Improving Usable LDACS Data Rate via Certificate Validity Optimization

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

2022 Integrated Communication, Navigation and Surveillance Conference (ICNS) | 978-1-6654-8419-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICNS54818.2022.9771500

***Abstract*—Since the beginning of the century, an increasing amount of air traffic has pushed current aeronautical communication systems to their limits. Therefore, a modernization process is ongoing, envisioning to digitalize previously analog systems and prepare them for future requirements. Among these efforts is the L-Band Digital Aeronautical Communications System (LDACS), which is a cellular broadband digital data link system, foreseen for regularity-of-flight and safety-communications. Any newly developed system must provide strong cybersecurity, especially when deployed within critical infrastructures. Similar to other communication systems, LDACS will utilize digital certificates within its Public Key Infrastructure (PKI). Such certificates must be available to the respective communication partner, and therefore might have to be transmitted via the radio link upon first contact. With bandwidth generally being a restricting factor in wireless communication, especially in the spectrum-scarce L-band different certificate lifetimes have varying impacts on the amount of security data. In previous research work, reduction of the LDACS security overhead has already been considered in e.g., the secure cell-attachment procedure between ground and aircraft stations or within a proposal for the utilization of group key distribution procedures in LDACS. However, the effect of different certificate lifetimes on the amount of security data and therefore the available user data rate has not been investigated so far. The objective of this paper is to compare different approaches for certificate validity periods in respect to the additional network overheads being created. Computer simulations using historical flight data from the OpenSky Network and a dedicated LDACS simulator help identifying the most effective solution.**

***Index Terms*—LDACS, Cybersecurity, Certificates, PKI, OCSP, CRL, Communications Performance, OpenSky Network**

I. Introduction

In 2015, a Single European Sky ATM Research (SESAR) joint undertaking study revealed the capacity of VHF Data Link mode 2 (VDLm2) to reach its limit on single frequency by 2015, and with the extension by four frequencies, by 2025 [26]. It also recommends to prioritize the development of next generation datalinks. With the COVID-19 pandemic reducing European air traffic by 55% from its 2019 level, recovery from the pandemic progresses and is estimated to be completed by 2024 [10]. As such the limitations imposed by VDLm2 become a hindrance to civil aviation growth once more.

The currently by SESAR envisioned successor to VDLm2 for the European air traffic, is the L-band Digital Aeronautical Communication System (LDACS) [27]. LDACS is a cellular, ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight [33]. Internationally, LDACS is reflected in the Global Air Navigation Plan (GANP) of the International Civil Aviation Organization (ICAO) [17], currently under standardization in ICAO [18] and the Internet Engineering Task Force (IETF) [24] and has successfully been flight trialled [3], [29].

978-1-6654-8419-0/22/$31.00 ©2022 IEEE

As LDACS is envisioned to support ATS and AOC traffic transported via ACARS, ATN/OSI [16] or the ATN/IPS [15], link layer security imposed by ICAO Doc 9896 [15] or ARINC P858 [1] applies. The current LDACS security architecture foresees the usage of a dedicated LDACS Public Key Infrastructure (PKI), mutual authentication of ground and aircraft, key establishment, protection of user and control channels, as well as multiple security levels to cope with future requirements on security [12], [23], [25].

One open question is setting the validity period duration of LDACS certificates. While Air Traffic Network (ATN)/Internet Protocol Suite (IPS) certificates assume a three year period for aircraft and a one day period for ground, these times might not be optimized for the LDACS use case [30]. In [25] a Ground Station (GS) certificate lifetime of one year was proposed.

The objective of this paper is to compare the one day and one year LDACS GS certificate validity periods in terms of certificate management effort and security data overhead.

In Section II, we introduce LDACS, its trust architecture and the overall concept for certificate revocations. Section III covers our method and we provide details about the LDACS cell-attachment handshake and the database of flight movements we used throughout this work. Section IV lays out our findings, which we put into perspective in Section V by discussing pros and cons before concluding in Section VI.

II. Background

In this Section, we introduce LDACS, its security and trust infrastructure and necessary details about certificate revocations such as Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs).

A. Introduction to LDACS

The Federal Aviation Administration (FAA) together with EUROCONTROL identified relevant features and requirements to support growth of civil aviation as early as 2007 in a joint study called action plan 17 [11]. This sparked the

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

development of new digital data-links as no communications system at the time was deemed sufficient to support long term growth. These findings were confirmed in the previously mentioned 2015 SESAR VDLm2 study [26]. New data-links in the Future Communications Infrastructure (FCI) are Aeronautical Mobile Airport Communication System (AeroMACS) for Airport (APT), LDACS for long-range terrestrial Terminal Maneuvering Area (TMA) and En-Route (ENR) and SatCOM for Oceanic, Polar and Remote (OPR) communications [33]. While AeroMACS is already deployed at more than 47 airports around the world and SatCOM is widely implemented by Iridium and Inmarsat satellite clusters, long-range terrestrial communications is still served by the 32-year old VDLm2 system [21]. To move forward, LDACS is envisioned as its successor. LDACS is a cellular, ground-based digital communications system for flight guidance and communications related to the safety and regularity of flight [33]. Internationally, LDACS is reflected in the GANP of the ICAO, and is currently under standardization in ICAO and the IETF [18], [24]. Standards and Recommended Practises (SARPS) have already been defined in 2018 [18], a deployment strategy has been finalized [5] and technical capabilities up to a technical readiness level of five were demonstrated in flight trials in 2013 and 2019 [3], [29], [33]. The most prominent features of LDACS are the increase in data throughput by one to two magnitudes compared to the current system in use, inherent message prioritization ensuring timely delivery of safety critical messages, enabling new technologies such as 4D-trajectories and offering sound cybersecurity feature [3], [23], [25]. As part of those features will be the major focus of this work, we are going to introduce them next.

