Global Resilient Aviation Network Concept of Operations

For a secure and trusted exchange of information

Table of Contents

Executive Summary

Aviation is a safety critical business. The air navigation system is becoming more complex due to the continuously growth of air traffic —expected to double within the next fifteen years moving passengers and cargo around the globe— and the emergence of "new entrants" with significantly different operational characteristics and needs. Therefore, to manage this complexity and improve the safety and efficiency of operations which ultimately provide financial or operating benefits, the air navigation system must transform and build upon the use of emerging technologies, information, connectivity and concept of operations, some of them not specifically designed for aviation purposes.

The secure exchange of information on a global basis, enabled by a global resilient aviation network built upon a trust framework, is essential to allow this transformation, as reflected in the Global Air Navigation Plan. This places a premium on aviation's approach to cybersecurity.

This concept of operations highlights the importance of embracing a global approach for the secure and trust exchange of information among the aviation community members and describes the consequences of a do nothing scenario or implementing isolated solutions. As part of this global approach, it proposes a multilayer defense to cyber-attacks and outlines the characteristics of a global resilient aviation network.

To operationalize this resilience, this concept of operations builds upon the capabilities of a public key infrastructure, internet protocol version 6 (IPv6) addressing, a domain name system (DNS) and information security management systems. In this context, the concept of trust is emphasized, and the evolution of the existing Global Trust framework to a new digital environment is described. The digital Global Trust Framework addresses the policies, general specifications and procedures necessary to allow the deployment of a global resilient aviation network that would operate on a global basis and facilitate the exchange of information among all aviation stakeholders to full utilize the resources of the global air navigation system providing cost-effective and safe operations. Finally, it describes the operations of this global resilient aviation network and how the aviation community, as a whole, would benefit from its adoption.

The basic business drivers of this concept of operations are:

- Reduce long-term recurring operating cost through reduction of infrastructure cost and complexity
- Improve deployment timeline of new capabilities by reducing the complexity of integration and operations for interoperability
- Provide standardized methods of validating trust and managing cybersecurity risks that provide a direct business benefit to all stakeholders

The policies, general specifications and procedures described in this document are consistent with other industries best practices, however they are not meant to be a standalone solution; they are meant to provide methods that can be applied across the aviation ecosystem in order to provide an initial step in collectively improving cybersecurity.

These methods are scalable and designed to be implemented in a way that will allow the global aviation community to adopt these changes at a rate that can individually be supported. This allows each aviation community member to develop a unique plan to get to a common end state, at a rate that is achievable globally.

1 Introduction

Cyber threats are a growing global concern. The World Economic Forum 2018 Global Risk Report, which identifies and analyses the most pressing global risks[1], identifies cybersecurity as one of the four key risk areas:

"***Cybersecurity risks*** *are* ***growing****, both in* ***their prevalence and in their disruptive potential****. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails.* ***Another growing trend*** *is the use of* ***cyberattacks to target critical infrastructure and strategic industrial sectors****, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning."*

Cybersecurity risks growing prevalence and disruptive potential

Business interruption (BI) ranks as the most important global risk for the sixth year in a row[2], due to its serious negative impact on revenues. Companies face an increasing number of scenarios – from traditional exposures, such as the physical damage impact of natural catastrophes and fires on facilities and the supply chain to new triggers stemming from digitization and interconnectedness that typically come without physical damage, but high financial loss. Cybersecurity incidents are one the most feared BI trigger as they can also hurt customer perception. BI is also the main cause of economic loss for businesses after a cybersecurity incident. Cyber-rooted BI incidents have been increasing with increased attacks, such as ransomware incidents, but also because of technical failures and employee error.

Cyber incidents continue an upward trajectory to be the second most important business risk today, five years ago it ranked 15th. The number of cybersecurity incidents has been escalating, and like a natural disaster, a cyber attack can potentially impact hundreds of companies. The so-called "cyber hurricane" events, where attackers can disrupt large numbers of companies through common internet infrastructure dependencies, are increasing. Reputational damage is irrevocably linked to cybersecurity incidents if the response to a cybersecurity incident is inadequate; 75% of all companies which suffer a cyber-attack also incur reputational damage or loss. Furthermore, companies can suffer reputational damage without negative media coverage. If sensitive data is compromised, trust can be destroyed among core stakeholders without media involvement.

Transportation among the critical target infrastructure and strategic industrial sectors

Transportation is among this critical infrastructure, as shown in Figure 1 Marsh & McLennan 2018 World Economic Forum Risk Report Top Economic Risk.

[1] A "global risk" is defined as an uncertain event or condition that, if it occurs, can cause significant negative impact for several countries or industries within the next 10 years.
[2] Allianz Risk Barometer – Top risk business for 2018.

	Global Risk	Description
Economic	**Asset bubbles** in a major economy	Unsustainably overpriced assets such as commodities, housing, shares, etc. in a major economy or region
	Deflation in a major economy	Prolonged near-zero inflation or deflation in a major economy or region
	Failure of a major **financial mechanism or institution**	Collapse of a financial institution and/or malfunctioning of a financial system that impacts the global economy
	Failure/shortfall **of critical infrastructure**	Failure to adequately invest in, upgrade and/or secure infrastructure networks (e.g. energy, transportation and communications), leading to pressure or a breakdown with system-wide implications
	Fiscal crises in key economies	Excessive debt burdens that generate sovereign debt crises and/or liquidity crises
	High structural unemployment or underemployment	A sustained high level of unemployment or underutilization of the productive capacity of the employed population
	Illicit trade (e.g. illicit financial flows, tax evasion, human trafficking, organized crime, etc.)	Large-scale activities outside the legal framework such as illicit financial flows, tax evasion, human trafficking, counterfeiting and/or organized crime that undermine social interactions, regional or international collaboration, and global growth
	Severe **energy price shock** (increase or decrease)	Significant energy price increases or decreases that place further economic pressures on highly energy-dependent industries and consumers
	Unmanageable inflation	Unmanageable increases in the general price levels of goods and services in key economies

Figure 1 Marsh & McLennan 2018 World Economic Forum Risk Report Top Economic Risk

While digitization is revolutionizing business models and transforming daily lives, it is also making infrastructure more vulnerable to cyber-attacks, as shown in Figure 2 Marsh & McLennan 2018 World Economic Risk Report Top Technology Risk. The cyber threat is increasing and is expected to continue to do so as the world economy continues to digitize operations, supply chains, and businesses transactions, as well as employee and customer services.

Technological	**Adverse consequences of technological advances**	Intended or unintended adverse consequences of technological advances such as artificial intelligence, geo-engineering and synthetic biology causing human, environmental and economic damage
	Breakdown of critical information infrastructure and networks (**Critical information infrastructure breakdown**)	Cyber dependency that increases vulnerability to outage of critical information infrastructure (e.g. internet, satellites, etc.) and networks, causing widespread disruption
	Large-scale **cyberattacks**	Large-scale cyberattacks or malware causing large economic damages, geopolitical tensions or widespread loss of trust in the internet
	Massive incident of **data fraud/ theft**	Wrongful exploitation of private or official data that takes place on an unprecedented scale

Figure 2 Marsh & McLennan 2018 World Economic Risk Report Top Technology Risk

Industry should, therefore, take a proactive approach and effectively manage and operate the technology used to deliver services. This proactive approach will help mitigate technology risks associated with key aspects of critical infrastructure.

Aviation

Aviation has been operating with enviable safety records however it has also been the target of cyber-attacks, both physical and digital communications infrastructure. These attacks cause enormous losses to the industry and more generally to the world economy. Physical damages have been in the billions and loss of business due to lost consumer confidence surpasses the physical losses. The society has become aware of threats to aviation and threats can be as damaging to business as a successful attack.

2 Understanding the current and future aviation ecosystem

2.1 Activity growth and diversity

Traditional traffic growth

In 2016, airlines worldwide carried approximately 3.8 billion passengers with 7.1 trillion revenue passenger kilometers (RPKs). Fifty-three million tonnes of freight were transported by air, reaching 205 billion freight tonne kilometers (FTKs). Every day, more than 100,000 flights transports over 10 million passengers and around USD 18 billion worth of goods[3]. According to the Air Transport Action Group (ATAG) the total economic impact (direct, indirect, induced and tourism-connected) of the global aviation industry reached USD 2.7 trillion, some 3.5 % of world's gross domestic product (GDP) in 2014[4]. By 2034, both air passenger traffic and air freight traffic are expected to double, compared to 2016. Passenger traffic is expected to reach over 14 trillion RPKs (7 billion passengers annually) with a growth of 4.5 % per annum, and freight will expand by 4.2 % annually over the same time period, to 466 billion FTKs[5], as shown in Figure 3 Total passenger traffic: history and forecast.

