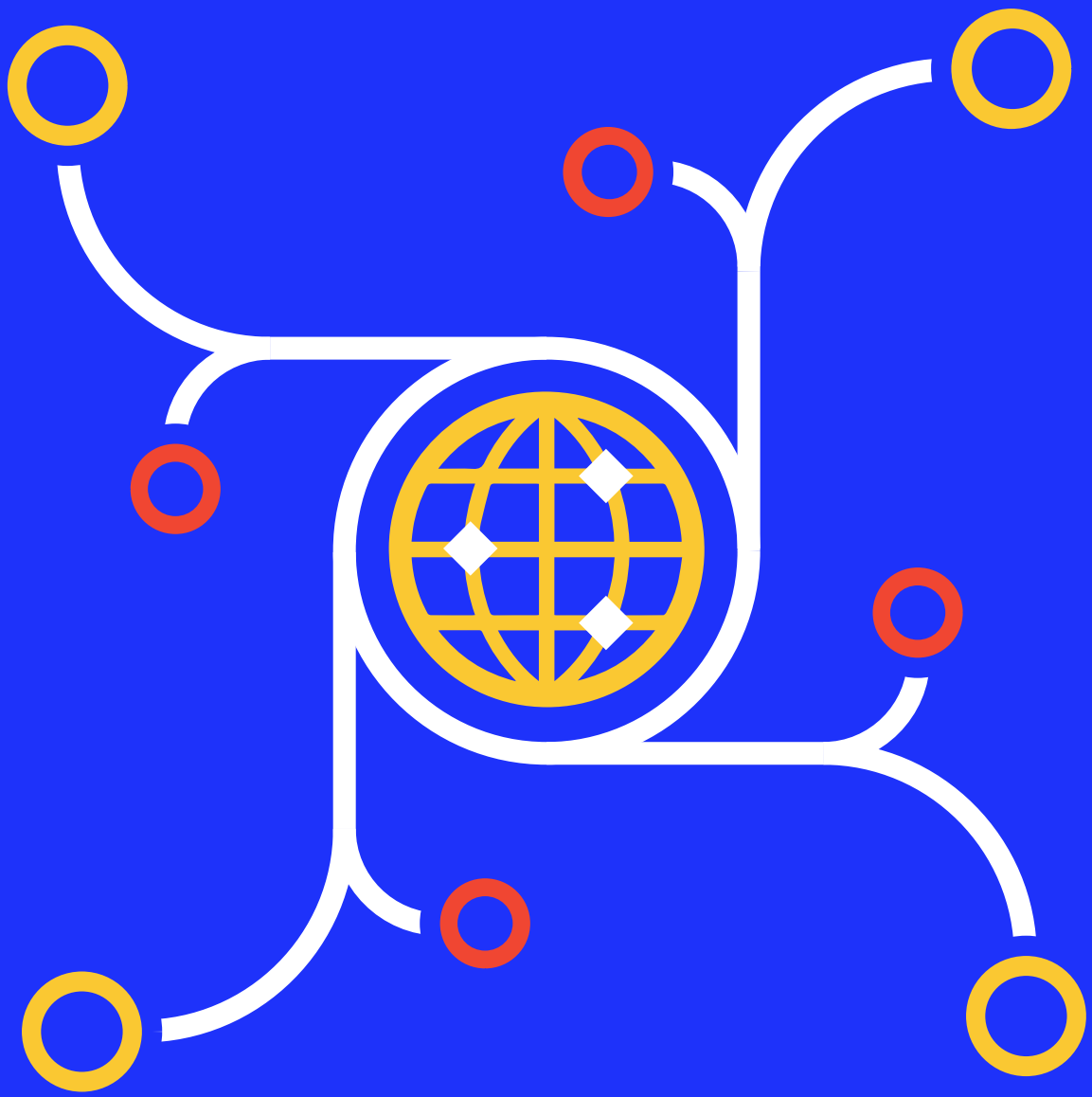
Cycle 2

Data and Technology Proof of Concept (PoC)

Position paper



IATA

Table of contents

Introduction

The aviation industry continues to navigate a period of profound digital transformation, where new technologies and the use of data are rapidly becoming foundational to how airlines operate, collaborate, and deliver.

Through structured innovation cycles, the IATA Data and Technology (DaT) Proof of Concept (PoC) Strategic Partnership program enables airlines, strategic partners and other stakeholders to jointly design, test, and validate innovative solutions to industry challenges. Each cycle delivers, real-world use cases that demonstrate how technologies can be applied across the aviation ecosystem while respecting the industry's requirements for security, reliability, and global interoperability.

This industry position paper articulates the outcome of Cycle 2 of the DaT PoC program, summarizing the insights and technical findings from the PoCs. Each PoC addresses a critical element of the industry's digital transformation:

- **Project Gaia – Global Data Bus**
  Explores a scalable, event-driven approach to real-time data exchange across aviation stakeholders.
- **Project Carina – AI Agent Multilateral Interoperability**
  Demonstrates how AI agents can enable automated collaboration and coordination for airline cargo shipments.
- **Digital Identity Verification in the Distribution Process**
  Examines the role of digital identity frameworks in strengthening trust across distribution channels and paving the way to a seamless journey.
- **Contactless Travel at Scale**
  Demonstrates how interoperable digital identity technologies can enable seamless and privacy-preserving passenger journeys.

Together, these PoCs demonstrate how emerging technologies and data can support a more connected, secure, and efficient aviation ecosystem. By validating architectures, operational models, and governance considerations, the PoCs provide practical insights that can help guide future industry collaboration and innovation.

Kim Macaulay
SVP Information and Data
Chief Information and Data Officer
IATA

1. Project Gaia (Global Data Bus)
Global Data Bus PoC

Executive Summary

The aviation industry relies on decades-old messaging infrastructures that are increasingly unable to meet today's requirements for real time, data rich, secure, and scalable information exchange. Current systems are constrained by rigid formats, high operating costs, complex point to point integrations, and security limitations. At the same time, emerging operational and customer experience use cases – Offer Order, multimodal journeys, AI driven automation, and real time disruption management – demand a modern, event driven data backbone.

Project Gaia - the Global Data Bus (GDB) Proof of Concept (PoC) demonstrates a new industry wide model that replaces fragmented integration landscapes with a secure, standardized, cloud agnostic, event streaming platform. Built on Apache Kafka–compatible technologies, the GDB introduces a shared transport layer with strict ordering, zero loss durability, and global scalability. Its architecture applies a Secure by Design, zero trust model: participants encrypt data at the edge, the transport remains content-blind, and routing is driven only by metadata. A centralized Identity Registry provides participant authentication, authorization, and cryptographic key management, establishing the foundation for trust across the ecosystem.

The PoC validated this model through real world exchanges between Qatar Airways and Los Angeles World Airports, spanning use cases such as boarding status, codeshare flight updates, gate changes, interline passenger counts, and baggage carousel assignment. Deployment across Azure and AWS regions showed that multi-cloud operation, inter-cluster replication, and real time routing can function reliably across geographies while respecting data sovereignty requirements. Software Development Kit (SDKs) and connectors simplified integration for both modern and legacy systems, demonstrating that participants can adopt the GDB without major reengineering.

The results confirm that a shared, event driven data bus can significantly reduce integration complexity, accelerate partner onboarding, and improve operational resilience. Latency and throughput improvements relative to legacy store and forward systems were evident, alongside the potential for meaningful cost efficiencies through reduced messaging fees and rationalized infrastructure. The PoC also proposed a potential governance model required for scale: a hybrid arrangement in which a central entity manages identity, trust, schemas, and standards, while transport and regional endpoints remain federated and vendor agnostic.

From an IATA standards perspective, the approaches described in this paper should be understood strictly as technical enablement mechanisms that build on existing standards and governance frameworks. They are not intended to define new industry standard. This is important to note to avoid ambiguity and ensure continued alignment with IATA's established standards ecosystem.

Overall, the GDB PoC provides strong evidence that the aviation industry can transition to a secure, scalable, many to many data exchange model that supports modernization, compliance, and innovation. With the foundations proven – technically, operationally, and architecturally – the GDB presents a credible path toward industry-wide adoption, unlocking real time collaboration, richer data flows, and improved passenger outcomes at global scale.

Problem Statement & Context

The aviation industry relies on a dense fabric of B2B messaging between airlines, airports, ground handlers, GDSs, regulators and technology providers. Legacy messaging systems and integration patterns have delivered global reach and reliability for decades, but they are increasingly at odds with today's requirements for real-time, data-rich, secure and cost-effective exchanges.

Taking cargo as an example, it operates across a highly fragmented ecosystem with wide variation in digital maturity and operational readiness. Any approach intended to scale across the industry must therefore explicitly account for phased adoption, coexistence with legacy environments, and realistic onboarding constraints across airlines, handlers, forwarders, and authorities.

Current integration landscapes typically exhibit the following constraints:

Rigid message formats and payload limits
Many industry interactions are constrained by fixed, text-based formats and strict size limits. This constrains the richness of data that can be exchanged, makes evolution slow and risky, and limits the use of modern analytics and AI techniques that depend on context-rich, structured data.

High operational costs
Store-and-forward networks and hub-and-spoke integration patterns impose significant fixed and variable costs. Messages are often billed by volume, and parallel infrastructures must be maintained for different protocols and partner communities. These costs are increasingly difficult to justify versus modern, internet-based alternatives.

Interoperability challenges and complex integration landscapes

Individual organizations operate dozens of point-to-point links, proprietary gateways and middleware platforms (Message Queues, Enterprise Service Bus, Integration Platform as a Service, custom APIs, etc.). Onboarding a new partner, use case or destination often requires a mini project per peer, with bespoke mappings and security models. This peer-to-peer complexity slows innovation and limits the ability to scale new services across the ecosystem.