B. LDACS Trust Architecture

LDACS cybersecurity architecture is based on a dedicated trust infrastructure, established via digital certificates incorporated into a PKI, building a chain of trust [25]. Certificates are distributed in a secure manner to aircraft and ground, while trust is originating from the same trusted Certificate Authority (CA). Please note, LDACS supports four different Security Level (SL), two pre-quantum and two post-quantum based SL all containing different security algorithms. As such signatures within LDACS certificates vary depending on the SL. Once an aircraft comes into the vicinity of a GS, the *CellEntry* procedure is performed, in which the Aircraft Station (AS) gains basic access to that specific LDACS cell and in which LDACS cipher-suites are negotiated. Before any user-data communications can take place, the next phase, the Mutual Authentication and Key Exchange (MAKE) procedure is performed in which AS and GS mutually authenticate to each other and establish keys for user-data and control-data protection. *CellEntry* and MAKE procedure together are called "cell-attachment" procedure and will be referred to during this work [25]. Lastly, using these keys and suitable efficient algorithms, user-data can be encrypted, integrity and authenticity protected, while control-data is integrity and authenticity protected. Upon handover from one cell to another one, the old

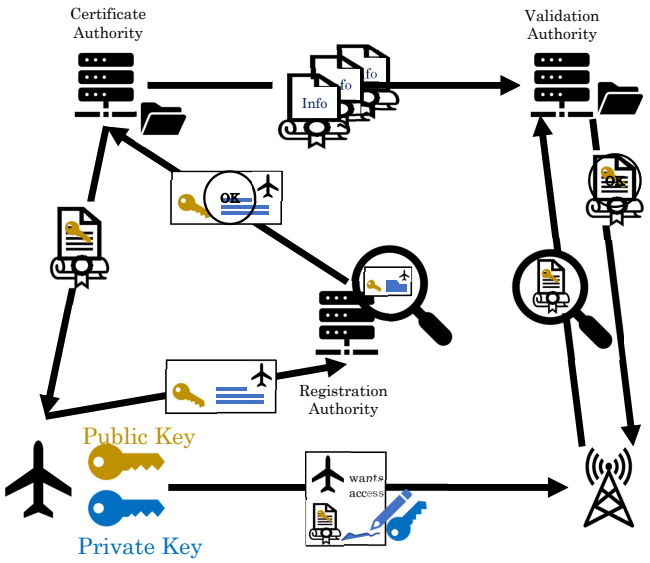


Fig. 1: Overview of PKI principles

GS communicates relevant security information via a secure channel outside the wireless scope of LDACS to the new GS so that the aircraft does need to undergo the entire procedure again and the handover can happen seamlessly. [25]

Since the focus of this work is on the LDACS certificate lifetime, we discuss the PKI in more depth next. Figure 1 shows principle entities of a PKI and their overall interrelations.

Before any certificate is issued, a root CA is installed with a self-signed certificate. From there all trust is derived further down the chain of trust to sub-CAs and finally the end-entities. When an end-entity requests a certificate, it identifies itself to a Registration Authority, which verifies user identities and forwards the certificate request to the CA, in case the identity check passes. This service can also be hosted inside the CA. Then, the CA issues a digital certificate to the end-entity, thus to AS or GS in the LDACS use case. Now the end-entities have public/private keys and a certificate which proves ownership of them via the CA's signature. Simultaneously information about the issuance of that certificate is stored at a Validation Authority (VA). The VA is responsible for holding states of certificate validity periods, hence when a certificate is revoked, the revocation status is stored here. This can be implemented for real time revocation state checkups via the OCSP [32]. When an AS demands access to an LDACS cell and the MAKE procedure is triggered, signatures of AS and GS are exchanged. The signatures are based on a predefined set of information and uses the private key of that entity. Hence, everyone in possession of the public key of that entity can verify the signature and together with the certificate of that entity, has proof that this public key actually belongs to the entity that claimed it. This is the case, as both, AS and GS trust the signature of the CA in the end-entity certificates and can verify it via the public key of the CA, which in term is proven to belong to the CA via its certificate. Now, the only problem that remains is finding out, whether a used certificate has already been revoked within its validity period or not. This

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

problem is discussed in the next section.

C. Certificate Revocations

Generally, a certificate can be used during its entire validity period as stated upon its creation. While different formats have been proposed in the past, the most commonly used structure is the X.509v3 format nowadays [4], [7]. The valid time period of a certificate can vary and is defined as the time between its *notBefore* and *notAfter* values. While restrictions might be enforced by individual systems, such as a maximum certificate lifetime of 398 days with major browser companies, the validity period can be of arbitrary length. [2], [6], [35].

Due to various reasons, such as the compromise of the private key or the compromise of a CA higher up in the trust chain, a certificate might become invalid before reaching its expiration date [7]. Therefore, possibilities to revoke a certificate are needed, which is often realized by the CA via a CRL or the OCSP [22]. While both options serve the same purpose, they differ in their content, distribution methods and scopes. A CRL is a periodically published list, often referred to as *denylist*, containing all revoked certificates by one CA. Issued with a time stamp, it is cryptographically signed by the respective CA and made available for public access. The validity of a certificate is verified by ensuring it is not included within the current CRL. The certificate validation is therefore also possible in retrospect, if the respective CRL of the time in question is known. While CRLs for a certain CA can be cached and made be available for later, even offline usage, they might not be suitable for bandwidth restricted environments. Even if only one certificate should be verified, the entire CRL has to be downloaded which, depending on the number of revoked certificates, can become quite large. [4]

If resource limitations are significant or periodic, frequent and recent information of a certificate's status are needed, OCSP [32] can be utilized. In contrast to CRLs, information about the validity of certificates is requested at a OCSP responder, and only results regarding the queried certificates are included in the response. The function of the OCSP responder can be fulfilled by the CA itself, a trusted responder or CA designated responder. As individual requests are answered, an online connection to the responder has to exist. [4], [32] Within the OCSP response, the certificate status can be identified via the status values *good*[1], *revoked*, or *unknown* [32]. Further, additional information such as the source of certificate revocation (i.e., the respective CRL) can be included.