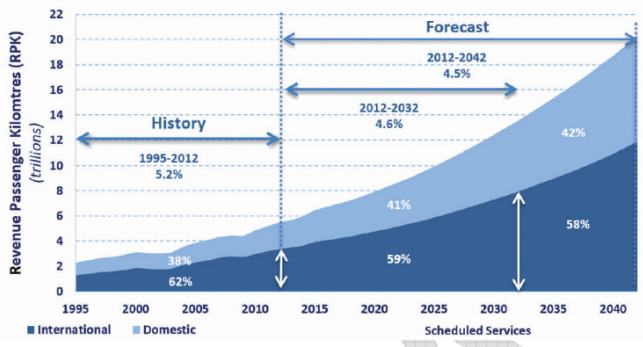

Figure 3 Total passenger traffic: history and forecast

The growth holds tremendous economic potential which will support all States in achieving the United Nations 2013 Agenda for Sustainable Development. In 2034, aviation will provide 99 million jobs and generate USD 5.9 trillion in GDP, a 122 % increase from 2014[6]. The future growth of air transport will likely depend on sustainable world economic and trade growth, as well as declining airline costs and ticket prices. Other factors, including regulatory regimes (such as liberalization of air transport), technological improvements and fuels costs will also impact future growth.

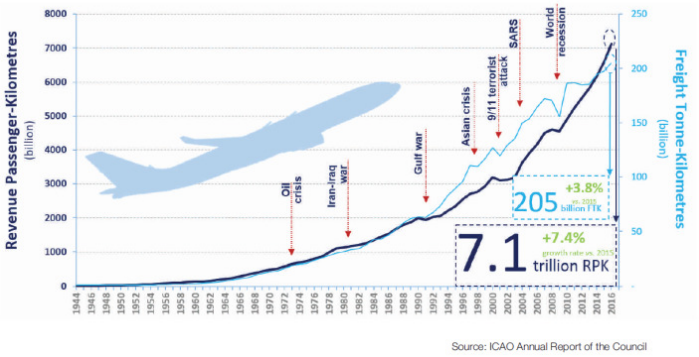

Figure 4 Air traffic growth defies recessionary cycles

Air transport has consistently defied recessionary cycles as it has served as one of the most effective tools for ending them, as shown in Figure 4 Air traffic growth defies recessionary cycles.

[3] ICAO Economic Development
[4] ABBB, 2016, ATAG
[5] ICAO Long Term Traffic Forecasts, 2016
[6] ABBB, 2016, ATAG

New entrants

A new era of aircraft ranging from small unmanned aircraft to autonomous urban air taxis, high altitude balloons, commercial space vehicles or upper atmosphere super and hyper-sonic flight are disrupting the air navigation system. These "new entrants", with significantly different operational characteristics and needs, are being used in increasing numbers to provide new services to society. Forecasts for Europe place the number of Unmanned Aircraft Systems (UAS) in commercial and government operation at 400,000 with a value of EUR 15 billion annually by 2050[7]. A forecast by the Federal Aviation Administration reported 110,000 UAS by the end of 2017 and forecast to exceed 400,000 commercial UAS by 2022[8]. These new entrants are leading indicators to what is coming for traditional manned aviation.

New entrants are different from traditional manned aircraft as they may not use the traditional aviation communications. Some of these new entrants will remain apart from the traditional ATM system, such as the smallest entrants, which do not require controller-pilot communications. In this case, all interaction between ATM and the new entrants is network-based information exchange. Additionally, these new entrants may use existing cellular networks to manage their flight operations and to share information among themselves to support their cooperative conflict avoidance. For those new entrants remaining within the ATM system, voice communications from pilot to controller may still be required, however, traditional air-ground radios may be replaced by voice over ground networks. In this case, all other interaction between the ATM system and the new entrants is network-based information exchange. New entrants such as space vehicle and long duration flying vehicles, operating in higher airspace, will also rely heavily on network information exchange.

Network information exchange becomes fundamental to safe and efficient operations within the new air navigation environment.

2.2 Transformational evolution: information exchange

The aviation ecosystem is becoming more complex as it supports the new demand. To manage this complexity and improve the safety and efficiency of operations which ultimately provide financial or operating benefits, the aviation system must adopt new concept of operations supported by better means for information exchange and emerging technologies, some of them not specifically designed for aviation purposes. It also requires a more integrated and dynamic operating environment between all aviation stakeholders.

In particular, as reflected in the Global Air Navigation Plan (GANP), the new entrants are introducing a next-generation of operating models by applying advanced technologies and sophisticated operational decision-making processes in an integrated manner. This will expand the traditional business models and accelerate the transition towards a digital information rich environment. This environment will burst an information revolution where flights, with known positions at all time, will be managed by (4D) trajectories. The information revolution will lead to a time where shared information will be accessible worldwide in a timely and accurate manner and full connectivity will be achieved in aviation by embracing the internet of things. This worldwide environment with a common

[7] SESAR European Drones Outlook Study 2016
[8] FAA Aerospace Forecasts FY 2018-2038

view of a single information (single universal aviation world of information), will then enable airspace users to make orchestrated and/or choreographed decisions in a total performance managed system.

This evolution will be enabled by a progressive increase in automation, advancements in technology and the use of standardized interoperable ground and air systems in an integrated infrastructure. This aviation infrastructure, based on the ubiquitous sharing of information, will interface with non-aviation transport systems to achieve an efficient, multi-modal transport system.

As reflected in the previous paragraphs, the evolution of the air navigation system strongly relies on information sharing and full connectivity which cannot be realized without a global aviation resilient operating network that connects all aviation stakeholders facilitating the secure and trusted exchange of digital information worldwide.

2.2.1 Current information exchange environment

Information is currently exchanged in the aviation ecosystem using multiple, unique and independent networks, specifically connected through dedicated air-ground and ground-ground communications, each within its own operating environment and, each using their unique methods and standards.

These independent networks, managed by different stakeholders (ANSP's, airline operators, manufacturers, and ground handling), only interface and interact on an as needed basis and require multiple unique connections between stakeholders for global providers.

Ground-ground communications

Until recently, the ground-ground networks were based on regional point-to-point dedicated transmission lines using dedicated connection oriented message exchange methods.

The communication service providers are replacing dedicated transmission lines with shared IP based network services infrastructure. As a result, the current ground-to-ground networks are evolving to regional IP based networks. In order to secure the communication, the operators of these regional networks are recreating the point-to-point connectivity using virtual private networks. Therefore, although these regional IP networks should increase the ability for users to exchange information, they are limited through the security design to point-to-point connections.

Air-ground communications

There are three distinct separate data domains within the aircraft, as shown in Figure 5 Aircraft data domains.

The equipment and controls used to safely operate and control the aircraft are located within the Aircraft Control Domain (ACD). It is for this reason that, air-air and air-ground interoperability is required within this domain among the different CSPs and ANSPs operating under the same area of responsibility and that is why this concept of operations focuses on the services that are unique and distinct to it.

Interoperability may also be required for some services and functions within the Airline Information Services Domain (AISD) such as electronic flight bags (EFB) and other applications.

The passenger information and entertainment domain provide a revenue stream to the airlines. This aircraft domain is not considered to be trusted. Explicit management and operations must be maintained to ensure that this domain does not compromise the safety environment.

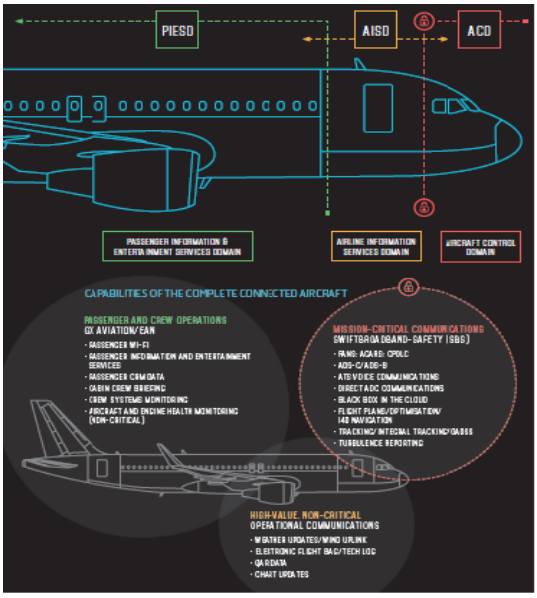

Figure 5 Aircraft data domains

Legacy exchange of information and technologies have been effective to achieve the aviation safety standards of the past. However, they have also impacted the aviation ecosystem in multiple ways, including:

- Complexity of operating environment and systems.
- Long time for integration and deployment of new capabilities.
- High complexity of integration between multiple stakeholders' systems.
- Widely varying complexity and cost for communications infrastructure.

