Air Traffic Management Blockchain Infrastructure for Security, Authentication, and Privacy

Ronald J. Reisman*
NASA Ames Research Center, Moffett Field, California, 94035

[Abstract] Current radar-based air traffic service providers may preserve privacy for military and corporate operations by procedurally preventing public release of selected flight plans, position, and state data. The FAA mandate for national adoption of Automatic Dependent Surveillance Broadcast (ADS-B) in 2020 does not include provisions for maintaining these same aircraft-privacy options, nor does it address the potential for spoofing, denial of service, and other well-documented risk factors. This paper presents an engineering prototype that embodies a design and method that may be applied to mitigate these ADS-B security issues. The design innovation is the use of an open source permissioned blockchain framework to enable aircraft privacy and anonymity while providing a secure and efficient method for communication with Air Traffic Services, Operations Support, or other authorized entities. This framework features certificate authority, smart contract support, and higher-bandwidth communication channels for private information that may be used for secure communication between any specific aircraft and any particular authorized member, sharing data in accordance with the terms specified in the form of smart contracts. The prototype demonstrates how this method can be economically and rapidly deployed in a scalable modular environment.

I. Introduction

Although the FAA has mandated that aircraft flying in the National Airspace System (NAS) must equip with the Automatic Dependent Surveillance System (ADS-B) by 2020[1,2], general aviation[3] and the US military[4] lag behind their implementation schedule. It is widely recognized that there are still unsolved issues that complicate ADS-B adoption for stakeholders[5] who want to maintain the current levels of privacy[6], anonymity[7], authentication[8] and resistance to malicious interference[9], including spoofing[10] and/or denial of service attacks.[11]

There have been many proposals for making the ADS-B system more secure, though none have been accepted by the stakeholders, and the FAA does not currently endorse any particular plan for addressing these issues. [12] The prior art in this field is often divided into two areas: secure location verification, and secure broadcast authorization. The approaches to secure location verification include multilateration[13], distance bounding[14], Kalman filtering[15], group verification[16], intent verification[17] data fusion[18], and traffic modeling[19]. The approaches to secure broadcast

* Aero Computer Engineer, Flight Trajectory Dynamics and Controls Branch, M/S 210-10

authorization include non-crypto schemes, such as fingerprinting[20], as opposed to explicitly cryptographic schemes, such as public key infrastructure (PKI)[21].

This paper is a contribution to cryptographic secure broadcast authorization approach by presenting a design and description of illustrative prototype software that addresses these ADS-B vulnerabilities via a novel blockchain-based PKI implementation. This design supports ADS-B aviation surveillance services that maintain or exceed current levels of aircraft privacy that are valued features of the present-day centralized NAS radar-based services. This paper introduces an "Aviation Blockchain Infrastructure" (ABI) design that enables aircraft to communicate effectively, securely, and privately with air traffic management and other properly authorized entities. The engineering prototype of the ABI described below, implemented in a widely-available open source permissioned blockchain framework, represents a scalable architecture and illustrates how such a serverless PKI infrastructure may be rapidly deployed and economically maintained.

II. Background

A. ADS-B Effect on Air Traffic Security & Privacy

Currently NAS Air Traffic Control (ATC) largely relies on a system of ground-based radar systems and Mode-C transponders to track aircraft. The FAA has exclusive possession of the totality of this air traffic surveillance data, enabling the Agency to establish administrative processes to also insure operational privacy for military and approved civil aircraft (who have valid requirements for keeping their activities private) before releasing the rest of this data to the general public. The administrative processes for "blocking" operations from public view (described below) is effective because NAS air traffic surveillance data originates from FAA-controlled radar-based aircraft-surveillance systems.

ADS-B data, however, are not subject to the same sort of exclusive control. The ADS-B, as its name suggests, broadcasts data omnidirectionally in plaintext to any receiver within range. Privately-owned inexpensive listening-posts are operated by amateurs and entrepreneurs to form international air traffic surveillance networks that aggregate, record, and display this surveillance data to the world-wide public[22]. The FAA's mandate for universal adoption of ADS-B is complicated by stakeholders' concerns about that system's lack of a robust security model.

It has been widely reported that ADS-B is subject to third-party spoofing (false aircraft position-reports) e.g., Greenberg (2012) wrote: "The threat of ADS-B spoofing is of concern to many organizations and altering existing and planned ADS-B infrastructure to prevent such spoofing would require extensive investment in revising existing infrastructure and also changing out ADS-B equipment in existing aircraft." [23]

Although there are a number of proposals employing techniques to overcome spoofing, there is no operational plan for mitigation that is both widely-accepted and sufficiently effective. Strohmeier, et al (2015), conclude: "…it seems that the solutions currently under consideration (and in use in practice such as multilateration) can only be a fill-in, providing a quick improvement to the security of the current system." [24]

Several studies have expressed concern about the privacy and security of ADS-B unencrypted "plaintext" broadcasts[25,26,27]. One study suggested: "…without appropriate countermeasures, critical air traffic management decision processes should not rely on ADS-B derived data." [28]

The FAA has announced that it will provide air traffic control services exclusively to aircraft equipped with ADS-B by 2020, though the regulations will allow aircraft to operate in an "anonymous" ADS-B mode. Air traffic services, however, will not be provided to aircraft who attempt to either operate ADS-B in "anonymous" mode or to disguise their identity.[29] Though some military missions may not require civilian air traffic services, most other military aircraft and the vast majority of corporate flights do require ATC services.

These unresolved issues complicate the adoption of ADS-B by military and corporate aircraft operators. These stakeholders express concern about broadcasting their positions every second in plain text, thus compromising present levels of operational privacy and security. The uncertainties regarding these stakeholders' participation in the ADS-B Mandate has a direct effect on a wide range of the FAA's Next Generation (NextGen) Air Traffic Control modernization and automation programs. Many of the NextGen systems are premised on ADS-B usage in the NAS, and so non-adopting aircraft may not be recognized by NextGen systems, and this particular form of data-loss often egregiously degrades their performance.

