uniqueness* in both directions. Further, we proof *secrecy* and *perfect forward secrecy* as well as *key consistency*, again in both directions. Definitions of these terms can be found in [20], [21], [26].

For the proof of Figure 4, we implemented two instances, once for a necessary *ChangeCipherSpec* (i.e., KAM-7) and one without (i.e., KAM-CCS). All proofs can be found on github[2]. All lemmas were proven with the Tamarin prover version 1.6.1 on Ubuntu 20.04 LTS with an Intel(R) Core(TM) i7-8850H CPU and 64GB RAM. Note that proofs are given in order of the protocols appearing in Section IV.

Please note, where *key consistency* is specified as possible, but not directly achieved by the protocol itself (denoted (✔)), refers to the fact, that once communication starts and data is secured via the established session key, key confirmation is reached. It is just not directly provided by the protocol message exchange itself. This also upholds for the authentication properties for the MK KDF HO (cf. Figure 8) protocol, where yet another authentication protocol using K_{AC} as base (e.g., the ISO/IEC 9798-2:2019 two-pass mutual authentication protocol [30]) can be woven into the user-data exchange for explicit additional mutual entity authentication.

TABLE V: Sizes of security additions in Byte [B]

Security Level	Symbol								
	P_A	ID_A	σ_A	t_A	$OCSP_A$	$Cert_A$	$ECIES$	K_A	T_A
128 bit	33	3	64	16	174	348	65	16	4
256 bit	49	3	96	32	206	396	113	32	4

TABLE VI: Cryptographic overhead in Byte [B] per protocol

Protocol	Datalink		Access Network	
	Security Level		Security Level	
	128	256	128	256
KAM-7	282	442	(282)	(442)
KAM-7*	456	648	(456)	(648)
KAM-7**	804	1044	(804)	(1044)
KAM-7 +CCS	+ 37	+ 53	(+ 37)	(+ 53)
SKTM-3	179	291	27	43
KEM-3	24	40	27	43
KEM-3+ KEM-5	136	216	47	79
KEM-3 MK KDF	24	40	117	197

B. Performance Evaluation

Here, only the added security data overhead caused on the air gap, i.e., the FCI datalink, and the ground access network is evaluated based on common sizes for cryptographic primitives given in Table V. For ECDH and ECDSA, ECC-256/ECC-384 with compressed points and SHA-256/SHA-384 is assumed, AES-CMAC for MAC tags, AES-GCM-SIV for AEAD encryption, OCSP responses by RFC 6960 [31], certificates as X.509 version 3 by RFC 5280 [32], 32 bit Unix timestamps for T and for ECIES we follow [25].

This results in the following cryptographic overheads, given in Table VI, induced by the various protocols introduced throughout Section IV. For additional message parts we assume 16 Byte for $list$ and 2 Byte for $algo, HO$ and $ChangeCipherSuite$ each. With the KAM-7 protocol has different versions: one without any certificate or OCSP exchange (denoted KAM-7), one with an added OCSP exchange (denoted KAM-7*) and one with both (denoted KAM-7**). Since the $ChangeCipherSuite$ (denoted as CCS) only adds a static amount of byte to the protocol it is given with "+", meaning that the values must be added to the specific version of KAM-7.

The first observation from Table VI is that data-overhead-wise, it is very efficient to have certificates of entities per-stored in the respective radios prior to any initial authentication attempt, since one ECDSA certificate is larger than the entire KAM-7 protocol without $OCSP$ and $Cert$ transmissions. Additionally, if ground/SatCOM radio certificates permit, a short 24 hour lifetime, with regular renewals and thus possibly removing the need for OCSP further reduces the data load upon initial authentication.

