TBD
Internet-Draft
Intended status: Informational
Expires: 1 October 2026

R. Moskowitz, Ed.
HTT Consulting
J.M. Fernandez
Bastionnage Consulting
M. Ngambo
Polytechnique Montral
S. Card
AX Enterprize, LLC
A. Wiethuechter
AX Enterprize
30 March 2026

ADS-B Authentication
draft-moskowitz-ads-b-auth-00

Abstract

The Automatic Dependent Surveillance Broadcast (ADS-B) is a surveillance technology mandated in many airspaces. It is now widely deployed but suffers a lack of security and privacy. From a security point of view, it is relatively easy to spoof the ADS-B messages. With the appropriate readily available hardware and software. From a privacy point of view, all the messages contain the aircraft's assigned 24-bit ICAO address, which makes it easy to link to data about the aircraft, in particular to know when a particular aircraft has flown and where to. In addition, the main transmission medium utilized for ADS-B, i.e. the 1090 MHz frequency used by Extended Squitter (1090ES), is approaching saturation in some parts of the world, resulting in packet loss in certain areas [RF_Usage].

This paper presents how to use the IETF TESLA protocol along with X.509 certificates issued by ICAO member states for each aircraft to authenticate all ADS-B messaging. It leverages the 8PSK phase overlay (PO) scheme proposed in the Minimum Operational Performance Standards (MOPS) for ADS-B (RTCA [DO-260C]), which enables 1090ES ADS-B transmissions to convey three times more information, to support the transmission of the extra security information required by the authentication scheme. By doing so, the impact of authentication on channel usage is negligible. Beyond message authentication, this scheme proposed has two important additional benefits: 1) the possibility to implement a Flight Authorization scheme, allowing ATC and intercepting aircraft to not only authenticate an aircraft but to verify that it is authorizes to conduct that flight and 2) a methodology for adequately protecting the privacy by assigning rotating 24-bit identifiers to designated aircraft, while maintaining the possibility to (blindly) authenticate their ADS-B transmissions.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

1.1. Problem statement

The Automatic Dependent Surveillance Broadcast (ADS-B) technology is an aviation surveillance protocol that periodically broadcasts the aircraft's position and other related data, enabling the aircraft to be tracked. ADS-B does not require an interrogation signal from the ground or from other aircraft to activate its transmissions. ADS-B can also function point-to-point with other nearby ADS-B equipped aircraft to provide traffic situational awareness and support self-separation.

ADS-B messaging is subject to spoofing attacks with readily available hardware and software, an important security threat. In addition, it exposes potentially confidential information about the aircraft, which is problematic for general and business aviation (i.e. disclosure of Personally Identifiable Information (PII) such as itinerary), as well as military aircraft (disclosure of classified flight trajectories). Both the security and the privacy threats are recognized to have an impact on aviation safety and need to be addressed.

Another problem, unrelated to ADS-B, is the difficulty for Air Traffic Control (ATC) or a military air force to quickly ensure that a given aircraft approaching restricted airspace (e.g. Temporary Flight Restriction (TFR) zones, or Air Defense Identification Zone (ADIZ)) is indeed authorized to fly through that airspace. Current solutions rely on the cross-verification of flight authorizations issued prior to the flight (e.g. flight plan, authorization code) with immediate aircraft identification through transponder code or other visual means. This is problematic and can lead to potentially dangerous situations, especially in zones of conflict or during emergency situations (e.g. ESCAT, ATC Zero).

1.2. Solution Proposal Overview

This proposal provides an augmentation to ADS-B. First, it effectively prevents spoofing attacks by providing a means to verify the authenticity and origin of each ADS-B message. Second, it also, optionally, allows for the off-line verification of flight authorization for airborne aircraft, and this from ADS-B transmissions alone. Third, by transmitting more data in a single ADS-B message via the Phase Overlay, fewer transmissions are needed provided the receivers support this proposal, thereby reducing channel utilization. Fourth, it provides an optional mechanism to eliminate the transmission of sensitive information that might lead to undesired disclosure of PII (general and business aviation) or

classified information (military aviation).

The proposal uses TESLA [RFC4082] to provide message origin authentication, while it relies on the use of Public-Key Infrastructure (PKI) to provide sender identity (entity) authentication. In the overall process, identity authentication (using certificates and signatures) is performed to verify that the sender is who they claim to be. With the sender's identity is established, TESLA is used to ensure that the received messages were indeed generated by that sender and have not been forged. This is done by having the aircraft sign the TESLA "Key Anchor", K_0 (Section 3.3.1.1.1), for a particular flight. The Air Navigation Service Provider (ANSP) can also sign the initial session key, which provides a means to verify flight authorization, i.e. that the aircraft is authorized to fly at that time.

Optionally, the confidentiality problem can also be handled by replacing the fixed 24-bit aircraft address with a 24-bit identifier different for every flight that only authorized organizations can resolve to the underlying identifier. This is similar to the FAA Privacy ICAO Address program, except that the proposal supports a different identifier for every flight.

Our proposal relies on the use of the 8PSK Phase Overlay (PO) modulation proposed in the Minimum Operational Performance Standards (MOPS) for 1090 MHz Extended Squitter (1090ES) ADS-B RTCA [DO-260C]. We do this in order to minimize the impact of message authentication and entity authentication on channel use 1090ES. Note that the use of PO can also lead to channel usage reduction since it allows for more information to be sent in the same amount of packet transmission time. The conditions under which such channel decluttering can be obtained are discussed in Section 4.4.

This proposal herewith builds on the Compatible Authenticated Bandwidth-efficient Broadcast for ADS-B proposal [CABBA]. It provides additional detail on implementation with the DO-260C standard and how to implement the PKI based on the Drone Remote Identification Protocol (DRIP) standard [RFC9374].

1.3. Out-of-scope applications

An alternate transmission channel for ADS-B is the Universal Access Transceiver at 978 MHz. Currently, UAT is of limited use outside of the USA. As far as we know, there is no current proposal for the introduction of phase modulation for UAT. Message and entity authentication in UAT-based ADS-B is in principle possible following a similar approach but is out-of-scope for this proposal which concentrates on 1090ES exclusively.

In addition to information sent by the aircraft (ADS-B Out), ADS-B can be used (e.g. through UAT in the USA) to send useful information to aircraft by ground stations, i.e. Traffic Information Services Broadcast (TIS-B) and Flight Information Services - Broadcast (FIS-B). Again, a TESLA-based approach could in principle be adopted to authenticate TIS-B and FIS-B transmission. In fact, identity authentication and the underlying PKI would be even simpler since there would be fewer transmitting identities. Nonetheless, this is also beyond the scope of this proposal.

2. Terms and Definitions

2.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Notation

||
: Signifies concatenation of information (e.g., X || Y is the concatenation of X with Y).

Ltrunc (x, K)
: Denotes the lowest order K bits of the input x.

2.3. Definitions

EUROCAE
: European Organisation for Civil Aviation Equipment. Aviation SDO, originally European, now with broader membership. Cooperates extensively with RTCA.

CAA
: Civil Aviation Authority of a regulatory jurisdiction. Often so named, but other examples include the United States Federal Aviation Administration (FAA) and the Japan Civil Aviation Bureau.

DET
: DRIP Entity Tags (DETs) are a specific type of Hierarchical Host Identit Tags (HHIT) as defined in Section 3 of [RFC9374].

HDA (HHIT Domain Authority):
: The 14-bit field in a DET that identifies the HHIT Domain Authority under a Registered Assigning Authority (RAA).

ICAO
: International Civil Aviation Organization. A specialized agency of the United Nations that develops and harmonizes international standards relating to aviation.

RAA (Registered Assigning Authority):
: The 14-bit field in a DET identifying the business or organization that manages a registry of HDAs. RAAs are typically allocated to CAAs as in Section 6.2.1 of [RFC9886].

RTCA
: Radio Technical Commission for Aeronautics. US aviation SDO. Cooperates extensively with EUROCAE.

Safety
: "The state in which risks associated with aviation activities, related to, or in direct support of the operation of aircraft, are reduced and controlled to an acceptable level" (from Annex 19 of the Chicago Convention, quoted in [ICAODEFS]).

Security
: "Safeguarding civil aviation against acts of unlawful interference" (from Annex 17 of the Chicago Convention, quoted in [ICAODEFS]).

3. Proposed ADS-B Authentication Mechanism

This paper presents a framework to secure ADS-B communications. It uses X.509 certificates issued within a state-managed PKI for identity authentication and TESLA for message origin authentication. The RTCA [DO-260C] 8PSK phase overlay is leveraged to convey additional data within 1090ES transmissions with minimal communication overhead.

3.1. Proposal Sketch

The solution operates in two mechanisms:

1. Message origin authentication

2. Identity authentication

3.1.1. Message Origin Authentication

ADS-B messages are authenticated using TESLA. During transmission, three messages are sent along with a MAC computed over all of them, all carried within a single 1090ES signal. One of the messages is encoded in the amplitude of the 1090MHz carrier using Pulse-Position Modulation (PPM), while the other two messages and the MAC are encoded in the phase of the PPM-modulated carrier using the Phase Overlay mechanism (8PSK modulation).

The MAC is generated using a TESLA interval key known only to the sender at the time of transmission. This key evolves at fixed intervals according to a predetermined key chain. The interval key is disclosed after a short delay, ensuring that the messages and the MAC are received before the key becomes available, thereby preventing real-time forgery.

Upon key disclosure, the receiver performs two checks:

1. It verifies that the newly disclosed interval key is valid, by checking that it belongs to the same key chain as previously disclosed keys, hence ensuring that it was sent by the same sender.