For instance, in 2018 the U.S. Government Accountability Office reported that in the absence of security assurances by the FAA, the Department of Defense (DOD): "… had not taken significant action or fully implemented … Integrating NextGen requirements into plans and policies … did not integrate the needs and requirements of DOD components related to ADS-B into cohesive plans and policies for inclusion in NextGen joint planning and development, as directed by the Deputy Secretary of Defense in 2007…. the DOD Mid-Term NextGen Concept of Operations and the DOD Mid-Term NextGen Implementation Plan do not discuss planning for ADS-B Out requirements, which are critical to NextGen Military Aircraft Tracking."[30]

Although there are a number of proposals and designs for hardening ADS-B systems, none have been approved for implementation in the NAS. Some of the factors complicating a decision to choose an ADS-B security architecture include the difficulties in establishing universally accepted Client-Server standards that will support an equivalent of a Public-Key/Private-Key Infrastructure (PKI). As yet (2018 Nov.), the aviation industry has not adopted any standard method for this purpose, nor has the FAA and DOD developed procedural or engineering support for these security and privacy issues. The recent U.S. Accountability Office report strongly recommends solutions: "address operations, physical, cyber-attack, and electronic warfare security risks; and risks associated with divesting secondary-surveillance radars. The solution or mitigations should be approved as soon as possible."[31]

B. **Military Issues**

1. NAS Military Operations

A characterization of the military and civil aviation data subset (published for the first time in this paper) provides a basis for estimating the participation and impact of these aircraft in the NAS. This derived from a data sample from the 20 Air Route Traffic Control Centers (ARTCCs) which cover the continental United States (CONUS). These data were collected from January 1 to Nov 22 (inclusive), 2016. On a typical day in the CONUS well over a thousand unique military flights were recorded squawking Mode-C transponder data, and on some days over 2,000 such flights were recorded. This represents an average of ~4% of the total amount (~33,000) of all filed flights in CONUS Class A Airspace. On any given day, military operations represent between 6.4% and less than %1 of the total number of flights, with a standard deviation of 1.7%. However, the impact of military flights on civil aviation is partially mitigated by geographical separations between these two populations. Military flights that fly on their own route structures and within special use airspaces will consume less civil airspace and route resources than equivalent quantities of corporate operations, since the latter share these resources with commercial and other civilian operators.

FAA air traffic control radar surveillance systems routinely capture documentary data on a wide variety of military operations in the NAS, including: Bomber patrol; UAS border patrols (including into bordering nations); Fighters and interceptors; Training, including: Combat Aviation Support, Command/Control/Communications & Intelligence, Service Support, Combat Air Assault, Search & Rescue, Ordinance (e.g. bombing practice), Tactical experimentation & modification (indicating strategic evolution); Air Transport, including: Troop and materiel movement, Mission Support, Military Air Routes (geographically separated from civilian routes; see above).

The military has a valid operational requirement for maintaining the privacy of the track-histories (e.g. position and state reports) of these flights, and so may object to mandated plaintext ADS-B broadcasts.

2. Controlled Unclassified Information

Military aircraft traffic data are considered, at minimum, Controlled Unclassified Information (CUI), and more specifically is referred to as Department of Defense (DoD) "Critical Infrastructure Security Information," defined as: "Information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities …."[32]

Considering the variety and nature of military missions described above and the sensitivity of air traffic data, the military requirement for confidentiality is likely to remain decisive in their adoption and use of ADS-B.[33]

C. **Civilian Aviation Concerns**

1. NAS Corporate Operations

The 11-month sample of traffic from the 20 CONUS ARTCCs mentioned in the above *NAS Military Operations* was analyzed with a filter based on the "SCBlockAtIndustry" list employed by the FAA to identify aircraft approved for privacy procedures (as explained in *Aircraft Situation Display to Industry*, below). This sample shows that in an average 24-hour period there were ~33070 filed flight plans, and an average of 1444 of those were "blocked" aircraft. This analysis therefore identifies an average of 4.37% of the total number of non-military aircraft that would be shielded from public view on a typical day. Though this number is just slightly larger than the number of daily CONUS military flights, the impact of these civilian aircraft (particularly corporate business jets) is far greater on NAS resources, since all civilian aircraft must share the same civil airspace and routes, whereas military flights often use other options.

2. Aircraft Situation Display to Industry (ASDI)

The FAA currently makes aircraft surveillance data available to the public via the Aircraft Situation Display for Industry (ASDI) program. The ASDI data are derived from the FAA Traffic Flow Management System (TFMS), which collects filed flight plans, amendments, and one-minute-update radar-based position reports from all ARTCCs. The TFMS data is primarily used for Traffic Flow Control application and therefore includes all aircraft tracked in every Center, including military and corporate.

The FAA first filters and deletes the military CUI data from TFMS data, and the remaining data covers all non-military aircraft tracked by the FAA's Centers. Since the FAA's process for Identification and Protection of military flights does not filter non-military aircraft, the FAA has instituted a separate process called Blocked Aircraft Registration Request (BARR) to remove approved privately-owned aircraft from ASDI publication. This civilian aircraft population includes corporate operators who would prefer to keep their activities private for a number of valid reasons, including prevention of corporate espionage by competitors who are motivated to track the movements of executives.

The FAA has therefore instituted BARR procedures for "blocking" such sensitive data from publication via ASDI, offering aircraft operators two methods for "blocking":[34]

1) **ASDI Subscriber Level Blocking:** The FAA sends data to ASDI providers in a manner that can only be accessed by authorized users (aka “subscribers”). This method enables subnets of “subscribers” to share information about their own aircraft among themselves and with air traffic services and yet remain hidden from public view. Subscriber Level Blocking is often used by corporate aircraft owners who want to keep operations private from the public, and especially from their competitors, though they may want their support services and other associates to track their movements in near-real-time.