Security and compliance gaps

Many legacy solutions were not designed with modern security and regulatory expectations in mind. Encryption, strong identity, non-repudiation, granular access control and end-to-end auditability are often bolted on, if present at all. Emerging regulations (e.g., around cybersecurity and data protection in addition to legislation and legal requirements for the protection of personal data) require architectures that are secure-by-design, not retrofitted.

Heavy reliance on manual, human-driven processes

Despite existing messaging systems, many critical interactions still depend on manual communication and ad-hoc coordination. For example, information about passengers requiring assistance is often shared between airlines, airports and ground staff through manual handovers, with limited ability to track status, confirm delivery, or obtain timely feedback. This introduces delays, inconsistency, over- and under-provisioning, and operational risk, precisely in areas where reliability, accountability and experiences are the most important.

Maintenance of existing messaging recipients and networks

It is plausible that large amounts of messages are simply not received or not relevant to the recipient given the lack of auditability of legacy messaging.

At the same time, operational and customer experience use cases are becoming more demanding. Flight disruption management, Passengers with Reduced Mobility (PRM) services, dynamic offers and orders, multimodal journeys, and AI-driven automation all require richer, more frequent, and more contextual data exchanges than traditional messaging infrastructures were designed to support.

Simultaneously, the industry looks to migrate from legacy Passenger Services Systems (PSS) to Offer Order systems, increasing the need for two-way messaging events between multiple service providers and drastically increasing the number of messages over time.

Market Drivers & Urgency

The GDB PoC is not a technology-first initiative, but a direct response to specific friction points and requirements across the aviation ecosystem:

The Demand for Rich, Real-Time Data

Legacy systems are constrained by rigid message formats and strict payload limits, which restrict data richness and slow evolution. Operational resilience now demands shared, real-time visibility. Moving beyond static snapshots and batch processing, the ecosystem requires continuous event streams to reflect the current operational state, not yesterday's plan.

Lower Total Cost of Ownership (TCO)

Store-and-forward networks and hub-and-spoke integration patterns impose significant fixed and variable costs that are increasingly difficult to justify. To decouple costs from volume, the GDB utilizes cloud architectures that offer lower per-message rates and simpler maintenance than legacy networks.

Seamless Ecosystem Integration

Individual organizations currently operate dozens of point-to-point links and proprietary gateways, with each new partner requiring bespoke mappings and security models. As the value chain expands to include AI, analytics, and multimodal providers, this peer-to-peer complexity becomes economically unviable. The GDB resolves this with a scalable "connect once, reach many" model.

Enabling Modern Digital Initiatives

Transformations like Offer Order and Agentic AI require high-frequency, structured data at volumes legacy systems cannot support. The GDB's streaming paradigm provides the necessary throughput and context they cannot support.

Vision

Project Gaia - Global Data Bus PoC initiative is a response to the industry's need to move away from fragmented peer-to-peer integrations and legacy messaging networks toward a shared, event-driven backbone that supports secure, real-time, standardized exchanges across the global aviation ecosystem. Its vision is to establish a unified, standards-based infrastructure that replaces high-cost, opaque legacy systems with a scalable, secure, and transparent platform enabling stakeholders to exchange data consistently and efficiently at a global level.

However, a clear separation must be maintained between standards and business semantics owned by their own domain governance bodies and technical enablement mechanisms, which support interoperability and coordination. Without this separation, there is a risk of scope ambiguity and misinterpretation of ownership as these concepts evolve.

Core Design Principles

The GDB PoC architecture relies on five foundational principles to ensure trust and scalability.

Secure-by-Design

The GDB adopts a Secure-by-Design philosophy, treating security as foundational rather than an afterthought. Utilizing a Zero Trust model that separates the control layer from the transport layer, it ensures that data integrity, sovereignty, and access policies are maintained throughout the transmission lifecycle. This includes End-to-End Encryption (E2EE) and Decentralized Identifiers (DIDs).

Interoperability via Open Standards

Rejecting legacy 'black box' models, the GDB champions a 'glass box' architecture built on open standards and technologies. It ensures seamless interoperability through standard data formats (JSON, Avro) and full alignment with industry standards like IATA Offers & Orders and Aviation Information Data Exchange (AIDX), all while supporting robust schema evolution.

High Throughput, Low Latency, Global Scale

Engineered for the immense volume of global aviation, the GDB backbone delivers high-throughput messaging with global single digit second latency. Its hyper-scale, geo-distributed architecture ensures elastic scalability and high availability across the globe.

"Plug and Play" Integration

Adoption relies on lowering barriers to entry. The GDB minimizes integration costs through standard connectors and offers native compatibility with major cloud platforms, allowing participants to minimize one-time integration costs.

Vendor-Agnostic Architecture

To prevent commercial lock-in, the GDB defines a vendor-neutral reference architecture based on the open-source Apache Kafka platform. While implementations may use specific technologies (in the case of the PoC – Confluent and AWS MSK flavours of Kafka), standardized interfaces ensure the ecosystem remains independent of any single provider.

PoC Objectives

The GDB PoC aims to demonstrate whether the vision is technically and operationally viable in a practical, real-world setting, used by multiple stakeholders and utilizing different messaging payloads. The main objectives include validating end-to-end message delivery across various domains and participants, demonstrating secure transmission and consumption of messages by authorized parties, enabling near-real-time responses and ensuring auditability and traceability of messaging for record-keeping purposes.

Furthermore, we aim to demonstrate measurable improvements compared to legacy baselines. This includes comparing latency, throughput and integration complexity against traditional models such as store-and-forward networks and point-to-point API meshes. Additionally, the PoC seeks to highlight potential cost efficiencies, such as reduced per-message costs, simplified partner onboarding, infrastructure consolidation, and new business opportunities enabled by richer, real-time data.

The PoC is dedicated to establishing trust and identity flows for B2B exchanges. This involves implementing a trust framework where each participant is registered, identified and authorized through a secure shared registry. To ensure the integrity and non-repudiation of messages as well as the confidentiality of payloads, cryptographic mechanisms such as signing and encryption are employed. Additionally, the PoC showcases multi-cloud and multi-region interoperability by replicating and consuming data in various regions and clouds. Integration with cloud-native services like AWS EventBridge, Azure Event Hub, managed Kafka services and data warehouses is demonstrated to illustrate throughput, resilience and observability within the system.

The practical scope of the PoC involved implementing real world message flows over the GDB between Qatar Airways and Los Angeles World Airports. These exchanges covered secure, custom payloads for data points such as Boarding Status Messaging, Codeshare Flight Status, Gate Changes, Interline PAX Counts, and Baggage Carousel Assignments. To support the geographical distribution of participants, the core component was deployed across two clusters: an Apache Kafka Confluent based deployment running in Azure UAE and an AWS Managed Streaming for Kafka (MSK) deployment in US West 2. The PoC also focused on simplifying how participants interact with the GDB for both producing and consuming messages. To enable this, we delivered a Java SDK that streamlines message submission, along with several connectors capable of writing payloads directly into the consumer's IT systems - removing the need for polling, while still supporting it where required.

Reference Architecture

To meet the demands of modern aviation, the core component of the GBD is built on Apache Kafka-compatible technology, moving the industry away from "fire-and-forget" systems toward a persistent "Distributed Ledger of Events" that guarantees durability and strict ordering. This foundational layer creates an immutable history of operations, ensuring that every event, from a checked bag to a gate change, is captured, replicated across availability zones, and made available for replay, providing a single source of truth that survives infrastructure failures.

Surrounding this transport core is an advanced governance framework reliant on two distinct registries to secure and direct the flow of information. A Schema Registry acts as the authority, enforcing strict structural standards to ensure every message is universally readable by any receiver, while a separate Identity Registry functions as the secure address book, managing authorized participants, their specific routing and encryption keys. Participants interact with these components via the GDB SDK, a smart wrapper that prepares the "Digital Envelope" by handling encryption and the envelope schema including GDB DIDs, and eventually additional optimizations such as payload compression. Once the message is ingested, the architecture leverages Apache Flink (or equivalent) as an intelligent sorting engine. In transit, Flink analyses the envelope's metadata in real-time to route the message to the correct destination topic and geographical region, ensuring precise delivery without ever opening the encrypted payload.

To ensure universal interoperability across the diverse technological landscape of global aviation, the architecture concludes with a flexible integration layer powered by Connectors. This component bridges the gap between the modern event stream and existing legacy infrastructure by supporting both "push" and "pull" delivery models. While digital-native participants can pick up messages directly from the bus, the system utilizes Managed Sinks to actively push data downstream into heritage environments, such as MQs, cloud based ESBs or relational databases, in their native formats. This decoupling allows airlines, airports and other stakeholders to connect to the global messaging backbone without refactoring their core operational systems, ensuring the GDB functions as a non-intrusive, seamless utility.