2. It computes the MAC of messages received in the previous interval with the newly disclosed key, and compares it with the received MAC, to verify that the corresponding group of messages covered by those MAC originate from the key's owner and have not been altered in transit.

3.1.2. Identity Authentication

Each aircraft transmitter is provisioned with a cryptographic key pair and an X.509 certificate issued by its operator (or ANSP or CAA) within a state-managed PKI. The certificate binds the aircraft's 24-bit address (ICAO or anonymous) to a DRIP Entity Tag (DET [RFC9575]), enabling receivers to verify that the sender controls the corresponding private key. A signed "token", extracted from the certificate is periodically broadcast to support real-time, over the air, validation. This token is designed to provide the cryptographic proofs needed by receivers, yet fit within the ADS-B transmission constants. Alternatively, the certificates can be cached or pre-loaded by the receiver which obviates the need to broadcast the tokens often (this will be discussed further in Section 3). This step authenticates the sender's identity but does not guarantee by itself the integrity or authenticity of the ADS-B messages it transmits.

While TESLA ensures message origin authentication (two messages come from the same sender because they were MACed with interval keys in the same key schedule), it does not ensure who that sender is. In order to bind a particular key schedule, and hence a sender, to an identity, it is necessary to periodically send a signed interval key. This key is signed by the aircraft and optionally also by an ANSP (flight authorization).

3.2. ADS-B Messaging

This section describes the structure of ADS-B messages, focusing on the key difference between baseline and phase overlay (PO) messages. Baseline messages correspond to standard ADS-B messages and are transmitted using PPM on a 1090 MHz carrier, where information is encoded in the amplitude of the signal.

PO messages, introduced in MOPS DO-260C, allow additional information to be transmitted using the same PPM-modulated carrier. This additional information is encoded in the phase of said signal by applying 8PSK modulation. As a result, a single transmission can carry both a baseline ADS-B message and additional data, which may correspond to another ADS-B message or to other types of information.

Thus, the PO capability enables the simultaneous use of both amplitude and phase domains. This can be exploited in three main ways:

1. to transmit independent and unrelated messages in each domain

2. to transmit related information, such as a message together with its associated authentication data (e.g., MAC, signature, certificate)

3. to extend a single message by distributing its content across both domains

3.2.1. Baseline Message

The current, “baseline” , ADS-B datagram is 112 bits of which only 51 are for message data. This 51-bit message is identified by an ICAO 24-bit aircraft address (herein referred to as 24AA) and a 5-bit Message Type Code (TC).

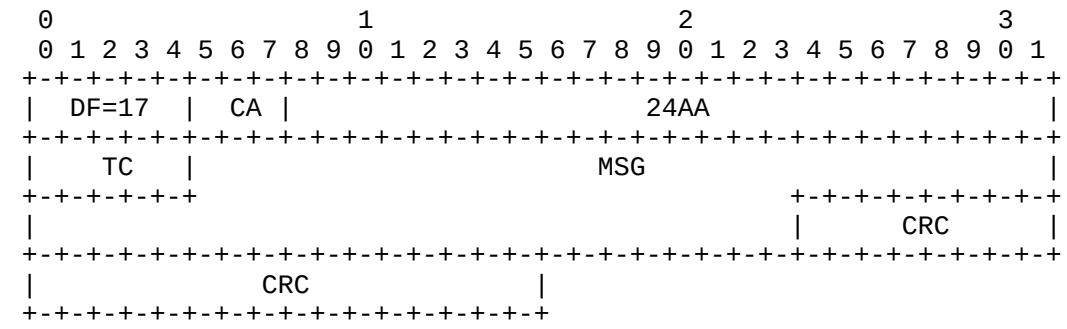

Figure 1: ADS-B baseline message

3.2.2. Phase Overlay Messages

In 2020, RTCA proposed the use of Phase Overlay (PO) encoding for ADS-B in 1090ES [DO-260C]. The phase shift keying schemed proposed was 8PSK, which allows for 3 bits encoded in phase in each 1 s pulse encoding 1 bit of the baseline signal. The alternate scheme 16PSK has been proposed by some researchers, but was not retained in the MOPS. While 16PSK has greater spectral efficiency than 8PSK, preliminary analysis of Bit Error Rate (BER) in typical ADS-B use-case scenarios [CABBA], indicates that the BER using 16PSK would be too high. In the rest of this paper, we therefore propose and use 8PSK as mandated in the MOPS.

Baseline packets consist of 112 pulses, encoding 112 bits, with a total duration of 112 s; with 8PSK PO additional 336 bits can be sent during that same period. However, as depicted in Figure 2, there is a 12-bit Reference Synchronization Phase (Sync) and 120-bit Parity Correction which leaves only 204 bits for data. From which the first 8 bits are for the Message Type field (MT) and followed by the 24 bits mandatory 24AA which leaves 172 bits for actual message content. This is still 3x greater than the 56 bits in the baseline message. Following IEEE 802 and IETF protocols, the common practice would be 24AA then MT. However, the DO-260C State and Status message ([DO-260C], sec 2.2.3.5.5.1.1) has the fields in this MT then 24AA order, so that is used here for consistent message processing.

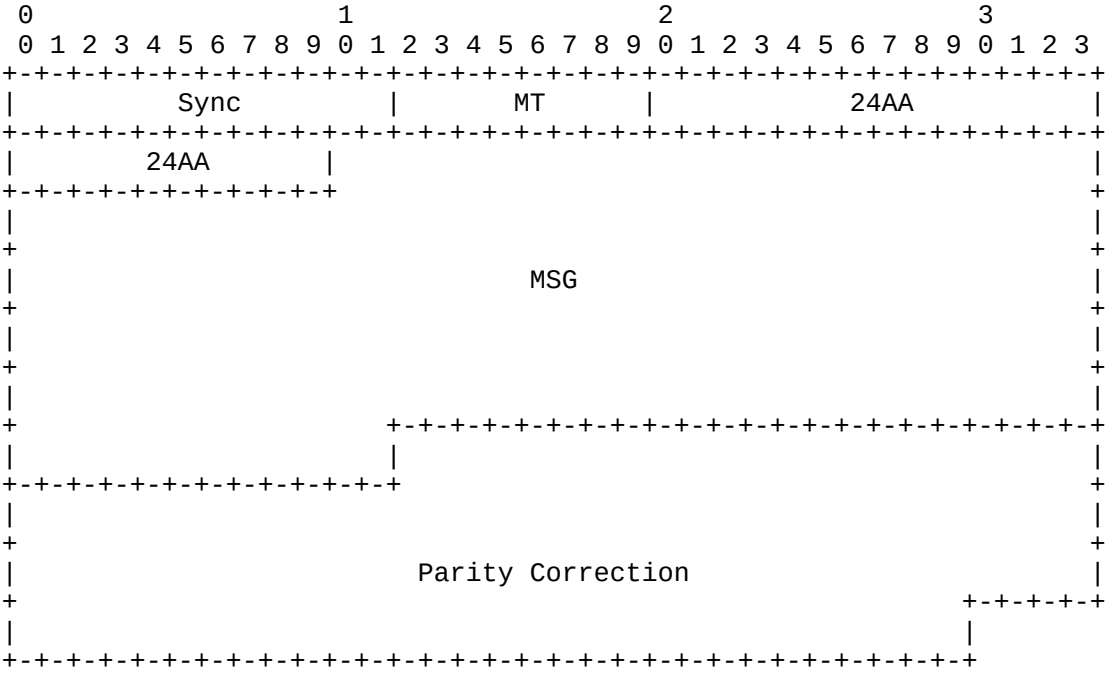

Figure 2: ADS-B Phase Overlay (PO) message

RTCA in DO-260C, and perhaps other entities, are providing PO-specific messages that are more efficient than the baseline messages they replace. Support of these messages require changes in the ADS-B application both in the sender and receiver.

Where the Phase Overlay frame content is being covered, with either baseline or new PO messages, all diagrams will only show the makeup of these 172 bits.

The new PO message from RTCA, and potentially other entities, present a challenge if they do not allow for the TESLA MAC. For this proposal, ALL PO messages (other than the TESLA specific messages below) MUST have the 28-bit TESLA MAC and should have a 32-bit timestamp (note: ongoing research for a shorter, effective timestamp). As illustrated in Figure 3, this leaves 112 bits for content (the equivalent of two 56-bit legacy baseline messages).

The current (baseline) and the new PO ADS-B messaging do NOT include any message ordering content (e.g. no Sequence Number or Timestamp). Due to the ADS-B rebroadcast (ADS-R) and space-based ADS-B feature to enlarge coverage area, receivers MUST expect duplication and out-of-order packet delivery. This has significant impact on the authentication approach used herein. The addition of a timestamp as shown in Figure 3 is highly recommended for all new PO messages.