2) **FAA Source Blocking:** FAA blocks the data at the source, such that ASDI providers never receive the information on these aircraft.

The FAA's Performance Analysis organization maintains the list of the ~19,000 civil aircraft that are blocked from ASDI publication. This list is available to authorized entities (e.g., FAA, NASA, DoD) in a text file that is maintained on the FAA System-wide Information Management Aeronautical Data Exchange website.[35] The “SCBlockAtIndustry” file is updated monthly, and the FAA sends notifications to authorized parties each month when new versions are posted.

D. ADS-B Cryptography Prior Art

Finke, et al (2012)[36] proposed that an algorithm called “FFX” (an acronym meant to suggest: Format-preserving, Feistel-based encryption)[37] would be a good fit for ADS-B application because it is both secure and computationally efficient. This efficiency may enable software based on the FFX algorithm to run on the same internal processor(s) that are used in current ADS-B hardware. [38] Finke, et al, propose several scenarios for distributing the encryption keys, although they identify these key exchanges as a potential stumbling block to their (and other) ADS-B security schemes, concluding: “The primary obstructions concerning implementation, however, relate to key management and distribution.”

Lee, et al, and others have proposed to address these key-distribution problems by using variations of PKI to exchange a symmetric key that can be used to encrypt ADS-B messages.[39] An outstanding issue in most of these PKI schemes is the difficulty of implementing the public key framework in a manner that can be utilized by aircraft in flight.

A key challenge to implementing an aviation-oriented PKI infrastructure concerns issues of allowing and managing participants’ access to information that is distributed by centralized data service systems. Most PKI infrastructures have similar end user requirements defined in PKI Certification Authority (CA) Practice Statements issued by a central authority. Although there are alternatives to centralized CA organization, they may be characterized by the observations of Ferguson & Schneier: “PGP has its own strange PKI-like structure called the web of trust. In practice, it is too complicated to explain to users, and it is only used on a limited scale.”[40]

The practical organizational requirements for end user participation in most PKI systems puts a very large impediment to adoption and maintenance. If, for instance, we envisioned a new set of potentially expensive technical training and operational requirements that all aero end users (e.g. airlines) must adopt as a precondition to participation in a PKI infrastructure for aviation, then we may expect the expense and complication of such new mandates would create potent obstructions to adoption.

The employment of enterprise-oriented blockchain technology offers a potential solution to overcoming these practical difficulties in establishing an “on-ramp” for aircraft to join an ABI network. A virtue of theses blockchain schemas is that they enable implementation of a PKI infrastructure in which end users are not required to belong to any single organization, or adhere to any single client/server protocol, and therefore end users are not burdened with the kinds of server-based PKI requirements and impediments described above.

In summary, previous work has identified ADS-B security, privacy, and authentication vulnerabilities; and recognized the potential of using PKI to distribute symmetrical keys, enabling efficient encryption and decryption of ADS-B messages.

III. Concept of Operation

This paper will present a design that addresses these ADS-B vulnerabilities via a novel blockchain-based PKI for aviation surveillance application. We propose to use a "lightly permissioned" Blockchain framework to enable the ADS-B systems to meet or exceed the same levels of privacy and security currently provided by radar-based systems in the NAS.

The ABI is based on a software platform that is primarily designed to support use-cases where some data are permissible to be shared among all participants, while other data are protected and only observable by selected entities under the appropriate conditions. Figure 1 illustrates several goals of the theory of operation for purposes of near-future air traffic management, e.g., military aircraft may withhold their information from any other non-military entities (except ATC).

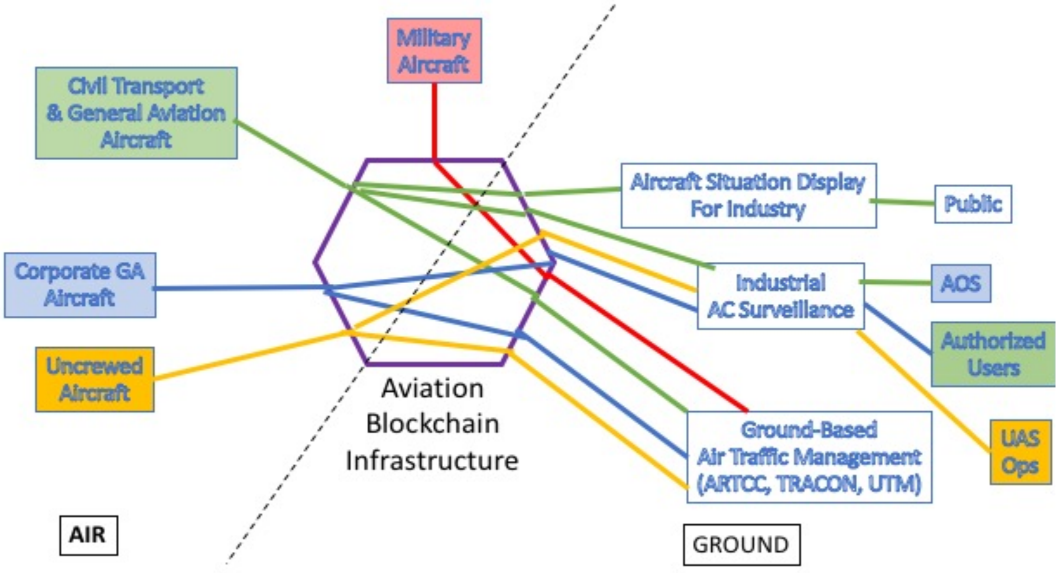
Military Aircraft
Civil Transport & General Aviation Aircraft
Corporate GA Aircraft
Uncrewed Aircraft
Aviation Blockchain Infrastructure
Aircraft Situation Display For Industry
Public
Industrial AC Surveillance
AOS
Authorized Users
UAS Ops
Ground-Based Air Traffic Management (ARTCC, TRACON, UTM)
AIR
GROUND

Figure 1. Notional design of blockchain-mitigated channels of communication. Chaincode (aka 'Smart Contracts') routes the information appropriately between aircraft and the ground-based ATM and other support services.