In order to increase the efficiency of operations and meet the new needs that have been rising as a consequence of modernization in the aviation ecosystem, it's time for making investments in and incorporating new technologies for more capabilities that increase operational performance.

2.2.2 Future information exchange environment

A fully robust information-sharing environment is necessary, in support of the increasing traffic as well as the increasing number of entrants and their increasingly varied business interests.

The multiple, unique and independent networks, managed by the different stakeholders, need to be connected and operated as a global aviation single network where all aviation members can easily exchange information regardless of the information's origin or destination. This will require a single operating environment with common standards and procedures.

Converged communications

The need for specific dedicated air-ground or ground-ground communications is not required anymore, giving way to communication performance specifications in support of different operational functionalities. The achievement of a more integrated operating environment that far exceeds the way the aviation system is connected today, see Figure 6 The interconnectedness evolution of the system, depends on the ability of the aviation ecosystem to evolve to the use of commercially offered networks and techniques, creating a full intranet of aviation operating very much like the public Internet.

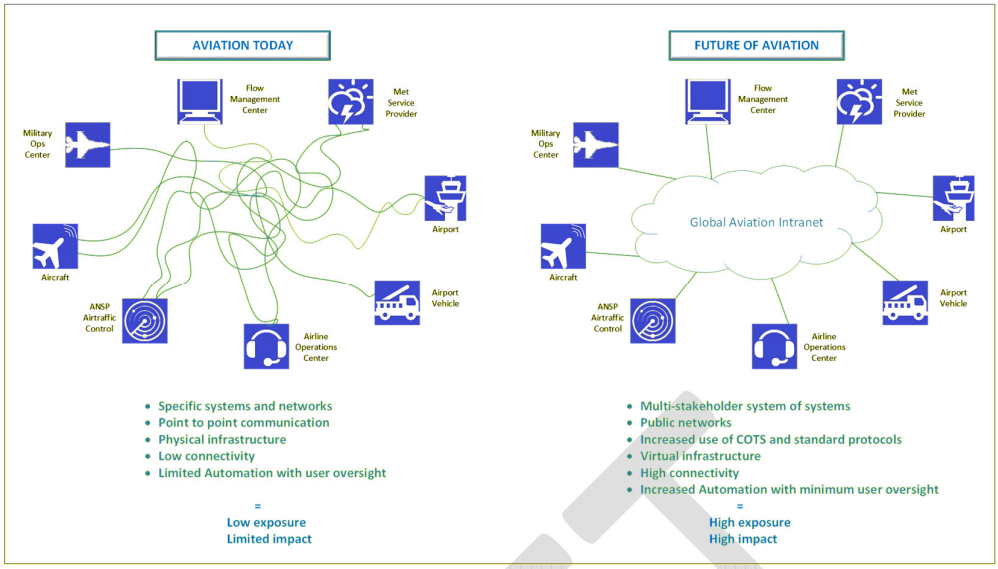

Figure 6 The interconnectedness evolution of the system

The global aviation intranet will consist of new commercial network services, either replacing or coupling aviation's existing multiple independent networks to converge to one performance-based network. The global aviation intranet will use the same commercially available infrastructure as the public internet: Internet Protocol (IP), IPv6 addressing and Domain Name System (DNS). The commercial network providers will use the same core network infrastructure as the public internet but will leverage the aviation specific IPv6 addressing and security to logically segregate the aviation intranet communication from the public internet.

The global aviation intranet provides the ability for any application (see section 4.1.1.3) to communicate with any other application regardless to which organization or State the application belongs and whether the applications are airborne or on the ground. Since there are varying performance requirements across: safety critical applications, Remotely Piloted Aircraft System (RPAS) applications, unmanned aircraft system (UAS) applications, Airline Operation system applications, maintenance applications; the network service providers can configure its services to support different communication performance requirements such as availability, bandwidth, latency, guaranteed delivery, resilience and security.

3 The need for a global resilient aviation network

In the past, because of the technology and lack of integration among the independent dedicated networks used by different stakeholders to exchange information (see section 2.2.1), cyber threats did not require the level of diligence that they do nowadays with the necessary adoption and implementation of new technologies and network integration (see section 2.2.2) to enable the evolution of the aviation ecosystem.

3.1 Lack of security by design in the exchange of information

The current aviation systems were designed during a period of time when the overall security of interconnecting information exchange systems did not introduce high enough risks to cause serious

concern. As a result, the existing communication systems were designed with a "safety-first" approach so that they were highly resistant to operational failure. The shift to digital data communications, based on these safe but open and unprotected communication channels, has created an increased surface for cyber-attacks. This has been compounded by the increase easiness to perform an attack. In the past information was exchanged using aviation specific technology and protocols, attacking this information required insider knowledge and specialized hardware and software. Today with the migration to digital data communication, inexpensive tools, software and public knowledge are available for attacks.

3.2 Lack of resiliency and new vulnerabilities

Multiple stakeholders are often required to exchange information inside and outside the aviation system. This leads to an aviation ecosystem, where many networks are connected to form a single global aviation operating network for the exchange of information. The multiple required interconnections among the aviation stakeholders for the exchange of information makes managing risk very complex.

Historically, the aviation ecosystem relied upon legacy technology with embedded limitations to broad and dynamic integration. In this non-integrated environment, each stakeholder in the aviation ecosystem established unique policies and technical standards for implementing trusted and secured voice and data communications, creating isolated and unique trusted information exchange environments. Today, however, both, air-ground and ground-ground operating environments, are converging to utilize the IP protocol. Owing to the standardization of technology, functionally the same type of software and hardware is used across all Internet Protocol based networks including the Internet, data centers and suppliers. This type of software and hardware is also used in the aviation systems. Therefore, the existing threats for the Internet are now applicable to the aviation ecosystem.

The increasing interconnectivity within a more integrated aviation ecosystem, enabled by a shared core network infrastructure with the Internet, opens up new vulnerabilities that need to be addressed. The direct consequence is that a breach in one of the components of the aviation ecosystem can easily spread an attack across the entire ecosystem, and put aircraft safety and the efficiency of flight operations at risk.

In this regard, the aviation community needs to include methods and techniques of cybersecurity risk reduction for safe and efficient flight operations. These risks include but are not limited to:

- Loss of communication system between aircrafts and air traffic controllers
- Injection of rogue commands by impersonation of ATC
- Luring pilots with forged flight plans
- Modification of flight recording data which impair the maintenance process
- Corruption of data loading system to penetrate avionics computer
- Disrupt activity in airports
- Disorganize the air traffic control by attacking the integrity of the supporting infrastructure
- Disruption or attacks on the aircraft cabin network that cause loss of confidence in airworthiness
- The safety risk associated with the described vulnerabilities increases with the introduction of more automation, combined with a reduction of human oversight and ultimately autonomous or remote aircraft command and control.

3.3 Non-Interoperability and cost

Today the aviation ecosystem has a very decentralized operating environment by evolution and localized design, based on technology and standards that are decades old. Over time, all stakeholders have bolted on improvements both in the use of technology and capabilities.

The changes were made by each individual stakeholder, based on individual needs and capabilities, resulting in a global operating environment with a mixed use of local and/or regionally implemented technology and capabilities. This creates both interoperability risks and vulnerabilities to all stakeholders with added cost that affect the efficiencies of the system.

Introducing information exchange security as an afterthought to this decentralized operating environment will cause the users to bear the cost of implementing multiple incompatible security solutions. For example, an international airline will have to comply with as many security implementation as the number of regions or even States it flies to. Also any aviation stakeholder will bear the cost to manage and own as many digital or other identities as the number of systems they need to communicate to. Example: compare this to the number of user names and passwords every individual has to manage to interact with individual websites on the internet versus having one identity. The use of a single identity requires multilateral trust between the issuer of the identity, the user of the identity and the relying system accepting the identity. The current decentralized approach is not conducive to establishing this trust on a global scale.

3.4 Non-holistic approach

No single State, organization or region can solve the problem of cybersecurity by itself. Both from a regulatory and from an organizational point of view, there is no coherent global approach for containing cyber threats. Each region has their own cybersecurity standards, ranging from non-existing standards, ad-hoc standards to competing standards such as National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). No approach exists to exchange cybersecurity compliance information to help establishing trust. Since no standard approach is in place it is clear that the technical implementation for secured information exchange is either lacking or incompatible across organizations and aviation stakeholders.