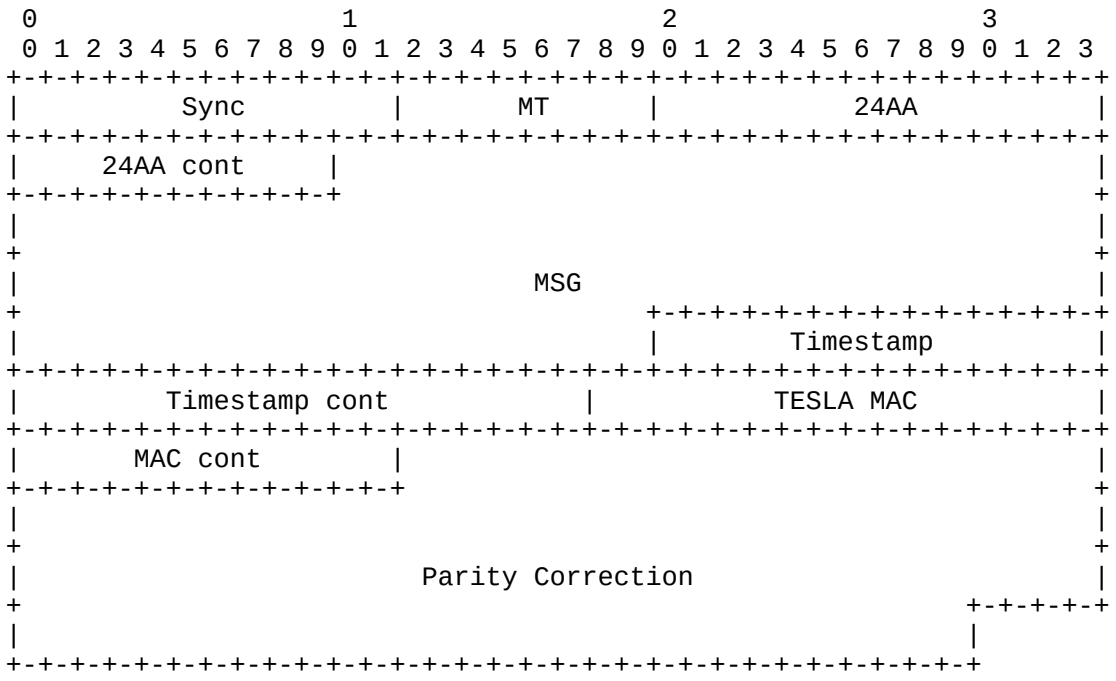

Figure 3: ADS-B Phase Overlay (PO) message with TESLA MAC

3.3. ADS-B Authentication

This section describes the mechanisms used to authenticate ADS-B messages, including data origin authentication using TESLA and sender identity authentication using digital certificates managed by PKI.

3.3.1. Authentication Technologies

TESLA [RFC4082] is the authentication technology used here. X.509 digital certificates, managed within a globally-scoped PKI (or Federated PKIs) provide the trust mechanism required by TESLA.

3.3.1.1. TESLA Basics

TESLA is a protocol that provides data origin authentication for broadcast and multicast messages. Each message carries a Keyed Message Authentication Code (Keyed MAC). The TESLA key used to generate the MAC is disclosed only after a short delay, allowing receivers to verify the authenticity of past messages while preventing forgeries.

3.3.1.1.1. TESLA Key Chain Generation

Before broadcasting, the sender divides the broadcast period into N equal time intervals and generates a one-way key chain of at least N+1 keys: one key for each interval and an additional key K_0 that serves as a commitment or “anchor” for the entire chain.

The key chain is generated as follows:

1. Randomly choose the key for the last interval, K_N.

2. Compute the preceding keys and the commitment K_0 by repeatedly applying a one-way function F to the next key in the chain:

| K_i=F(K_(i+1)) for i=N-1,n-2,...,0

This produces the key chain in generation order:

| K_N -> K_(N-1) -> ... -> K_1 -> K_0

During message authentication, TESLA keys are used and disclosed in forward order:

| K_1 -> K_2 -> ... -> K_N

K_0 is never used to generate MACs; it serves solely as a commitment, allowing the receiver to verify the authenticity of all TESLA keys.

Once the key chain is generated, the sender securely communicates a key disclosure schedule to the receivers. This schedule specifies:

- Interval duration T_int, broadcast start time t_i, and total number of intervals N

- Key disclosure delay d

- Commitment to the key chain K_0

Using this schedule, receivers can verify each disclosed TESLA key against the commitment K_0, ensuring that all messages originate from the legitimate sender.

3.3.1.1.2. Message Transmission (Sender side)

1. Derive the authentication key from the interval key K_i using a one-way function F:

| K_i=F(K_i)

2. Compute the MAC of the message using the derived key:

| MAC_j=MAC_Ki(m_j)

3. Construct the TESLA packet containing only the message and its MAC:

| P_j=m_j||MAC_(K_i)(m_j)

4. Transmit the packet over the network.

The interval key (or TESLA key) K_i is disclosed only after a predefined delay d, so the receiver must temporarily store (or treat them as “authentication pending”) the received packets until the corresponding key is revealed.

3.3.1.1.3. Messages reception and authentication (Receiver side)

Upon receiving TESLA packets, the receiver uses the time synchronization protocol to determine whether the TESLA key for the corresponding interval has been disclosed. If not, the packets are temporarily stored or flagged “authentication pending”.

Once the TESLA key K_(i-d) for a past interval is disclosed the receiver:

1. Verify the key’s authenticity against the chain commitment K_0:

| K_0=F^v(K_(i-d))

2. Derive the authentication key for the interval:

| K^(’)_(i-d)=F^(’)(K_(i-d))

3. Recompute the MACs for all stored messages from interval i d and compare them with the received MACs. A match confirms that the messages were indeed sent by the entity who generated the key chain and have not been altered.

3.3.2. TESLA in ADS-B

Even with only 172 bits of message in each PO frame, the ADS-B TESLA MAC can follow the TESLA RFC with the MAC as part of the message (Figure 3 above). It is not necessary to follow the TESLA design done for GNSS SBAS (Global Navigation Satellite System, Satellite-Based Augmentation Systems) Authentication, i.e. with the MAC is in a separate frame.

TESLA uses a keyed-hash function to start the hash-chain construction and then a hash function to build the hash-chain and for receivers to authenticate disclosed K_n back to K_0. Further, TESLA uses a keyed-hash to MAC messages with the currently undisclosed K_n and for receivers to authenticate these messages after K_n is disclosed and authenticated back to K_0 (or the last authenticated disclosed Key).

For the TESLA hash-chain and MAC, cSHAKE128 and KMAC128 [NIST.SP.800-185] are recommended for their lower timing operation over a truncated HMAC (2 SHA operations compared to one sponge SHA3 operation). ASCON-CXOF128 and ASCON-KMAC128 [NIST.SP.800-232] are a more efficient choice to use here. ASCON is specially designed for applications like ADS-B Authentication. Note that an ASCON-KMAC is not specifically provided in NIST SP800-232, but it is a direct function of CXOF. Thus, this being “greenfield”, ASCON should be given serious consideration over even cSHAKE/KMAC.

For authenticating the TESLA hash-chain, EdDSA25519 X.509 certificates are used here. This provides the smallest, NIST-approved, signature (64 bytes) and public key (32 bytes) available. CBOR ([RFC8949], Concise Binary Object Representation) encoding of key fields of the X.509 certificates are used to reduce the signing certificate size for in-band transmissions (what amounts to a signed token, rather than classic “certificate”).

At this writing, it is unclear which Post-Quantum Cryptography (PQC) algorithms will fit within the current ADS-B messaging constraints. None of the current approved PQC algorithms are workable within these constraints.

3.3.2.1. Authentication Messages

In the first stage of implementation, four PO messages are used for ADS-B Authentication. A more detailed explanation of their content and transmission time is provided in Table 1. The four messages are:

- 2-Pack with TESLA MAC

  Two baseline messages along with their TESLA MAC (see figures 3 and 4).

- TESLA Unsigned Key Disclosure

  The TESLA key from a previous interval (see Figure 3).

- TESLA Signed Key Disclosure

  The TESLA key from a previous interval along with its signature.

- Key Authentication Signing Token

  The TESLA key from a previous interval along with its signature.

Using PO messages for authentication — that is, inserting the security information in the phase of the 1090MHz carrier — is a safer approach at the start, because it guarantees backward compatibility with current receivers that do not yet support Phase Overlay. Once all equipment has this capability, the messages described above can be enhanced. This enhancement could consist of the following two approaches:

(1) Linking the PPM message to the PO message by incorporating the PPM content into the MAC computation, with the MAC transmitted in the PO message. The messages generated in this approach are:

- 3-Pack with TESLA MAC

- MACed TESLA Unsigned Key Disclosure + PPM

(2) Treating the PPM as an extension of the PO content. The messages generated in this approach are:

- Enhanced TESLA Signed Key Disclosure

- Enhanced Key Authentication Signing Token

It will be shown that the PPM portion can provide as many as 78 bits to the PO message capacity. This is very valuable for these particular messages, as it reduces how many PO messages are needed.

Message	Content	PO Msgs required	1090ES Tx required	Tx time (s)	Overhead?
2-Pack with TESLA MAC	2 baselines messages (2*56 bits) Timestamp (32 bits) MAC (28 bits)	1	1	120	No
TESLA Signed Key Disclosure	TESLA key (128 bits)	1	1	120	No
TESLA Unsigned Key Disclosure	TESLA key (128 bits) DET of ADS-B signing certificate (128 bits) Signature (512 bits) TESLA Broadcast Start Time (24 bits) TESLA Total number of intervals N (24 bits)	5	5	600	Yes
Key Authentication Signing Token	Syntax version (1 byte) Certificate Validity	7	7	840	Yes

	Dates (6 bytes) ADS-B 24AA (4 bytes) ADS-B DET (17 bytes) Certificate Issuer DET(17 bytes) Certificate Public Key (33 bytes) Signature of these fields by Issuer (65 bytes)				

Table 1: Messages used to authenticate

A critical addition in the TESLA Signed Key Disclosure is the 128-bit DET [RFC9374]. It is the DET that provides the linkage to the full certificates (and situations where in-band certificate transmission is not possible or not needed) and the trustworthy identifier for use in back-end systems. It is the inclusion of the DET that provides the trustworthy indirection to safely remove the PII-revealing 24AA, i.e. the possibility of replacing a fixed 24AA with a randomized per-flight 24AA.

