ELEVATING AVIATION COMPONENT TRACEABILITY: STRATEGIC INTEGRATION OF NEXT-GENERATION DIGITAL IDENTITY AND INTEGRITY SOLUTIONS FOR ENHANCED DATA GOVERNANCE

M. Schuchard*, F. Hübner*, M. Ilic*, C.-S. Sandvoß*, U. Bestmann*
* Institut für Flugführung, TU Braunschweig, Hermann-Blenk-Str. 27, 38108 Braunschweig, Germany

Abstract

The comprehensive and consistent traceability of aircraft and components throughout their entire lifecycle requires accurate documentation. This is particularly critical for safety-related parts such as Life Limited Parts (LLPs), which have a limited service life and must be closely tracked back-to-birth to ensure the airworthiness of an aircraft. Prevailing documentation and certification procedures rely on physical stamps and signatures by authorized personnel. Next-generation digital identity and integrity solutions in the context of Blockchain and digital twins have the potential to transform the existing paper-based documentation into a more secure and reliable digital record of all aircraft components. To achieve a valid solution, stakeholders and requirements are determined, technical concepts are analysed and a novel approach based on interconnected hash chains and asymmetric cryptography is introduced. The proposed concept further enhances the immutability, integrity and security of the documentation process and can be used in addition to established concepts, which enables a gradual introduction.

Keywords

Aviation Component Traceability; Blockchain; Digital Twin; Lifecycle; Back-to-Birth History; Chain of Trust; Hashing; Asymmetric Cryptography

1. INTRODUCTION

To ensure the continued airworthiness of an aircraft, a comprehensive record of all aircraft components is required throughout its operational life cycle from production to scrapping. This documentation is regulated by the European Union Aviation Safety Agency (EASA) and concerns the origin, condition, and utilisation of aircraft components and parts [1]. Consequently, providing a reliable back-to-birth record of safety-relevant Life Limited Parts (LLPs) along with certification of Maintenance, Repair and Overhaul (MRO) events requires accurate documentation. While paper-based documentation continues to predominate procedures in the aviation industry, cloud-based applications attempt to facilitate the component traceability through digitisation of existing documents [2,3]. Other applications focus on digital MRO optimisation, digitising the flight operations technical log and aircraft fleet monitoring [4–6]. In addition, an independent data platform for the entire aviation industry is being developed by one of the MRO market leaders [7].

However, the emerging solutions fail to create a more secure record of aircraft components by relying on existing analog documentation procedures and on trust in people responsible for handling the data. Simultaneously, the documentation complexity obstructs the development of an ecologically beneficial and resource-efficient secondary market. Trending technologies such as Blockchain and digital twins, beyond mere headlines, reveal significant potential to address these issues for component traceability in the aviation industry. Previous concepts have successfully explored the potential of Blockchain-based data management in the context of life cycle assessment (LCA), linking multiple stakeholders and tracking data [8]. The objective of this paper is to introduce a novel approach based on interconnected hash chains and asymmetric cryptography to further enhance the traceability of aircraft components.

To achieve these objectives, the first step was to identify the documentation requirements of aircraft and their components throughout their life cycle and to characterise the stakeholders involved (section 2). Subsequently, the key technical concepts such as hashing, asymmetric cryptography, digital signatures and chain of trust in the context of Blockchain and digital twins were discussed (section 3). These technologies were then compared to the identified documentation requirements to assess their effectiveness and suitability in addressing the challenges of aviation component traceability. In conclusion, a conceptual solution based on the presented technologies was proposed to address the previously identified challenges (section 4).

While maintaining decentralisation, the proposed model of interconnected Blockchains individually created for each component and each aircraft does not require

doi: 10.25967/630294

a distributed architecture. Furthermore, the model explores the introduction of an authority-based signature methodology utilising asymmetric cryptography to further enhance the integrity and immutability of the documentation process. It is shown how revision-proof and time-stamped documentation of events for each component and aircraft can be achieved using a Blockchain-like structure. Finally, an outlook on potential future research is given. Overall the proposed concept could lead to significant enhancements in operational efficiency, safety, and sustainability within the aviation industry.

2. REQUIREMENTS AND STANDARD PROCEDURES IN AIRCRAFT COMPONENT DOCUMENTATION

Maintaining the airworthiness of a commercial aircraft requires complete documentation of flight operations and maintenance. These documentation regulations are governed by the EASA within Part-M Section A Subpart B Continuing Airworthiness [1]. The operator of the aircraft, e.g. the airline, is obliged to establish a system for the storage of all relevant documents and data in a format that is acceptable to the relevant authority. The Aircraft Continuing Airworthiness Record System should provide evidence that the aircraft meets the current airworthiness requirements and complies with an appropriate maintenance program. Contents of the record system include the date of entry, total In-Service Life of the component or aircraft, maintenance reports including the Certificate of Release to Service (CRS) and in particular the current status of LLPs and Time Controlled Components (TCCs). Furthermore, an Aircraft Technical Log is necessary, containing, for example, details of each flight, the current CRS, the current maintenance status of the aircraft and all existing defects for the preceding 36 months prior to the latest entry. Also, the history of all changes must be documented, meaning all entries and corrections to the record system must be clear and recognizable. [1]

The responsible operator of the aircraft determines whether the record system is configured in an analogue format as paper-based documentation or in a digital format. The use of IT systems is accompanied by a number

Stakeholder	Responsibilities	Key Interests
Owner (e. g. leasing company, airline)	Aircraft Continuing Airworthiness Record System, Aircraft Technical Log, Maintenance Program	Maintain airworthiness and value of the aircraft
Operator (e. g. airline)	Usage according to lease agreement	Maximise operating time
Authority responsible (e. g. EASA, LBA)	Regulation and monitoring of airworthiness, Certification of MRO workshops and aviation personnel	Aviation safety, complete documentation of A/C and components
MRO	Adherence to maintenance regulations, create maintenance reports	Trustworthiness and fulfillment of documentation requirements
CAMO	Aircraft Continuing Airworthiness Record System, Aircraft Technical Log, Maintenance Program	Trustworthiness and fulfillment of documentation requirements
OEM and suppliers	Initial certification, Maintenance manual, Certificate of Birth (components)	Trustworthiness and fulfillment of documentation requirements
Aircraft manufacturer	Initial certification, Maintenance manual, Certificate of Birth (aircraft)	Trustworthiness and fulfillment of documentation requirements
Seller (market)	Provide airworthiness documentation, transfer of ownership	Trustworthiness, addressing a broad buyer market
Buyer (market)	Transfer of ownership	Reliable documentation and serviceable components with complete documentation
Individuals in charge of the duties	Conducting the tasks of all stated stakeholders above and responsible for the documentation. Signing/Stamping the documentation off and personally liable for ensuring that the information provided is accurate and that work has been carried out correctly	Only document verified/correct events due to personal liability. Minimize workload.