The Aeronautical Radio Incorporated (ARINC) technical specification P858 [1] foresees the possible use of OCSP and CRLs. Due to the previously mentioned disadvantages of CRLs in resource restricted environments, only OCSP will be discussed throughout this work.

[1]Please note, that the status *good* only indicates, that no certificate with the listed serial number has been revoked within its validity period. It is not required to check, whether the respective certificate has ever been issued. [32]

III. Method

In order to evaluate the impact of different GS certificate lifetimes on the user data rate of LDACS, both the number of AS entering a cell over time, as well as the respective amount of bytes for *CellEntry*, MAKE (i.e., cell-attachment) and optional certificate transmission, have to be known. While the latter can be identified by analyzing the individual messages during cell entry, traffic movements are more difficult to predict. Therefore, utilizing data, collected from the OpenSky Network [34], will help gathering the required information.

A. Handshake Data Analysis

Upon entering an LDACS cell, each AS will be mutually authenticated to the respective GS by the means of a MAKE procedure as described in section II. The utilized certificates have to be known to the respective communication parties, and therefore must be known beforehand or are required to be transferred via the radio link for public key verification.

With all GSs having a secured ground-based communication channel with the VA, providing a much higher bandwidth than the LDACS wireless connection, AS certificates and their respective OCSP can be retrieved periodically by a GS via this channel. Thus, no transfer via the radio link is needed.

Distributing GS certificates to the AS can be done in two ways: (1) transmitting recent GS certificates via the LDACS data-link or (2) install GS certificates offline, i.e., during maintenance, outside the scope of the LDACS data-link. Deciding on the choice of GS certificate distribution highly depends on the lifetime of GS certificates: a shorter lifetime demands regular, swift online updates (possibly via LDACS), a longer lifetime allows for handling these updates offline in a cost-effective manner.

With validity periods of one year, distribution to the AS could occur within the scope of a navigational database update of the aircraft's systems. Happening mostly offline, but outside the LDACS system, bandwidth will not be affected. However, to prevent the usage of revoked certificates, validity verification via OCSP is necessary. Short validation periods, within the scope of days, make a maintenance update impractical, and therefore require a transmission upon cell entry via the radio link from the GS to the AS.

The chosen method is therefore reflected in the content of the exchanged messages during the MAKE procedure.

With daily updated certificates, one AS could still pass through the same LDACS cell multiple times during an 24 hour GS period. As the certificate could thus already be stored within the system's cache, the AS has to indicate in its cell entry request message, whether the GS certificate has to be transmitted during the ongoing MAKE procedure. This occurs in the last *CellEntry* message (i.e., *CellEntryResponse*) , transferred from GS to AS. Here, either the respective GS certificate is being transmitted, or current OCSP responses are included to confirm that no revocation has occurred, if yearly lifetimes are used.

With this being the major difference, effects on bandwidth can therefore be identified as the difference of certificate and

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

TABLE I: LDACS Security Level (SL) with according signature algorithms, public key and signature sizes [25]

SL	Algorithm	Public Key Size	Signature Size
1 pre-q	ECDSA256	257 bit	512 bit
2 pre-q	ECDSA384	385 bit	768 bit
1 post-q	Falcon512	7,176 bit	5,328 bit
2 psot-q	Falcon1024	14,344 bit	10,240 bit

OCSP response sizes, multiplied by the amount of cell entries per hour. Therefore, the structure of X.509v3 certificates as well as OCSP responses has to be analyzed in order to determine reasonable sizes.

B. Certificate Structure Analysis

Both structures, X.509v3 certificates and OCSP responses, are encoded using Distinguished Encoding Rules (DER) of the Abstract Syntax Notation One (ASN.1), which is representing values in a tag-length-value (TLV) format [7], [20], [32].

```
1  ( 2) Certificate {
2  ( 2)    tbsCertificate {
3  ( 5)        version,
4  (22)        serialNumber,
5  (12)        signature,
6  (84)        issuer,
7  (32)        validity,
8  (84)        subject,
9  (px)        subjectPublicKeyInfo
10 ( )       },
11 (12)    signatureAlgorithm,
12 (sx)    signatureValue
13  }
```

Listing 1: X.509 certificates basic fields and field sizes in bytes in parenthesis [7]

```
1  ( 2) OCSPResponse {
2  ( 4)   responseStatus,
3  ( 2)   responseBytes {
4  ( 3)     responseType,
5  ( 2)     response {
6  ( 2)       tbsResponseData {
7  (22)         responderID,
8  (15)         producedAt,
9  ( 2)         responses {
10 ( 2)             {
11 (24)               certID,
12 ( 4)               certStatus,
13 (15)               thisUpdate
14                  }
15               },
16           },
17 (12)       signatureAlgorithm,
18 (sx)       signature
19         }
20       }
21     }
```

Listing 2: OCSP response basic fields and field sizes in bytes in parenthesis [32]

Therefore, individual fields can be of arbitrary length and adjusted to the current use case.