3.5 Impact

The aviation community has identified many operational improvements to increase the safety and efficiency of flight operations as reflected in the Aviation System Block Upgrade (ASBU) framework as part of the Global Air Navigation Plan. However, most of these operational improvements depend on the secure exchange of information worldwide enabled by a global resilient aviation network. Therefore, the desired levels of safety, efficiency and interoperability can only be accomplished through the global adoption of a new solution —supported by existing technology, industry standards, and global policies— to overcome the challenges above and secure the exchange of information worldwide.

4 Global resilient aviation network operational concept

This chapter describes a global solution for the secure exchange of information within a global resilient aviation network. In this regard, it starts describing the approach, followed by the objective, the supporting capabilities and the operations.

4.1 Architecture

This concept of operations is designed to minimize cyber security risks. To do this, it assumes a layered defence in depth where network, system, and applications have their own individual cybersecurity protections in place.

4.1.1.1 Network

The aviation ecosystem will formed by a number of interconnected networks operating as a single global network as illustrated in Figure 7 The poodle: cyber resilience perspective of an aviation network. Furthermore, within the aviation ecosystem, systems will be connected to the network using applications to exchange messages over IP due to the minimal bandwidth and processing overhead associated with this communication design. In this environment, the performance of the message exchange will rely on the specifications of the IP network service used.

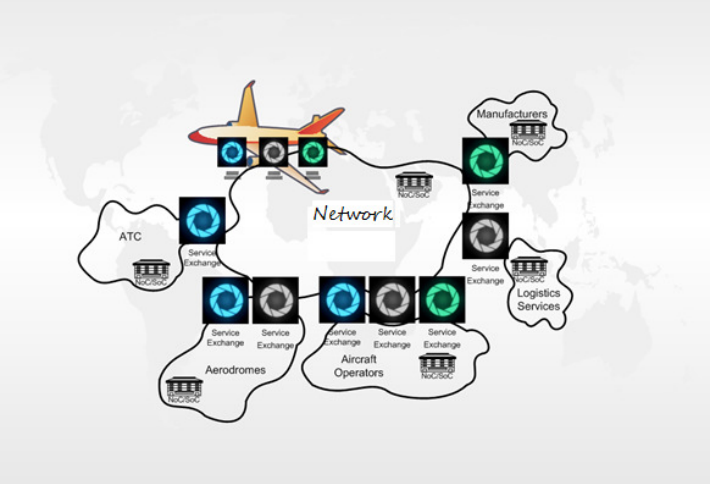

Figure 7 The poodle: cyber resilience perspective of an aviation network

Between networks, the messages will pass through a Service Exchange environment that will consist of multiple cybersecurity controls and processes. While implementation of specific cybersecurity controls and processes may vary at each Service Exchange, based on local impact threat analysis, the full set of cybersecurity controls and processes will be available at every instance to ensure rapid response to changing threats.

At the most basic level, a simple white-list access control firewall will preclude outsiders from affecting the more processing intensive controls. One of the additional processes in each Service Exchange will be a policy enforcement point to do a sanity check of the messages before they are routed via the network to their destination. At the destination network boundary, another policy enforcement point on the receiving side will verify the messages. Policy enforcement points will provide the same integrity checking of the message as applications do but will be able to do additional verification and correlation of all the messages from one source and identity in relation to message context specific attributes such as message frequency, destination, time of day, geospatial location of the sender, etc... Policy enforcement points will also allow rapid deployment of message access and flow control rules, protecting applications, systems and network against new cyber threats.

4.1.1.2 Systems

Systems will be configured to limit access only to pre-defined network ports. Network ports will be associated with, and identify specific applications. In this way, systems will only expose specific applications to the network, thus an attacker will have increased difficulty in attacking the application host system as it will not have direct access to the operating system. Remote access to the operating system via the network will be disabled or will be performed through secured, privileged, and authenticated access only, eliminating potential cyber-attacks through malware or other sources.

4.1.1.3 Applications

Applications will run on systems and communicate with each other. Before two applications initiate a communication session, they must perform mutual authentication, using a digital identity, to ensure they have not been redirected to a rogue application hosted by an intruder.

Applications will communicate through message exchange. These messages will follow a pattern whose header will define the message type, its length, its data type, and its integrity signature. These message integrity signatures will be created by the emitting applications, using their digital identities, to ensure that messages are not modified or replayed by an intruder. If confidentiality is required, the emitting applications will also be able to use their digital identity to encrypt the messages. The message header will allow the receiving application to check the authenticity and integrity of the message and prevent it from processing corrupted or spoofed messages. In this regard, if the message header is incorrect or the message integrity signature does not match its content, the message will be dropped.

Some applications will use standard commercial of the shelf message exchange protocols, such as Java Message Service (JMS) and Advanced Message Queuing Protocol (AMQP), which do not support a message integrity signature. In those cases, the applications will be configured to establish a session level virtual private network (VPN) using the transport layer security (TLS): the integrity signature will be added to the transport layer and will be verified by the transport layer. If a message is modified in transit or spoofed by an intruder, the transport layer will discard the message. The integrity verification will be transparent to the application.

4.2 Resilience

Cyber resilience consists of six components: identification, protection, detection, mitigation, recovery, and compliance. These six components are described below in the context and scope of this concept of operations.

4.2.1 Identification

All stakeholders connected to the global aviation operating network, will identify the resources that support critical functions (e.g.: critical functions for the safety of flight operations) and their related cyber vulnerabilities and associated risks.

To do so, each stakeholder will manage the configuration and version information of the assets used to provide critical resources, to then use this asset's information to correlate cyber threats against vulnerabilities and determine the associated risks. This will be especially important for Certificate authority (CA) managing digital identities, network service providers (domain name system operators

and communications service providers) and application providers due to their critical role in the aviation ecosystem.

Information sharing, between all aviation stakeholders, of identified cyber vulnerabilities and associated risks will be essential to strengthen the cyber resilience of the global aviation operating network.

4.2.2 Protection

Protection is the ability to prevent potential cyber events as well as to limit or contain their impact. Some of the protection methods are authentication/access control, data security, information protection processes and procedures, maintenance, and protective technology.

4.2.2.1 Authentication/Access Control

Access control will be implemented at multiple communication levels (application, system and network) by all the key stakeholders. And, although the type of access control technologies and policies will not be the same, these access controls will comply with minimum performance requirements based on industry best practices.

Two communication parties will perform mutual authentication based on the exchange of their globally trusted and interoperable digital identities (see section 4.3.2.3). The receiving party will verify the authenticity of the emitting party to determine whether or at what level it is allowed access. If communication parties use non-trusted or non-interoperable digital identities, each party will have to maintain as many identities as it needs to communicate globally with as many other parties as required. In addition, the maintenance of this vast amount of digital identities will become a complex task leading to shortcuts and vulnerabilities.

4.2.2.2 Data Security

Data security protects the information exchanged between the communication parties from unauthorized modification (integrity) or if needed from unauthorized data inspection (confidentiality). Once communication parties perform mutual authentication with their digital identities, each of them will use their digital identity to sign or encrypt as needed the data.

4.2.2.3 Information Protection Processes and Procedures

Each aviation stakeholder will define information protection processes and procedures that document the data security controls and procedures used to protect the critical aviation services. These processes and procedures will follow global recommended practices or procedures.

4.2.2.4 Maintenance

In order to protect the aviation network from cyber threats, each aviation stakeholder participating in the aviation network will update the applications, software, firmware, hardware, and security configurations based on identified cyber vulnerabilities and the state of their assets determined in section 4.2.1.

4.2.2.5 Protective Technology

Each aviation stakeholder will implement protective technology such as policy enforcement points, firewalls, intrusion protection systems, network flow control etc. as needed, based on their network architecture and the cyber risk assessment performed for critical aviation services (see section 4.2.1).

4.2.3 Detection

Detection capabilities enable the timely discovery of cybersecurity events. In order to detect intrusion, each aviation stakeholder will have a role in detecting and reporting security events so that a central correlation of security events can isolate and detect security anomalies.

The Certificate Authorities (CAs) will detect anomalous identity discovery and validation requests. The Bridge Certificate Authorities (BCAs) will detect anomalous certificate policy mapping requests, and anomalous cross certificate validation requests, based on origin, destination frequency, policy, time of day etc. The applications will detect anomalous authentication, access requests and message integrity events. The air-ground and ground-ground network service providers will detect anomalous network flow attempts, denial of service attempts, intrusion attempts, etc. Only through correlation of all these different events, the full scope of an actual cyber-attack will be detected.

4.2.4 Mitigation or Response

Mitigation or response is the ability to contain the impact of a potential cybersecurity event. In this regard, each aviation stakeholder will document the appropriate activities needed to detect cybersecurity event. This documentation will include technical processes to isolate, analyze, and block cybersecurity attacks, communication processes, and mitigation processes.