Corporate and industrial aircraft may want to prevent business competitors from observing their operations, while still enabling their supporting aviation operations services (AOS) to track them. An Uncrewed Aviation System (UAS) may also similarly refrain from sharing their information with the public, while remaining in communication with their own AOS providers. Most general aviation and airline traffic may opt to make their flight information public, in a manner similar to the current levels of privacy offered by ASDI, though more robustly resistant to spoofing.

Although this paper focuses primarily on issues relating to operational privacy, it should also be noted that the design and implementation methods (described below) could also be used to enable ADS-B systems that broadcast in plaintext to include an identifying cryptographic token that could be embedded in the transmission and could be used to authenticate the transmission, and therefore could effectively counter malicious and pernicious "spoofing" and denial-of-service attacks.

IV. Methods and Materials

A. Blockchain Channels, Subnets, and Smart Contracts

The ABI described in this paper is based on an open source blockchain platform called "Hyperledger Fabric"[41] that is specifically designed for enterprise transactions that resemble typical air traffic management interactions.

Hyperledger Fabric also provides services called "private channels" as a means to communicate private information at a comparatively high bandwidth. These private channels may be used to pass a private key (or time-key data structure) suitable for encrypting ADS-B Out transmissions between any specific aircraft and any particular authorized member in accordance with the terms of the smart contracts associated with the particular private channel (and subnet). The use of cyphertext enables ADS-B users to maintain privacy and anonymity from general public while also providing a secure and efficient method for communication with authorized entities, such as Air Traffic Services or Airline Operations Services.

Aircraft operating a Traffic Alert and Collision Avoidance System (TCAS) should also receive ADS-B information in a form that may be used within the system requirements to avoid loss of separation. The precise method for inter-aircraft communication was not fully modeled the ABI prototype code, however, and the algorithmic solution to this issue must be fully solved in a manner that is acceptable to the aviation community as a precondition for operational use of an ABI implementation.

Theoretically, many blockchain system implementations grant members the power to conduct private and confidential transactions while coexisting with restricted members on the same blockchain network.[42] Controlling members define one or more channels to isolate peers into subnets and create private ledgers. Each channel's ledger is only accessible to its member peer nodes. The channel's organizations (entities) must approve each peer's membership to the channel. Client requests are routed to a specified channel to run a smart contract that is deployed on that channel. The results are endorsed and verified, and then updated in that channel's ledger.

Channels are used for conducting confidential transactions. For example, aircraft state information (e.g., altitude, latitude, longitude, indicated airspeed, heading, etc.) may be kept secure via a private channel, while the public aspects of the aircraft's flight plan information (e.g., aircraft id -- aka callsign, aircraft type and equipage, origin, destination, filed route of flight, etc.) may be published on a channel that's open to all approved members.

B. Blockchain Platform Design: Enterprise vs. "Coin" Use-Cases

A variety of different Blockchain platform technologies are currently available. Typically, a platform is primarily characterized by the token blockchain, as opposed to the underlying technology that implements the project platform. The most popular is Ethereum, a blockchain platform designed to implement decentralized applications called smart contracts.[43]

Ethereum claims a >80% market share, followed by other platforms, including (in order of market share popularity): Waves, Bitcoin Fork, Stratis, Graphene, Hyperledger, Ethereum Classic, Maidsafe, Litecoin Fork, NEO, and Rootstock.[44] All of the above platforms were designed to support "coin" (monetary) applications, and although non-monetary contracts and communications may be accomplished, the implementations often lack cohesion, flexibility, and consistency due to the platforms' design limitations.

The design limitations of these "financial tech" ("fintech") foundations have prompted the development of an alternative blockchain foundation that is better suited for transactions and communications that cater to the requirements of business use-cases. The Linux Foundation, in association with a number of corporations (e.g., IBM, Oracle) hosts a number of open-source "Hyperledger" projects. One of these projects, "Hyperledger Fabric," is a blockchain framework implementation designed for commercial enterprise applications, and is intended as a development foundation with a modular architecture that allows plug-and-play components. These applications, usually called "smart contracts" in other blockchain platforms are called "chaincode" in Hyperledger Fabric parlance.[45, 46]

Hyperledger Fabric features a number of distinctive design innovations intended to differentiate it from "fintech" systems and make it more versatile and appropriate for enterprise transactions that support air traffic surveillance use-cases. These features include: permissioned membership, consensus management, private channels and contracts, decentralized implementation, full-featured computer-languages used in chaincode, and open source code that may be modified to meet air traffic surveillance requirements (e.g. implementing high-speed channels to meet system transport-delay constraints). The Hypertext Fabric platform was chosen among the other alternatives because it conforms more closely to requirements that were identified for provision of systemic remedies to ADS-B security issues.

For instance, most fintech platforms are characterized as networks available to the public that allow unknown identities to participate, with few hard-engineered provisions for a permission management process. The "proof of work" (PoW) protocols employed in these platforms to establish consensus are required precisely because these networks are open permissionless systems populated by participants with unknown identities. Fabric's seminal difference from these systems is that it is an explicitly private and permissioned Distributed Ledger Technology (DLT) platform that is specifically designed for enterprise services.

Specific features of this "permissioned" platform are designed to meet practical enterprise use-case requirements for near-real-time transactions between securely identified participants. These features include: 1) Participants must be identified/identifiable; 2) Networks are required to be permissioned; 3) High transaction throughput performance; 4) Low latency of transaction confirmation; 5) Authentication, privacy and confidentiality of tracking and communication between clients (e.g. aircraft) and providers (e.g. air and services) is consistently supported.