The TESLA parameters include:

1. Interval duration

2. (unsigned) key disclosure frequency

The ADS-B TESLA parameters further include:

3. signed key disclosure frequency (note: not all interval keys must necessarily be signed)

4. in-band certificate transmission frequency

For per-flight certificates (i.e. for privacy or flight authorization purposes), the Certificate Validity Dates provides the Broadcast Start Time (Not Before Date) and total intervals N ((Not After Date Not Before Date) / interval duration). Thus, none of the TESLA parameters are sent over the channel. Otherwise, for longer-lived certificates, e.g. those issued for individual aircraft by Civil Aviation Authorities (CAA), their distribution method can either be in-band or through other means (e.g. Internet-based PKI certificate lookup leveraging the DET).

Note, for example, that if the interval duration is 5s and the flight is 20h, N=14400.

The TESLA Broadcast Start Time (1 minute accuracy), and Total number of intervals (N) parameters are encoded in the Signed Key Disclosure messages, as they are specific to each authentication chain. For per-flight certificates, the following conditions must additionally be met:

1. The Broadcast Start Time MUST be after the notBeforeTime in the certificate,

2. The beginning of the last transmission interval MUST be before the notAfterTime in the certificate, however,

3. The last transmission (i.e. Broadcast Start Time + N * interval duration) MAY be after notAfterTime in the certificate, but MUST be before notAfterTime + interval duration (or a at least fraction thereof).

For reference, the CABBA proposal [CABBA] explored the compromise between Channel Occupancy Rate (COR) and safety margins (in both ATC and airborne traffic awareness scenarios) for the following possible parameter values:

1. Interval duration: 5 seconds

2. Unsigned key disclosure frequency: every 5 seconds (every interval)

3. Signed key disclosure frequency: every 5, 10, 15 seconds (every interval, every 2^nd or 3^rd interval)

4. In-band signed token transmission: every 5, 15, 20 and 30 seconds (every interval, every 3^rd, 4^th or 5^th interval)

All of these values provided limited overhead in terms of COR, while providing mostly adequate safety margins. Nonetheless, further analysis is required to determine adequate values for deployment in a new ADS-B standard.

At the start of a flight the transmitter starts using the Signed Key Disclosure message with a Start Time as close as possible to and before the current time. It discards any unused interval keys that are for a prior start time. The transmitter SHOULD send the Signed Key Disclosure messages at the start of flight and at some pre-determined frequency. The receivers may cache previously received batches of Signed Key Disclosure messages even before receiving any ADS-B messages or certificates for that aircraft. For any Unsigned Key Disclosure message received there MAY be more than one possible Signed Key Disclosure message to consider, but only one will validate the Key, or the Key is fraudulent.

The receiver may have multiple Signed Key Disclosures for a single 24AA with different Start Times. The transmitter may have distributed these in advance to cover the day’s flights. Thus when hashing an unsigned Key back to a Signed key, the receiver must check against all such Signed Keys. Once this unsigned Key is validated to a Signed Key, all Signed Keys with an earlier Start Time may be discarded.

This caching authenticates previously received messages. The receivers (avionics and ground stations) should be appropriately engineered to support caching of multiple aircraft within the time window of interest (a few minutes for aircraft to fractions of an hour for ATC).

3.3.2.2. Baseline messaging within PO The 2-Pack message with MAC

The minimum impact on current use of ADS-B and maximum backward compatibility is to use PO as a “Bump-in-the-Stack”. That is, ADS-B applications can continue to build the pre-existing 56-bit baseline message formats and can even package them into the full 112 bits made available by the PO. As these messages move down the stack from the application layer to the transmission layer, the 56 bits are packed into the 112-bit payload. Thus, 2 baseline messages may be packed into one PO message. A 32-bit timestamp is affixed and the whole message is TESLA MACed with ZERO in the MAC field.

The PO Message Type of <PO1-TBD> is used. The message is as follows:

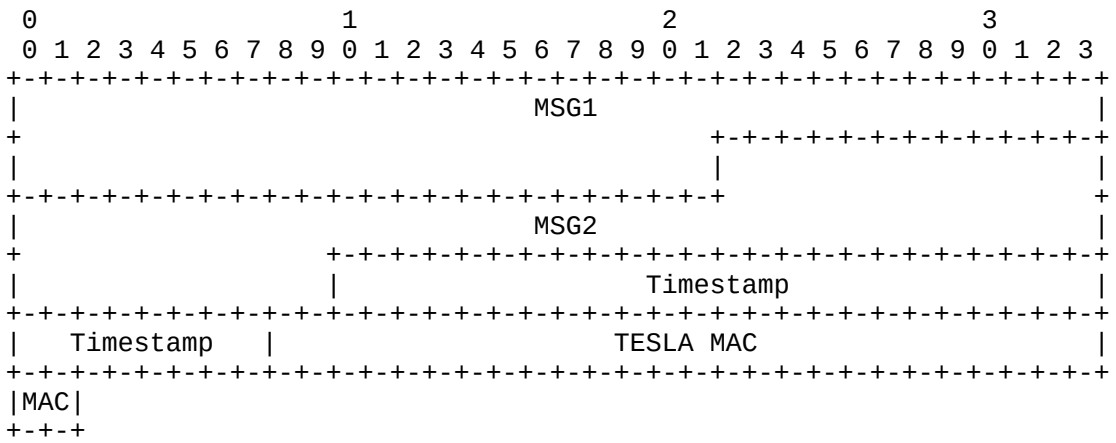

Figure 4: PO 2-Pack MACed ADS-B message

This message has no reserved bits; a smaller timestamp may be needed here, as there may be additional considerations. Furthermore, this is not compatible with the alternate PO formats being proposed by RTCA DO-260C, which do not leave room for neither a timestamp nor a MAC.

The ADS-B transmitter determines how to pack up to 2 baseline messages and when to transmit them. For example, two different message types for the same time may be packaged together (e.g. air data and position report), allowing this type of information (message type) to be sent twice as often, thus increasing safety margins. Alternatively, the transmitter may decide to send the same information at the same frequency but reduce channel occupancy in half by combining two packets. On the other hand, in a transition phase where ADS-B transmitters could be required to send all information at the same frequency in baseline messages to support backward compatibility with legacy receivers, the transmitter might decide to include a single message (the same as in the baseline) padded with ZERO. Message queuing is needed here to manage the packing. Empty message slots are filled with ZERO before computing the MAC and transmission.

On the receiver side, the PO is split into the 2 messages and sent up to the application layer. ZERO slots are ignored. Thus, the 2-Pack takes advantage of the added capacity of PO with minimal system changes.

The TESLA MAC is authenticated on receipt of the disclosed interval key. Below is an visualization of a 5 second stream (at 6.2 msg/sec) of the 2-Pack messages (shown on the PO line as “B”) including an Unsigned Key Disclosure message (“U”).

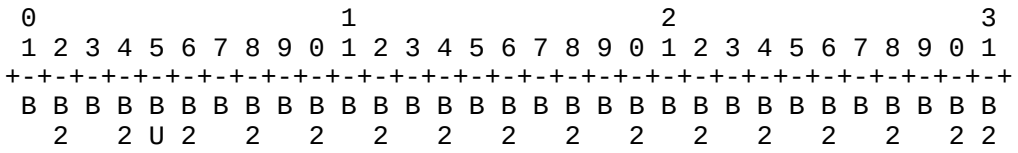

Figure 5: PO 2-Pack message stream

As discussed, the 2-Pack approach may reduce channel use by 50%. This reduction ONLY comes about if the transmitter ONLY sends PO frames, i.e. if transmission on the baseline is not required for backward compatibility.

3.3.2.3. Baseline messaging within PO+PPM The 3-Pack message with MAC

An natural extension to the 2-Pack message is a 3-Pack message where the TESLA MAC is extended to include the ADS-B message in the PPM encoding.