A CA may revoke one or more identities based of their involvement in a cybersecurity incident. The Bridge Certificate Authority may revoke the cross certification of all identities of a CA when it detects or is notified that the CA has been compromised. A bridge certificate authority may limit the certificate policy mapping for certificates from a policy domain based on the domain's trustworthiness. An air-ground or ground-ground network service provider may block or redirect a specific network flow originating from a suspicious source to protect the aviation network against a Distributed Denial of Service (DDoS) or impersonation attacks.

4.2.5 Recovery

Recovery relates to restoring any capabilities or services that were impaired due to a cyber-event. In this regard, each aviation stakeholder will document appropriate recovery activities, a lessons-learned process for continuous improvement and a recovery communication plan for users and other stakeholders.

4.3 Enablers for a resilient network

Information security management systems, a public key infrastructure, iPv6 addressing and Domain Name System are enablers for a resilient network.

4.3.1 Information Security Management System

The global resilient operating network infrastructure will be designed natively with cybersecurity protection, which requires proper operation in order to maintain the protection over the time. As part

of the security operations, cybersecurity-related processes will be put in place and a timely re-assessment of risks will be conducted. This is part of an Information Security Management System (ISMS), for which a set of standard do exist (i.e. ISO 27001-27005), and will be deployed across the aviation system (see section 4.4.1).

As part of the ISMS, monitoring cybersecurity related events will be necessary to control the information exchange status of the aviation system as well as the possible cyber-attacks. Monitoring will also allow discovering vulnerabilities that might give way to attacks. Those vulnerabilities will be shared among all stakeholders connected to the global resilient operating network, to leverage lessons learned and to allow for decreasing the number of "weakest links" in the infrastructure.

4.3.2 Public Key Infrastructure

A public key infrastructure (PKI) is a set of rules, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of digital information. It is required for activities where simple passwords are an inadequate authentication method and another more rigorous method is required to confirm the identity of the parties involved in the communication and validate the information being transferred.

In cryptography, a PKI is an arrangement that binds public keys with respective identities of entities (like people and organizations). The binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA). Depending on the assurance level of the binding, this may be carried out by an automated process or under human supervision.

The PKI role that assures valid and correct registration is called a registration authority (RA). A RA is responsible for accepting requests for digital certificates and authenticating the identity of the entity making the request.

An entity must be uniquely identifiable within each CA domain based on information about that entity.

A PKI is also a system for the creation, storage, and distribution of digital certificates that are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository and revokes them if needed.

A PKI consists of:

- A certificate authority (CA) that stores, issues and signs the digital certificates
- A registration authority (RA) which verifies the identity of entities requesting their digital certificates to be stored at the CA
- A central directory—i.e., a secure location in which to store and index keys
- A certificate management system managing for instance the access to stored certificates or the delivery of the certificates to be issued.
- A certificate policy stating the PKI's requirements concerning its procedures. Its purpose is to allow outsiders to analyze the PKI's trustworthiness.

4.3.2.1 Certificate Authority

The primary role of the Certificate Authority (CA) is to digitally sign and publish the public key bound to a given entity. This is done using the CA's own private key, so that trust in the entities' key relies on one's trust in the validity of the CA's key. The key-to-entity binding is established, depending on the level of assurance the binding has, by software or under human supervision. Secondary roles are the regular publication of a revocation list containing the keys no longer valid and hosting an Online Certificate Status Protocol (OCSP) responder. The OCSP responder is used by relying parties for obtaining the revocation status of a public key. CA's can delegate the signing and publishing of public keys to sub-CA's, in which case the main CA is called the root CA. The root CA, signs and publishes the sub-CA's key.

4.3.2.2 Bridge Certificate Authority

In order to create an aviation PKI there are three main architectural approaches:

1. A single root Certificate Authority (CA) with a sub-CA's for each state, region or organization.
2. A root CA per State, region or organization with individual bi-lateral agreements for cross certification between each root CA.
3. A Bridge Certificate Authority (BCA) with member root or BCA's per State, region or organization. The BCA provides bi-directional cross certification between each root CA and itself.

The single root CA requires existing Aviation root CA's to become sub-CA's and to modify and re-configure every system using the PKI to adopt the new PKI hierarchy. Also it put the liability of the PKI in the hands of one root CA.

The second option, a root CA per State, region or organization requires the establishment and maintenance of N * (N-1) / 2 number of bi-lateral agreements between the root CA's. N is the total number of root CA's in the PKI. Also the validation of the public keys requires the discovery and validation of N*(N-1)/2 number of path's which is time consuming and error prone.

The third option, a BCA is the most scalable approach to unify existing aviation PKI's with future PKI's. Each root CA continues to sign and publish its own keys and manage its own liabilities. Although the validation of the keys is still complex, there is only one deterministic path to validate.

A BCA is a third party service provider that brings communities together to establish and agree to common standards, processes and governance for a trusted identity (see section 4.4). Governance includes a model and structure for validation, auditing, sharing, and allocating liabilities. A BCA enables the recognition of CA credentials issued by many different organizations. A BCA is the infrastructure element that links together these organizations. It is vital for a relying party to be able to verify the validity of a presented credential and a BCA enables the validation through cross certification.

A BCA needs a trust framework that establishes cybersecurity specific standards, policies and enforceable governance with a focus on a globally interconnected community and the use of a common operating environment.

4.3.2.3 Digital Certificate/Identity

In cryptography, a digital certificate or digital identity, also known as a public key certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner, and the digital signature of an entity that has verified the certificate's contents. If the signature is valid, and the software examining the certificate trusts the entity that has verified the certificate's contents, then it can use that key to communicate securely with the certificate's owner.

For future airspace management, a digital identity can be used identifying all airspace users and equipment from airports to aircraft. For continued safety of flight, this invariant digital identity will uniquely identify not only the aircraft itself, but also many of its major components. Just as an aircraft can be simultaneously known as its flight number for flight operations and its tail number for fleet management or maintenance purposes, the vast array of objects related to management of the airspace may have an alias that is specific to the context of the interacting parties. Having a common digital identity will enable electronic tracking of aircraft as they move between operators, as well as components like engines as they move between aircraft, in a manner similar to traditional processes using mechanically affixed serial numbers. This digital identity of each entity will be unique, persistent, and invariant.

4.3.3 Internet Protocol version 6 (IPv6) Addressing

An Internet Protocol address is a logical numeric identifier that serves the purpose of identifying an individual network interface of a communication party, locating it on the global network, and thus permitting the routing of IP messages between communication parties. For routing, IP addresses are present in fields of the message header where they indicate origin and destination of the message. IP addresses are roughly similar in concept to postal addresses where messages that are intended to be delivered to a specific location need a destination (the address) and a method of getting to that address (known as “routing” in IP-based networks).

The IP address standard in current wide-use is IPv4. A new standard known as IPv6 is now available and resolves a number of issues that makes IPv4 unsuitable for a global aviation communications system. The number of available addresses is far larger (64 bit address space vs. 32 bit addresses in IPv4) allowing each device to have a unique address that only it possesses, allowing multicasting operations where one transmission can be sent to multiple destinations at once (IPv4 is point-to-point only), including native support for built-in security standards missing in IPv4, and simplifying the routing process described above.

The two versions are not directly compatible with each other. Both types of addresses can exist on the same network, however an IPv4 address can only access another IPv4 address, and the same for IPv6. Therefore, a transition to an IPv6 addressing schema is necessary to support a common operating environment for the aviation community.

4.3.4 Domain Name System (DNS) and Generic Top-Level Domain (gTLD)

As the aviation community leverages the use of the Internet Protocol (IP), some of the same common underlying services that are used with IP networking today need to be adopted.

One of those required underlying services is the Domain Name System (DNS). The DNS is the directory service that provides a conversion between a human readable address and the technical, hard to memorize address. In this regard, the DNS enables access to Internet resources by domain names instead of IP addresses, by translating domain names to numeric IP addresses and back. The DNS infrastructure consists of computing and communication entities called Name Servers each of which contains information about a small portion of the domain name space. The domain name data provided by DNS is intended to be available to any computer located anywhere on the Internet. The primary security goals for DNS are data integrity and source authentication, which are needed to ensure the authenticity of domain name information and maintain the integrity of domain name information in transit.

This service is essential but also vulnerable to some attacks that allow an attacker to hijack traffic to rogue systems or servers in order to inject forged, modified information.

The protection of DNS is then critical to protect the network service by combining the following two techniques:

- Use of intrinsically protected DNS service called Domain Name System Security Extensions (DNSSEC). The DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications for securing information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. This service is also relying upon a PKI service.
- Use of private DNS service which is not accessible from outside the aviation ecosystem, i.e. the networks on Internet.