TAB 1. Responsibilities, tasks and interests of stakeholders involved in continuing airworthiness documentation.

of requirements that must be fulfilled. The digital record system must be capable of being searched, transferred, and accessed only by authorised personnel [1]. Moreover, it is essential that the IT system ensures the integrity and authenticity of the records, and that it is capable of being stored and backed up [1]. Currently, cloud-based applications are available to fulfil the stated requirements for IT systems, including the ability to search, store redundantly and in addition create historical timelines from digitised paper documents [2, 3]. The technical concepts of Blockchain, asymmetric cryptography and hashing fulfil several of the stated requirements equally and offer advancements as described in the novel approach of interconnected hash chains (see section 4). A comprehensive description of the technical functionalities associated with the technical concepts is provided in section 3.

In addition to the aircraft´s operator, other stakeholders are involved in the aircraft component documentation. They have a wide range of responsibilities, tasks and interests as shown in table 1. While the main interest of the operator as key stakeholder is to maintain the airworthiness of the aircraft, the responsible authority focuses on the overall aviation safety through regulation and certification processes. The manufacturing and maintenance of aircraft and their components involve multiple stakeholders, with a key interest in a reliable and trustworthy documentation processes that also influences market participants.

The owner or operator bears the responsibility for maintaining the airworthiness and providing a full history of events of an aircraft or component. Consequently, they are confronted with the burden of a substantial amount of documents which are hard to search and require constant attention to ensure the presence of required signatures or stamps at all times. A particularly important status for the owner is whether a component is either serviceable or unserviceable. It is essential that the status of all components is monitored and that maintenance is scheduled in accordance with the recommended service life. This tracking and scheduling can also be delegated to a continuing airworthiness maintenance organization (CAMO). In the use case presented in subsection 4.1 we assume that CAMO, owner and operator are one personal body. However, in the case of leasing an aircraft, the airline is primarily interested in maximizing the utilization of the aircraft, whereas the lessor's primary objective is to maintain the value of the aircraft and receive evidence that it has been used in accordance with the agreed-upon terms. Due to the regulations and in order to avoid possible liability claims, the MRO on the other hand would like to document the proper execution of removal, maintenance by qualified personnel and release to service of parts.

By contrast, aviation safety authorities, such as EASA and in Germany the Luftfahrt Bundesamt (LBA), aim to ensure the safety of aircraft in their operations and therefore want to check compliance with all regulations and processes. They require searchable access to the documentation and, due to the number of inspection tasks, want to be able to identify irregularities as easily as possible or delegate inspection tasks to the operators themselves. Furthermore, the regulatory authorities are responsible for certifying maintenance workshops and personnel. However, they also aim to facilitate the autonomy of companies by implementing a system of regular certification and inspections.

Aircraft manufacturers, OEMs (Original Equipment Manufacturers) and suppliers introduce new aircraft, components and parts into the market. They issue a certificate of birth for the corresponding item and thus create the first documentation for any part. Furthermore they are responsible for certifying each new type of aircraft and part in accordance with the requirements of the aviation saf ety authorities and for drawing up an associated maintenance programme and updating it over time if necessary [9]. These obligations ensure both that manufacturers and suppliers are allowed to operate in the market at all and that other market participants are willing to do business with them due to the establishment of trustworthiness.

In the event that a component is to be sold on the secondary market at some point in the future, the seller may benefit financially if they can demonstrate that the component has been fully and effectively maintained. This is because, depending on the criticality of the component being sold, the condition of the component may first have to be evaluated through a costly overhaul, and certain maintenance tasks may have to be carried out prematurely. Nevertheless, the owner is reluctant to disclose a significant amount of information about his operations to the prospective purchaser, as the airline's routing could potentially be of interest to competitors.

For each participant in the activities listed above responsible for the documentation, it is of the utmost importance that only activities for which the corresponding certification and responsibility exist are signed off. Furthermore, these persons must ensure that the activities carried out comply with the specifications. This is crucial as they may be personally responsible and liable in the event of an error or accident. In this respect, it is also in the interests of those responsible to ensure that their signature is not misused.

In conclusion, the ability to trace the history of an aircraft or its components from production to scrapping is of interest not only to the supervising authority but also to other stakeholders involved in the aircraft's operation, maintenance and sale.

3. TECHNICAL CONCEPTS OF DIGITAL IDENTITY AND INTEGRITY SOLUTIONS

Details of the technical components, on which the concept presented in section 4 is based, are explained in this section. Concerning Blockchain, it is important

to de-hype its reputation and clarify the technical aspects, which are not well known in the general public. Blockchain is, as most systems, not a one size fits all solution and has advantages as well as disadvantages. Regarding the presented concept, not all of the features are planned to be used. One of the features of Blockchain is the possibility to decentralise it (Distributed Ledger Technology). While it has many advantages to shift away from centralised to more decentralised systems, the added complexity (e.g. consensus mechanisms) is unnecessary and thus not used in the concept. The relevant features of Blockchain for the concept presented in section 4 are immutability and integrity.