[2] https://github.com/NilsMaeurer/fci-security, accessed July 16, 2023

Combining gained knowledge from Table IV and Table VI, allows for a clearer answer to the question which of the three concepts in Figure 3 is best suitable for FCI security.

a) Summary: As initial authentication and key establishment mechanism for any FCI data link, we strongly recommend the use of a PKI and the instantiated version of the KAM-7. As for HO protocols, we observe:

Security wise, using *Concept #1* without exporting keys from the TPM and either running KAM-7 or SKTM-3 with ECIES per HO, is preferable as a new security association is established per new radio/SatCOM radio. SKTM-3 with ECIES also strikes a good balance between security and data overhead cost.

However, when exporting keys is an option, we recommend *Concept #2* with KEM-3 plus KEM-5, which ensures perfect forward secrecy for every new connection at very data overhead cost. If a network provider hosts all datalink types in one secured multilink access network, then we can equally recommend the KEM-3 MK KDF HO protocol for *Concept #2/#3*, since it requires the least data on the data link and follows established ideas from 4G/5G systems.

VI. Conclusions

This work presents a link layer security solution for FCI datalinks in the FCI multilink. We introduce AeroMACS, LDACS, VDLm2, HFN as terrestrial datalinks, and Inmarsat SB and Iridium Certus as space-based datalinks within the FCI. Security requirements for these datalinks are derived from ARINC standard 858. We propose suitable solutions for trust, initial authentication and key establishment, and secure handover protocols. Three architectural concepts for FCI multilink security are discussed, establishing security associations between aircraft and ground/SatCOM radio (*Concept #1*), aircraft and AAA server within the datalink access network (*Concept #2*), and aircraft and AAA server within the multilink access network (*Concept #3*).

We present the ISO/IEC 11770:2021 KAM-7 FCI instantiation as a solution for the initial authentication and key establishment protocol. Handover protocols are provided for all three concepts, considering the network and security association architecture. The introduced protocols are evaluated using the symbolic model checker Tamarin, and security data overhead introduced is calculated per protocol, based on common sizes of cryptographic primitives.

Our conclusion suggests that *Concept #2*, utilizing the ISO/IEC 11770:2018 KEM-3 plus KEM-5 FCI instantiation, strikes the best balance between security data overhead and security. However, *Concept #3*, employing ISO/IEC 11770:2018 KEM-3 and a master key stored at the multilink AAA server, with fresh keys derived per handover and securely transmitted to the ground/SatCOM radio, also provides a good solution to the multilink security association handover problem.

For future work, we plan to incorporate post-quantum options and develop a comprehensive FCI multilink security concept that encompasses existing security solutions for datalinks such as AeroMACS or LDACS.

Acronyms

AAA	Authentication, Authorization and Accounting
AEAD	Authenticated Encryption with Associated Data
AeroMACS	Aeronautical Mobile Airport Communications System
AS	Aircraft Station
ATN	Aeronautical Telecommunications Network
ECDSA	Elliptic Curve Digital Signature Algorithm
FCI	Future Communications Infrastructure
GS	Ground Station
GSC	Ground Station Controller
HFN	High Frequency Next
HKDF	HMAC Key Derivation Function
HO	Handover
IPS	IP-Protocol Suite
KAM	Key Agreement Mechanism
KDF	Key Derivation Function
KEM	Key Establishment Mechanism
LDACS	L-band Digital Aeronautical Communications System
MAC	Message Authentication Code
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
SKTM	Secret Key Transport Mechanism
TPM	Trusted Processing Module
VDLm2	VHF Data Link mode 2

References

[1] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and G.-C. S., “Security in Digital Aeronautical Communications - A Comprehensive Gap Analysis,” *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100549, 2022.

[2] RTCA, “DO-346, Minimum Operational Performance Standards (MOPS) for the Aeronautical Mobile Airport Communication System (AeroMACS,” https://www.rtca.org/products/do-346-electronic/ (accessed January 20, 2023), Radio Technical Commission for Aeronautics (RTCA), Tech. Rep. DO-346, 2014.

[3] 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)*, London, UK, 2018, pp. 1–10.