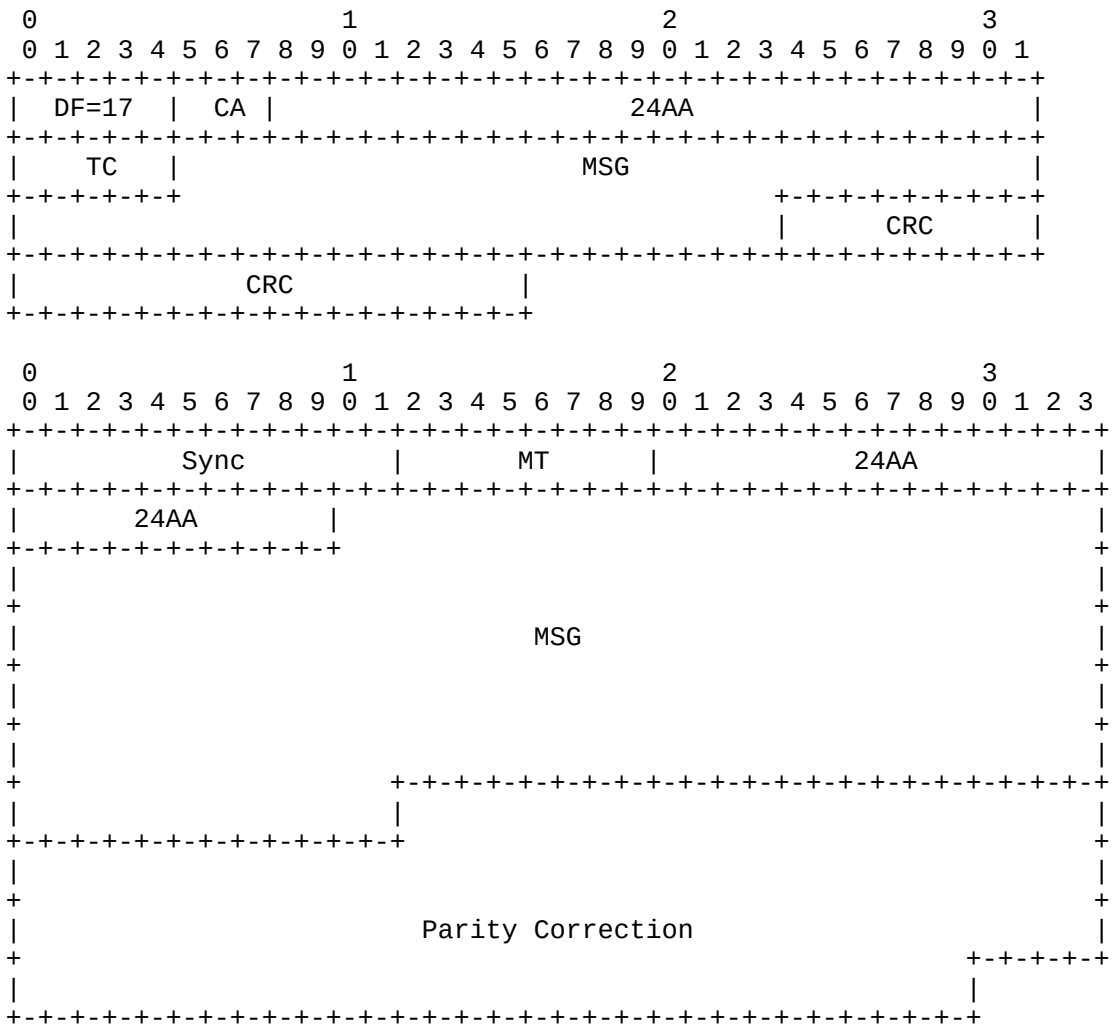

Figure 6: The PPM and PO messages viewed together

Here the 2 messages in the PO may be the prior 2 ADS-B messages resulting in a potential channel usage reduction of 2/3rds.

The PO content is the same as in the 2-Pack message, with just the different MACing input.

A negative consideration of the 3 vs the 2-Pack is risk of loss information to receivers if this message is lost. Use of the 3-Pack is a desired end-point in deploying this proposal. It offers the greatest channel usage reduction without needing to design the applications for new messaging.

Below is an visualization of a 5 second stream (at 6.2 msg/sec) of the 3-Pack messages (shown on the PO line as “B”) including an Unsigned Key Disclosure message (“U”).

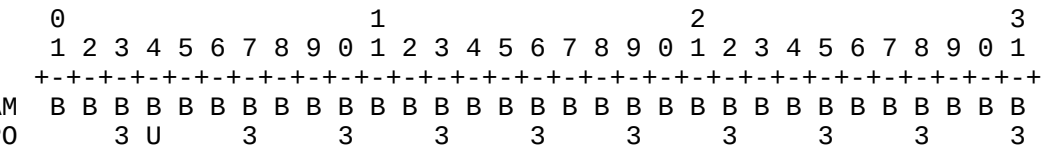

Figure 7: PO 3-Pack message stream

The PO Message Type of <PO2-TBD> is used.

3.3.2.4. The ADS-B TESLA Unsigned Key Disclosure Message

The TESLA Unsigned Key Disclosure is sent in one full PO message with a MT=<UKD>. Its sole content in the 172-bit message is the current TESLA key (128 bits) with the rest of the message ZERO padded. The receiver validates this TESLA key by performing the TESLA Key hashing function until reaching the most current prior validated disclosed TESLA key. This MAY be K_0, or a latter key K_i, obtained via a TESLA Signed Key Disclosure, or K_0 obtained through another out-of-band authenticated channel.

One potential use of the Timestamp value in this message is to calculate which was the last message MACed with this key (time < This-Timestamp Disclosure-Delay). Messages in “Validation Pending” status are divided into those prior to this time and SHOULD be authenticated with this key and those after this time and are still Pending (waiting for next Key).

The MACing of this message is more perfunctory, to maintain message structure. The Key either hashes back to the last validated Key and thus valid or it does not and is potentially fraudulent.

Thus, the worst case is performing N hashes to K_0. For example, with the proposed interval duration of 5s, a long 14-hour flight from Sydney AU to London UK may require close to 10,000 hash operations to verify the validity of the last interval keys. If signed keys are transmitted regularly, the number of hash computations would never be so high. For example, with the parameters explored in the CABBA

paper [CABBA], signed keys were sent at most at every 5th interval, thus limiting the number of hash computations to five. Nonetheless, a reasonable scenario where computation of the full hash chain for a flight would be required is where signed keys were never sent in-band but rather sent through another authenticated channel, e.g. in future PQC-compliant ADS-B Tesla implementations where signature sizes are to large to be sent in-band. In all cases, the use of the more efficient ASCON-CXOF128 over cSHAKE128 (or even less efficient HMAC) is preferable.

There are operational approaches to receive through other connections prior authenticated TESLA keys, to avoid this long hashing operation.

3.3.2.5. The ADS-B MACed TESLA Unsigned Key Disclosure + PPM Message

As with the 3-Pack message, this is a natural extension to the TESLA Unsigned Key Disclosure message. As with the 3-Pack, the TESLA MAC operation is extended to include the PPM message content. Here the TESLA MAC in this message is needed to authenticate the PPM content.

Thus the PPM message need not be sent again in any 2- or 3-Pack message.

The PO Message Type of <UKD2> is used.

3.3.2.6. The ADS-B TESLA Signed Key Disclosure Message

The TESLA Signed Key Disclosure provides the trust of the TESLA hash-chain to a specific ADS-B transmitter. Initially, the key here is K_0, which is never used in the MACing process. The first key used is K_1. Thus, any prepublication of K_0 does not compromise the TESLA authentication.

If the regular transmission of signed keys is implemented, then transmitter may transmit a more “current” signed TESLA Ki key for a past i-th interval. Each such message will include 1) a Broadcast Start Time (format TBD), corresponding to the beginning of the interval of the signed key, and 2) the total number of intervals N, each 3 bytes. It may be more secure if this is the remaining number of intervals. This will require more study.

This message needs 5 full PO messages when the ADS-B Certificate Public Key algorithm is EdDSA25519. This message has a MT=<SKD>. The whole 816-bit message is:

- Current TESLA key (128 bits)
- DET of ADS-B signing certificate (128 bits)

- Signature (512 bits)

- TESLA Broadcast Start Time (24 bits)

- TESLA Total number of intervals N (24 bits)

These 816 bits would need 5 PO messages, thus either using that many Message Types, or add a 3-bit subType field. The subType reduces the payload to 169 bits; this still fits into 5 messages. Thus the whole 816-bit message in a 845-bit design is:

- Current TESLA key (128 bits)

- DET of ADS-B signing certificate (128 bits)

- Signature (512 bits)

- TESLA Broadcast Start Time (24 bits)

- TESLA Total number of intervals N (24 bits)

- Reserved (29 bits)

Note that dropping the DET does not reduce this to 4 PO messages.

These messages would be:

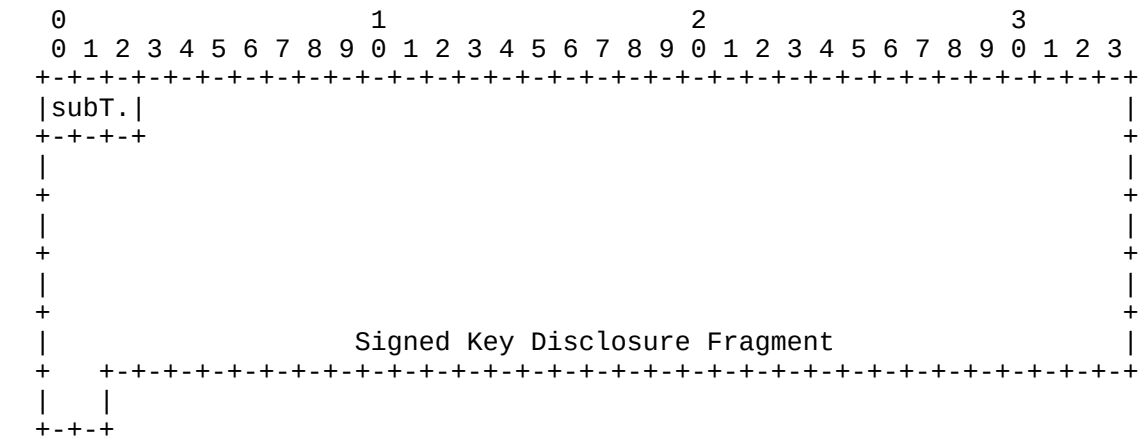

Figure 8: TESLA Signed Key Disclosure fragment message

The risk of dropping 1 out of 5 messages in ADS-B is real, thus a FEC message is recommended. If sent serially, these messages occupy the channel for 0.6 ms, where any other transmission could disrupt one or

two messages. Thus, it is recommended that the transmitter use some strategy for ensuring complete reception of the 5-message set. The specific FEC algorithm is yet to be selected. See Appendix B for more discussions on FEC.

It may well be that this Signed Key Disclosure message need only be sent once per minute or even less often, as discussed in the CABBA paper. It depends on how soon receivers need to identify the cryptographically true source of the messages. Note that the 24AA is in all ADS-B messages (in the header portion), but any sender can make any claim of a 24AA without this Signed Key Disclosure message or some other trusted published link of the TESLA K_0 to the 24AA.

For future PostQuantumCrypto (PQC), a different Signed Key Disclosure, needing more than 5 PO messages and a single FEC may not provide proper FEC behavior. This is a challenge to be addressed in future work.