Including optional fields and possible extensions, certificate or OCSP response sizes can vary accordingly. Thus, we have determined necessary fields, to our best judgement, together with the respective amount of bytes needed for their representation in ASN.1 DER.

TABLE II: Certificate related data amount per AS cell-attachment, dependent on LDACS SL and GS certificate validity period. "Yearly" signifies the transmission of an OSCP response via LDACS, "daily" the transmission of the actual GS certificate via LDACS

SL	Yearly Certificates (OCSP Response)	Daily Certificates (Certificate Transmission)
1 pre-q	175 Byte	352 Byte
2 pre-q	207 Byte	400 Byte
1 post-q	777 Byte	1,818 Byte
2 post-q	1,391 Byte	3,328 Byte

Listing 1 provides an overview of the structure of a basic X.509 certificate as described in [7]. The numbers in parenthesis indicate the estimated amount of bytes needed for each line / part, either due to ASN.1 requirements or content.

While every of the above fields can be of arbitrary length, the *subjectPublicKeyInfo* and *signatureValue*, marked as *px* and *sx* above, depend on the security level chosen in LDACS. Therefore, the size of one certificate is composed of a base 255 bytes in size plus the respective public key and signature lengths as seen in Table I.

Listing 2 depicts the structure of an OCSP response. As it can be assumed, that a GS would only relay a response indicating a *good* certificate status, only that case is being shown there.

Similar to X.509 certificates, the final size of a OCSP response is depending on the selected LDACS security level as well. A base structure with 111 bytes can be identified, that is increased by the ASN.1 encoded signature values depicted in Table I.

Finally, to sum up this section, Table II[2] depicts the certificate validity period-depending amount of data to be transferred during cell entry also listed depending on security levels. In order to only list differences related to the selected lifetime (i.e., one day vs. one year GS certificate validity period), bytes generated by the handshake are disregarded as they are similar for both approaches.

C. OpenSky Network

Having determined the different data amount required for both, daily renewed certificates as well as OCSP responses (i.e., the yearly renewed GS certificate scenario), effects on available data rates can only be calculated if the number of cell-attachment procedures per time interval are known.

Organizations like EUROCONTROL release information such as the recorded Instrument Flight Rules (IFR) flights per year in an aggregated form [10] or provide different traffic forecast scenarios for the upcoming years [8], [9]. However, for our purposes, more detailed temporal and geographically information are needed, which can be retrieved

[2]Please note, the sizes in this table disregard the ASN.1 extra encoding bytes for the signature and public key, as they are not determined yet for FALCON. Also, as signatures are included in both OCSP response and certificate transmission, the bytes due to the public key encoding signifies the only size difference between both methods.

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

from Automatic Dependent Surveillance Broadcast (ADS-B) data collection networks. The OpenSky Network, a non-profit receiver network, provides its collection of surveillance data for academic and institutional researchers [34]. Since its start in 2013, over 25 trillion position reports have been collected worldwide [34]. As timestamp updates with up to second-precision are provided, the data suits our requirements perfectly.

Data within the OpenSky Network are available in different formats such as aggregated per flight, flight state or unprocessed raw data. Due to flexibility in the database queries, pre-processed position reports have been utilized. As LDACS will be initially deployed within Europe [13], the analyzed data has been restricted within the latitudes 34 degrees North and 70 degrees North as well as the longitudes 11 degrees West and 30 degrees East. Furthermore, as the difference between OCSP and daily renewed certificates becomes more significant with increasing number of flights, the worst case scenario would be resembled by the busiest periods up to now. With 2019 being the busiest year of air traffic [19], the 25th of June 2019 has been chosen as one of the busiest days in civil aviation history, according to EUROCONTROL [10]. The available position reports in the OpenSky Network database were not assigned to a particular flight, hence, certain rules were applied to the collected data by a pre-processor in order to retrieve individual flight paths:

- A flight starts, when the first record for an aircraft's ICAO 24 bit address is detected and no previous active flight is known
- A flight ends, when the aircraft reports *on ground*. Alternatively, if no position report within 15 minutes has been received, the flight is ended as the *on ground* message might not have been received due to e.g., shadowing of the signal near ground.
- As the operation area of LDACS is the ENR, only flights reaching an altitude over 10,000 ft are considered.

Having applied the pre-processor, 28,944 complete flight traces were available for this day. The difference to the official EUROCONTROL data, listing 35,270 flights, can be explained geographically, as our evaluation area differs. Areas such as Turkey (3,341 flights), Ukraine (582 flights), Marocco (555 flights), Israel (533 flights), or Cyprus (243 flights) are not (fully) included in our traces, while being part of the official EUROCONTROL data. The remaining difference of 1,072 flights results from incomplete traces or filtering conditions of our preprocessor.

Current LDACS cell planning foresees 84 GS with a radius of 120 Nautical Miles (NM) or 40 NM to cover continental Europe [13], [28]. As cell radius and location might vary for each GS, the allocations of the different cell sizes have been estimated with the OpenSky Network traces. The observed area has hereby been partitioned into squares of similar area, resulting from taking the area of a circle with 40 NM and 120 NM radius as a basis[3].

Finally, the resulting 656 squares in the 40 NM cell-size case and the 84 squares in the 120 NM cell-size case present the geographical base for our computations.

Our computation methodology is as follows: The traces retrieved from Opensky Network have been used as an input for the Framework for Aeronautical Communications and Traffic Simulations 2 (FACTS2) [14] simulation in order to analyze the traffic for each individual cell. Focus has been both the daily and hourly number of cell entry events, as well as the maximum amount of aircraft simultaneously within a charted cell.