3.1. Blockchain

One key component of the presented concept in this paper is Blockchain. Its fundamental working principles are explained here, as they are needed to understand the concept as a whole. Blockchain and Bitcoin are often used synonymously. Bitcoin, however, is a financial product based on the Blockchain technology [10]. Blockchain consists of blocks containing information which are saved in an immutable way [11]. As information of the previous block is part of the information of the current block, a chain of linked blocks is formed [12, 13]. Due to this structure, the order of blocks can not be altered after integration in the chain [14]. The chain thus becomes resistant against modifications. On top of this, the goal of Distributed Ledger Technology is to distribute such a chain on multiple, independent carriers and establish a common ground of truth between participants, who not necessarily trust each other. Consent mechanisms control the agreement process among all participants about a new block to be added to the global chain [11]. Proof of Work is a consent mechanism in which the signed block of a participant is added, who solves a complex calculation problem, like finding the next prime number, the fastest [15–18]. This mechanism is resource-democratic, as it ensures that on average all participants who collectively own 50% of the computing power may add a new block. One drawback is the high energy consumption for the intensive calculations. Proof of Stake is a consent mechanism in which the participants who hold the majority of shares, e.g. the crypto currency itself, decide about the next block to be added [15–18]. Proof of Authority is a consent mechanism in which only an authority trusted by all participants may add a new block [15–18]. The concept presented in this paper utilizes existing centralized systems (authority, e.g. EASA, FAA) and stand-alone decentralized systems (owner, operator, MRO, CAMO, OEM, supplier, manufacturer, seller, buyer). As outlined in the next chapters, these different systems shall neither be converted into one fully decentralized system nor be replaced by a mere digital system. The aim of the concept is to strengthen the current documentation system, making it even more secure and reliable by using the most practical aspects of Blockchain. For this, a validation method similar to the consent mechanism Proof of Authority is applied.

3.2. Hashing

An important aspect regarding the described concept is that only hashes of information, rather than the information itself, are stored in the Blockchain. Possible information are files like maintenance reports or certificates of release to service. With storing the hashes in the Blockchain it acts as an additional verification system, in that the history of changes made to information can be tracked and reconstructed. So not all information has to be digitised, only their hashes. Hashing is a method to map an input value (key) of arbitrary length onto a value of determined length (hash), as shown in figure 1, and thus is not injective [13, 19, 20].

FIG 1. Working principle of hashing

Safe hash functions generate hash values which belong to one source of input data only [21]. Collisions occur if two different inputs result in the exact same hash value [22] but shall be statistically unlikely. Because of the difference in length of input and output collisions are in principle unavoidable. Collisions can be avoided when the input data is known or limited [22]. The requirements for safe hash functions are a uniform distribution of generated hash values, so the full defined range of possible hash values is utilised [21]. Any input should map to the hash value range, every hash value in this range should be producible, thus surjectivity is required. An additional requirement for hash functions is efficiency [21]. Hash values shall be calculated quickly and take small storage space. For cryptography further requirements are diffusion, in which very similar inputs generate totally different hash values, confusion, in which conclusion to the input data is impossible, and irreversibility, in which re-calculation of the input data from a given hash value is highly impractical [13, 19, 20]. Hash values are used in many different ways. In secure IT systems, passwords are not stored as plain text. Instead, they are hashed and their hash value is stored in a database. To check if an entered password is the correct one, the hash value generated from the entered password and the one stored in the database are compared. Access is granted only if both hash values match. Checksums are hash values which verify the integrity of transmitted data. Software downloads often come with a checksum to allow the user to verify that the downloaded software has not been modified, either in transit or at the download site. In cryptology, hash values are also used for integrity check of data and digital signatures. Popular hashing algorithms are Secure Hash Algorithm (SHA) or Message-Digest Algorithm (MD5) [22]. Blockchain uses hashes to verify the integrity of the block and so does our concept. Additionally hashes of related data are stored inside the blocks as described in the concept chapter.

3.3. Asymmetric cryptography

While storing the hashes of information in blocks and hashing the blocks itself, the information can already be tracked and any tampering detected. The validity of the information must be proven by another mechanism (does the information or transaction correspond to the facts?). Additionally signing data and creating integrity is done in the discussed concept based on asymmetric cryptography. Signatures and verification of those ensure correctness of data and legitimacy of actions and work similarly to encoding and decoding a message. Asymmetric cryptography enables a way of exchanging encrypted, signed and verified information between one or multiple participants without sharing a common secret key like in symmetric cryptography [13, 19]. Instead, each user has a private key, which has to be kept secret, and a public key, which has to be made public for other users. The keys are provided by a generator and are personal, as shown in figure 2.

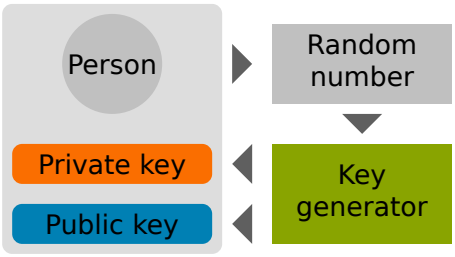


FIG 2. Generated private and public key of a user for asymmetric cryptography.

An advantage of the asymmetric system over the symmetric one is a higher security, as each user has their own key. If the key in a symmetric system is exposed by one user, communication of all participants becomes unsafe. In an asymmetric system a sender can encrypt a message with the public key of the recipient and then the recipient can decrypt the message with the private key. For an asymmetric system to be secure, it is mandatory that the private key can not be calculated from the public key. Hence, the process of generating the private and public key pair based on the used one-way function must be practically irreversible. A further requirement is that a public key is assigned to the correct user with the corresponding private key. Digital certificates, which are designated by an authority, can verify the owner of a public key. Without a central authority, mutual certification is a possibility (web of trust). In case of digital signatures only their hash value is verified, but the message is not encrypted.

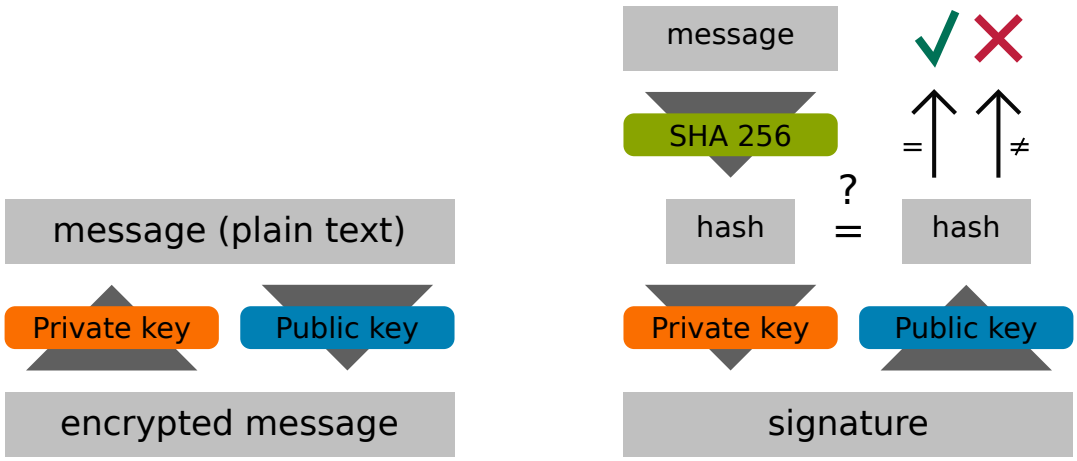
So for comparison, encryption is done with the public key and decryption with the private key, as shown in figure 3a, adding a digital signature to an (un)encrypted message is done with the private key and validated with the public key, as shown in figure 3b. Signing and validating guarantees integrity and authenticity.