3.3.2.7. The ADS-B TESLA Enhanced Signed Key Disclosure Message

An important consequence Signed Key Disclosure message is the PPM content is NOT authenticated. These 5 (or 6 including a FEC frame) messages would have to be authenticated in a series of three 3-Pack messages. This is a potential negative impact to sending the Signed Key Disclosure message.

There is an alternate approach. This proposal recommends creating a new PPM message called “PO Enhanced” with a TC=<PO-Enhanced>.

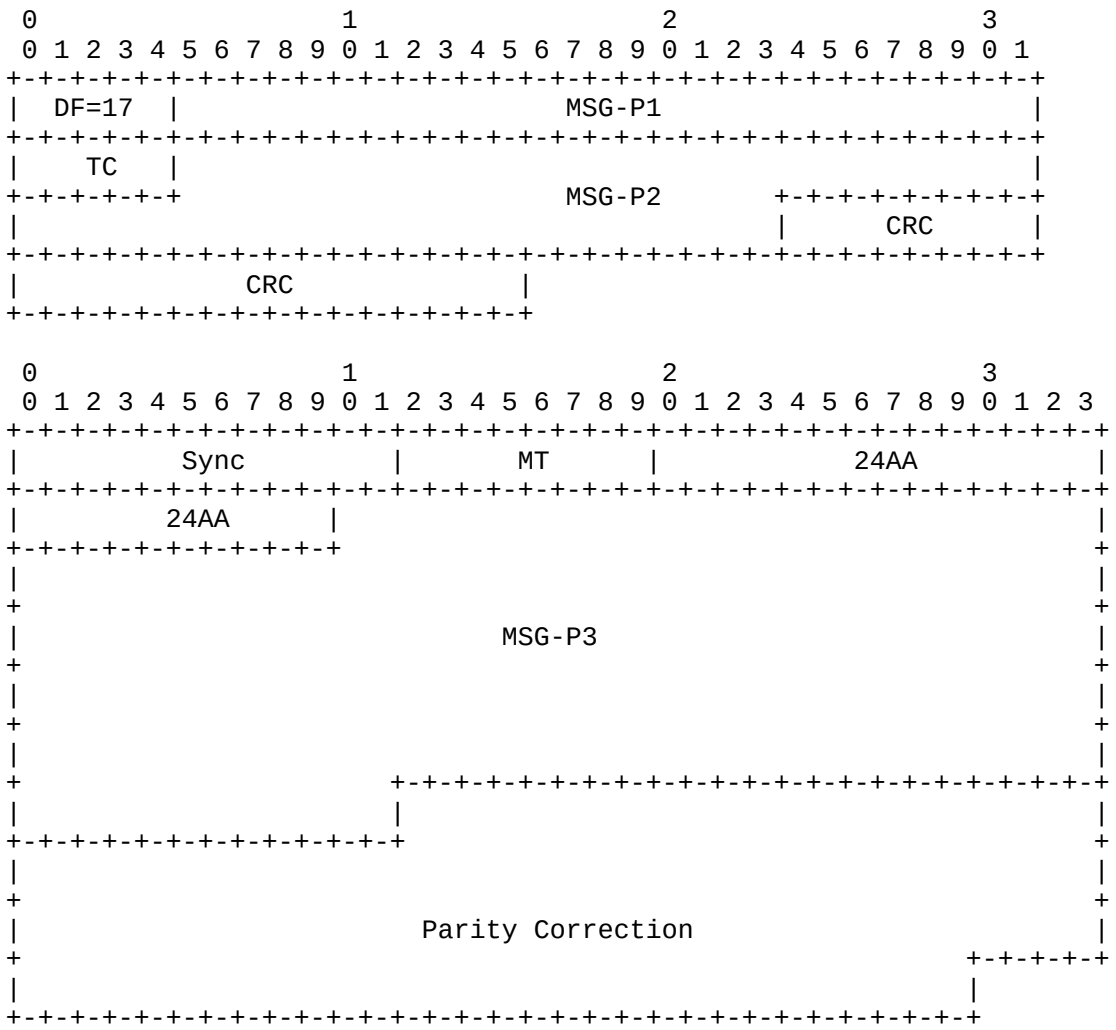

Figure 9: The Enhanced PO message, with PO data in PPM

As this TC is unknown to existing ADS-B receivers, it will be ignored. The 78 bits (MSG-P1 = {Capacity and 24AA fields} and MSG-P2 = {51-bit message field}) are used as extended bits to the 172 bits in the PO portion of the message (MSG-P3), for a total availability of 250 bits. Even with the 3-bit subCode, the 816-bit Signed Key Disclosure message would fit into 4 frames.

The PO Message Type of <SKD2> is used.

With the 4th frame only having 75 bits of the message, there are design approaches that can limit the blocking of normal PPM messaging. For example only the first 2 segments are sent “Enhance”. Then 2 segments of “regular” Signed Key Disclosure message segments. And those 2 PPM messages are authenticated by a following 3-Pack.

More research is needed to the most effective way to send the Signed Key Disclosure. The burst-mode (7 msg/sec potential) may be of value here to push out the 2 Enhanced PO messages, followed by the PO+PPM frames.

3.3.2.8. The ADS-B Compact Signed Token

Each member State’s PKI will have different certificate content, making it challenging to work with. ADS-B certificates are more fully covered in Section2.4.

The inclusion of the DET addresses a common, hierarchical, identifier, but ALL these certificates will be too large to transmit in-band. For TESLA Signed Key Disclosure, only a few X.509 OIDs (Object Identifiers) from the certificates are actually needed. These are:

- Certificate Validity Dates
- ADS-B 24AA
- ADS-B DET
- Certificate Issuer DET
- Certificate Public Key (note Algorithm is in SuiteID in DET)
- Signature of these fields only by Issuer

These OIDs can be encoded in CBOR as:

```
[
  syntax-version:  1 byte
  notBefore: days since t (e.g. t = 2026-01-01T00:00:00 UTC):
       1 + max 2 byte
  notAfter: days since notAfter: 1 + max 2 byte
  issuer’s DET: IPv6, 1 + max 16 byte
  aircraft’s DET: IPv6, 16 byte): 1 + max 16 byte
  aircraft’s number: 1 + 3 byte
  subjectPublicKeyValue:  1 + 32 byte
  issuerSignature:  1 + 64 byte
]
```

Such a CBOR encoded object is 143 bytes (1144 bits); this is technically NOT X.509, nor a CBOR encoded X.509 certificate; it is more appropriately called a CBOR Signed Token. Thus “Token” will be used in all discussions of this object, not to cause confusion in that this is NOT a form of an X.509 certificate.

It is an extraction of those X.509 OIDs that are needed for validating the TESLA Signed Key Disclosure. Following the payload formatting for the TESLA Signed Key Disclosure (Section 3.3.2.6) this would take 7 PO payloads, with MT=<CC>. Adding a FEC is recommended for a total of 8 payloads. Thus, the subType SHOULD be 4-bits. Even with the drop to 168 bits payload, this still fits into 7 PO messages. Note that it is possible to further reduce the size of this CBOR object by not maintaining the X.509 objects. For example, the 16-byte DETs can be reduced to 100 bits by not sending the IANA assigned 28-bit prefix. However, it would be needed to reduce this CBOR object to 126 bytes to fit into 6 PO messages. This may only be possible with a custom compressed “endorsement” like that used in [RFC9575]. It may well be that any such attempt at reducing the size of this compressed certificate will not result in a reduction of fragments, thus not pursued at this time.

This expands considerably with any of the PQC algorithms.

Note that with the DET in the Key Disclosure message, a receiver with Internet access can retrieve the full certificate as per [RFC9886].

3.3.2.9. The ADS-B Enhanced Compact Signed Token

As with the Signed Key Disclosure message, this Compact Signed Token is challenging. The 7 PPM messages would have to be authenticated in a string of following (or interlaced) 3-Pack messages.

Here too, an Enhanced PO approach would be beneficial. Only 5 Enhanced messages (MT=<CC2>) would be needed. Also a mix of Enhanced and “regular” may be a valid approach.

Further study is needed for the most effective transmission method.

3.4. ADS-B Certificates and PKI

The ADS-B Certificates follow the ICAO [DOC-10169] (sec 10.2.7, Aircraft Equipment Signature Certificate) ACCP with important additions. Each ADS-B transmitter’s certificate MUST contain these specific X.509 OIDs:

- Aircraft DET in subjectAlternateName (SAN) as IPv6

- Aircraft 24AA in SAN as IPv4 (with first octet of ZERO)

- Issuer's DET (CAA) in issuerAlternateName (IAN) as IPv6

  o Note that IAN is NOT included in the current version of 10169

Each member State may run their PKI as they need with whatever other elements from sec 10.2.7 as appropriate provided the above OIDs are included. The transmitter's certificate MUST have all these OIDs.

Each State runs their root according to 10169. They MUST have a long-lived intermediate level. They MUST have an issuing level that may be long-lived, or short-livedi. They MUST support certificate roll-over at all levels, though not necessarily for transmitter s (see below). The root, intermediate, and issuing certificates MUST have the DETs in their SAN; the 24AA allocated range under this level's control may be stored in SAN or IAN as IPv4Network.

It is the presence of these DETs, and their storage in DNS [RFC9886] (with DNSSEC at appropriate levels), that creates the ADS-B Federated PKI.

Aircraft certificates should be issued per Doc 10169 recommendations. Validity dates SHOULD NOT exceed 3 years and should be shorter. CRL support in aircraft may be challenging and short-lived certificates may lessen the need of CRLs. EdDSA25519 is the best algorithm for ADS-B use, as explained below. Although ECDSA also has 64-byte signatures, support for the compressed 33-byte public keys is spotty (legacy of the Certicom patent). This not only impacts cost of in-band certificate transmissions, but also storage costs for the 65-byte standard public key format.