IV. Results

Here, we present our results, which were obtained by using the OpenSky data as input for FACTS2 and calculated based on the previously discussed LDACS cell-sized geographical squares.

A. Data Overhead of Daily and Yearly Certificates

The results of the evaluation are shown in Figures 2a and 2b for the 40 NM case and in Figure 3a and 3b for the 120 NM case respectively. While the number of cell entries differs with cell sizes and time periods, all evaluations have shown the area around Paris, London and Frankfurt to have the densest air traffic in the considered area on the selected day. On an hourly basis, the smaller sized cell of 40NM showed a maximum of 333 cell entries while the larger counterpart peaked at 487. Aggregating the daily number of events portray the same cells as the busiest ones as well, with 4945 within 40 NM and 7850 within 120 NM.

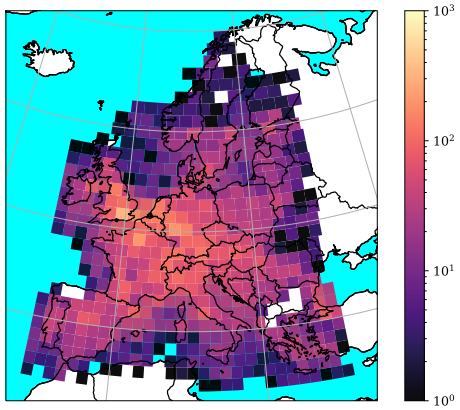
With the amount of bytes needed to be transferred per cell-attachment, as discussed in Section III, calculating the transmitted bytes in the maximum-AS-per-hour and maximum-AS-per-day case and also the average bandwidth per second for each security level and certificate lifetime, is possible now. The results are presented in Table III and IV respectively. Within that table, we refer with "daily" to the case, that GS certificates are renewed daily and, hence, sent online via the LDACS data-link and to "yearly" meaning the case that GS certificates are renewed yearly outside the scope of the LDACS data-link, and only OCSP responses are sent via LDACS.

It comes to no surprise, that certificate-dependent transmission values are larger for the maximum-AS-per-hour case, as here the absolute per amount of AS enters (and leaves) an LDACS cell that day, compared to the maximum-AS-per-day, which already contains the averaging affect of containing the busy and non-busy hours of the day. As expected, the daily renewal of GS certificates poses a 93% to 140% increase of transmitted certificate data, compared to the yearly renewal of GS case.

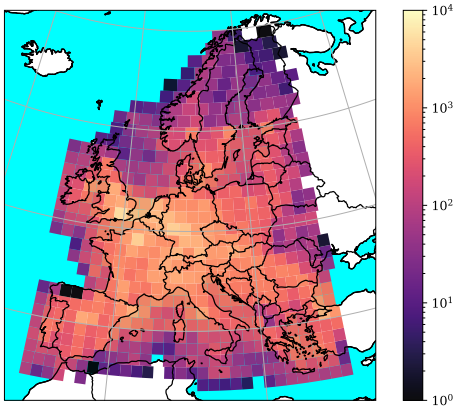
The bandwidth results from Table III range from 81 bit/s (yearly, SL 1 pre-q) to 2,463 bit/s (daily, SL 2 post-q) for the

[3]While radio wave propagation will occur in a circle or ellipse shaped pattern, squares have been used to simply simulation computations

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.



(a) 333 maximum cell-attachments per hour at 12:00 - 13:00 UTC on 2019-06-25 at 50.8, -1.5 for a 40 NM LDACS cell.

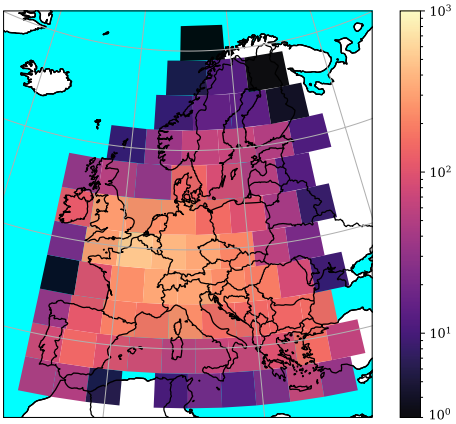


(b) 4945 maximum cell-attachments per day on 2019-06-25 at 50.8, -1.5 for a 40 NM LDACS cell.

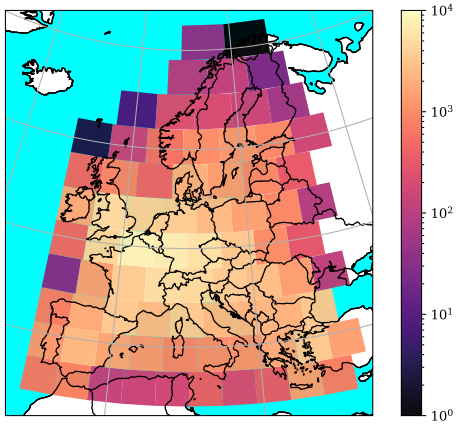
Fig. 2: Results for the 40 NM case. Please note, the graphic is colored on a logarithmic scale.

TABLE III: Summary of total certificate-dependent byte transfers and bandwidth requirement for LDACS, calculated based on maximum events per hour and maximum events per day, dependent on yearly/daily renewed GS certificates in a 40 NM cell.