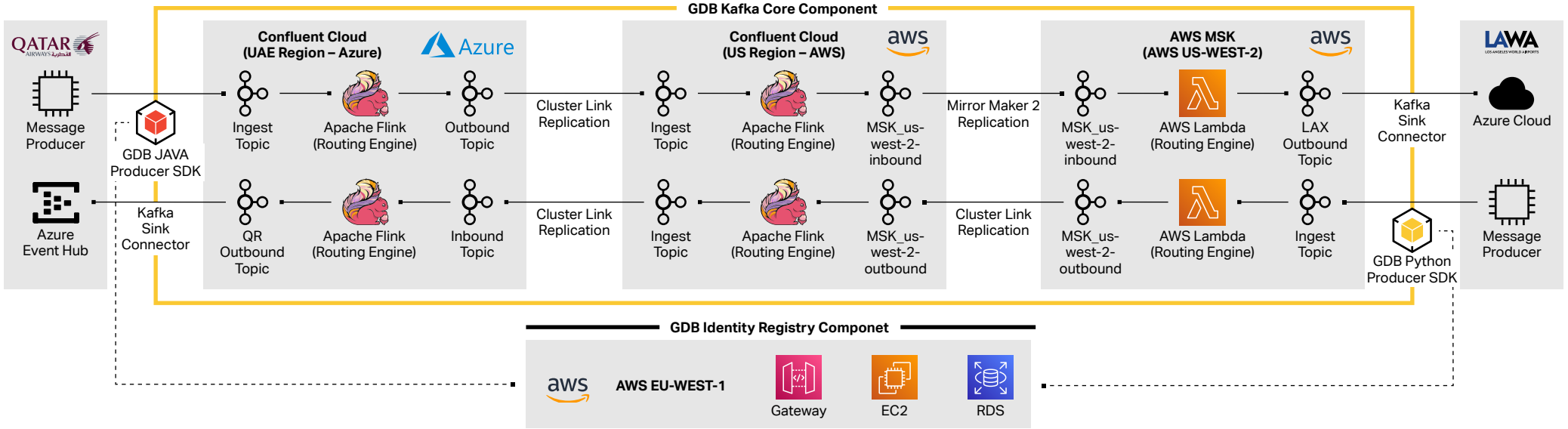
Determinism and Guaranteed Event Ordering

In aviation operations, the sequence of events is as critical as the data itself. A "Baggage Loaded" event occurring before a "Passenger Checked-in" event is a logical impossibility that can disrupt downstream automated systems.

Kafka based core component provides **Strict Deterministic Ordering** through its partitioning logic. By utilizing specific keys, the bus ensures that all related events are written to the same physical partition in the exact order they occurred.

This architecture enforces **Sequential Integrity**, fundamentally distinguishing the Core Bus from legacy load-balanced queues where messages often arrive out of sync. Instead, the bus guarantees a "First-In, First-Out" (FIFO) delivery at the partition level. This foundational reliability drives Predictable Outcomes, empowering airlines and airports to automate complex, state-dependent decisions, from dynamic gate assignments to precise fuel load calculations, with absolute confidence in the chronological accuracy of their data.

Figure 1: GDB PoC Scope and Flow: Qatar Airways <-> LAX Airport



The "Zero-Loss" Mandate: Durability and Record-of-Truth

For an airline, a missing message isn't just a technical glitch. It is a potential operational delay or a safety reporting gap. To mitigate this, the Core Bus is designed with a "Nothing is Lost" philosophy, treating data persistence as an operational imperative rather than a background process.

Append-Only Immutability

The foundation of this durability is the platform's append-only structure. Unlike traditional databases that overwrite old values with new ones, the Kafka based core component appends every event to an immutable log. Once a flight status or passenger record is written, it cannot be altered or deleted by subsequent events. This creates a tamper-proof historical lineage, ensuring that the system captures not just the current state of an operation, but the complete narrative of how that state was reached.

Distributed Acknowledgment and Resilience

To guarantee survival against infrastructure failure, the bus employs a rigorous "synchronous replication" model. A message is only acknowledged as "received" once it has been successfully written to multiple independent brokers across isolated physical availability zones. This ensures that even in the event of a total node failure or a zonal outage, the data persists elsewhere uninterrupted, maintaining zero data loss for critical aviation streams.

"Audit of Record"

Because the Kafka based core component acts as a durable retention engine rather than a transient pipe, it serves as the definitive "Audit of Record" for the ecosystem. This decoupling means that if a downstream system, such as a baggage handling app or flight display, fails or goes offline, the data is not lost. The messages remain safely stored on the bus, allowing the recovered system to "replay" events from the point of failure. This mechanism provides intrinsic resilience for IT operations and a comprehensive, verifiable audit trail for regulators and partners.

Multi-Cloud Deployment: Strategic Sovereignty and Localized Latency

Aviation is a global industry operating under local laws. The **Kafka based core component** is instantiated as a **unified fabric across multiple hyperscalers** (e.g., AWS, Azure, Google Cloud, AliCloud), managed via Terraform-based Infrastructure as Code. This deployment model is driven by three requirements:

Data Sovereignty and Residency

Regulated regions impose strict requirements on where flight and passenger data must reside. The GDB addresses this by deploying localized clusters directly onto regional hyperscalers. This architecture ensures that sensitive Personally Identifiable Information (PII) or sovereign flight data remains physically stored within national borders, fully compliant with regulations like GDPR or local aviation statutes. However, the architecture is flexible enough to selectively replicate non-sensitive metadata, allowing local operations to remain compliant while still contributing to the global value chain.

Latency Optimization and Geo-Proximity

To ensure true real-time performance, latency must be minimized at the point of ingestion. Participants connect to their nearest regional "Connection Point", ensuring that data enters the bus at the edge rather than traversing continents first. Once ingested, messages are routed via managed, high-speed inter-cluster links. This mechanism replicates data across regions in the background, bypassing the unpredictability of the public internet for long-haul transport and ensuring that a gate change in Los Angels is reflected in a Doha operations center with second-level promptness.

Vendor Neutrality and Portability

By deliberately avoiding a single-cloud and Kafka flavor dependency, the GDB protects the aviation industry from vendor lock-in and proprietary gravity. The architecture is cloud-agnostic, treating underlying infrastructure as a utility rather than a constraint. This ensures the bus remains an open, standards-based ecosystem, capable of evolving with the market and guaranteeing that the industry's critical data backbone is never beholden to the roadmap or pricing model of a single cloud provider.

The Envelope Principle: Blind Routing and Deep Security

To maintain absolute segregation of duties, the **Kafka based core component** operates as a **Pure Transport Layer**, strictly adhering to a "Postal Service" metaphor. It is responsible for the Envelope, not the Letter. This distinction is architectural, not just conceptual, ensuring that the infrastructure providers never possess the technical ability to access the sensitive business logic flowing through the system.

Content Blindness and Edge Encryption

The "body" of every message, containing the actual business data, is treated as an opaque, serialized byte array. Before a message ever leaves the participant environment, it is encrypted at the "Edge" using keys held exclusively by the data owner. Consequently, the **Kafka based core component** maintains strict Content Blindness; it stores and transports the payload without having any visibility into, or understanding of, the encrypted content within.

Metadata-Driven Routing

Routing decisions are made solely by analyzing the "headers" of the envelope, unencrypted metadata such as Sender ID, Recipient ID, and Message Type. This separation allows the bus to perform high-speed filtering and apply global governance policies, such as verifying that a specific airline is authorized to publish to a specific topic, without ever needing to "open" the payload. This ensures that performance and governance can scale independently of data sensitivity.

Zero-Trust Architecture

This architecture provides a final layer of Fail-Safe Privacy. In the rare event of a misrouting due to a configuration error, the data remains cryptographically secure, because the encryption keys are managed entirely outside of the **Kafka based core component** (via the Identity Registry component detailed later), an unintended recipient effectively receives nothing more than digital noise. A participant who accidentally receives a message intended for another airline would find only an unreadable, encrypted string. The "keys to the letter" simply never travel with the "delivery truck".

Elasticity and Economic Efficiency

To handle the unpredictable volume of global aviation without over-provisioning, the GDB architecture could leverage Confluent Freight Clusters, which provide a specialized, high-throughput tier capable of scaling to gigabytes per second of ingress while reducing data transport costs by up to 90% compared to traditional on-premise hardware.

Complementing this transport layer, the processing engine utilizes the Flink Autoscaler, which dynamically adjusts compute resources in real-time to match traffic spikes, ensuring that complex event streams are processed with sub-second latency even during peak operational windows. This "serverless" alignment of infrastructure to actual demand allows the industry to move from a Capital Expenditure model to a strictly consumption-based utility, effectively decoupling the cost of safety and compliance from the volume of data generated.

Inter-Cluster Linking: A Unified Global Backbone

To bridge these multi-cloud environments, the GDB utilizes Cluster Linking and Mirror Maker 2 technology. This allows Kafka topics to be mirrored across different clouds and continents natively, ensuring that data travels as fluidly as the aircraft it tracks. For instance, if a flight departs London – originating in an AWS environment – and arrives in Singapore – hosted on Azure – the relevant event streams automatically follow the flight's journey across this global GDB cluster mesh. This ensures that operational context is preserved across borders without requiring manual data synchronization between disparately hosted systems.

This interconnected architecture ensures extreme resilience by design. Even in the event of a total hyperscaler outage in one region, the GDB as the "Global Postal System" remains active, with messages safely buffered in alternate regions until local connections are restored or failovers are configured. At the heart of this resilience lies the distributed event streaming platform based on Apache Kafka–compatible technologies, which replaces transient messaging with append-only, durable logs. This structure guarantees that event streams are not only ordered and replay-able but can also scale horizontally via partitioning to handle the immense throughput of global aviation data without bottlenecks.

To deliver the necessary performance and fault tolerance, the system employs rigorous replication across brokers and regions, ensuring geo-redundancy while utilizing consumer groups for scalable, parallel processing. In the current PoC this core bus is instantiated using fully managed Kafka services orchestrated via Terraform-based Infrastructure as Code on top of Confluent running on Azure and AWS Managed Streaming for Kafka. This approach allows for the rapid, consistent deployment of clusters and inter-cluster links across disparate regions and cloud providers, establishing a standardized utility that abstracts away the complexity of the underlying physical infrastructure.