[4] N. Mäurer, T. Gräupl, and C. Schmitt, “Efficient Control-Channel Security for the Aeronautical Communications System LDACS,” in *Proceedings-24th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks Workshops (WoWMoM) 2023*, 2023, pp. 1–6.

[5] RTCA, “DO-343C, Minimum Aviation System Performance Standard for AMS(R)S Data and Voice Communications Supporting Required Communications Performance (RCP) and Required Surveillance Performance (RSP),” https://www.rtca.org/products/do-343c-electronic/ (accessed January 20, 2023), Radio Technical Commission for Aeronautics (RTCA), Tech. Rep. DO-343C, 2020.

[6] ARINC, “Internet Protocol Suite (IPS) for Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements,” https://standards.globalspec.com/std/14391274/858p1 (accessed January 20, 2023), Aeronautical Radio, Incorporated (ARINC), Tech. Rep. ARINC SPECIFICATION 858P1, 2021.

[7] RTCA, “DO-281C, Minimum Operational Performance Standards (MOPS) for Aircraft VDL Mode 2 Physical Link and Network Layer,” Radio Technical Commission for Aeronautics (RTCA), Tech. Rep. DO-281C, 2018, https://www.rtca.org/products/do-281c-electronic/ (accessed January 20, 2023).

[8] SESAR JU, “VDL Mode 2 Capacity and Performance Analysis,” https://www.sesarju.eu/sites/default/files/documents/news/SJU_VDL_Mode_2_Capacity_and_Performance_Analysis.pdf (accessed January 20, 2023), European Union (EU), SESAR SJU Study v.1., 2015.

[9] N. Ricard, “The Satellite Communications System for Safe and Secure Air Traffic Management Data Links and Voice,” https://artes.esa.int/sites/default/files/FinalWhitePaperrev3.pdf (accessed January 20, 2023), European Space Agency (ESA), Tech. Rep. rev3, 2020.

[10] S. D. Ilčev, “Airborne Satellite CNS Systems and Networks,” in *Global Aeronautical Distress and Safety Systems (GADSS)*, S. D. Ilčev, Ed. Springer International Publishing, 2019, pp. 437–582.

[11] S. L. Barbera, A. Miglietta, S. Sureda-Perez, K. Mineck, N. Fistas, R. Zaruba, S. Tamalet, and L. Albiol, “Future Satellite Communications Data Link in SESAR 2020 and ESA Iris Programme,” in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, Herndon, VA, USA, 2019, pp. 1–11.

[12] 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, 2021.

[13] T. Gräupl, D. M. Mielke, M. A. Bellido-Manganell, L. J. Jansen, N. Mäurer, A. Gürbüz, A. Filip-Dhaubhadel, L. Schalk, D. Becker, M. Skorepa, F. Wrobel, K. Morioka, S. Kurz, and J. Meser, “LDACS Flight Trials: Demonstration of ATS-B2, IPS, and Seamless Mobility,” in *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, Herndon, VA, USA, 2023, pp. 1–13.

[14] 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 January 20, 2023), German Aerospace Center (DLR), Tech. Rep. SESAR2020 PJ14-02-01 D3.3.030, 2020.

[15] N. Mäurer, T. Gräupl, and C. Schmitt, “L-Band Digital Aeronautical Communications System (LDACS),” RFC 9372, Mar. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9372

[16] N. Mäurer, T. Ewert, L. J. Jansen, T. Gräupl, K. Morioka, and C. Schmitt, “International LDACS Security Validation Activities - A Cooperation Effort between DLR and ENRI,” in *2023 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, Herndon, VA, USA, 2023, pp. 1–10.

[17] Y. Sumiya, K. Morioka, N. Kanada, N. Yonemoto, S. Futatsumori, and A. Kohmura, “SARPs Validation Using Aero MACS Prototype – Example of Future Aeronautical Mobile Airport Communication System for SWIM,” in *2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems*, 2015, pp. 192–195.