SL	333 Events per Hour				4945 Events per Day			
	Yearly		Daily		Yearly		Daily	
	# Bytes	Bandwidth	# Bytes	Bandwidth	# Bytes	Bandwidth	# Bytes	Bandwidth
1 pre-q	58,275 B	130 bit/s	117,216 B	261 bit/s	865,375 B	81 bit/s	1,740,640 B	161 bit/s
2 pre-q	68,931 B	154 bit/s	133,200 B	296 bit/s	1,023,615 B	95 bit/s	1,978,000 B	184 bit/s
1 post-q	258,741 B	575 bit/s	605,394 B	1,346 bit/s	3,842,265 B	356 bit/s	8,990,010 B	833 bit/s
2 post-q	463,203 B	1,030 bit/s	1,108,224 B	2,463 bit/s	6,878,495 B	637 bit/s	16,456,960 B	1,524 bit/s



(a) 487 maximum cell-attachments per hour at 10:00 - 11:00 UTC on 2019-06-25 at 48.0, -0.4 for a 120 NM LDACS cell.



(b) 7850 maximum cell-attachments per day on 2019-06-25 at 48.0, -0.4 for a 120 NM LDACS cell.

Fig. 3: Results for the 120 NM case. Please note, the graphic is colored on a logarithmic scale.

TABLE IV: Summary of total certificate-dependent byte transfers and bandwidth requirement for LDACS, calculated based on maximum events per hour and maximum events per day, dependent on yearly/daily renewed GS certificates in a 120 NM cell.

SL	487 Events per Hour				7850 Events per Day			
	Yearly		Daily		Yearly		Daily	
	# Bytes	Bandwidth	# Bytes	Bandwidth	# Bytes	Bandwidth	# Bytes	Bandwidth
1 pre-q	85,225 B	190 bit/s	171,424 B	381 bit/s	1,373,750 B	128 bit/s	2,763,200 B	256 bit/s
2 pre-q	100,809 B	225 bit/s	194,800 B	433 bit/s	1,624,950 B	151 bit/s	3,140,000 B	291 bit/s
1 post-q	378,399 B	841 bit/s	885,366 B	1,968 bit/s	6,099,450 B	565 bit/s	14,271,300 B	1,322 bit/s
2 post-q	677,417 B	1,506 bit/s	1,620,736 B	3,602 bit/s	10,919,350 B	1,012 bit/s	26,124,800 B	2,419 bit/s

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

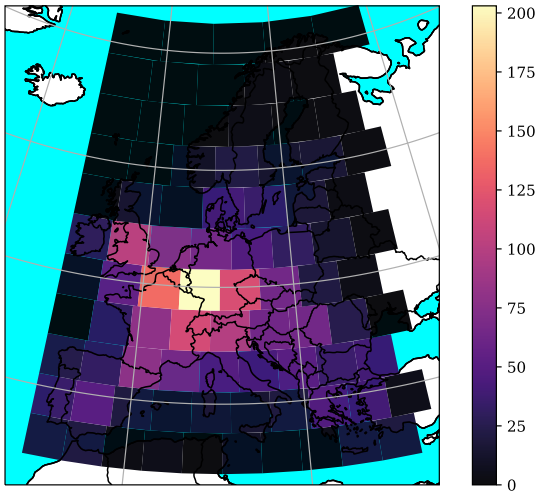


Fig. 4: Maximum amount of aircraft within an LDACS cell at a certain point in time on 2019-06-25. Here, a maximum of 203 distinct aircraft are within the cell at 48.0, 4.9 at precisely 15:31:59 UTC.

40 NM case and in Table IV from 128 bit/s (yearly, SL 1 pre-q) to 3,602 bit/s (daily, SL 2 post-q) for the 120 NM case. An interpretation of these results is given in the next Section V.

B. Future Readiness of LDACS

Within the analysis of aircraft movements through our simulated LDACS system, the amount of simultaneously present AS in each cell is of particular interest as well. Similar to previous scenarios, the results are analyzed for the biggest LDACS cell (120 NM) and are mapped over the considered are within Europe in Figure 4. The area of Frankfurt, Germany to London, UK shows the densest airspace, which is also in accordance with similar researches like [31]. Within our time interval, the busiest traffic time was found to be at 15:31:59 UTC with a maximum of 203 AS being within the same LDACS cell at the same time. With current LDACS design foreseeing an operating limit of 512 AS per cell, 203 AS represent a roughly 40% workload. The selected day has been one of the busiest days within 2019, which again has been the busiest year in air traffic. The comparably low workload confirms the future readiness of LDACS, as even a doubling of traffic numbers of 2019 would not push the system above its limits.

V. Discussion

Within LDACS, communication between an AS to an GS (Reverse Link (RL)) can be differentiated from the corresponding ground-to-air direction (Forward Link (FL)). As both OCSP responses as well as certificates have to be transferred from an GS to the AS, different lifetimes will influence the available bandwidth mainly in the FL. Within LDACS, no fixed bandwidth is set but determined by a dynamic Coding and Modulation Scheme (CMS). Depending on the channel quality, between 230.53 to 1428.27 kbps can be provided in the FL. With the results from table III it can be seen, that sending OCSP responses would require from 0.006% in the best to 0.44% in the worst case of the FL bandwidth. Daily certificate updates are higher, with 0.011% to 1.1%. Using the same calculations for 120 NM cells (Table IV), OCSP results to 0.009% - 0.65% and daily renewed certificates to 0.018% - 1.56% respectively.

Comparing the different approaches with another, it can be seen that daily transmitted certificates require approximately twice the data than yearly updated ones. However, relative to the total available bandwidth, both scenarios represent a relatively small overhead and never exceed a required bandwidth rate of 2%.