Beyond internal synchronization, the bus leverages a rich ecosystem of connectors to integrate seamlessly with cloud-native event buses like AWS EventBridge or Azure EventHub and downstream analytical stores such as Snowflake. However, it is crucial to maintain strict architectural boundaries: the Kafka based core component remains solely responsible for the transport, durability, and availability of the data. It does not enforce business semantics or trust verification; those higher-level concerns are delegated to specialized components, ensuring the transport layer remains a lightweight, agnostic, and highly efficient carrier.

Enabling Trust

The early ideas around GDB PoC were intended to design a fully decentralized system – to eliminate even the slight possibility of potential lock-in. However practical implications lead the requirement to be achieved through a hybrid setup: Kafka based core component as a distributed message delivery component, and centralized Identity Registry – the key element of the system which enables the Trust between Participants.

The registry plays a central role in establishing trust across the Global Data Bus by managing participant identities, cryptographic keys, lookup capabilities, schemas, and policy metadata. It begins with participant identity management, where organizations such as airlines, airports, handlers, service providers, and others - along with their technical systems and applications - are registered and issued unique identifiers and API credentials. These identities form the basis for authentication and authorization across the ecosystem.

In the PoC, a key function of the registry is its approach to cryptographic key management. Each participant uploads only their public key, never their private key. By design, the private key remains solely within the participant's own secure environment and is never shared. Other participants retrieve these public keys from the registry and use them to encrypt the payloads they send. Because only the intended recipient holds the matching private key, only they can decrypt the message. This mechanism ensures true end-to-end encryption: the sender encrypts at the source, the transport layer remains completely blind to the content, and the recipient alone can read the data. The registry supports the full lifecycle of these keys - rotation, revocation, and expiry - while ensuring that older messages remain decryptable when appropriate. To facilitate this, participants can retrieve updated keys programmatically through dedicated APIs.

Beyond cryptographic trust, the registry also serves as the ecosystem's address book through its Participant Catalogue and Lookup capability. Participants can be discovered using a variety of fields such as name, IATA code, or location, enabling seamless peer discovery across the global network.

Although schema and contract management is out of scope for the PoC, the long-term vision for the registry includes hosting and versioning data schemas, enforcing compatibility rules, and making contracts discoverable across the ecosystem. This ensures that data exchanged through the GDB remains structurally consistent and evolves safely over time.

Finally, the registry maintains essential policy and routing metadata. It records which participants are permitted to publish or subscribe to which global cluster instances making up the Kafka based core component and supports routing policies such as direct messaging, multicast distribution, or public versus restricted topics. By centralizing this governance information, the registry ensures consistent, transparent, and secure message flow while allowing the underlying bus to remain simple, scalable, and reusable.

The registry enables a decentralized but coordinated trust model: messages can be exchanged directly between participants (peer-to-peer semantics) while still relying on a shared framework for identity, keys, schemas and policies.

Use Cases

The aviation industry currently operates on point-to-point messaging models that create data silos, latency and complexity with a mixture of overlapping standards and custom implementations. The Global Data Bus introduces a paradigm shift treating information as events published to a shared, secure backbone where the producer manages the visibility, protected with encryption, of any message to a set of actors that are registered, publicly available and whose identity has been confirmed and affirmed by a registration process handled by a trusted governance framework. The GDB has been designed as a seamless, secure end-to-end encrypted channel to connect airlines and service in a many-to-many context.

While the GDB is designed to be domain-agnostic, this section examines uses cases that demonstrate how it can handle different messaging standards – from broad community broadcasts to highly sensitive private data exchanges between specific parties – while providing support for existing and emerging industry standards.

Operational Resilience: AIDX Based and Public Broadcast

In this use case, the data involved is operational information that must be broadly accessible to trusted ecosystem partners – such as airlines, airports, air traffic control, and service providers – to maintain situational awareness. While it is important to verify the integrity of the sender, the payload itself does not contain sensitive personal information or commercially confidential content. The relevant standard here is AIDX, specifically the FlightLegNotifRQ message, which communicates essential flight status, gate, and timing details.

Today, when a flight is delayed, an airline must send separate Type B messages to the airport AODB, the ground handler, and codeshare partners. This fragmented approach often leads to latency and outdated information – sometimes causing gates to remain assigned to aircraft that are no longer on schedule simply because updates did not propagate in real time.

With the Global Data Bus, the airline could publish a single message that is delivered securely to all relevant consumers. The platform replicates and stores the message reliably, ensuring every authorized party can access it immediately. As soon as the airport receives the event, it can dynamically reallocate gates and resources, and, if required, trigger additional notifications to other providers through the bus. Ground handlers, receiving the same event, can adjust staffing plans accordingly. Throughout the process, the GDB ensures low latency delivery, strict message ordering, and validation of the producer's identity, allowing operational systems to react quickly and consistently without the overhead of multiple bespoke integrations.

The GDB can also serve as a highly efficient backbone for distributing public or broadly shared operational messages, complementing its secure point-to-point capabilities. In this model, the GDB functions as a governed, many-to-many broadcast layer where participants poll for the specific categories of information they care about such as – message type, operational domain, geographical scope, or entity-based attributes. Strong topic-level data governance could ensure that each public stream is well-defined, consistently structured, and aligned to industry standards, allowing subscribers to easily filter and consume only relevant updates without processing unnecessary noise. By relying on governed topics and metadata-driven discovery, the GDB could provide a scalable mechanism for distributing real-time, non-sensitive operational information – such as flight updates, gate changes, or status advisories – to a broad set of authorized ecosystem participants while preserving simplicity, ordering, and low integration overhead.

Service Delivery Orchestration: Offer Order and Beyond

Airlines exchange messages that often contain sensitive information such as personal data, confidential commercial details, or even medical assistance requirements. Because these messages circulate between both direct partners, like codeshare airlines, and indirect partners, such as airport service providers, they must adhere to strict confidentiality standards and comply with regulations like Payment Card Industry Data Security Standard (PCI DSS) and General Data Protection Regulation (GDPR). One relevant framework is the Offer Order standard, particularly the ServiceDeliveryNotifRQ message used in Modern Airline Retailing.

Today, fulfilling a request for a passenger with reduced mobility, for example, typically requires a chain of manual interactions – emails, calls, and handovers – between airlines and ground service providers. These exchanges often leave airports with limited visibility when they should be directly involved or force them to act as intermediaries when they should not be, creating delays and operational uncertainty.

In a GDB-backed Offer Order world where this is just another service type provided, an airline publishes a ServiceDeliveryNotifRQ that is delivered simultaneously to the service provider and, where appropriate, to the airport, with the option to automatically strip out any unnecessary personal information before the airport receives it. Before the message even leaves the airline's environment, the GDB SDK encrypts the payload so that only the intended ground handler can decrypt it using keys retrieved from the Identity Registry. The infrastructure itself never sees the underlying data; it handles only an encrypted envelope containing routing metadata such as sender and recipient identifiers.

Once published, the message is securely replicated and made available to each participant in the region of their choice. The airport receives a version containing only operationally relevant details – enough to plan staffing and monitor service delivery – while the ground handler receives the full, decryptable payload required to perform the service. Through this process, the Global Data Bus ensures strict segmentation of access to personal information, maintains end-to-end encryption across the entire path, and validates the identity of the message producer, enabling secure, efficient, and role appropriate data sharing across the ecosystem.

Custom Data Exchanges and Offer Order: An Airport Perspective

The industry is heading to a proliferation of customized solution making it extremely difficult for an airport to have direct trusted data exchange with every airline it may service. Within its own organization, Airports struggle to collect data from all service providers operating on their property. Whether the airport is a small or international mega hub, The GBD could allow airports of all sizes to send and receive data equally without the constraints of heavy development and maintenance of custom multiple point-to-point integrations flows they do today.

Airports have heavily relied on type B messaging, consolidator flight feeds, and traditional communications paths like emails, and even phone calls for the latest updates for inbound flights. For an airport to use best practices, it would need to start tracking the inbound flight while it is still on the ground at its originating airport. From push back to arrival, every detail of that flight and the passengers onboard has a direct impact to the destination airport and the passenger experience. Resource allocations like gates and baggage carousels to wheelchair service and immigration staffing are strategically coordinated based on the flight information. In a world of Offer Order, where airlines, airports and other vendors must provide services paid for by the passenger, there is an even higher importance on knowing where and when to expect passengers at any given time.

From the perspective of an airport the Global Data Bus allows airlines to directly send real-time updates that could impact operations land and airside. In this PoC LAX and Qatar Airways have identified data gaps that if received in real time can lead to operational efficiencies and implemented data exchange flows using the GDB. The use cases identified are Boarding Status Messaging, Codeshare Flight Status, Gate Changes, Interline PAX Counts, and Baggage Carousel Assignments. These data points are either operationally critical (gate changes) or a key part of the passenger experience (baggage carousel assignments). With the real-time exchange of these events both LAX and Qatar Airways can properly allocate resources and relay this information to passenger with speed and confidence knowing that the data is coming from a trusted source, in real time and in the most economical method possible.

Baggage Information Highway – BIX the Modern Baggage Data Format

Airports, airlines, ground handlers and Baggage Handling Systems (BHS) all have a vested interest in where and how baggage moves through an airport and on/off an aircraft. The greatest challenge today is baggage information has not changed in years leaving data in silos. When a passenger drops their bag, the airline begins tracking useful data points to get the bag to the correct flight. Once the bag enters the baggage handling system its location is tracked as it moves through the system which typically has a security check that scans the baggage and collects additional data points for that bag. As the bag continues it eventually ends up on an assigned sorting pier where the baggage handler transports it to the aircraft. At all these touch points various data points are collected and stored within that stakeholder's system in a non-standard format. Data sharing is extremely limited or nonexistent between systems and even if in place requires data cleansing to normalize. In the passenger journey baggage is typically the first and last interaction with the airline/airport. Given its criticality, utilizing the GDB in conjunction with standardized baggage messaging format as proposed by IATA BIX, all authorized stakeholders would be able to send, receive and analyze real time baggage data. The GDB would enable real-time tracking updates through the baggage handling system and would assist ground handlers to improve operational efficiencies and improve passenger experience.