All members of a Fabric network are required to enroll through a trusted Membership Service Provider (MSP). The "enrollment" protocols provide capabilities that enable greater flexibility in consensus management. Whereas most coin-oriented ledger platforms employ Byzantine Fault Tolerant (BFT) methods to determine consensus, another distinct design feature of Fabric that differentiates it from other "permissioned" platforms (i.e., that it particularly appropriate for air traffic surveillance applications) is its support for alternative consensus protocols[47], such as Crash Fault Tolerance (CFT), that are both more computationally efficient and practical for many transactional uses-cases.

Fabric's consensus protocol flexibility allows for parallel code execution, effectively increasing system-wide performance and eliminating vulnerabilities caused by non-determinism, and therefore Fabric does not require specialized domain-specific languages (DSL) for smart contract coding to preserve the reliability of the network. Fabric therefore differs from DSL-constrained platforms by supporting smart contracts ("chaincode") implemented in general-purpose programming languages such as Node.js, Python, Java, and Go (aka "golang").

Furthermore, every execution of a smart contract in most DSL-based systems is "public" since the transaction, and often the source code itself, are usually fully visible by other participants. This "public" feature of DSL implementations often complicates or impedes exchange of private data and private (algorithmic) agreements between participants. Many use-cases require subgroups of participants to share information that is kept private from other participants. Fabric achieves such confidentiality by using its channel architecture to restrict the distribution of confidential information exclusively to authorized nodes.

The Hyperledger Fabric platform provides for a standardized PKI infrastructure that may provide identity management for aircraft operators who will acquire a PKI-supplied synchronous cypher ("key"). The key will enable transmission of ADS-B data to Air Traffic, other selected services, and nearby aircraft in an encrypted format ("cyphertext"). The ADS-B data will be received and authenticated by participants who share knowledge of the key. The privacy of the aircraft, or ADS-B data, is maintained by the encryption of the beacon messages.

In the context of air traffic use-cases, one of the principal engineering challenges would be the issue of the "on-ramp," i.e. the method that participants (e.g., aircraft operators) use to gain entry to this "permissioned" system. The "on-ramp" method must operate over a wide geographic area, potentially globally. Previous PKI methods have been complicated and sometimes compromised by confusing variations in organizational and international computational conventions.

In the following example we describe prototype software employing Hyperledger Fabric that demonstrates the capacity to meet the ADS-B authentication and privacy objectives described above. The software was developed on a Dell 7720 laptop running Red Hat Enterprise Linux (RHEL) 7.5. The chaincode was written in the "go" language and was typically run inside Docker[48] "containers".

V. Description of Prototype

The aircraft-PKI-onramp issue is addressed through the Hyperledger Fabric Certificate Authority (CA), which provides features for registration of digital identities, and the issuance, renewal, and revocation of Enrollment Certificates (ECerts). These are (most commonly) X.509 standard cryptographically validated digital certificates. All communication to the CA server is accomplished via secure Representational State Transfer (REST) application program interfaces (API), as specified in a JavaScript Object Notation (JSON) configuration file.

The Fabric CA is a private Root CA capable of providing and managing its own certificates as well as (optionally) using third-party public/commercial CA (e.g., Symantec, GoDaddy, DigiCert) to provide identification. The Fabric Membership Service Provider (MSP) uses the enrollment CA ECerts to define members of functional organizations, roles, and access privileges.

The Fabric CA is designed to be used as the Root CA node in conjunction with Intermediate CAs running on peer nodes. These peer nodes are architected to be far-flung geographically and still maintain identity-management processing efficiency. The connections and various means and methods that peer nodes may use to accept input from aircraft operators, air traffic management services, and other users, are heterogeneous and may vary greatly in local implementations. Once a participant is “Enrolled” into a defined Membership, however, the modes of communication are well-defined by Fabric standards.

All blockchain network peer nodes hold copies of ledgers and chaincode (aka smart contracts). Most of these platforms require all nodes to hold essentially identical ledgers, which contain an immutable record of every transaction from every member. Fabric’s privacy-oriented design differs from this design (exemplified by Bitcoin), and allows private chaincode relationships between any two (or more) members and multiple ledgers into private data collections. Fabric “Membership” conveys permissions to transact with other “members” through their private data collections. A single enrolled Identity may be a Member of several different Fabric organizations, and many different relationships and transactions may be defined in chaincode.

In the prototype, all simulated aircraft digital identities (created by a Fabric CA for test purposes) were enrolled by default as Members of the Air Traffic Management Services (ATMS) organization. All simulated ADS-B data from each of the aircraft Members were sent to ATMS by default, with no editing or redaction. This rule represents the requirement of real-world ATMS for uncensored air traffic surveillance. Each aircraft creates its own ledger, viewable only by itself and ATMS. The ATMS creates a ledger of all ADS-B transmissions from all aircraft, and it is the only Member with permission to access, so ATMS “knows” about all aircraft, though the aircraft only “know” about its own history.

The prototype also has an organization for Military ATMS (MATMS), representing a simplified abstraction of ground-based support services for military aircraft. The simulated flight plan “aircraft type” value was used by the software to detect aircraft operated by the U.S. Military, and each of these was enrolled in Membership to the MATMS organization, in addition to the default ATMS org. The MATMS chaincode resembles the ATMS contracts: ledgers are kept for each military aircraft, accessible only by that particular aircraft and the MATMS. Each simulated “military” aircraft receives a lightweight crypto synchronous cypher that was shared between the aircraft, ATMS, and MATMS. The cypher can be used to encrypt ADS-B data and broadcast its cyphertext from the aircraft, while ATMS and MATMS could use it to authenticate the data as originating from the only aircraft that should be in possession of the cypher-key.