3.4. Digital signatures

Asymmetric cryptography can be used by multiple participants to sign and verify data with their private and public key. This is applied in the concept described in the next chapter. Each participant holds a digital signature. Digital signatures are asymmetric cryptographic systems which use a private and a public key per user [13, 19]. The private key is kept secret by its user, while the public key must be made available to all contacts of the user. For digital signatures it is mandatory that only one private key belongs to one public key. As a first step, the private key generates a unique value of the document or message to be signed. Usually this value is generated from the hash value of the message [22]. In the second step both the generated value and the message are sent to its recipient. The third and last step allows the recipient to verify the integrity and authorship of the received message by checking the value with the public key.
The public key of a user can be published in a certificate, which can be signed by a certification authority in a PKI (public key infrastructure) to qualify the holder of the certificate. Those infrastructures establish a hierarchical chain of trust, in which higher level authorities manage lower level authorities down to the individual user. The highest level of authority contains the root certificate and acts as a trust anchor, on which all other certificates are based. An example for a public key infrastructure (PKI), in which a chain of trust is established, is Transport Layer Security (TLS) for the internet communication protocol Hypertext Transfer Protocol (HTTP) [23]. This secure variant of HTTP is Hypertext Transfer Protocol Secure (HTTPS). TLS enables authenticity and confidentiality between client and server. Authenticity is established in a TLS Handshake, in which the client and server certificates are mutually validated with the exchange of the public keys of an asymmetric cryptographic system and a shared key for a symmetric system is negotiated. Usually only the server identifies itself towards the client, who validates the certificate of the server. Certificates have an expiration date and have to be renewed on a regular basis. The client side validation of the servers certificates fails, when the certificate is outdated or other issues occur. The chain of trust is thus established from top to bottom with signed certificates and from bottom to top with validation of those certificates. In such a PKI, higher level entities sign certificates of lower level entities with their private keys. In return, lower level entities can validate the certificate with the public key of the higher level entity. When authentication succeeds, confidentiality is established in a TLS Record, in which the previously negotiated key of the symmetric cryptographic system, e.g. End-to-end encryption (E2EE), is shared and used.

4. NOVEL APPROACH FOR AVIATION COMPONENT TRACEABILITY

The following section presents a novel approach that aims to enhance the traceability of aircraft components by utilising interconnected hash chains. The fundamental concept of the approach is the establishment of a high level



(a) Encrypting and decrypting a message **(b) Signing and validating a message**

FIG 3. Comparison of encrypting a message and digital signatures using asymmetric cryptography.

of control through small, distributed actors. First, the intended use case and its stakeholders are described. Subsequently, the suitability of the technologies presented in section 3 within a Blockchain-based model of interconnected hash chains is discussed. In addition, the application of digital signatures in order to ensure authenticity and integrity of the hash chain elements is discussed. In conclusion, the proposed model is compared to the requirements of the stakeholders involved, and an outlook on the implementation of the concept is presented.

4.1. Use Case

In order to keep the concept comprehensible and to emphasize the special features and advantages, we will introduce the concept using a smaller case study. It will later be discussed where it is applicable and beneficial to be extended. The core of the concept is creating audit-proof documentation of aircraft components and the digitisation of the underlying process beyond mere paperlessness, while maintaining trust in the current regulatory and certification structures overseen by authorities such as EASA. It should be noted in particular that the proposed concept is to be understood as a supplement to the existing mechanisms and is by no means intended to directly replace them. The use case shall for now be limited to aircraft without considering engines in order to reduce complexity. An aircraft component is defined as the smallest unit that can be split, and thus has no subparts.

In our example we consider one landing gear as one component falling under LLP requirements. We observe this part being manufactured and integrated into one new aircraft by the OEM. It shall be assumed, that a back to birth history needs to be documented for the component. The commercial aircraft is operated by one airline as the owner, while tracking flight cycles and flight hours by the pilots. The airline contracts a MRO workshop to conduct routine maintenance events such as changing tires and A/B/C/D-checks, which may involve the removal of the component. After a removal and release to service, the component may be installed on the same aircraft or, as an exchange, on another aircraft belonging to the same owner or another owner in the case of material pooling. Moreover, the component may be sold on the market, where complete documentation from birth to the present is of particular importance whilst concealing the internal operations of the airline. At the end of its operational life, the aircraft and its components are scrapped.

The MRO workshop is a certified maintenance organization according to EASA regulations Part-145 and provides a quality assurance system [24]. In the MRO workshop, certified maintenance personnel conduct the required maintenance tasks and issue the necessary documentation for the release to service of the component [24].

4.2. Interconnected Hash Chains for Aircraft and Components

To create a more secure and reliable record of aircraft and its components from production to scrapping, we suggest to implement interconnected hash chains in a Blockchain-based structure. In contrast to common Blockchain systems, the model of interconnected hash chains does not require a distributed architecture. Following established responsibilities, the hash chain is stored by the responsible actor (e. g. operator, owner) in a matter that complies with IT system requirements (see section 2). Procedures and systems for archiving and backing up data such as cloud storage, magnet tapes or even paper are well established and functioning and it is not expected to gain any benefits by changing the technology. Furthermore, the actors are required to sign their respective Blockchain elements, thereby assuming liability. Therefore there is no consent mechanism such as proof of authority needed for the Blockchain suggested in the concept. In addition, as stated earlier, we aim to follow the existing regulations and digitize but not change the established processes.