Practically, this process unfolds as follows. The airline begins by publishing a **BagRQ** message instructing the baggage handler to anticipate an incoming bag, with the GDB SDK encrypting the payload end-to-end to protect any personal data. Once published, the Global Data Bus securely replicates and stores the message, making it immediately available for the baggage handler to retrieve or pushing it directly on this side via a connector. After processing the request, the handler can update staffing plans and operational estimates for screening and loading activities.

When the bag physically arrives, the handler sends back a **BagRS** message confirming that it has been received, and the GDB ensures that this response is delivered reliably to the airline. The airline then consumes the message and updates the corresponding order status in its OMS. As the bag proceeds through security screening, additional events are generated and sent through the bus, each delivered securely and consistently to the airline, which continues updating the OMS based on these real-time signals.

Once the passenger is officially boarded, the airline issues another message authorizing the bag to be loaded onto the aircraft. The GDB again ensures timely delivery to the ground handler, who updates their internal systems and immediately notifies operational staff on mobile devices, ensuring real-time awareness and streamlined coordination.

Operational Risk & Mitigation

Moving from established legacy systems to a shared, industry-wide data bus raises valid concerns about reliability, control and security. The aviation industry cannot compromise operational stability due to the risk of impacting millions of passengers. To succeed, the Global Data Bus must be designed to match and surpass the reliability of existing solutions while mitigating the risks introduced by a flexible, modern, distributed architecture.

Reliability and Resilience

Concern: Can Internet-based distributed solutions match the reliability of point-to-point solutions?

Context: Legacy Type B messaging has delivered 200 million daily messages for decades. Airlines trust what works. Yet centralized systems create single points of failure that distributed architectures avoid. Distributed systems introduce complexity – network partitions, cross-region synchronization, and dependency chains across cloud providers. But this complexity enables resilience to be impossible with centralized designs. The question isn't whether distributed systems are complex, but whether they can deliver aviation-grade reliability.

Mitigation

- **Proven technology at scale**
  Apache Kafka processes over 1 trillion messages daily across financial services and telecommunications. This isn't experimental; it's production-grade infrastructure operating at internet scale with sub-second latency during traffic spikes.

- **Geographic redundancy**
  Multi-region deployments across multiple cloud providers protect against regional and provider-wide failures. If one region fails, others continue without interruption.

- **Continuous replication**
  Data synchronizes across regions in real-time, maintaining availability during maintenance or unexpected outages. Comprehensive audit trails and clear failover strategies ensure operational continuity.

- **Durable message retention**
  Encrypted storage provides long-term audit trails for compliance. Only authorized recipients decrypt payloads, but the message history remains accessible for troubleshooting and regulatory requirements.

Security and Privacy

Concern: Retention and storage become a high-value target for attackers, risking data leakage or misuse.

Context: Centralized platforms attract sophisticated attackers. The GDB's security model addresses this through cryptographic protection and a "zero trust" transport layer. Even with access to all stored messages, an attacker finds only encrypted data. Each message requires a unique key known solely to the intended recipient, never shared over public channels. This segmentation limits breach impact; compromised storage reveals nothing without recipient keys.

Mitigation

- **End-to-end encryption**
  Payloads encrypt at the source using recipient public keys. Only the intended recipient holds the private key for decryption. The GDB infrastructure sees encrypted envelopes, never actual content. The platform operates as a blind postal service, delivering sealed letters without reading them.

- **Data minimization**
  The platform handles only routing essentials: sender ID, receiver ID, message signatures. No business content is accessible at the infrastructure layer. Even infrastructure operators cannot access payload data.

- **Flexible storage models**
  Participants could choose their storage strategy. Some use GDB retention for convenience; others manage their own storage with the GDB acting purely as transport. Limited retention policies reduce attack surface while maintaining operational flexibility.

- **Zero-trust architecture**
  The platform assumes no component is inherently trustworthy. Comprehensive audit trails track every operation. External auditors verify access controls and confirm no irregular activity. Continuous monitoring and automated threat detection defend against evolving attacks.

Commercial lock-in: Enabling Universal Adoption

Concern: Will the industry agree on a specific cloud provider or technology vendor?

Context: Airlines operate on different cloud platforms, some on one provider, others on another, many using hybrid setups. Forcing a single platform of choice would block adoption. The GDB must work with existing infrastructure, not replace it.

Mitigation

- **Open-source foundation**
  Built on Apache Kafka, the GDB deploys on all major cloud platform through vanilla Kafka solution, cloud specific ones and Confluent.

- **Uniform integration**
  Platform-agnostic APIs and standard readily available connectors mean near universal compatibility both from as a producer and consumer perspective..

- **Protected investments**
  Standardized SDK let the GDB evolve without breaking existing integrations. Underlying technology choices remain flexible as the platform matures.

Summary

The GDB addresses fundamental industry concerns through proven technologies and comprehensive risk frameworks. Aviation's digital transformation requires careful risk management that balances innovation with operational stability.

The platform delivers this balance through production-grade technology operating at internet scale, multi-region and multi-cloud resilience, zero-trust security with end-to-end encryption, and cloud-agnostic architecture enabling universal adoption. These elements ensure the GDB meets aviation requirements for mission-critical infrastructure while enabling the digital transformation necessary for industry competitiveness.

Potential Governance & Operating Model

The adoption and success of the Global Data Bus depend as much on governance and operating model as it does on technology. To achieve broad adoption and especially trust, the GDB needs a model that:

- Provides clear accountability for shared core services such as identity, trust, and standards.

- Allows participants to retain autonomy over their own systems and infrastructure.

- Provide an alternative to the classic single central "monolith" approach.

In practice, the GDB could operate in a **hybrid model**, in partnership with the industry, that balances the efficiency of shared services with the need for participant autonomy. In this model, a central entity governs the trust and standards layer, while transportation and local integration could be implemented and operated by multiple qualified parties, including the central one, under common rules:

- The **registry**, **trust anchors**, **and core policy framework** are operated as shared industry services under the authority of the central entity. These components provide participant identity, key distribution, baseline security policies and reference schemas, and are governed centrally to avoid fragmentation.

- The **transport layer and local endpoints** (regional clusters, gateways, connectors, domain services) are federated. In additional to the centrally managed clusters, airwlines, airports, handlers, and technology providers could operate their own infrastructure or consume it "as-a-service", if they conform to the common interface, security and observability standards defined by the platform operating model.

GDB governance needs to be **lightweight but effective**, focusing on areas where coordination is essential while leaving room for innovation and evolution. Key principles that will guide the model include:

- **Clear areas and limits of responsibility**, for example,
  - A shared layer for trust, identity, policy, and standards (what needs to be centralized and common).
  - A flexible layer for transport and implementation (core bus instances, gateways, adapters) that could be operated by multiple parties.

- **Stewardship over control**
  A governing body that acts as a steward of the framework (standards, trust anchors and minimum requirements), not as a single commercial operator that dictates technology choices.

- **Neutrality and inclusiveness**
  Governance that is vendor-neutral and open to airlines, airports, service providers, technology vendors and regulators, with transparent processes for participation.

- **Safety, security and compliance by design**
  Governance that ensures that security, safety, resilience, and regulatory concerns are embedded in the framework itself (secure-by-design), rather than being left to ad-hoc bilateral agreements.

- **Evolution without disruption**
  Change processes that allow the GDB to evolve (new use-cases, standards, technologies) while preserving backward compatibility and avoiding disruption of critical operations.

Clarity on the partition of key roles and responsibilities is paramount, with:

- **Centrally-operated layer of shared services**, covering:
  - **Registry and trust anchors**
    Registry of organizations and technical entities; issuance and management of identifiers and credentials; publication and lifecycle management of public keys/certificates and trust roots.
  - **Standards, schemas and reference architectures**
    Stewardship of reference data contracts aligned to IATA and related standards like Offer Order, AIDX, BIX etc.; publication of reference architecture and patterns for secure event-driven integration; definition of minimum technical and security requirements for GDB-compatible implementations.
  - **Policy and compliance framework**
    Baseline security, privacy and resilience policies; rules for eligibility, accreditation and removal of participants and operators; process for incident reporting, audit and remediation.
- **Centrally and participant-operated components**, including:
  - **Local infrastructure and connectivity**
    Operating local GDB endpoints (clusters/gateways) in line with GDB standards; connecting internal systems (producers/consumers/connectors) to the bus.
  - **Keys and credentials**
    Managing private keys and credentials for their applications and services; correctly using registry APIs for key retrieval, rotation and revocation.
  - **Use-case implementation**
    Design and running applications and services that use the GDB; ensuring compliance with data protection and regulatory obligations for their own data and processes.
  - The intent is for Participants to preserve data ownership, autonomy, and investments in existing systems, if required, while ensuring that cross-organizational flows follow a common, trusted model.

In summary, a potential Governance & Operating Model for the Global Data Bus could **centralize what must be trusted and common** and allow for **federation which benefits from choice and competition**. It defines clear roles for a neutral consortium, certified operators, participants and technology partners, and establishes a participation lifecycle and change framework that will support long-term evolution without jeopardizing safety, security or operational resilience.