[18] Collins Aerospace, “HF Next Technical Overview,” https://www.icao.int/safety/FSMP/MeetingDocs/FSMP%20WG8/Presentations/FSMP-WG08-PP01_HF%20Next%20Technical%20Overview.pptx (accessed July 11, 2023), International Civil Aviation Organization (ICAO), ICAO Presentation v.1., 2019.

[19] G. Lowe, “A Hierarchy of Authentication Specifications,” in *Proceedings 10th Computer Security Foundations Workshop*, Rockport, MA, USA, 1997, pp. 31–43.

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

[21] ISO/IEC, “ISO/IEC 11770-3:2021 Information security — Key management — Part 3: Mechanisms using asymmetric techniques,” https://www.iso.org/obp/ui#iso:std:iso-iec:11770:-3:ed-4:v1:en (accessed January 20, 2023), International Standardization Organization (ISO)/International Electrotechnical Commission (IEC), ISO 11770-3:2021, 2021.

[22] NIST, “Digital Signature Standard (DSS),” https://doi.org/10.6028/NIST.FIPS.186-4 (accessed January 20, 2023), National Institute of Standards and Technology (NIST), Tech. Rep. FIPS.186-4, 2013.

[23] J. Merkle and M. Lochter, “Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation,” https://www.rfc-editor.org/info/rfc5639 (accessed January 20, 2023), RFC Editor, RFC 5639, 2010.

[24] H. Krawczyk and P. Eronen, “HMAC-based Extract-and-Expand Key Derivation Function (HKDF),” https://www.rfc-editor.org/info/rfc5869 (accessed January 20, 2023), RFC Editor, RFC 5869, 2010.

[25] ISO/IEC, “ISO/IEC 18033-2:2006 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers,” https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18033:-2:ed-1:v1:en (accessed July 10, 2023), International Standardization Organization (ISO)/International Electrotechnical Commission (IEC), ISO 18033-2:2006, 2006.

[26] ——, “ISO/IEC 11770-2:2018 Information security — Key management — Part 2: Mechanisms using symmetric techniques,” https://www.iso.org/obp/ui#iso:std:iso-iec:11770:-2:ed-3:v1:en (accessed July 10, 2023), International Standardization Organization (ISO)/International Electrotechnical Commission (IEC), ISO 11770-2:2018, 2018.

[27] 3GPP, “3GPP System Architecture Evolution (SAE); Security Architecture,” https://www.3gpp.org/ftp/Specs/archive/33_series/33.401/33401-h10.zip (accessed January 20, 2023), 3rd Generation Partnership Project (3GPP), Tech. Rep. 33.401 - Release 17, 2022.

[28] ——, “Security architecture and procedures for 5G system,” https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h42.zip (accessed January 20, 2023), 3rd Generation Partnership Project (3GPP), Tech. Rep. 33.501 - Release 17, 2022.

[29] S. Meier, B. Schmidt, C. Cremers, and D. Basin, “The TAMARIN Prover For The Symbolic Analysis Of Security Protocols,” in *25th International Conference on Computer Aided Verification (CAV)*. Springer, 2013, p. 696–701.

[30] ISO/IEC, “ISO/IEC 9798-2:2019(en) IT Security techniques — Entity authentication — Part 2: Mechanisms using authenticated encryption,” https://www.iso.org/obp/ui/#iso:std:iso-iec:9798:-2:ed-4:v1:en (accessed July 10, 2023), International Standardization Organization (ISO)/International Electrotechnical Commission (IEC), ISO 9798-2:2019, 2019.

[31] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP,” https://www.rfc-editor.org/info/rfc6960 (accessed January 20, 2023), RFC Editor, RFC 6960, 2013.

[32] 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,” https://www.rfc-editor.org/info/rfc5280 (accessed January 20, 2023), RFC Editor, RFC 5280, 2008.