Another underlying service required is a generic Top-Level Domain (gTLD). A generic Top-Level domain is a top-level domain (TLD) maintained by the Internet Assigned Numbers Authority (IANA) for use in the Domain Name System of the Internet. A top-level domain is the last level of every fully qualified domain name.

4.4 Trust framework

Aviation is a global business built upon the concept of trustable exchange of information. This concept of trust encompasses two fundamental notions: the identity of the communication parties and the integrity of the message involved in the exchange of information.

The aviation ecosystem is under a digital transformation, which holds great promise, but also new challenges. In order to keep the trustable exchange of information in a digital environment, the Global Trust framework, aviation is built upon nowadays, should evolve.

The principles of this global trust framework include:

- Interoperability between all stakeholders is assured through a common trust framework and architecture for seamless and efficient messaging services on a global scale.
- Resiliency of the communications is maximized by utilizing design concepts that limit the threat surface. This includes compartmentalization of the network and the applications, as well as layering of protections in the infrastructure and limiting the number of systems participating.
- Strong identification, authentication, authorization, integrity, and confidentiality

Establishing trusted communications links between the aviation stakeholders and being able to trust the exchanged information are fundamental to the evolution of the aviation system and to manage the complexity of the future demand while keeping the defined levels of safety.

The global trust framework in a digital environment relies upon cryptography to establish a technical trust between parties or stakeholders of the aviation community. This global trust framework is necessary for the enablers presented in the previous section to establish a resilient network.

4.4.1 Network cyber hygiene

In order to establish complete trust between applications and between networks operated by different States and international organizations, the parties must trust the cyber hygiene of the interconnected networks.

Cyber hygiene is defined as implementing and abiding by an agreed cybersecurity policy as documented in the ISO/IEC 27000 family - Information security management systems (ISMS). ISMS is a systematic approach to managing information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Networks and organizations operating them (operators) must be ISO 27000 certified to demonstrate their compliance to the cybersecurity policy. ISO Accredited certification bodies perform regular audits of the network and operator organization and provide the ISO 27000 certification. The certification report is reviewed and approved by ICAO and is made available to all network operators.

4.4.2 Trusted digital identity

Figure 8 shows the necessary administrative documents, legal agreements, operational functions and organizations involved to ensure that all members of the aviation community (e.g. States, airspace users, ANSP's etc.) trust each other's digital identities.

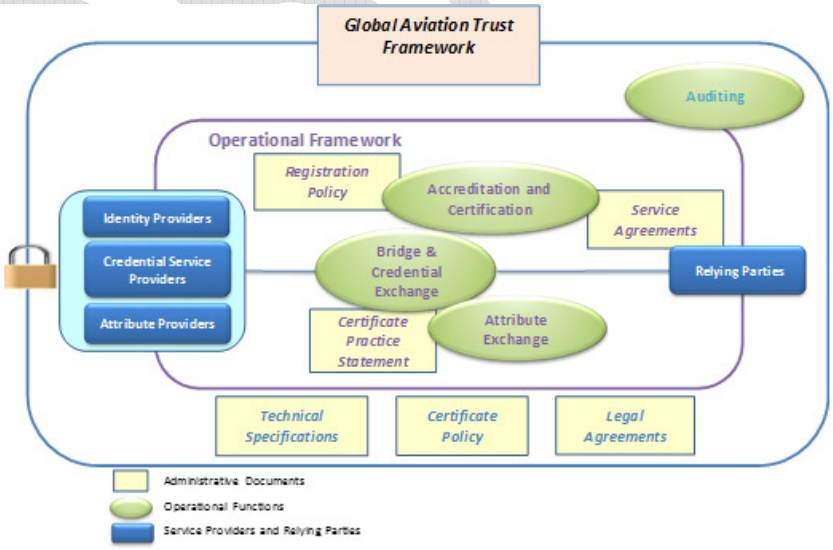

Figure 8 Framework for a trusted identity

4.4.2.1.1 Organizations

Identity providers in Figure 8 Framework for a trusted identity are the Registration Authorities that have the delegated authority from the States to collect and verify the necessary information for the creation of a digital identity.

Credential service providers are the Certificate Authorities that manage and issue the digital identities in the form of a public and private key certificate based on the information received from the Identity providers.

Attribute providers are organizations that can provide supplemental identity attributes used to increase the trustworthiness of an identity. The identity provider can perform this trustworthiness verification using the attribute provider before issuing an identity or the credential service provider can validate the trustworthiness in real time.

The relying parties are the applications using the digital identities for mutual authentication and digital integrity signature generation.

4.4.2.1.2 Governance

The governance of the framework presented in Figure 8 consists of the following set of agreed documents managed and applied by the governing body of the framework:

- Legal Agreements specify the liability and risk (legal, commercial and operational) assigned and agreed between the members.
- Certificate Policy defines the procedural and operational requirements that the trust framework requires organizations to adhere to when registering, issuing, managing, verifying, validating and using identities
- Technical Specifications specify the tools, interfaces and standards used to operate the framework for a trusted identity.

The governing body of this framework performs an auditing role based on an auditing policy documented in the certificate policy. The auditing function monitors, reviews and reports on conformance with the certificate policy, legal agreements and technical specifications.

4.4.2.1.3 Operational

The operational part of this framework consists of a set of administrative documents and operational functions.

Administrative documents:

- The registration policy documents the processes and requirements used by the identity providers to verify the physical identity of entities in order to register the necessary attributes for a digital identity.
- The Certificate Practice Statement documents the processes and requirements that a specific credential provider uses to issue, manage and validate digital identities.
- The service agreements document the functional and performance requirements for the services and technical interfaces from the service providers.

Operational Functions:

- Accreditation and Certification is the process of evaluating, describing, testing, and validating digital identities.
- Bridge and Credential Exchange is the function used to establish trust between digital identities issued by different credential service providers by creating an affiliated relationship through cross certification at a level of assurance asserted by those credentials.
- Attribute Exchange performs a real time exchange of identity attributes between identity, attribute and credential service providers.

4.4.3 Private IPv6 address block

The issuance and maintenance of a trusted identity is extremely important, but alone not sufficient to ensure interoperability, safety, and resiliency. IP address control is a proven method to help minimize cyber exposure across public infrastructure, consistent with other industries and governments best practices. This is also an effective means of dealing with integration issues across the aviation community for both public and private networks.

Acquiring an address range that is globally unique for aviation, allows public Internet Service Providers to provide an additional layer of isolation by rejecting direct routes to that block as they do for other documented private use blocks. When an IP address is private it cannot be routed on the Internet. This avoids traffic being directly accessible on public networks, thus reducing the possibilities of an attacker to access the IP traffic.

There are many advantages to the use of a private IPv6 address block for the aviation community:

- Allows for connectivity and communications across the private and public infrastructure
- Allows organizations to utilize provided IP address for internal operations
- Allows organizations to utilize their own registered IPv6 addressing for both public and private use across the aviation infrastructure
- Standardizes methods to limit risk to IP infrastructure by limiting the range of IP addresses
- Allows for future connectivity following the future communications infrastructure
- Simplifies protection of network assets through whitelisting of aviation IP addresses or domain

A transition to IPv6 does present some challenges for the aviation community, including:

- Cost associated with transition to include configuration, testing, equipment
- The migration of some legacy systems may present some difficulties.

4.4.4 A generic top level domain (gTLD) and a private Domain Name System (DNS)

Leveraging lessons learned from other global industries, having a generic top level domain for aviation creates another layer of protection to limit the exposure of the aviation community on public and private networks. This requires the establishment of both governance processes and technical standards.

Furthermore, in today's aviation operating environment, DNS has not been a broadly needed capability because everyone is connected in very isolated environments. As the aviation community becomes more interconnected, running uncoordinated DNS services across the aviation system

becomes a highly inefficient method of operating and brings an unnecessary burden to all stakeholders.

A private DNS for the aviation generic top-level domain (gTLD) is necessary for IP to be effectively utilized across the global aviation community and to limit and isolate the cyber risk that can come with the use of DNS. A DNS structure that follows the IP addressing schema and meets the needs of the aviation community needs to be defined.

This method of limiting cyber risk in an IP environment is implemented across industries and governments. An example of this is used by the military community in which the military has publically accessible sites that end in ".mil" DNS name. When a request is received by the receiving system, the system will validate if the request is coming from a valid DNS name that could simply be ".mil" and will then validate that the DNS corresponds to a valid IP address or IP address range approved for use. If either of these two criteria do not match, the request is ignored. This creates a simple method of protecting against broad access to publically accessible sites and infrastructure.