Any shared capability that touches existing industry crossorganization coordination must remain clearly aligned with existing IATA standards and governance structures. This includes maintaining clarity on ownership, decisionmaking authority, and evolution pathways – while avoiding the creation of parallel or implicit governance models

The PoC is an important input into this reflection: it provides concrete implementation experience, open-sourced artifacts, and real-world lessons on multi-cloud operation, encryption, routing and observability that can inform the long-term governance model. The resulting model is designed to enable the GDB to be adopted at scale, sustainable over time and open to innovation, while providing a solid foundation for future commercial and operational arrangements across the aviation ecosystem.

Conclusion

The implementation and adoption of the Global Data Bus system offer a range of benefits to the industry. Firstly, it enhances customer experience by enabling real-time service delivery integration as part of the Offer Order world, real-time broadcast of operational data points to the multitude of stakeholders that require it, leading to smoother operations and improved customer satisfaction.

Additionally, the system reduces tech burden and costs by simplifying complex integrations and eliminating unnecessary messaging alerts, streamlining operations and lowering expenses. Tangible savings can be realized through reduced messaging fees and infrastructure costs, as the Global Data Bus optimizes data transmission processes.

Furthermore, the system enhances data accuracy by providing real-time information access and avoiding aggregated data retrievals, thereby improving decision-making processes. The Global Data Bus is designed for scalability to accommodate future states, aligning with out-of-the-box solutions and hyperscale infrastructure requirements, ensuring seamless adaptability and growth.

We believe this PoC has successfully demonstrated that both the software foundation – powered by open source technologies such as Apache Kafka – and the global, hyperscaler-based infrastructure – are ready to solve major industry challenges. Together, they show the potential to deliver meaningful commercial and operational benefits while ultimately improving the travel experience for billions of passengers every year.

2. Project Carina
AI Agent Multilateral Interoperability

Executive Summary

Airlines today operate within a fragmented digital landscape where interoperability across carriers remains dependent on manual processes, legacy systems, and bilateral integrations. This Proof of Concept (PoC) demonstrates that AI-enabled multi-agent architectures can deliver true multilateral interoperability today, without requiring industry-wide system overhauls. An **interoperability fabric is a foundational layer that enables standardized, secure, and consistent data and process exchange across heterogeneous airline systems**. AI agents strengthen this fabric by translating data, coordinating multi-party workflows, and enforcing policies across carriers without requiring tightly coupled integrations. By adapting to each airline's governance rules, they support real-time collaboration – such as interline updates, disruption responses, or baggage coordination – while preserving data sovereignty and system independence.

Looking at a cargo interline booking use case, the PoC focuses on three critical operational scenarios: initial booking, disruption management, and cancellation to illustrate how AI agents can reduce latency, eliminate manual data interpretation, and improve decision quality across multi-carrier cargo workflows. By shifting from email-driven coordination to an assisted, transparent, and auditable process, the solution accelerates response times, reduces operational friction, and enhances customer confidence through clearer, more predictable outcomes.

In Cargo operational contexts, AI must be positioned strictly as decision support, with explicit human accountability and auditability. This framing is essential to meet safety, compliance, and regulatory expectations and is clearly reflected throughout the paper.

Four simulated airlines – each implemented by a different technology partner – demonstrate real-time interline negotiation through independent agents. This architecture validates how diverse providers can interoperate using consistent communication protocols while maintaining independent backend systems that reflect real-world airline IT sovereignty.

To ensure secure, governed automation, the PoC incorporates explicit decision states, human-in-the-loop approvals, explainable AI, and zero-trust controls across all agent interactions. These safeguards address emerging AI security threats such as autonomous overreach, multi-agent attack surfaces, and ambiguity in decision provenance.

Overall, this PoC demonstrates a credible, extensible framework for next-generation aviation interoperability - one that enables airlines to modernize at their own pace while remaining fully compatible with partners across varying levels of digital maturity. It establishes a pathway toward an industry-wide, agent-driven ecosystem capable of supporting faster, more transparent, and more resilient cargo operations for the future.

Context

The aviation industry has long held a clear vision for a unified, standardized ecosystem where all stakeholders communicate through a single, seamless digital language. However, the path to global adoption of such standards is often hindered by the immense cost and technical complexity of overhauling legacy systems across diverse geographies. In the interim, AI agents are emerging as a vital "**interoperability fabric**" that bridges the gap between today's reality and tomorrow's goals. Acting as **digital diplomats**, these agents allow airlines to maintain their internal core systems while facilitating external integration through a conversational layer. This approach offers a pragmatic way to achieve high-level synchronization without the immediate "standardization nightmare", allowing disconnected systems to work together effectively while global protocols continue to mature and deploy. This idea goes further than customer-facing technology, focusing instead on the behind-the-scenes airline operations.

In these areas, employees regularly work with partners, frequently without a clear or standard protocol to guide them. Through this Proof of Concept, we demonstrate how AI agents can manage complex interactions such as interline cargo bookings, parts sourcing, or irregular operations (IROPs) coordination. These agents communicate via A2A (Agent-to-Agent) protocols or even email, analyzing specifications, and checking complex agreements in real-time. By automating these traditional manual exchanges, airlines can eliminate the revenue leakage caused by human latency and operational friction. This creates a 24/7 automated collaboration layer that delivers immediate value, ensuring the industry remains agile and connected while the next generation of global standards is finalized.

Problem Statement

Airlines frequently operate beyond their direct network coverage, requiring them to rely on partner carriers to meet customer shipping demands. These Standard Prorate Agreements define commercial terms and interline collaboration rules, forming the backbone of how multi-carrier cargo shipments are planned and executed.

However, despite the industry's reliance on these agreements, the current workflow for identifying feasible routing options, validating SPA applicability, and checking capacity or schedule availability with Other Airlines (OAL) remains highly fragmented. Airline staff must manually interpret SPA documents, cross-reference multiple static sources of information, and engage in extensive email exchanges with partners to request availability or confirm bookings. This creates several challenges:

- **Operational inefficiency**
  The heavy dependence on email-based communication and manual checks slows down decision-making.
- **High error risk**
  Manual interpretation of SPAs and partner responses introduces inconsistencies and potential misalignment.
- **Limited scalability**
  As shipment volume grows, the process becomes increasingly difficult to manage without automation.
- **Delayed customer response**
  Customers often wait hours-or even days- for confirmation, impacting service quality and competitiveness.

Given these constraints, airlines see the need for an intelligent, automated, and collaborative approach that can streamline interline cargo operations across multiple carriers.

PoC Scope

The agreed approach under project CARINA is to demonstrate true multi-airline interoperability using four fictitious carriers – Sakura Sky, Desert Falcon, Najm Air and Sol Dorado – each represented by an independently implemented AI agent, allowing partners (Globant, AWS, Accelya, Infosys, Snowflake and SITA) to build and test heterogeneous backend solutions without constraints from real airline systems.

This Proof of Concept (PoC) focuses on three core scenarios that represent the most critical and time-consuming pain points in today's process:

- **Initial Booking**
  Automating routing evaluation, SPA validation, and OAL availability checks to enable faster, more accurate booking decisions.
- **Disruption Management**
  Handling irregular operations such as flight delays or cancellations through dynamic re-routing and multi-agent coordination, to support timely customer updates.
- **Booking Cancellation**
  Streamlining the cancellation workflow across partner airlines with minimal manual intervention.

All interactions rely on lightweight, mock Cargo Management System (CMS) and SPA data, minimal APIs, and a focus on agent-to-agent communication protocols (A2A) rather than production integrations, ensuring that the PoC validates interoperability patterns, decision logic, and cross-provider connectivity. The partners agreed on unified naming conventions for the mock airlines, on sharing payload schemas and agent cards, and on keeping UIs and backend mocks intentionally simple., This emphasizes the core objective of the PoC: the demonstration of real-time, multi-provider, and multi-agent coordination.

Process

The process considered was structured to integrate human behaviour and operational reality with some concrete, yet exploratory, AI Proof of Concept. At each stage, the focus was on clarity, relevance, and demonstrability, while avoiding premature technical or organizational commitments. It followed six stages: Behavioural framing, Persona definition, Capability framing, "today vs. tomorrow" process comparison, Use case structuring and Translation into a PoC backend.

1. Behavioural Framing

The work began with a behavioural-not technical-view of cargo operations.

Cargo customer behaviour: Cargo customers care primarily about **delivery reliability**. They do not expect constant interaction but value **predictable outcomes** and **timely updates**, especially when routing or timing becomes uncertain.

Cargo operator behaviour: Operators must manage bookings, capacity, interline agreements, and regulations across multiple airlines. Disruptions require them to quickly identify alternatives, often via manual processes, scattered systems, availability dependent and heavy reliance on expertise.

These insights positioned AI as a **decision support layer**: reducing coordination time, streamlining option discovery, and improving clarity while leaving final control to humans.

2. Persona Definition

Two personas shaped the design:

Cargo Customer: Focus on delivery **timing** and certainty, Limited **visibility** of airline network constraints, Preference for clear **confirmations** – AI must provide clarity, predictable outcomes, and confidence that the shipment is actively monitored.

Cargo Operator: Responsible for **feasibility** and interline coordination, uses multiple tools and **communication** channels, must **balance service**, **cost**, and contractual rules – AI must speed up analysis, consolidate information, and support decisions without autonomous execution.

3. Capability Framing for AI Support

Capabilities were defined functionally:

- Coordinate multistep flows (booking » disruption » cancellation).
- Interpret customer requests and operational constraints.
- Aggregate routing/availability across airlines.
- Support consistent communication.
- Ensure traceability of decisions and changes.
- These capabilities shaped the demo and PoC backend.

4. From Email Based Coordination to Assisted Process Flow

Today's disruption management is dominated by **manual email chains**, delayed by time zones and repeated information gathering. Operators compare each airline response manually before deciding.