Hence, the decision on one or the other GS validity period should be done taking additional factors into account. Since OCSP is required for the 3-year valid AS certificates anyway, the integration of GS certificates within that OCSP framework seems doable with little effort. Also, issuing GS certificates on daily basis and distributing them to the respective stations in a secure manner might be more complicated than regular (i.e., 48h) updates on their OCSP status and, if necessary, updating them accordingly throughout their yearly validity period. As such, we recommend a one year validity period for GS certificates and adding GS certificates to the LDACS OCSP framework to ease certificate issuing complexity and necessary, certifiacte-dependent load on the LDACS data-link.

VI. Conclusions

This work has analyzed the effect of two different GS certificate lifetimes on the available LDACS user data rate. We have provided a comprehensive overview of the LDACS system, its trust architecture as well as certificate revocation techniques. As current proposals suggest a certificate lifetime of one day while requiring transmission of GS certificates via LDACS, the differences to a year long validity period were analyzed in two steps. First, the handshake executed during the cell-attachment procedure was inspected, to identify the difference between both approaches to be the transfer of either an OCSP response or the actual GS certificate. The respective byte sizes for X.509 certificate or OCSP response were estimated using their respective Request for Commentss (RFCs). Second, data from the OpenSky Network was utilized to analyse flight traces for a very busy day in June 2019, June 25th, 2019.

Matching the flight traces to LDACS cell-sized rectangles of similar size, distributed over Europe, resulted in the average cell-attachment events per time and regions. Combining results of both steps revealed daily renewed certificates to require approximately twice the LDACS bandwidth than yearly updated certificates. However, assuming worst case scenarios and highest security levels, the difference between both validity periods was less than 1% of the available user bandwidth of LDACS. In order to maximize the usage of resources provided by LDACS, adjusting the system to support GS OCSP responses should be considered. The analysis of flight movements however also revealed, that on the selected day in

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

2019, the busiest year in air traffic to this day, would have used only approximately 40 % of LDACS maximum cell allocation in its peak times. The future readiness of LDACS has therefore clearly been shown.

Future work now focuses on reworking previous LDACS cell-attachment protocols to incorporate GS certificate-based OCSP responses, as well as increasing the complexity of our simulation to reflect the actual, region-dependent cell-planning of LDACS.

Acronyms

ACARS	Aircraft Communications Addressing and Reporting System
ADS-B	Automatic Dependent Surveillance Broadcast
AeroMACS	Aeronautical Mobile Airport Communication System
AOC	Aeronautical Operational Control
APT	Airport
ARINC	Aeronautical Radio Incorporated
AS	Aircraft Station
ASN.1	Abstract Syntax Notation One
ATN	Air Traffic Network
ATS	Air Traffic Services
CA	Certificate Authority
CMS	Coding and Modulation Scheme
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
ENR	En-Route
FAA	Federal Aviation Administration
FCI	Future Communications Infrastructure
FL	Forward Link
GANP	Global Air Navigation Plan
GS	Ground Station
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
IFR	Instrument Flight Rules
IPS	Internet Protocol Suite
LDACS	L-band Digital Aeronautical Communication System
MAKE	Mutual Authentication and Key Exchange
NM	Nautical Miles
OCSP	Online Certificate Status Protocol
OPR	Oceanic, Polar and Remote
OSI	Open Systems Interconnected
PKI	Public Key Infrastructure
RFC	Request for Comments
RL	Reverse Link
SARPS	Standards and Recommended Practises
SESAR	Single European Sky ATM Research
SL	Security Level
TLV	tag-length-value
TMA	Terminal Maneuvering Area
VA	Validation Authority
VDLm2	VHF Data Link mode 2

References

[1] Aeronautical Radio, Incorporated (ARINC), "Internet Protocol Suite (IPS) for Aeronautical Safety Services Part 1 Airborne IPS System Technical Requirements," https://standards.globalspec.com/std/14391274/858p1, accessed 03/02/2022, ARINC, ARINC SPECIFICATION 858P1, 06 2021.

[2] Apple Inc., "About upcoming limits on trusted certificates," https://support.apple.com/en-us/HT211025, accessed 01/31/2021, Apple Inc., Tech. Rep., March 2020.

[3] M. 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*, pp. 1–19, 09 2021.

[4] D. Berbecaru, A. Desai, and A. Lioy, "A unified and flexible solution for integrating CRL and OCSP into PKI applications," *Software: Practice and Experience*, vol. 39, no. 10, pp. 891–921, 2009. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.918

[5] T. Boegl, M. Rautenberg, B. Haindl, C. Rihacek, J. Meser, P. Fantappie, N. Pringvanich, J. Micallef, H. Klauspeter, J. MacBride, P. Sacre, B. v. d. Einden, T. Graeupl, and M. Schnell, "LDACS White Paper – A Roll-out Scenario," https://www.ldacs.com/wp-content/uploads/2013/12/ACP-DCIWG-IP01-LDACS-White-Paper.pdf, accessed 10/23/2021, International Civil Aviation Organization (ICAO), Tech. Rep., 10 2019.

[6] CA/Browser Forum, "Ballot 193 – 825-day Certificate Lifetimes," https://cabforum.org/2017/03/17/ballot-193-825-day-certificate-lifetimes/, accessed 01/31/2021, CA/Browser Forum, Tech. Rep., March 2017.

[7] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Internet Requests for Comments, RFC Editor, RFC 5280, May 2008, http://www.rfc-editor.org/rfc/rfc5280.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5280.txt

[8] EUROCONTROL, "Long-Term Forecast: IFR Flight Movements 2010-2030," https://www.eurocontrol.int/sites/default/files/publication/files/long-term-forecast-2010-2030.pdf, accessed 01/29/2022, EUROCONTROL, Brussels, Belgium, Tech. Rep., 12 2010.