Several organizations representing airlines were also simulated. If the first three characters of an aircraft’s ID (aka “callsign”) matched one of these “airline” organizations (e.g. “AAL,” “DAL”) then private ledgers were created, again with permissions for aircraft and “airline” to access only the ledge of its own messages, and the “Airline” organization possessing exclusive access of all the flight information from the simulated aircraft it “owned” in its cumulative ledger. There is no presumption that Airlines will encrypt their aircraft data, since they currently transmit ADS-B in plaintext.

Organizations representing corporate aircraft ground-services were simulated. These functioned similarly to the “Airline” organizations (selected by callsign-matching to corporate aircraft “inventory” lists), again creating individual ledgers for aircraft and cumulative ledgers for all aircraft associated with each “corporation.” These aircraft would be processed similarly to the Military in real-world scenarios: Corporate aircraft could maintain privacy by broadcasting encrypted ADS-B, interpretable only by ATMS and their own support service organizations. Neither Military nor Corporate ADS-B could be detectable by conventional ADS-B receivers unless the aircraft operators decided to intentionally transmit the data in plaintext.

Another class of ledger contained data only from the simulated cumulative Airline traffic and the civil (non-corporate) aircraft. The algorithm, which is simplistic for demonstration purposes, used to select these latter aircraft was: 1) “N” prefix in their callsign; and 2) that callsign is not in lists of “corporate” aircraft inventory organizations. This ledger was therefore a representation of air traffic data that is nominally available to the public, and is therefore the ledger of the “Aircraft Situation Display to Industry” (ASDI) organization. The ASDI ledger is accessible by everyone, and may be published with impunity inside and outside the Hyperledger Framework.

The last type of ledger and accompanying chaincode represented aircraft-to-aircraft communication suitable for TCAS applications. This portion of the prototype was left as “toy” code, insofar as the algorithmic method for passing identities between aircraft that were within three nautical miles of each other was implemented in a manner too simplified for operational use. In real-world applications these various ledgers would be routinely archived to conserve mass-storage resources, since there is little need to store historical data on operational ATM systems. This ability to archive obsolete transactions is another differentiator between Fabric and “financial tech” blockchain platforms which require storage of constantly-growing ledger files, making maintenance of a Fabric-based ABI more practical for aviation use-cases.

Concluding Remarks

This paper’s proposes to leverage an industrial-strength open-source enterprise-blockchain framework called Hyperledger Fabric to demonstrate potential solutions to vexing technical issues that threaten the adoption of ADS-B by Military, Corporate, and other aircraft operators who do not want their operations and movements discernable by the general public.

This approach is intended to contribute to an eventual systemic solution for the privacy management requirements of ~9% of CONUS flights (~4.4% Corporate; ~4.2% Military). These flights are currently not visible to the public. These two stakeholders’ privacy concerns may complicate their adoption of the FAA mandate for full ADS-B (plaintext transmission) operation by 2020.

Although this approach is not perfected, it is based on available technology. The prototype chaincode demonstrates methods that may be used to create and maintain a permissioned ledger-based network that could contribute to the solution to maintaining privacy for NAS stakeholders.

The Hyperledger Fabric software was selected as the platform for our prototype because it is designed as to meet Enterprise requirements transactional use-cases, including Root Certification Authorization (CA) mechanisms that provide robust features for security and authentication.

One of the features that was not completed was the scheme for guaranteed reception by each aircraft’s Traffic Alert and Collision Avoidance System and Cockpit Display of Traffic Information of all nearby aircraft ADS-B transmissions, regardless of whether they may be encrypted or in plaintext. This is a non-trivial problem and should be designed, coded, demonstrated, and evaluated before this scheme may be judged sufficient for operational use.

The most interesting next steps may be the development and demonstration of ADS-B modifications (hopefully largely restricted to software running on the ADS-B processors) that might enable an end-to-end demonstration of a practical ADS-B usage model that satisfies the privacy concerns of military and corporate stakeholders.

Acknowledgements

The author thanks those who contributed in various ways to this study, including: W. Blacker of the FAA BARR Program; M. Ma, L. Bagasol, J. Cisek, and the FAA WJH Technical Center for maintaining the NAS research data base; M. Grey, S. Bunyan and J. Cheng, et al, for systems support; and J. Saucedo, G. Gilmore, B. Behlendorf, and W. Diffie for constructive criticism.

References

[1] Federal Register, Vol. 75, No. 103, DEPARTMENT OF TRANSPORTATION Federal Aviation Administration 14 CFR Part 91 [Docket No. FAA–2007–29305; Amdt. No. 91–314] RIN 2120–AI92 Automatic Dependent Surveillance— Broadcast (ADS–B) Out Performance Requirements To Support Air Traffic Control (ATC) Service Final Rule. May 28, 2010, URL: https://www.gpo.gov/fdsys/pkg/FR-2010-05-28/pdf/2010-12645.pdf [cited 30 April 2018]

[2] US Code of Federal Regulation, Title 14: Aeronautics and Space, PART 91 — GENERAL OPERATING AND FLIGHT RULES, Subpart C—Equipment, Instrument, and Certificate Requirements, §91.225 Automatic Dependent Surveillance-Broadcast (ADS-B) Out equipment and use. & §91.227 Automatic Dependent Surveillance-Broadcast (ADS-B) Out equipment performance requirements, URL:
https://www.ecfr.gov/cgi-bin/text-idx?SID=8137158693744ba666e318c1f474d81b&node=se14.2.91_1225&rgn=div8
and: URL:
https://www.ecfr.gov/cgibin/retrieveECFR?gp=&SID=92976e93abb3045a3360432d29325bb5&mc=true&r=SECTION&n=se14.2.91_1227 [cited 30 April 2018]

[3] Croft, John, "General Aviation May Not Meet FAA ADS-B Mandate For 2020," Aviation Week and Space Technology, 23 Dec. 2016

[4] Carey, Bill, "GAO: Pentagon, FAA Lag In Addressing ADS-B Risks," Aerospace Daily & Defense Report, Jan 25, 2018. URL: http://aviationweek.com/awindefense/gao-pentagon-faa-lag-addressing-ads-b-risks [cited 3 Dec. 2018]