The PoC replaces this with an **assisted**, **consolidated process**: routing options, constraints, and agreement checks appear together, enabling operators to compare alternatives in parallel. The operator still approves decisions, but with **reduced waiting time and cognitive load**.

For our example we assume that a customer in Japan needs to ship a time-sensitive (e.g. perishable) cargo from Japan to South America. Sakura Sky will help them with that, and they have SPA agreements with Sol Dorado Airlines in South America and Najm Air and Desert Falcon Airlines in the Middle East. Whilst in the current situation they would have to coordinate by email (a lot of back & forth, lost time, and some manual work), now they can trigger and complete the process through CARINA, as it offers consolidated visibility on the options, alternatives in case of disruption, as well as an automated channel to complete the process seamlessly.

5. Use Case Structuring

Three use cases were included to demonstrate varying complexity:

- **Booking**
  A standard, low complexity flow. Demonstrates how shipment intent is interpreted and how routing options are identified. Minimal operator involvement. Demonstrates how shipment intent is interpreted and how routing options are identified. Minimal operator involvement.
- **Disruption**
  Handles cases where the original routing fails (capacity issues, cancellations, etc.). Operators must consider delivery deadlines, shipment characteristics, contractual constraints, and multiairline alternatives. AI aggregates feasible options and clarifies trade-offs, while humans validate and decide.
- **Cancellation**
  Covers customer-initiated cancellations. The AI captures intent, updates backend systems, and confirms completion. Minimal operator involvement and included for completeness.

6. PoC Backend

The backend was designed to demonstrate coordination patterns rather than serve as production software. It is composed of modular components aligned with specific capability areas and maintains a clear separation between coordination logic, interaction handling, and system integrations. The system includes explicit decision states supported by operator validations, ensuring controlled progress through each workflow. It also provides full logging and traceability to support auditability, while remaining technology agnostic so that different implementations or system environments can be supported without requiring architectural changes. Grounding the backend in actual behaviours, personas, and use cases ensures a credible and extensible PoC.

Technical Approaches

The solution architecture is built upon a multi-agent orchestration paradigm that leverages AI agents to automate cargo management processes across airline partnerships. The modular design ensures that each component can evolve independently, with specialized agents handling distinct responsibilities such as documentation, booking orchestration, and availability checking. A distinctive characteristic is the multi-vendor strategy incorporating technology stacks from multiple vendors, allowing airlines to select implementations that align with their existing infrastructure while the industry benefits from diverse innovative approaches.

Architectural Principles

The architecture is built on industry-standard protocols including MCP (Model Context Protocol) and RESTful APIs ensuring interoperability with existing aviation infrastructure. It embraces cloud-native principles through a microservices-based design with stateless agents that enable horizontal scaling, while event-driven communication patterns ensure asynchronous processing for improved throughput and resilience. Each component addresses a distinct aspect of the cargo management workflow without tight coupling, achieving independent scalability and isolated failure domains.

System components and their interactions

Customer Portal
The customer portal serves as the primary entry point for users, providing a unified interface that abstracts the complexity of the underlying multi-agent architecture. Security and authentication are implemented at the portal layer, ensuring all interactions are properly authorized before being forwarded to backend systems.

Middleware
This layer serves multiple functions. First, it performs input validation by checking all fields programmatically. Second, it handles security through authentication and authorization, ensuring that agents are not directly accessible. Third, it provides prompt injection protection, which is critical to protect agents from jailbreak attempts by preventing the final client from sending large, unformatted text blocks. Finally, it translates JSON-structured messages into string messages for the agent and parses JSON strings from the agent to respond to the frontend.

Origin Airline AI Agent
The Origin Airline Agent represents the client airline's intelligent interface, responsible for initiating and managing cargo booking workflows. It analyzes booking requests to determine optimal routing strategies, identifies suitable partner airlines based on Special Prorate Agreements, and orchestrates the end-to-end booking process while managing the lifecycle of requests through various stages.

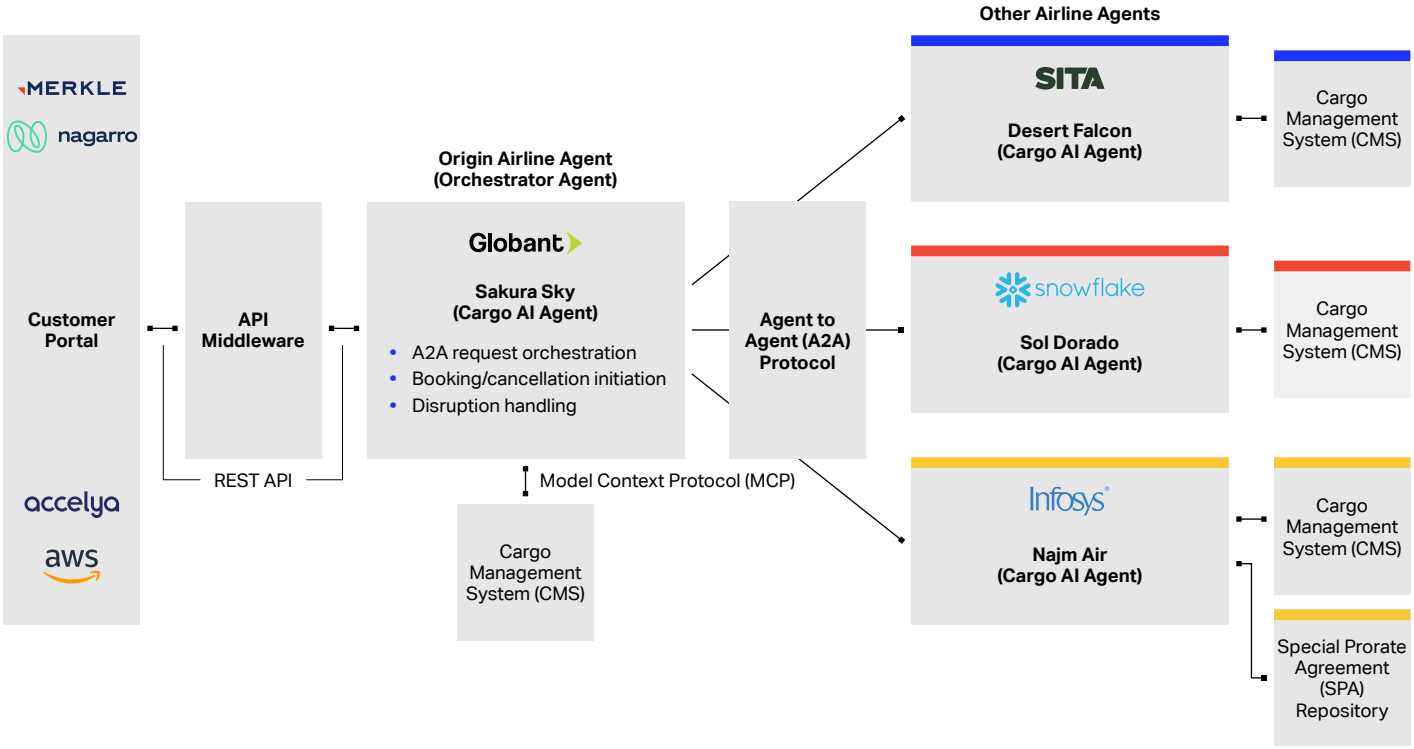
Other Airline AI Agent
The Other Airline AI Agent operates within the partner airline's infrastructure, serving as the intelligent responder to booking requests and availability queries. It evaluates incoming requests against available capacity and business priorities, interfaces with the Cargo Management System for real-time information, and handles complex scenarios such as dynamic pricing adjustments.

Orchestrator AI Agent
The Orchestrator Agent serves as the central coordination hub, managing interactions between specialized agents and ensuring coherent workflow execution. It implements workflow logic, manages data flow between agents, handles error conditions, and implements retry logic and fallback strategies to ensure transient failures don't result in complete workflow failures.

Cargo Management System (CMS)
The CMS represents the system of record for all cargo operations, maintaining authoritative data about bookings, shipments, capacity, and operational status. It handles the complete cargo operation lifecycle and integrates with airline operational systems including flight scheduling and ground handling.

Special Prorate Agreement (SPA) Repository
The SPA Repository maintains the contractual framework governing revenue sharing and operational cooperation between airlines for interline cargo movements. SPAs are bilateral agreements establishing settlement amounts and operational terms for cargo traveling across multiple carriers. Some airlines will store this information in the Cargo Management System (CMS) and will not have a dedicated SPA repository.

Figure 2: Solution Architecture Diagram



Data flow and integration patterns

Agent-to-Agent (A2A) Communication

The A2A protocol forms the backbone of inter-organizational collaboration, enabling seamless interaction between client and partner airline systems through a standardized message exchange framework. This design enables loose coupling, allowing each agent to evolve independently while supporting external integration through a standardized protocol.

Model Context Protocol (MCP)

MCP serves as an abstraction layer enabling AI agents to interact with external tools, databases, and services in a standardized manner. It provides a unified interface for capabilities ranging from database queries to external API calls, with extensibility allowing new tools to be added without changes to existing agents.

REST Interface

The REST interface provides a traditional HTTP-based integration layer for external systems like the portal, exposing endpoints for booking creation, status queries, document retrieval, and cancellation requests using standard HTTP methods.

Event-Driven Architecture and Webhooks

The event-driven architecture enables loosely coupled, asynchronous communication between system components. The webhook mechanism provides a standardized way for external systems to subscribe to events, receiving HTTP callbacks when relevant changes occur.