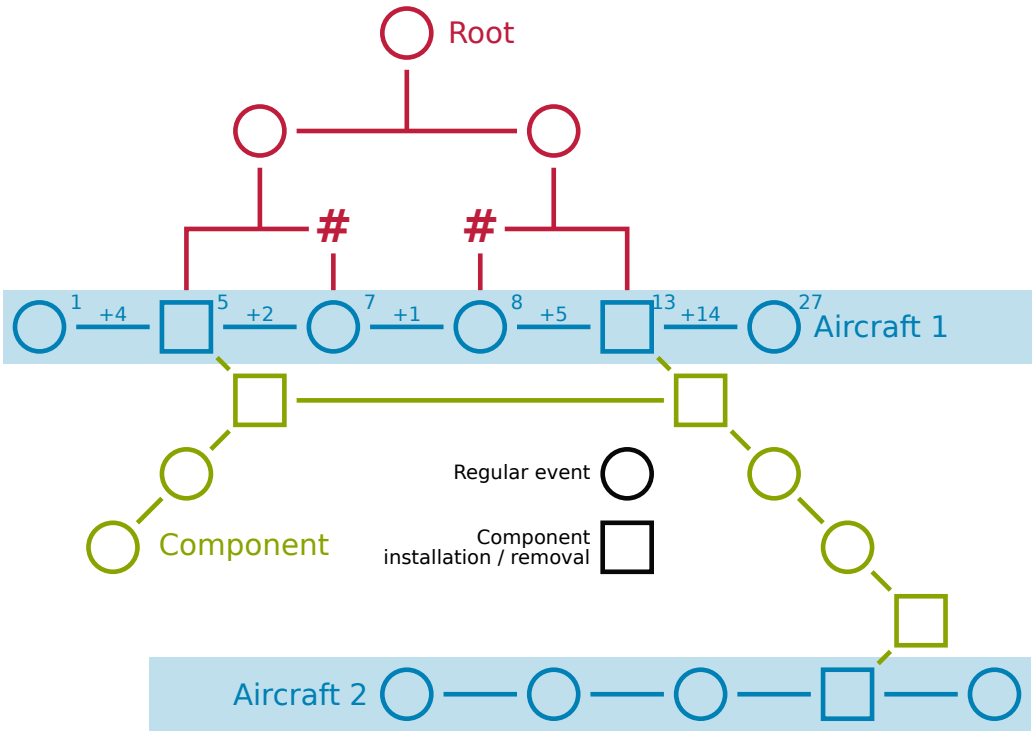


FIG 4. Flowchart of proposed aircraft parts traceability concept showing the history of events regarding two aircraft and one component.

The hash chain represents a historical record of events during the operational lifetime of an aircraft or component, accompanied by the required documentation as specified by the relevant authorities (see section 2). Once a component has been manufactured, the OEM issues a certificate of birth along with a part number and serial number. The certificate provides documentation of the manufacturing and testing processes, ensuring compliance with the relevant design requirements and documentation. The birth of the component is documented in a Blockchain element as well as any following events during its lifetime as detailed in figure 4.

Each block consists of a header in which the required metadata along with a timestamp of the current and previous event is stored and readable in plain text format (see figure 5). As described in section 3, the timestamps ensure immutability and integrity of a chain. On top of this, the payload of each block contains a hash of the documentation data such as birth certificates or maintenance reports and its filename. The documentation can be of any format, for now we assume a zipped container of PDF-documents. The original documents must be stored additionally unaltered as described above and then be used to create a hash value. The storage of the original documents is not within the scope of this concept, and established procedures such as the use of databases remain unaltered. The documents itself do not need to be signed.

The payload is accompanied by a public key chain of the signing individuals in order to be able to verify the signatures at any point in time without the necessity of any other additional information or database except a trusted root certificate. As the digital or digitised original documents remain separate from the chain, the established procedures remain untouched and a classic check for compliance remains possible at any time. Furthermore, this separation ensures that the data size of the chain remains relatively small. The additional effort is low and should be clearly outweighed by the security gained.

The Blockchain element must be signed by one individual entitled to do so. For example, the maintenance mechanic uses his private key to sign the block in which he documents his completion of the overhaul of a component. The mechanic is personally responsible and liable that the given information and documentation is correct. The signature is created based on the asymmetric cryptography technology as described above and verifiable by a chain of certificates. Following established certification processes in the aviation industry, the regulating aviation safety authorities such as EASA act as trusted root for the digital signatures and chain of trust. In the special case of releasing a component to service, our concept offers the opportunity to sign the Blockchain element by two individuals following two-person integrity procedure. In the hash chain, this is achieved by signing the signed hash by another party (see section 4.3). In the prevailing paper-based documentation, the signature process is similar to the proposed concept using asymmetric cryptography. In that context, individual stamps are protected from third parties and used for signing printed documents. In comparison to the paper-based documentation, the digital process of the proposed concept offers the advantage of automated signature verification and consequently the ability to validate the

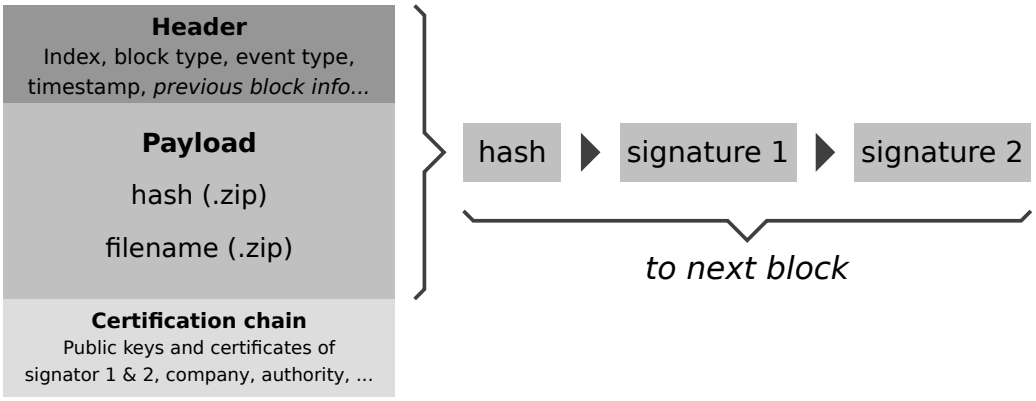


FIG 5. Blockchain element of the concept of interconnected hash chains with a dual digital signature.

history of a component.