4.5 Operations of the network

The network services will be provided by a consortium of traditional aviation network providers of ground-ground and air-ground networks and new entrants providing LTE based network services and low earth orbit network services based on balloons or drones. The consortium will be formed based on network users and network providers using global standards for:

1. Network service requirements
2. Network interface requirements and policy
3. Network security requirements and policy

The participants in the consortium will use a global multilateral agreement to interconnect their networks and to exchange network traffic to provide a global resilient aviation network. Each of the network providers will be able to increase the amount of bandwidth they can sell to their network users when their users can reach and need a larger number of aviation services worldwide. The principle of network traffic exchange between network providers and network bandwidth demand driven by global service offering is the basis of the success of the World Wide Web (Internet).

When an aviation user wants to obtain a global aviation service (e.g. an ANSP from country A wants to obtain flight information from an aircraft from airline X), the first step is for the user to obtain a digital identity. The user obtains the digital identity by registering its actual identity with the RA of its State. The RA provides the validated identity information to the CA that is member of the framework for a trusted identity. The CA issues the digital certificate, which is equivalent to the digital identity. The next step is for the aviation user to obtain a network connection from a global resilient aviation network provider. Before the user can obtain the connection, the user needs to provide proof that the system or network that needs to be connected to the global resilient aviation network is compliant to the network interface requirements and policy and to the Network security requirements and policy. Once compliance has been established, the global resilient aviation network provider can connect the user's system or network and provide a network service. Once the network connection has been established, assuming that the global aviation service provider has provided service access to all identities issued by the user CA by group policy, the user can obtain the global aviation service.

4.5.1 Network service requirements

The network service requirements define a standard set of services that each of the service providers within the consortium can provide. A network service is defined by the following parameters:

- Available bandwidth
- Maximum latency based on message size
- Availability, Mean time between failure and mean time to restore, measured over a defined period of time
- Network protocol support (e.g. UDP, TCP, SNMP, DNS)
- Local scope (within the providers' network) or global scope (within all of the global resilient aviation network)

The network service providers will offer a catalogue of network services with different bandwidths, latency, availability, protocol support and local or global scope to their network users.

4.5.2 Network interface requirements and policy

The network interface requirements and policy define how the network providers within the consortium interconnect their networks. The requirements specify the technical interface standards for the interconnection. The network interface requirements will specify the use of global IPv6 addresses for aviation between the network providers and the network users. The policy describes the process to follow for interconnecting providers' networks, the roles and responsibilities in the process, and the legal liabilities for each network provider. The policy also describes how to obtain and assign IPv6 addresses to the network.

4.5.3 Network security requirements and policy

The Network security requirements and policy define the standards for the security controls the network providers and interconnected users must use and the process to prove that they are compliant.

5 Summary of impact

The full connectivity enabled by digital transformation of the aviation system is occurring now, and will continue. The question is whether this proceeds in a coordinated fashion that enhances interoperability and reduces the threat surface or not. Communication service providers, aircraft manufactures, and avionics producers, are all putting in place their own systems of identity and trust as a matter of necessity. That means in the near future, an aircraft may need different digital certificates to communicate with its satellite communications provider, retrieve data from the airline operations centre, update its avionics, download engines monitoring data and other functions. The potential number of proprietary secure links is nearly endless. This patchwork of disparate efforts to reduce the threat surface to air and ground operations will add complexity to the system that will be costly to maintain and will offer a myriad of gaps for adversaries to exploit.

Similar problems are already being encountered on the ground as ANSPs, Airports, and other service providers attempt to exchange information as outlined in the Global and Regional Air Navigation Plan (GANP/ANPs). States and Regions are putting in place their own internal systems of identity and trust

to allow them to operate. These systems will not be able to connect to internal or external entities to the aviation community unless trusted mechanisms for digital identification are recognized and put in place at a global level.

It is also important to note the opportunity that is about to be lost regarding the new entrants into the system. Across the world, several Civil Aviation Authorities are responding to the massive influx of UAS. Many are putting in place registries systems and there are ongoing debates around the possibility of an electronic identification system. In the absence of direction global direction, different manufactures and different States will take different approaches. A globally acceptable system of identity and trust would channel the innovation that drives this emerging industry in the direction of interoperability, and increase levels of safety in a connected environment.

There are many aspects of the concept of a trust framework that appear daunting, and it will take years for the full operational vision to be realized. However, substantial benefits will be realized long before the system becomes fully operational. At this moment, the entire aviation community is responding to the increase in the threat surface with different and uncoordinated actions. This divergence, and its effect on interoperability, is crucial for the aviation system. This divergence will begin to reverse once a global approach is agreed among the aviation community.

Appendix 1: Acronyms

Note: Appendix not completed and under development

ACAS	Advanced Collision Avoidance System
ACARS	Aircraft Communications Addressing and Reporting System
ACD	Aircraft Control Domain
ADS-B	Automatic Dependent Surveillance – Broadcast
ADS-C	Automatic Dependent Surveillance – Contract
AEEC	Airline Electronic Engineering Committee
AGL	Above Ground Level
AISD	Airline Information Services Domain
AMHS	Automated Message Handling System
ANSP	Air Navigation Service Provider
AOC	Airline Operations Centre
ASBU	Aviation System Block Upgrade
ATA SPEC	Air Transport Association Specification
ATC	Air Traffic Control
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATS	Air Traffic Service
BCA	Bridger certificate authority
BI	Business interruption
CA	Certificate authority
CANSO	Civil Air Navigation Services Organization
CONOPS	Concept of operations
COTS	Commercial off the shelf
CP	Certificate policy
CPDLC	Controller pilot data link communication
CPS	Certificate practice statement
CSP	Communication service provider
DDOS	Distributed denial of service
DNS	Domain name service
EASA	European Aviation Safety Agency
EFB	Electronic flight bag
FF-ICE	Flight and flow Information for a collaborative environment
FL	Flight level
FTK	Freight tonne kilometers
GA	General aviation
GANP	Global Air Navigation Plan
GDP	Gross domestic product
gTLD	Generic top level domain

HF	High frequency
IAM	Identity access management
IATA	International Air Transport Association
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
IFR	Instrument flight rules
IoW	Internet of wings
IP	Internet protocol
IPv6	Internet Protocol version 6
IPS	Internet protocol suite
ISMS	Information security management system
ISO	International Standards Organization
ISP	Internet service provider
ITU	International Telecommunication Union
OSI	Open systems interconnection
PANS	Procedures for air navigation services
PIESD	Passenger information & Entertainment services domain
PKI	Public key infrastructure
RNP	Required navigation performance
RPA	Remotely piloted aircraft
RPAS	Remotely piloted aircraft system
RPK	Revenue passenger kilometers
SARP	Standard and Recommended Practice
SCVP	Server certification validation servers
SDS	Secure dialogue service
SWIM	System wide information management
UAS	Unmanned aircraft system
VHF	Very high frequency

Appendix 2: Definitions

Note: Appendix not completed and under development

TERMS	DEFINITION	Source
Accreditation	The formal recognition by an independent body, generally known as an accreditation body that a certification body operates according to international standards.	ISO
Authentication	To prove or serve to prove to be real, true, or genuine authenticate a user.	Merriam-Webster
Certification	The provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements.	ISO
Communication session	In computer science, in particular networking, a session is a semi-permanent interactive information interchange between two or more communicating devices, or between a computer and user	Wikipedia
Confidentiality	The state of keeping or being kept secret or private.	Oxford dictionaries
Digital identity	A digital identity is information on an entity used by computer systems to represent an external agent. That agent may be a person, organization, application, or device. ISO/IEC 24760-1 defines identity as "set of attributes related to an entity".	Wikipedia
Digital signature	A digital signature is a mathematical scheme for presenting the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).	Wikipedia
Integrity	A Definition of Data Integrity. Data integrity refers to the accuracy and consistency (validity) of data over its lifecycle. Compromised data, after all, is of little use to enterprises, not to mention the dangers presented by sensitive data loss.	Digital Guardian
Network Port	A process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Diagram Protocol (UDP) and Transmission Control Protocol (TCP).	Techopedia
Network services		
Privileged	not subject to the usual rules or penalties because of some special circumstance;	Merriam-Webster
Policy Enforcement Point	The Policy Enforcement Point (PEP) is a network device on which policy decisions are carried out or enforced. When a user tries to access a file or other resource on a computer network or server that uses policy-based access management, the PEP will describe the user's attributes to other entities on the system.	CCSK Guide
Secured	trustworthy, dependable	Merriam-Webster
Service Exchange environment	A collection of network devices, implementing all the necessary cybersecurity controls and processes to detect, protect, mitigate and respond to cybersecurity threats	Rob Segers

Appendix 3: Roles and responsibilities within the current and future exchange of information environment

Note: Appendix not completed and under development.