[5] Bellamy, W., "What is the Answer to Business Aviation's ADS-B Privacy Concern?" Avionics International, October—November, 2018. URL: http://interactive.aviationtoday.com/avionicsmagazine/october-november-2018/what-is-the-answer-to-business-aviations-ads-b-privacy-concern/ [cited 3 Dec. 2018]

[6] Sampigethaya, K., and Poovendran,R., "Privacy of future air traffic management broadcasts, Digital Avionics Systems Conference,". 28th Digital Avionics Systems Conference, Orlando, FL, October 25-29, 2009. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5347456 [cited 30 April 2018]

[7] FAA (AIR-130) Advisory Circular, "Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems," AC No: 20-16, 2010 May 10, URL: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2020-165.pdf [cited 30 April 2018]

[8] McCallie, D., Butts J., and Mills, R., "Security analysis of the ADS-B implementation in the next generation air transportation system," International Journal of Critical Infrastructure Protection, 4 (2) , pp. 78-87, 2011

[9] Costin, A., and Francillon, A.,"Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," Black Hat Conference, July 21-26, 2012 URL: http://www.eurecom.fr/en/publication/3788/download/rs-publi-3788.pdf [cited 30 April 2018]

[10] Haines, Brad, and Fostrer, Nick, "Spoofing ADS-B," from "Hackers + Airplanes = No good can come of this" presented at Defcon 20, Las Vegas, NV, 2012. URL: https://www.youtube.com/watch?v=NSLqRXyxiBo [cited 30 April 2018]

[11] Strohmeier, M., Schäfer, M., Lenders, V., Martinovic, I., "Realities and Challenges of NextGen Air Traffic Management: The Case of ADS-B," Communications Magazine, IEEE 52 (5), pp. 111-118. May, 2014 URL: https://ieeexplore.ieee.org/abstract/document/6815901 [cited 27 Nov 2018]

[12] Gauthier, Ryan, and Seker, Remzi, "Addressing Operator Privacy in Automatic Dependent Surveillance – Broadcast (ADS-B)," Proceedings of the 51st Hawaii International Conference on System Sciences, pp. 5554—5563. 2018 URL: https://scholarspace.manoa.hawaii.edu/bitstream/10125/50582/1/paper0695.pdf [cited 30 April 2018]

[13] Smith, A., Cassell, R., Breen, T., Hulstrom, R., and Evers, C., "Methods to provide system-wide ADS-B back-up, validation and security," in Proceedings of the 25th Digital Avionics Systems Conference (DASC), pp. 1–7, 2006.

[14] Purton, L., Abbass, H., and Alam, S., "Identification of ADS-B system vulnerabilities and threats," in Proceedings of the Australasian Transport Research Forum 2010, Canberra, Australia, pp. 8, 2010. URL: https://atrf.info/papers/2010/2010_Purton_Abbass_Alam.pdf [cited 1 Dec 2018]

[15] Kovell, B., Mellish, B., Newman, T., and Kajopaiye, O., "Comparative analysis of ADS-B verification techniques," M.S. thesis, Univ. Colorado, Boulder, BO, USA, pp. 6 & 7, 2012. URL: https://morse.colorado.edu/~tlen5710/12s/ADSBVerification.pdf [cited 1 Dec 2018]

[16] Sampigethaya, K., and Poovendran, R., "Security and privacy of future aircraft wireless communications with offboard systems," in Proceedings of the Third International Conference on Communication Systems and Networks (COMSNETS 2011), pp. 1–6, Jan. 2011. URL: https://ieeexplore.ieee.org/document/5716527 [cited 1 Dec 2018]

[17] Krozel, J., Andrisani, D., Ayoubi, M., Hoshizaki, T., and Schwalm, C., "Aircraft ADS-B Data Integrity Check", in AIAA 4th Aviation Technology, Integration and Operations (ATIO) Forum, pp. 1–11. 2004. URL: https://arc.aiaa.org/doi/pdf/10.2514/6.2004-6263 [cited 1 Dec 2018]

[18] Liu, W., Wei, J., Liang, M., Cao, Y., and Hwang, I., "Multi-sensor fusion and fault detection using hybrid estimation for air traffic surveillance," IEEE Trans. Aerospace Electronics Systems, vol. 49, no. 4, pp. 2323–2339, Oct. 2013.

[19] Leinmuller, T., Schoch, E., and Kargl, F., "Position verification approaches for vehicular ad-hoc networks", IEEE Wireless Communications, vol. 13, no. 5, pp. 16–21, October 2006.

[20] Zeng, K., Govindan, K., and Mohapatra, P., "Non-Cryptographic Authentication and Identification in Wireless Networks", IEEE Wireless Communications, pp. 1–8, 2010. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5601959 [cited 1 Dec 2018]

[21] Ziliang, F., Weijun, P., and Yang, W., "A Data Authentication Solution Of ADS-B System Based On X.509 Certificate", in 27th International Congress of the Aeronautical Sciences, 2010. URL: http://www.icas.org/ICAS_ARCHIVE/ICAS2010/PAPERS/062.PDF [cited 1 Dec 2018]

[22] "FlightRadar24.com. Live Air Traffic," URL: https://www.flightradar24.com [cited 27 Nov 2018]

[23] Greenberg, A.,"Next-gen air traffic control vulnerable to hackers spoofing planes out of thin air." Forbes, July 25, 2012: URL: http://www.forbes.com/sites/andygreenberg/2012/07/25/next-gen-air-traffic-control-vulnerable-to-hackers-spoofing-planes-out-of-thin-air/ [cited 30 April 2018]

[24] Strohmeier, Martin, Lenders, Vincent, and Martinovic, Ivan, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol." IEEE Communication Surveys & Tutorials, Vol. 17, No. 2, Second Quarter, 2015, URL: http://www.lenders.ch/publications/journals/CST15.pdf [cited 30 April 2018]