Each constituent element of the Blockchain is constructed based on the preceding element in the chain. Thus, any alteration to any given element would render the entire structure invalid. The Blockchain contains the history of a component including but not limited to events such as it's installation on an aircraft, wear down along with the cycles/flight-hours or it being dismounted. As there is a high demand to immutably track the wear down of a component and as well the aircraft, we propose to construct another Blockchain per individual aircraft with blocks being added per flight, tracking the cycles and flight hours. This creates the same immutable and verifiable structure for an Aircraft Technical Log as side effect of the proposed concept.

The Aircraft Technical Log is another required documentation to maintain the airworthiness of an aircraft (see section 2). In our use case, the pilot is responsible for tracking the aircraft movement during operation and maintenance. By implementing the logbook in a separate Blockchain, the aircraft's activity is recorded in a reliable mode. Given the frequent rotation of the pilot in command of an aircraft, the process of documentation is shared among multiple liable actors, thereby ensuring a more secure record than could be achieved with a conventional cloud application. Yet the concept intends to supplement the existing applications regarding the flight logbook rather than replace established structures.

Both chains, the component chain and the aircraft chain are interconnected at the time of installation and removal of a component. Figure 4 outlines that the most recent aircraft block element is stored in the component chain before installation and removal of the component including current sum of flight hours and cycles of the aircraft. In order to conceal the specific operation of the aircraft and reduce the required data storage in the Blockchain, the flight activities are stored in the components Blockchain in an accumulated form using the Merkle tree when removing the component from the aircraft. Thus, competitors are unable to retrace the operation of another airline when purchasing components on the secondary market while maintaining the ability to validate the history of a component. For this, the required Merkle tree hashes and the root hash are stored in the removal block of the component.

The history of events that are recorded within the chain are traceable and immutable by the Blockchain-like structure, as described above. In the hash chain of a component and in the chain of an aircraft, there are multiple types of events that create a new element in the chain, following the documentation requirements:

- Installation, removal, maintenance and modification (MRO)
- Birth and scrap
- Transfer of ownership (on secondary market)
- Flight event: flight hours, cycles, start, end (aircraft Blockchain: every flight event is implemented in the chain; component: aggregated amount of flight hours and cycles are implemented in the chain using only one block and Merkle tree hashes)

Summing up, the concept proposes individual Blockchains per component and aircraft in which block elements are signed by individuals. The chain of the aircraft gets interconnected to the chain of the component at installation and removal. The trustworthiness and eligibility of the signing individuals are proven by chain of trust (see section 4.3). A distributed architecture is not considered beneficial. In the following sections, the signature concept, which we believe offers the greatest benefits to stakeholders, is described in more detail, the specific implications of the concept for stakeholders are analysed, and implications for implementation are discussed.

4.3. Authorised and Identifiable Signatures

The Blockchain-like structure of constituent elements prevents individual elements from being altered by the owner of the chain. As shown in figure 5, the Blockchain elements are additionally signed by authorized personnel using asymmetric cryptography to further increase the immutability of the recorded events. In order to digitally sign a Blockchain element, the header, which contains the metadata of the record, and the payload, which contains the hash value of the additionally stored documentation, are used to generate a hash value.

Subsequently, the responsible party for the recorded event uses the generated hash value of the Blockchain element and digitally signs it using their private key. Furthermore when releasing a component to service, following two-person integrity procedure the created signature is digitally signed by a supervisor of the responsible party. The digital signatures of the Blockchain element and its index are then stored within the header of the subsequent element.

In the context of our use case, the MRO workshop creates documents for landing gear maintenance and its release to service. The documents are digitally stored by the airline and a Blockchain element is created containing metadata of the event, the hash value of the corresponding documents including the filename and the public key-chain. Subsequently the hash value of header and payload of the block element is digitally signed by the responsible mechanic and a supervisor of the MRO workshop. This procedure follows existing authority structures and certification procedures in the aviation industry. The responsible authority such as EASA certifies the MRO workshop as Part-145 maintenance organization [24]. The MRO workshop subsequently authorises their personnel to conduct maintenance of aircraft components.

In order to reflect this authority structure in the proposed Blockchain concept, we use the chain of trust for digitally signing the chain elements (see figure 6). As described in section 3, the relevant highest level authority, such as EASA, signs a certificate with their private key and passes the certificate to an MRO workshop. Following this, the MRO workshop also signs a certificate with their private key and passes that certificate to their personnel. Validation happens in the other direction: The certificate of the MRO personnel is validated with the public key of the MRO workshop and the certificate of the MRO workshop is validated with the public key of the governing authority. EASA publishing a public key is comparable to the issuance of a root certificate. The public key chain of the parties involved in the maintenance of the landing gear is stored within the regarding Blockchain element in a readable format in addition to the payload. Furthermore, the public certificates retrieved from the superordinate instance of each party are also stored within the Blockchain element.

The digital signatures of the maintenance event of the landing gear are therefore authorised using the chain of trust, which is constituted by the regulating authorities at the top. The authenticity of the maintenance event can then be validated by using the public key chain and the associated certificates, which are stored in a readable format in the Blockchain. The storage of both the public key chain and certificates in the Blockchain provides the required information to validate the history of a component without the necessity of a global database. Thus it is sufficient that only a root certificate, issued by the relevant authority, is globally available and accessible.

In the specific context of the installation or removal of a component on an aircraft, both Blockchain types are interconnected. In order to verify the integrity of the two chains, it is necessary to implement the digital signatures of each chain into the other. When installing a component, the most recent Blockchain element of the aircraft is recorded by appending its digital signatures and its index to the header of the installation block of the component. Similarly, when dismounting a component this process is extended by adding the required Merkle tree hashes (see section 4.2) and the sum of flight hours and cycles to the removal block of the component. Equally, in the Blockchain of the aircraft an element is created for installation and removal containing the digital signatures and index of the most recent Blockchain element of the regarding component.