Per-flight certificates MAY be issued per flight authorization with the validity dates reflecting the planned start and ending of the flight. This may even be the preferred mode with permanent 24AA. These certificates are stored in the DET DNS zone. The Issuer operator is responsible for storing the appropriate information (at least that in [RFC9886]) in DNS and removing expired certificates. Revocation is simply handled by removing the DET structure from DNS. This short lifetime obviates the need of certificate roll-over support for transmitter certificates.

3.4.1. Algorithms

EdDSA25519 is the default algorithm based on its public key and signature sizes. Thus, at this time, aircraft certificates MUST use EdDSA25519 and the issuing CA SHOULD use EdDSA25519. If the issuing CA does not, it will have no impact on the TESLA Signed Key Disclosure message but it may not be practical to send the transmitter certificates in-band.

With the real concern over Quantum Computer attacks on ECC, the root and intermediate CAs should use some PQC algorithm. To maintain FIPS 140-3 compliance, DL-DSA or FN-DSA are preferred. DL-DSA HSMs are "in the pipeline" with FN-DSA lagging behind. However, FN-DSA is more attractive with its smaller sizes, based on the number of root and intermediate certificates a receiver may need to cache. One issue is that the math for FN-DSA signing is very complex and easy to get wrong. Any CA signing with FN-DSA MUST be developed and maintained by those that are able to deal with its implementation complexities. FN-DSA does not have this challenge in verification.

For issuing aircraft certificates with PQC, the expectation is that one of the "NIST Additional Algorithms" will be available in time before "Q Day" and the ensuing rush. Even these have size challenges that may make in-band transmissions problematic. Thus, PQC at these levels of the PKI is an open issue.

Note that at this time, there is no DET SuiteID PQC Algorithm assignments.

3.4.2. DETs for ADS-B

The DET format is defined in [RFC9374]; it is a valid, though non-routable, IPv6 address. Amongst a number of advantages this provides, there is a well deployed distributed database in DNS ip.arpa zone. Note the following discussion may change for any PQC TESLA Signed Key Disclosure.

Following Section 6.2.1 of [RFC9886], RAAs 4048 5071 are allocated for ADS-B use. Each member State gets 4 RAAs assigned by an ICAO State numbering scheme (TBD). Each of these RAAs may have 163884 HDAs allocated per the State's delegation process (For RAA, Registered Assigning Authority, and HDA, HHIT Domain Authority, in DETs see [RFC9374]). In practice, both the Intermediate CA and the Issuing CA have their own HDA value, so there are potentially fewer HDA-level entities, based on the State's policies. For example, as the Intermediate level is long-lived, 64 entities, allocated 4 each HDAs to roll through over the years would each have 12 HDAs for rolling Issuing CAs. The details of this need further study.

Each RAA and HDA MUST maintain their respective DNS zone in 3.0.0.1.0.0.2.ip6.arpa., per [RFC9886]. This zone provides the global certificate retrieval database. It also may replace the CRL function. For all this DNSSEC is mandatory. This does present signing challenges at the HDA level. Further study is needed here. Is hourly signing, similar to timing for CRLs sufficient?

3.4.3. DETs per flight registration

It is envisioned that as part of registering a flight plan and obtaining flight authorization, a Certificate Signing Request (CSR) from the aircraft is included. The party responsible for filing a flight plan communicates the CSR plus other needed information (e.g. validity dates) to their RA (i.e. the ANSP) to get the per-flight certificate which is then loaded (along with any needed PKI chains) into the ADS-B transmitter.

An important edge case is when a flight starts without a flight plan submission (there are legal situations where this does occur). The aircraft certificate in the ADS-B transmitter is expired. How does the transmitter get a current certificate? One possibility is to break from standard practice and have the ADS-B transmitter create a new compress certificate, signed by its expired certificate and then BOTH certificates are sent in-band. Further study is needed on the preferred method to handle this operational case.

In all of these cases, per flight registration or renewal of expired aircraft certificate, the process would be greatly simplified if a means of authenticated digital communication is provided between the aircraft avionics and the ANSP or CAA. This could be achieved through existing datalink communications (though not currently authenticated), the planned future ATN infrastructure or COTS Internet connectivity technologies available on aircraft such as 5G or satellite communications.

4. Implementation and Deployment Notes

This proposal has two significant additions to the current ADS-B technology. It works best with the new Phase Overlay, in fact at this time the baseline authentication has not be fully developed without using Phase Overlay for the authentication messages. It adds cryptographic functions. Both of these require at least software updates on both transmitters and receivers. In some cases, new hardware will be needed.

Thus, a phased-in approach is the only practical roll-out plan.

4.1. Impact on Transponders and Receivers the Phase Overlay

The team behind the CABBA proposal performed laboratory tests in collaboration with Collins Aerospace to test backward compatibility of this approach. These tests involved sending the PO packets in D8PSK and making sure that that they did not interfere with legacy equipment reading and interpreting the 112 bits in the baseline signal. These tests were successfully tested against two different COTS ADS-B receivers (one certified, the other not).

The question is how much would be involved for certified avionics manufacturers of ADS-B In receiver equipment (this would typically include transmitters, TCAS boxes, digital communication units, depending on the type/size of aircraft) to support the phase overlay in the MOPS.

Our thinking is that most modern avionics use some kind of digital architecture (similar to software defined radios) where this could be achieved with a firmware upgrade, without adding new components. Many of them could be using FPGA to do the heavy lifting in terms of coding/decoding, and those could theoretically be reconfigured by a firmware update. That matters as it would influence the cost and speed of deployment of such a solution. As for old legacy equipment (e.g. General Aviation ADS-B transceivers and transmitters), we are most likely out of luck as encoding/decoding is probably hard coded in the hardware. Hence, the importance of having a backward compatible solution for the transition period.

4.2. Impact on Transponders and Receivers Cryptography

The transmitters are expected to generate their EdDSA25519 keypairs, and communicate the public key in an X.509 CSR during the flight plan submission process. The X.509 certificate is returned for storage in the transmitter. For key store, the transmitter should have an HSM; few do. To avoid requiring an immediate hardware replacement for implementation, the keys could be stored in secure memory (or such) and operate under ICAO doc 10169 Level Of Assurance (LOA) of 2 (Low Device). It may be possible to comply with LOA=5. The CAA may want to separate, for policy reasons those transmitters operating at LOA=2 and/or 5 from those with HSM and LOA of at least 9. This separation can be handled by using different HDAs.

In addition to generating and using the EdDSA25519 keys, the transmitters will need to maintain the TESLA hash chain and use it in KMAC operations on the messages. This is additional storage and code. Some currently deployed units may be able to handle this in a software update.

Future PQC requirements will most likely not be met with anything but the most recent hardware. This is a separate research issue.

4.3. Impact on Receivers Cryptography

Receivers will not be generating EdDSA25519 keying material nor signing messages. They do need to store many certificates and perform the EdDSA25519 and KMAC validations. For an Internet connected receiver, the storage requirement may be moderate. All certificates SHOULD be available via the DETs in a DNS lookup (reverse IPv6 retrieval). In a disconnected environment, the storage may be considerable. The FAA Aircraft test EdDSA25519 certificates with 600-800 bytes. There are potentially 1024 RAAs needing key rollover support. There are at least that many Intermediate HDAs and Issuing HDAs. Thus, planning should be upwards of 1024*3*1.5 = 55,296 certificates in a fully (every member State nonparticipating) situation.

Further if a PQC algorithm is used at the RAA and Intermediate HDA levels to position for the anticipated PQ crypto world, those certificates will be considerably larger (may be a magnitude larger). This further confounds the memory needs.

4.4. A prudent deployment plan

Any change to ADS-B will be disruptive. Airspace safety is best served by minimizing the disruption and spreading the changes out over time. With this change, however, the current Pulse Position Modulation and the new Phase Overlay can exist in the same time. A transmitter can send them simultaneously over the same pulses. A receiver can decode them from the same pulses. The two types of transmissions can completely co-exist.

This proposal works with a 5 second TESLA Key disclosure. In those 5 seconds, 31 baseline messages may be sent (5 * 6.2). Higher transmission rates are now allowed beyond the original 6.2 messages/sec, including 6.4 messages/sec, and a burst-mode of 7 messages/sec. These higher transmission rates are not covered here.

The TESLA authentication will send 1 unsigned key disclosure in that time interval (really the key for the prior interval, but still a disclosure). Those 31 baseline messages can be encoded in 16 2-Pack messages. A transmitter can send the 31 baseline messages in 5 seconds and at the same time send the 17 PO messages, spread out over the 5 seconds with 14 “slots” empty.

On day one, a transmitter that is PO-capable can immediately send both message types. Also ground receivers can start listening for, and use, PO messages and use their authentication to confirm proper receipt of the baseline messages (is there spoofing occurring?).

At some point, a region will be fully deployed to monitor use of PO messaging. The region can monitor baseline messaging without PO and determine their course of action. The Transmitter may stop sending baseline messaging to reduce the channel congestion. This may impact air-to-air where the other aircraft cannot receive PO messages.

There are immediate uses for some of those 14 empty slots. A FEC may be sent for the TESLA Key disclosure. The TESLA Signed Key disclosure can fit into one of the 5 second intervals in a 5-minute period as well as the compact token.

Finally, at some point new PO messages will come out to replace use of the 2-Pack, further reducing PO channel usage.