[9] ——, "Seven-Year Forecast," https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/forecasts/seven-year-flights-service-units-forecast-2015-2021-Feb2015.pdf, accessed 01/29/2022, EUROCONTROL, Brussels, Belgium, Tech. Rep., 02 2015.

[10] ——, "Daily Traffic Variation - States," https://www.eurocontrol.int/Economics/DailyTrafficVariation-States.html, accessed 12/11/2021, EUROCONTROL, Brussels, Belgium, Tech. Rep., 11 2021.

[11] F. EUROCONTROL, "Action Plan 17 Future Communications Study - Final Conclusions and Recommendations," https://www.icao.int/safety/acp/prl/acp-1-english/acp.1.wp.015.1.en.doc, accessed 02/02/2022, EUROCONTROL, FAA, Tech. Rep., 10 2007.

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

[13] 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 07/16/2021, German Aerospace Center (DLR), SESAR2020 PJ14-02-01 D3.3.030, 2020.

[14] 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

[15] ICAO, "Doc 9896 — Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols," International Civil Aviation Organization (ICAO), Tech. Rep., January 2015, [Online]. Available: https://standards.globalspec.com/std/10026940/icao-9896 [Accessed: March 19, 2021].

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.

[16] ——, "Doc 9880 — Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part I-IV," International Civil Aviation Organization (ICAO), Tech. Rep., January 2016, [Online]. Available: https://standards.globalspec.com/std/10183529/icao-9880-part-i [Accessed: February 12, 2021].

[17] ——, "Global Air Navigation Plan (DOC 9750)," International Civil Aviation Organization (ICAO), Tech. Rep., September 2019, [Online]. Available: https://www4.icao.int/demo/GANP/GANP_EN.pdf [Accessed: November 19, 2020].

[18] International Civil Aviation Organization (ICAO), "Finalization of LDACS Draft SARPs - Working Paper WP05 including Appendix," https://www.ldacs.com/wp-content/uploads/2018/03/WP05-DCIWG-2-LDACS_Draft_SARPs-Appendix.pdf, accessed 05/02/2022, International Civil Aviation Organization (ICAO), Montreal, Canada, Tech. Rep., October 2018.

[19] ——, "Presentation of 2019 Air Transport Statistical Results," https://www.icao.int/annual-report-2019/Documents/ARC_2019_AirTransportStatistics.pdf, accessed 08/30/2021, ICAO, Tech. Rep., 12 2020.

[20] International Telecommunication Union, "Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)," ITU-T Recommendation X.690, July 2002.

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

[22] M. Koschuch and R. Wagner, "Trust revoked — practical evaluation of ocsp- and crl-checking implementations," in *E-Business and Telecommunications*, M. Obaidat, A. Holzinger, and J. Filipe, Eds. Cham: Springer International Publishing, 2015, pp. 26–33.

[23] N. Mäurer and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)," in *37th Digital Avionics Systems Conference (DASC)*, 09 2018, pp. 1–10.

[24] N. Mäurer, T. Graeupl, and C. Schmitt, "L-Band Digital Aeronautical Communications System (LDACS)," https://datatracker.ietf.org/doc/draft-ietf-raw-ldacs/, accessed 11/10/2021, 10 2021.

[25] N. Mäurer, T. Gräupl, C. Gentsch, T. Guggemos, M. Tiepelt, C. Schmitt, and G. D. Rodosek, "A Secure Cell-Attachment Procedure for LDACS," in *1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS) on 6th European Symposium on Security and Privacy (Euro S&P)*, 07 2021.

[26] 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 06/02/2022, European Union (EU), Tech. Rep., 11 2015.

[27] ——, "European ATM Master Plan - Digitalising Europe's Aviation Infrastructure," https://www.atmmasterplan.eu/downloads/285, accessed 05/02/2022, European Union (EU), Tech. Rep., 07 2020.

[28] 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.

[29] N. Mäurer, T. Gräupl, M. A. Bellido-Manganell, D. M. Mielke, A. Filip-Dhaubhadel, O. Heirich, D. Gerbeth, M. Felux, L. M. Schalk, D. Becker, N. Schneckenburger, and M. Schnell, "Flight Trial Demonstration of Secure GBAS via the L-band Digital Aeronautical Communications System (LDACS)," *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, no. 4, pp. 8–17, 2021.

[30] 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 09/10/2021, International Civil Aviation Organization (ICAO), Tech. Rep., 05 2021.

[31] T. Pejovic, F. Netjasov, and D. Crnogorac, "Relationship between air traffic demand, safety and complexity in high-density airspace in Europe," in *Risk Assessment in Air Traffic Management*. IntechOpen, 2020.

[32] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," Internet Requests for Comments, RFC Editor, RFC 6960, June 2013, http://www.rfc-editor.org/rfc/rfc6960.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc6960.txt

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

[34] M. Schäfer, M. Strohmeier, V. Lenders, I. Martinovic, and M. Wilhelm, "Bringing up OpenSky: A Large-scale ADS-B Sensor Network for Research," in *Proceedings of the 13th IEEE/ACM International Symposium on Information Processing in Sensor Networks (IPSN)*, April 2014, pp. 83–94.

[35] B. Wilson, "Reducing TLS Certificate Lifespans to 398 Days," https://blog.mozilla.org/security/2020/07/09/reducing-tls-certificate-lifespans-to-398-days/, accessed 01/31/2021, Mozilla Corporation, Tech. Rep., July 2020.

2022 Integrated Communications Navigation and Surveillance (ICNS) Conference
April 5-7, 2022

Authorized licensed use limited to: Deutsches Zentrum fuer Luft- und Raumfahrt. Downloaded on August 02,2022 at 18:27:54 UTC from IEEE Xplore. Restrictions apply.