The certification of all stakeholders involved in the aircraft component documentation through the chain of trust encodes a validity period that decreases with the hierarchical level of the stakeholder. Therefore, the competent authority issues a certificate (public key) valid for several years. The certificate of the MRO workshop issued by the authority is valid for a shorter period of time, e.g. 12 months, after which the certification of its MRO personnel is valid for an even shorter period. If an employee leaves the MRO company or a certificate is revoked before its expiry date, the certificate will be blacklisted and will no longer be able to sign a Blockchain element.

4.4. Matching Stakeholders Requirements

In general, the presented concept complies with the standard procedures and requirements for Aircraft Continuing Airworthiness Record Systems issued by the authorities. The Blockchain-based concept ensures the immutability and integrity of airworthiness documentation, while assigning responsibilities to different stakeholders involved in the documentation process. This structure is reflected in the concept through the chain of trust, digital signatures and hashing.

A key aspect of the continuing airworthiness documentation of aircraft and their components is the maintenance performed by the MRO workshop. The concept provides a thorough documentation process as well as structured hierarchies and authorisation processes. This supports the MRO in the preparation of release to service documents together with proof of compliance with maintenance regulations. In addition, the validation of the maintenance history, especially with regard to life-limited parts, is made directly available. Moreover, individual stamps of maintenance personnel for signing printed documents are digitised and still protected from third parties.

When selling a component on the secondary market, the concept allows the seller to demonstrate that the component has been fully and effectively maintained

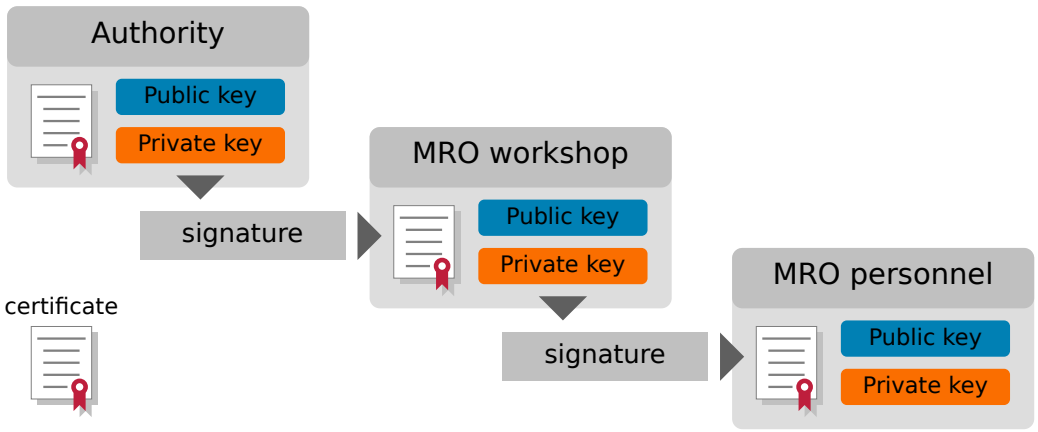


FIG 6. Concept of signing (certifying) and validating in order to form a chain of trust.

and may benefit financially. Whilst providing a secure history of the component, the seller discloses a significant amount of information about its operations to the prospective buyer. It needs to be discussed in which way the transfer of ownership, and therefore the transfer of the component's Blockchain, will take place. One possible way could be a newly introduced industry standard for the storage of Blockchains.

In the aviation industry, some operators/airlines share a material pool of aircraft components that are removed from an aircraft, repaired, and then reinstalled on another owner's aircraft [25]. This ensures the availability of serviceable components. The exchange of components can be addressed by the concept similar to market transactions. However, the implementation of the concept for a material pool, especially with regard to the storage of the chain of each component and the privacy of the airline's operations, is a special case that should be considered. Airline operations and flight activities are recorded by creating Blockchains for each aircraft. The constantly changing flight crew is responsible for creating a chain element, similar to the existing Aircraft Technical Log applications. Certificates of birth and scrapping are integrated in the same way as flight events, maintenance or transfer of ownership. In this way, the owner is provided with documentation covering the entire life cycle of aircraft and components.

4.5. Implementation of Concept

Having discussed the overall concept independently, the remaining questions are whether it would be challenging to implement the concept in an existing architecture and how the transition would occur. In our use case, we were considering a single aircraft component and a single aircraft, establishing the Blockchain after the completion of the manufacturing process. The concept can therefore be easily initialised for new components and aircraft. The use of a separate chain for each component allows a straightforward scaling of the system to a larger number of components and aircraft, without the necessity for alterations of the entire ecosystem at once.

Nevertheless, the conversion of an existing fleet is not a process that can be delayed until the aircraft and, consequently, the components are replaced. Accordingly, the initial Blockchain element of a LLP component may be established by the MRO workshop during the up-coming removal for maintenance. In contrast, the Blockchain of a non-LLP or non-back-to-birth component can be created at any time. Similarly, the aircraft's chain can be implemented at any point in time, but not later than the installation of a back-to-birth tracked component. The system therefore offers great flexibility regarding implementation.

In order to integrate an existing component or aircraft into a new chain, it is possible to record the existing documentation in the Blockchain all at once. It is a prerequisite that the existing documentation is stored digitally. The documentation is then consolidated into a single Blockchain element, which is signed once or individually for each event. However, this would require an authorized party to check the existing documentation, who then would be personally responsible for its accuracy. When the Blockchain is no longer required, for example after the end of the operational life of a component, it can simply be deleted.

Furthermore, before implementing the proposed approach, the technology or standards of the introduced technical concepts, such as X.509 for digital certificates, should be discussed. This discourse should be followed by the construction of a prototype. Moreover, the immutability of the Blockchain-based concept and its protection against hacking should be evaluated through the prototype. In the future, the concept itself could be extended by including engines, given that they contain a multitude of safety-relevant LLP parts.

5. CONCLUSION

The presented paper proposes a concept for traceability of aircraft components spanning their entire life cycle with technical elements of Blockchain. First, the necessity and the requirements for a tracking system were identified. For the continuing airworthiness of an aircraft,

a record system is needed to store all relevant events and approvals, whereby the use of a digital system is possible. The stakeholders, who are users of this system, were identified. Furthermore, the owner/operator of an aircraft is responsible for the documentation and authorities control the process.