Deploying ADS-B authentication comes at no channel utilization. As regions deploy reception of these messages and aircraft turn off their baseline messaging, overall channel utilization will decrease.

5. IANA Considerations

There are no items for IANA in this proposal.

6. Security Considerations

6.1. TESLA MAC size

TESLA [RFC4082] has no advise on the size of the Keyed MAC. For the ADS-B Authentication proposal, a MAC size of 28 bits was selected as adequate and fits within the payload constraints of ADS-B.

The key disclosure interval recommendation in this proposal is 5 seconds. With the ADS-B message transmission rate of 6.2 messages/ second (recent revisions allow 6.4 msg/sec with "burst rate" of 7 msg/sec), the small number of messages protected by a single key (31 - 35 messages) is deemed to be too little to afford attackers with enough information to attack the MAC.

6.2. TESLA Key Disclosure timed attack

A known attack with TESLA is to use a disclosed key to MAC messages and trick receivers into processing them as if they were sent prior to the disclosure.

With a disclosure delay of 0.5 seconds proposed here, even the rebroadcast nature of ADS-B (via mechanisms like ADS-R) does not make it possible for a reasonably time synchronized receiver to erroneously accept a forged message.

Any messages received after the key disclosure is expected (based on time since last disclosure) are either MAC with the next key in the hash-chain or are fraudulent. This does present a synchronization challenge for the first few time intervals observed by receivers.

6.3. PQC concerns for ADS-B Authentication

None of the currently NIST-approved Post Quantum Cryptography (PQC) algorithms are possible to send over the ADS-B channel. The are just too big.

This only impacts the Signed Key Disclosure and Compact Token messages. For ground-based receivers with Internet connectivity, this information could be gained using the DETs to retrieve this information [RFC9886].

Since it is the Signed Key Disclosure where the DET is associated with the TESLA hash-chain, this may require adding a new message (e.g. DET Disclosure) that fits into a single ADS-B message.

For A2A application, there is no clear way around the size of PQC algorithms and their impact on ADS-B Authentication. Further study is needed.

6.3.1. PQC size impact on ADS-B

The SNOVA algorithm (under consideration by NIST for additional PQC algorithms) is an example of PQC algorithm that MAY fit within ADS-B.

If EdDSA25519 is still used for the ADS-B certificate (as short-lived per-flight keys) and SNOVA is used for the Issuer certificate, only the Compact Token is impacted.

Using SNOVA (37,17,16,2 {sig = 106bytes, PK=9,842bytes}), the signature in the Compact Token grows by 42 bytes (106-64).

If SNOVA (25,8,16,3 {sig = 165bytes, PK=2,230bytes}) is used for EE as well, the impact is considerable.

The Signed Key Disclosure grows by 101 bytes (165-64) and the Compact Token grows by 2300 bytes (2230-32+165-64).

These numbers show the physical limitations of the ADS-B messaging and even the smallest considered PQC algorithm.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4082] Perrig, A., Song, D., Canetti, R., Tygar, J. D., and B. Briscoe, "Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction", RFC 4082, DOI 10.17487/RFC4082, June 2005, <https://www.rfc-editor.org/info/rfc4082>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/info/rfc9374>.

[RFC9575] Wiethuechter, A., Ed., Card, S., and R. Moskowitz, "DRIP Entity Tag (DET) Authentication Formats and Protocols for Broadcast Remote Identification (RID)", RFC 9575, DOI 10.17487/RFC9575, June 2024, <https://www.rfc-editor.org/info/rfc9575>.

7.2. Informative References

[CABBA] Ngambo, M.N., Niu, X.N., Fernandez, J.F., Nicolescu, G.N., Berthier, P.B., Benito, R.B., Joly, B.J., Biegler, S.P.B., and G.R. Rice, "CABBA: Compatible Authenticated Bandwidth-efficient Broadcast protocol for ADS-B", March 2025, <https://www.sciencedirect.com/science/article/pii/S1874548224000696>.

[DO-260C] Radio Technical Commission for Aeronautics, "DO-260C - Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services Broadcast (TIS-B)", December 2020, <https://my.rtca.org/productdetails?id=a1B1R00000LoY6mUAF>.

[DOC-10169] International Civil Aviation Organization, "Aviation Common Certificate Policy (Doc 10169)", March 2026, <https://store.icao.int/en/aviation-common-certificate-policy-doc-10169>.

[ICAODEFS] International Civil Aviation Organization, "Defined terms from the Annexes to the Chicago Convention and ICAO guidance material", July 2017, <https://www.icao.int/safety/cargosafety/Documents/Draft%20Glossary%20of%20terms.docx>.

[NIST.SP.800-185] Kelsey, J., Change, S., Perlner, R., and National Institute of Standards and Technology, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[NIST.SP.800-232] Turan, M. S., McKay, K. A, Chang, D., Kang, J., Kelsey, J., and National Institute of Standards and Technology (U.S.), "Ascon-based lightweight cryptography standards for constrained devices :", DOI 10.6028/nist.sp.800-232, 13 August 2025, <https://doi.org/10.6028/nist.sp.800-232>.

[RFC9886] Wiethuechter, A., Ed. and J. Reid, "DRIP Entity Tags (DETs) in the Domain Name System", RFC 9886, DOI 10.17487/RFC9886, December 2025, <https://www.rfc-editor.org/info/rfc9886>.

[RF_Usage] EUROCONTROL, "EUROCONTROL Guidelines on Mode S Interrogation Configuration to Reduce 1030/1090 MHz RF Usage", July 2025, <www.eurocontrol.int/archive_download/all/node/15368>.

Appendix A. Phase Overlay Message Types

Four messages are defined in this proposal, each with its own PO Message Type. Below is a list of these MT:

PO1-TBD	2-Pack Message
PO2-TBD	3-Pack Message
UKD	TESLA Unsigned Key Disclosure Message
UKD2	MACed TESLA Unsigned Key Disclosure + PPM Message
SKD	TESLA Signed Key Disclosure Message
SKD2	TESLA Enhanced Signed Key Disclosure Message
CC	Compact Signed Token Message
CC2	Enhanced Compact Signed Token Message

The actual MT value needs to be assigned by the SDO maintaining this field.

Appendix B. New PPM Type Code

One new PPM Type Code is defined in this proposal:

PO-Enhanced	The PPM data is an extension of the PO message

Appendix C. FEC (Forward Error Correction) recommendations

In all cases, use of FEC here is recommended, not mandatory. Use of a FEC is based on the calculated risk of message loss as covered in each section above.

Consider the following:

1. The message frame size (172 bits) and k (number of frames) into which the authentication structures are segmented are critical parameters. EVENODD and its derivative Row Diagonal Parity (RDP) are optimized for RAID6 where there are, instead of transmission frames, disks, typically k=4 for the original data. There we are concerned with the smallest number of disk failures (in an array) greater than 1, i.e. 2, because failure of 1 disk is infrequent so failure of 2 is rare and failure of more than 2 is very rare. Thus we have only a 50% overhead for RAID6 vs the 100% overhead for RAID1 (mirroring).

2. Both of these codes are defined only for w = number of "packets" (not what we mean by that word, instead a parameter that determines codeword substructure) that are 1 less than a prime number. So for the first few primes {2, 3, 5, 7, 11, 13} we get {1, 2, 4, 6, 10, 12}, of which 1 is useless.

3. Both of these codes are CPU efficient only if w is very close to k.

4. RDP requires w>=k. EVENODD requires w>k.

5. In Signed Key Disclosure k=5 and don't yet know for sure the others in a potential range from 4 to 7.

6. So worst case w=10 (for compact token k=7 using EVENODD) yielding (w-k)=6, a very inefficient code for the CPU operations.

7. If compact token can be reduced to k=6 and we use RDP rather than EVENODD, we could set w=6, yielding (w-k)=2 which is not great but not terrible for CPU efficiency.

8. Total number of "disks" (for us, transmission frames) in an array is n = (k+m) where for both of these erasure codes m=2 to correct for 2 lost "disks" (transmission frames). This yields a 50% overhead which is not great but not terrible for bandwidth efficiency.

9. It is not clear yet how to handle varying k, due to different sizes of different authentication structures, in a single consistent scheme. Zero filling parts of the codeword in encoding & decoding but not actually transmitting frames containing only zero fills presumably should work, probably at the cost of additional CPU overhead.

10. All this is to enable recovery from the loss of a 2nd frame out of fewer than 10 frames total (worst case for compact token including the added parity frames). That's a >20% frame loss rate when it happens (lower than that on average). If losing 2 frames out of so few is not rare, then losing 3 won't be very rare, and we still have a problem. There is already a 50% FEC overhead in the Phase Overlay frame to minimize such losses. Should we back down to simple parity (e.g. XOR FEC, see Section 5 of [RFC9575]), able to recover only a single loss, but costing half as much bandwidth overhead and less than half as much CPU overhead? What are the expected frame loss statistics?

Acknowledgments

TBD

Authors' Addresses

Robert Moskowitz (editor)
HTT Consulting
Oak Park, MI 48237
United States of America
Email: rgm@labs.htt-consult.com

Jos M. Fernandez
Bastionnage Consulting
Montreal
Canada
Email: jose.fernandez@bastionnage.ca

Mikala Ngambo
Polytechnique Montral
Montreal
Canada
Email: mikaela-stephanie-2.ngamboe-mvogo@polymtl.ca

Stuart W. Card
AX Enterprize, LLC
4947 Commercial Drive
Yorkville, NY 13495
United States of America
Email: stu.card@axenterprize.com

Adam Wiethuechter
AX Enterprize
4947 Commercial Drive
Yorkville, NY 13495
United States of America
Email: adam.wiethuechter@axenterprize.com