[25] Manesh, M., Kaabouch, N., Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," International Journal of Critical Infrastructure Protection, Volume 19, Pages 16-31, December 2017. URL: https://www.sciencedirect.com/science/article/pii/S1874548217300446 [cited 1 Dec 2018]

[26] Magazu, D., "Exploiting the Automatic Dependent Surveillance-Broadcast system via false target injection," Wright-Patterson Air Force Base, Dayton: Air Force Institute of Technology, 2012. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a561697.pdf [cited 1 Dec 2018]

[27] Giannatto, C., and Markowsky, G., "Potential Vulnerabilities of the Next Gen Air Traffic Control System," in World Congress in Computer Science, Computer Engineering and Applied Computing, 2014. URL: https://www.researchgate.net/publication/294457234_Potential_Vulnerabilities_of_the_NextGen_Air_Traffic_Control_System [cited 1 Dec 2018]

[28] Schäfer, Matthias, Lenders, Vincent, and Martinovic, Ivan, "Experimental analysis of attacks on next generation air traffic communication," Proceedings of the 11th international conference on Applied Cryptography and Network Security (ACNS'13), Michael Jacobson, Michael Locasto, Payman Mohassel, and Reihaneh Safavi-Naini (Eds.). Springer-Verlag, Berlin, Heidelberg, 253-271, 2013. URL: http://lenders.ch/publications/conferences/acns13.pdf [cited 30 April 2018]

[29] FAA (AIR-130) Advisory Circular, "Airworthiness Approval of Automatic Dependent Surveillance - Broadcast (ADS-B) Out Systems," AC No: 20-16, 2010 May 10, p.18: URL: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2020-165.pdf [cited 30 April 2018]

[30] United States Government Accountability Office, "HOMELAND DEFENSE Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft," GAO-18-177, January 2018, pp. 23, 24. URL: https://www.gao.gov/assets/690/689478.pdf [cited 30 April 2018]

[31] Ibid., p. 27

[32] National Archives CUI webpage, "CUI Category: DoD Critical Infrastructure Security Information," URL: https://www.archives.gov/cui/registry/category-detail/dod-critical-infrastructure-security-information [cited 30 April 2018]

[33] Department of Defense, DOD Policy Board on Federal Aviation, DOD Comments to Docket No. FAA -2007-29305 Notice No. 07-15, "Automatic Dependent Surveillance – Broadcast (ADS-B) Out Performance Requirements to Support ATC Service,"(Feb. 29, 2008).

[34] Federal Aviation Administration, "Aircraft Situation Display to Industry (ASDI) Block Program FAQ" URL: https://www.fly.faa.gov/ASDI/asdi.html [cited 27 Nov 2018]

[35] Federal Aviation Administration, "FAA Aeronautical Data Exchange [ADX]," URL: https://www.adx.faa.gov/portal/ [cited 27 Nov. 2018]

[36] Cindy Finke, Jonathan Butts, and Robert Mills, "ADS-B Encryption: Confidentiality in the Friendly Skies," CSIIRW '12, Oak Ridge, Tennessee, USA, October 30-November 2, 2012.

[37] Black, J., and Rogaway. P., "Ciphers with arbitrary finite domains," In Preneel, B., editor, Topics in Cryptology, U CT-RSA 2002, volume 2271 of Lecture Notes in Computer Science, pp. 185–203. Springer Berlin / Heidelberg, 2002. 10.1007/3-540-45760-79.

[38] Wesson, Kyle D., Humphreys, Todd E., and Evans, Brian L., "Can Cryptography Secure Next Generation Air Traffic Surveillance?" IEEE Security & Privacy, Vol. X, No. X.014. URL: https://pdfs.semanticscholar.org/94be/9dccbb8708a2ca1444ae8b24afb128026762.pdf [cited 30 April 2018]

[39] Lee, Seoung-Hyeon, Yong-Kyun Kim, Jong Wook Han and Deok-Gyu Lee. “Protection Method for Data Communication between ADS-B Sensor and Next-Generation Air Traffic Control Systems.” Information 5: pp. 622-633, 2014

[40] Ferguson, Niels, and Schneier, Bruce, “Practical Cryptography.” Indianapolis, Wiley Publishing, p. 333, 2003

[41] Androulaki, E., et al.: Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, pp. 30:1–30:15. ACM, New York (2018). URL: https://dl.acm.org/citation.cfm?id=3190538 [cited 10 Nov. 2018]

[42] Bergquist, Jonatan, “Blockchain Technology and Smart Contracts: Privacy-Preserving Tools,” Masters Thesis, Uppsala Universitet, Sweden, 2017, URL: http://www.diva-portal.org/smash/get/diva2:1107612/FULLTEXT01.pdf [cited 30 April 2018]

[43] Seong-il Lee, et al, “A Next-Generation Smart Contract and Decentralized Application Platform,” URL: https://github.com/ethereum/wiki/wiki/White-Paper [cited 30 April 2018]

[44] “ICO Statistics - By Blockchain Platform,” URL: https://icowatchlist.com/statistics/blockchain [cited 30 April 2018]

[45] URL: https://www.hyperledger.org/projects/fabric [cited 30 April 2018]

[46] URL: http://hyperledger-fabric.readthedocs.io/en/release-1.1/ [cited 30 April 2018]

[47] L. M. Bach, B. Mihaljevic, M. Zagar, "Comparative analysis of blockchain consensus algorithms", Information and Communication Technology Electronics and Microelectronics (MIPRO) 2018 41st International Convention on, pp. 1545-1550, 2018.

[48] Merkel, D., “Docker: lightweight linux containers for consistent development and deployment, ”Linux Journal, May 19, 2014 URL: https://www.linuxjournal.com/content/docker-lightweight-linux-containers-consistent-development-and-deployment [cited 10 Nov. 2018]