Blockchain is not a one-size-fits-all solution, as the hype around the technology suggests. Often confused technical aspects of Blockchain had to be broken down into its elements, the operating principle was described and the usefulness was analysed in relation to the proposed application. Blockchain is a chain of linked blocks which are hashed and signed with methods of asymmetric cryptography. Furthermore, Blockchain can be hosted in a decentralised manner by distributed participants who do not necessarily trust each other, making a consent mechanism essential. Finally, in a simplified use case with only one component and aircraft, a concept for a component tracking system was designed using Blockchain elements.

A Blockchain is created for each component, in which maintenance and other events are recorded as a block. Every hashed block is signed by an authorised person using a private key with reference to a personal digital certificate. Authorisation can be unambiguously verified by a certification chain. Through linking the component Blockchain with a similar structured chain belonging to the aircraft in which the component is installed, the immutable and thus true history of events can be tracked. The proposed concept demonstrates the benefits of immutability and integrity for all stakeholders.

In order to investigate the feasibility and potential of the concept, a detailed definition of the technology stack is required next, e.g. which hashing and encryption methods shall be used. In this context qualified electronic signatures [26] and the World Wide Web Consortium's PROV standard [27] are promising concepts which will be analysed for applicability and similarity to the proposed model. Based on these definitions a prototype implementation can be built and validated upon functionality. Quality feedback from the different stakeholders should also be gathered and thus disadvantages as well as advantages of a solution be highlighted.

Contact address:

malte.schuchard@tu-braunschweig.de

References

[1] European Union Aviation Safety Agency. Easy Access Rules for Continuing Airworthiness (Regulation (EU) No 1321/2014): Part-M, Section A, Subpart B, CONTINUING AIRWORTHINESS, July 2024.

[2] flydocs. Records management. https://flydocs.aero/records-management/. Accessed: 2024-09-04.

[3] ProvenAir. This is ProvenAir. https://www.provenair.com/. Accessed: 2024-09-04.

[4] AVIATAR. About AVIATAR. https://www.aviatar.com/en/about-aviatar. Accessed: 2024-09-04.

[5] MRO Quality Systems. MRO Quality Management Systems - AQM - Aviation Training Management. https://www.mroqualitysystems.com/. Accessed: 2024-09-04.

[6] VERYON. OPTIMIZED AIRCRAFT MRO MANAGEMENT. https://veryon.com/solutions/commercial-aviation/mro-management. Accessed: 2024-09-04.

[7] AVIATION DataHub. VIATION DataHub - The independent data company for the entire aviation industry. https://www.aviation-datahub.com/. Accessed: 2024-09-04.

[8] Maximilian Rolinck, Sebastian Gellrich, Christoph Bode, Mark Mennenga, Felipe Cerdas, Jens Friedrichs, and Christoph Herrmann. A Concept for Blockchain-Based LCA and its Application in the Context of Aircraft MRO. *Procedia CIRP*, 98:394–399, 2021. ISSN: 2212-8271.

[9] European Parliament and Council. Regulation (eu) no 748/2012 of the european parliament and of the council, July 2012. Laying down the airworthiness and environmental certification requirements for aviation products and parts and for the approval of design and production organizations. https://eur-lex.europa.eu/eli/reg/2012/748/oj.

[10] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008. Accessed: 2024-10-17.

[11] Gautami Tripathi, Mohd Abdul Ahad, and Gabriella Casalino. A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, 9:100344, 2023. ISSN: 2772-6622. DOI: https://doi.org/10.1016/j.dajour.2023.100344.

[12] Xun Yi, Xuechao Yang, Andrei Kelarev, Kwok Yan Lam, and Zahir Tari. *Blockchain Foundations and Applications*. SpringerBriefs in Applied Sciences and Technology. Springer Cham, 2022. ISBN: 978-3-031-09669-3.

[13] V. Schlatt, A. Schweizer, N. Urbach, and G. Fridgen. *Blockchain: Grundlagen, Anwendungen und Potenziale*. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Fraunhofer Institut für Angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik, Wittelsbacherring 10, 95444 Bayreuth, 2016. Accessed: 2024-10-17.

[14] Leila Ismail and Huned Materwala. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, 11(10), 2019. ISSN: 2073-8994. DOI: 10.3390/sym11101198.

[15] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2567–2572, Oct 2017. DOI: 10.1109/SMC.2017.8123011.

[16] Md Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, and Mohammad A. Hoque. A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182:103035, 2021. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2021.103035.

[17] Seyed Mojtaba Hosseini Bamakan, Amirhossein Motavali, and Alireza Babaei Bondarti. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, 154:113385, 2020. ISSN: 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2020.113385.

[18] L. M. Bach, B. Mihaljevic, and M. Zagar. Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1545–1550, May 2018. DOI: 10.23919/MIPRO.2018.8400278.

[19] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. Discrete Mathematics and Its Applications. CRC Press, Hoboken, 1997. ISBN: 0-8493-8523-7.

[20] William Easttom. *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. Springer International Publishing, 2021. ISBN: 978-3-03063114-7.

[21] W. Macharia. Cryptographic hash functions. https://www.researchgate.net/publication/351837904_Cryptographic_Hash_Functions, 2021. Accessed: 2024-11-07.

[22] I. Mironov. Hash functions: Theory, attacks, and applications. https://crypto.stanford.edu/~mironov/papers/hash_survey.pdf, 2005. Accessed: 2024-11-07.

[23] IETF. HTTP Over TLS. https://datatracker.ietf.org/doc/html/rfc2818, 2000. Accessed: 2024-09-13.

[24] European Union Aviation Safety Agency. Easy Access Rules for Continuing Airworthiness (Regulation (EU) No 1321/2014): Part-145, July 2024.

[25] Lufthansa Technik. Material Pooling. https://www.lufthansa-technik.com/en/material-pooling. Accessed: 2024-09-04.

[26] European Parliament and Council. Regulation (eu) no 910/2014 of the european parliament and of the council, July 2014. On electronic identification and trust services for electronic transactions in the internal market and repealing. https://eur-lex.europa.eu/eli/reg/2014/910/oj.

[27] W3C Provenance Working Group. Provenance data model. World Wide Web Consortium (W3C), April 2013. Accessed: 2024-10-17. https://www.w3.org/TR/prov-dm/.