It is important to understand who the relevant stakeholders of the aviation ecosystem are, where they operate and which are their roles and responsibilities.

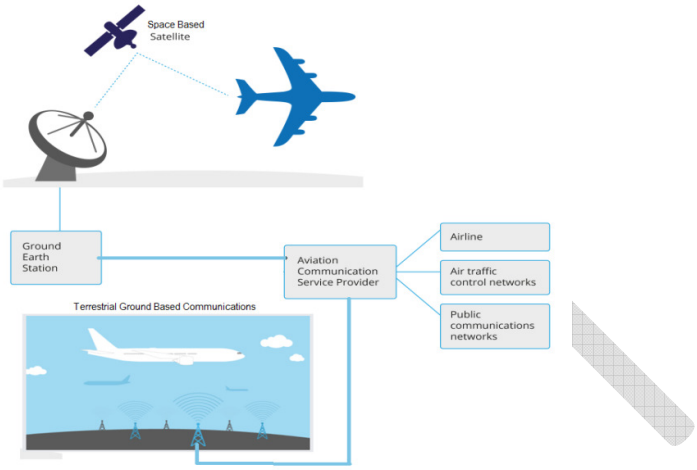

Figure 9 Communications architecture schema

- Air Navigation Service Providers (ANSPs)

ANSPs manage and operate the Air Traffic Service Network under their area of responsibility, and provide air traffic services to active flights. In some cases, ANSPs might delegate the management and operation of the network to a different service provider.

They will be involved in certification of users within their operational area. ANSPs will be the primary identifiers of critical systems and data to support resiliency in the global aviation network design. They are also a major participant in detection of cybersecurity events and the subsequent response.

- Airline Operations Centers (AOCs)

AOCs are connected to one or more ANSPs to support the exchange of information regarding flight planning as well as aeronautical and weather information as required for flight operations.

As a whole, the industry is moving toward a services -based model and require a more dynamic real-time exchange of information. Services utilizing SWIM and subscribing to information services such as FF-ICE for flight planning, Aeronautical information and others can only be fully realized in a more interconnected trusted operating environment that is both dynamic with and real-time access between aviation stakeholders to planning and approval of flight planning.

- ICAO

ICAO will mainly play a role in governing and auditing the organizations that operate and manage the Bridge Certificate Authority, the trusted Certificate Authorities, the Registration Authorities, the Domain Name service and the IPv6 address allocation. ICAO develops the Certificate Policy (CP), reviews and approves the Bridge Certificate Authority's Certificate Practice Statement (CPS) and approves the trust framework membership of Certificate Authorities. ICAO reviews and approves the DNS provider's DNS practice statement and approves the DNS providers' membership to the DNS hierarchy.

- States
- Network service providers
    - Communications Service Providers (CSPs)
        - Ground-based

Ground-based CSPs interface with ANSPs and provide them with the means to communicate with aircraft such as VHF or HF infrastructure. This service may also be provided by an ANSP, however, it is usually provided by a separate communication service provider.

There are only a few ground-based CSPs that provide this service on a global scale. These services are not only provided to ANSPs to communicate with aircraft flying under their area of responsibility, but also, if necessary, with Airline Operations Centers (AOCs). AOCs may also use these services to communicate with their own aircraft for specific purposes.

        - Space-based

Satellite communications have been predominantly used to support oceanic operations or as a backup to VHF ATCO-pilot communications when it is not available. In this latter case, satellite communications service providers traditionally interface with other CSPs who interface with ANSPs directly.

    - Ground Based Cabin/Internet Communications

These service providers are focused on providing the cabin (rear Passenger Domain) of the aircraft with broadband communications for the entertainment systems and other broadband access needs for IP communications. These services are outside the scope of this document.

    - Domain name system operator

An organization operating the Root DNS server in accordance with global standards. The DNS provider establishes a DNS practice statement describing the process used to operate the root DNS system.

- Certificate Authorities
    - Bridge certificate authorities

An organization operating the BCA system in accordance with global certificate policy standards. The BCA establishes a Certificate Practice Statement (CPS) describing the process used to operate the trust bridge.

Appendix 4: Operational scenarios

Note: Appendix not completed and under development.

Scenario 1: Air Traffic Management (ATM)

The Future Operations is Performance Based

The unprecedented future growth in global aviation demands an ATM concept that is adaptable, global, integrated and highly interoperable. Global modernization efforts will create a more agile environment to introduce air traffic management efficiencies and greater integration of information into planning and decision-support systems. Additionally, the introduction of new entrants demands agility and flexibility for managing air traffic.

Global ATM will always be a highly federated operational environment orchestrating the decisions of many actors, using many individual systems, collaborating across multiple organizations, with different interests. Technology advances in many segments of the aviation system, including aircraft avionics and other on-board systems, air-ground communications, ground-ground communications, new flying platforms such as unmanned aircraft systems (UAS), and spacecraft, improve automation and decision-making capabilities. This operational concept is adaptable, accommodating an operational environment that supports the needs of all States, tailored for regional customization, and scalable to meet their specific needs. Despite the urgency in implementing ATM changes to meet these wide ranging needs, growing traffic demands in certain areas and lack of infrastructure in others demonstrate the challenges that lie ahead in establishing a globally interoperable environment.

This future state delivers air traffic services in very dynamic environments, with stakeholders integrating shared information through automation systems, improving situational awareness through enhanced decision support capabilities equipped with improved information. These operational breakthroughs require increased interdependency between stakeholders and partner automation systems, achieved through greater access to information.

The Future is Interconnected

Achieving this vision requires a highly interconnected community of aviation partners. Establishing an environment that enables this interconnected future state will require technology, policy and diligence by authorized users. This infrastructure will be required to digitally exchange flight plans, flight trajectories and airspace user intent, in near real time, to improve airspace management and aerodrome operations for capacity/demand balancing and conflict management. To run effectively, this distributed environment requires data and information from different systems supporting independent strategic and tactical decision-making to work seamlessly. This future state demands a more highly integrated, trusted operating environment, supporting greater system interoperability, across an interconnected aviation community.

This operational concept is network-centric, enabling any authorized user connected to the network, access to information from any location. An internet protocol based network, supported by industry standards, will form the foundation of this environment. A network capable of supporting various data types, of varying sizes and priorities, and enabling secure exchange of these data. This new converged network erases today's boundaries, creating a seamless environment between ground based air traffic services, commercial and military flight operations, supporting vendors, airspace users, and

incorporates the aircraft as a node in this aviation network. The achievement of a more integrated operating environment that far exceeds the way the aviation system is connected today, requires the adoption of commercially available modern technology.

Today's boundaries between air-ground and ground-ground network communications are erased through improved technology, maturing industry standards and improved economies of scale. In line with the transnational boundaries nature of air traffic operations, this net-centric environment ensures the right information is delivered to the right/authorized user, when they needed, wherever they are. The interconnected global ATM environment requires advanced applications, equipped with algorithms that offer improved trajectory-based operational capabilities. In this net-centric operational model, new application systems share information in near real-time to empower decision-makers with key insights for managing air traffic. These applications have the ability to ingest and process information to inform these decision-makers, and this information requires the ability to share information across multiple stakeholders, easily.

The Future is Seamless

Information exchange is at the heart of these modernization efforts. Performance-based operations, rely heavily on trajectory management which includes knowing the planned trajectories and the airspace user intent. This information is shared between stakeholders, driving those new application systems and introducing airspace optimization efficiencies. Sharing information between these stakeholders, then establishes the foundation for realizing these efficiencies and improves interoperability.

Contemporary interoperability requires hard-wired connection using unsupported networking technology with dedicated channels and highly structured file formats. Any deviation from any of these hard-coded rules threatens current operations. This satisfied the purpose-built systems that enabled a safe and reliable air transportation system. As technology has evolved, however, this regimented ecosystem has stifled flexibility, agility and innovation. Emerging aviation requirements, however, demands a significantly more dynamic airspace and integrated ATM architecture.

System Wide Information Management, or SWIM, introduces service oriented architecture (SOA) to aviation. Simply, service orientation is designed to break down complex application systems into components and release data/information to enhance re-usability across the ATM enterprise. SWIM is envisaged as a global concept consisting of standards, infrastructure and governance designed to enable ATM-information management and interoperable exchange between qualified parties. SWIM establishes a data network overlaid on the physical network, and uses industry standards to enable information sharing through interoperability across all SWIM capable users. SWIM has the potential of leveraging innovations in information technology to radically reduce aviation operations costs.