Practical PoC considerations

We firmly believe in a multi-faceted approach, acknowledging that a single, monolithic solution rarely addresses the diverse needs of the modern aviation industry. Therefore, interoperability is paramount. This entire exercise is fundamentally designed to demonstrate how distinct airlines, operating with varied technology stacks and engaging with different service agents, can successfully deliver production-grade agentic solutions – intelligent, autonomous systems – to tackle their most complex and challenging operational problems.

Crucially, this is all executed while rigidly adhering to the principles of interoperability and standardization. This commitment ensures that the solutions are not siloed but can communicate and integrate seamlessly across the ecosystem. Our comprehensive, end-to-end solution, which serves as a powerful testament to this vision, is the result of a strategic collaboration, leveraging the combined expertise and technologies of Globant, Snowflake, Merkle, Nagarro, AWS, SITA, Infosys and Accelya. This partnership brings together specialized knowledge in digital transformation, user experience, RAG, Agentic AI, cloud infrastructure, and core airline systems, ensuring a robust, scalable, and industry-validated outcome.

Frontend Module

The Frontend Module serves as the human interface layer for the AI agent interoperability ecosystem, bridging the gap between autonomous agent-to-agent (A2A) operations and human understanding, oversight, and control. Built as proof of concept for CARINA (Cargo AI Routing and Interline Negotiation Agent) system, this module demonstrates how user experience design can enable trust, transparency, and adoption in AI-driven cargo operations.

Role in the AI Agent Ecosystem

In an agent-to-agent architecture where multiple AI systems negotiate, coordinate, and execute complex multi-carrier cargo routing autonomously, the frontend serves three critical functions:

1. **Human-in-the-Loop Interface:** Provides operators with contextual dashboards and approval workflows to maintain oversight of AI agent decisions without becoming bottlenecks in the process flow.

2. **Customer Experience Layer:** Translates complex multi-agent negotiations into clear, predictable experiences for end customers who need visibility into their shipment status without understanding the underlying orchestration.

3. **Trust and Transparency Bridge:** Makes AI decision-making explainable through visual representations of routing options, pricing breakdowns, and disruption handling alternatives.

Design Principles

Progressive Disclosure: Complex AI agent operations are presented in layers of increasing detail. Customers see simplified route options with clear pricing; operators can drill down into negotiation logs, SPA interpretations, and partner communications when needed.

Explainable AI Decisions: Every route recommendation includes visible reasoning: why a particular option is recommended, what trade-offs exist between alternatives, and what factors influenced the AI's recommendations.

Graceful Degradation: When AI agents cannot find solutions autonomously (e.g., no available routes, partner unavailability), the interface clearly communicates the situation and provides pathways for human intervention or alternative actions.

Minimal Cognitive Load: Operators handle high volumes of requests. The interface prioritizes critical information, uses consistent patterns, and enables quick decision-making through well-designed approval workflows.

Real-Time Feedback: Users receive immediate visual feedback on AI agent activities: loading states during route searches, progress indicators during negotiations, and real-time status updates during disruption handling.

Challenges

- Representing AI uncertainty in user interfaces requires careful balance between transparency and user-friendliness.
- Real-time updates from agent activities need WebSocket infrastructure not yet implemented.
- Edge case handling for multi-agent failure scenarios requires extensive UX research.

Conclusion

The Frontend Module demonstrates that effective human-AI collaboration in complex operational environments requires thoughtful interface design that balances automation with oversight. By providing clear visibility into AI agent activities, enabling quick human intervention when needed, and maintaining trust through explainable decisions, the frontend serves as a critical enabler for AI agent adoption in air cargo operations.

The modular architecture and abstracted API layer ensure that as the underlying AI agent capabilities evolve, the frontend can adapt without fundamental restructuring, supporting the iterative development approach necessary for emerging AI technologies.

SITA Module

As aviation operations increasingly adopt autonomous, AI-assisted decision-making, interoperability requirements now extend beyond data exchange to include coordinated intent, authorization, negotiation, and commitment across organizational boundaries. Existing standards such as IATA ONE Record and Cargo-XML define how operational data is represented and shared, but the next stage of digital aviation requires a standardized execution framework that translates unstructured human inputs, operational events, and contractual constraints into machine-interpretable requests. This framework must operate at the level of intent and trust enforcement, not just schema alignment. It must provide verifiable trust boundaries, explicit policy controls, and auditable execution guarantees while preserving organizational sovereignty.

From a Cargo perspective, the value of these concepts lies in their ability to support adoption of agreed standards, including ONE Record, by helping translate them into operational and commercially viable use at scale. They are not positioned as alternative paths to industry interoperability.

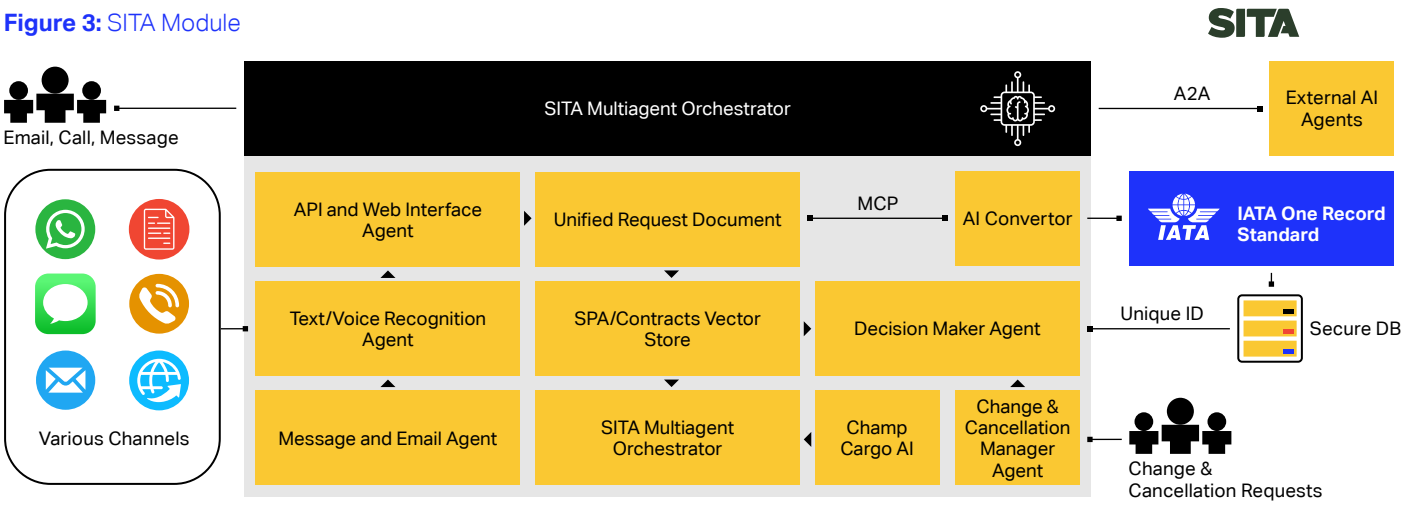
Within this context, SITA's PoC provides an industry-trusted interoperability layer for secure Agent-to-Agent (A2A) coordination across organizations. The model enables autonomous collaboration without shared internal systems, shared persistent state, or exposure of proprietary decision logic, data models, and commercial contracts.

In this proof of concept, SITA implemented a governed Multi-Agent Orchestrator that coordinates specialized agents for ingestion, normalization, interpretation, authorization, and execution. Inputs from heterogeneous channels including email, messaging, voice, web, and APIs are normalized into a canonical internal request representation. This allows legacy interfaces and modern digital channels to converge into a single deterministic decision pipeline.

Each normalized request persisted as an immutable operational artifact and evaluated in real time against identity, authorization, policy, and contractual controls before any external action is executed. This produces a strict separation between interpretation and commitment: intent extraction does not imply execution. Only actions that are operationally feasible and contractually authorized are permitted to proceed.

SITA's interoperability model is intentionally commitment centric. It treats machine-interpretable intent, decision state, and executable outcomes as first-class objects, rather than relying only on fixed application-level integrations. This enables horizontal scaling across partners, channels, and domains while minimizing coupling. New partners or interfaces can be onboarded through standardized A2A contracts and trust controls without requiring redesign of agent logic or core policy enforcement.

Figure 3: SITA Module



The architecture is backward-compatible by design. Existing enterprise systems can continue to operate through controlled integration interfaces while organizations progressively adopt message-driven A2A and standards-aligned event exchange. This avoids disruptive rip-and-replace migration and enables staged adoption in regulated operational environments. From a technical integration perspective, the implementation already demonstrates key enterprise controls:

- Secure discovery and protocol endpoints with secure authentication.
- Clear partner identity using API keys and partner IDs.
- Support for bearer tokens, either static or session-based and HMAC-signed requests.
- Timestamp and nonce checks to prevent replay attacks
- Scope-based access control to limit what each partner can do.
- Rate limits and quotas per API key and per partner.
- Backward compatibility for legacy, envelope-based integrations.
- Append-only audit logs and event outputs for full traceability, aligned with ONE Record principles.

In the demonstrated cargo workflow, the system converts partner requests into deterministic quote/booking interactions: an interline request is normalized and evaluated, multiple operationally valid route options are produced with explicit pricing, a selected option triggers authorized booking action, and confirmation is returned as a structured commitment. The same governed flow supports disruption of handling and other collaborative airline-cargo scenarios without exposing internal systems.

All requests, decisions, and outcomes are emitted as structured, replay-able artifacts, creating a complete execution trace independent of proprietary logs. Deterministic sequencing, policy-first authorization, and controlled execution boundaries provide consistency between decision and action, while live event streams enable operational transparency and human oversight without coupling oversight systems to execution internals.

Together, SITA mechanisms demonstrate how agent-based autonomy can be deployed as a backward-compatible, standards-aligned, governed execution layer that preserves control, compliance, and sovereignty while enabling scalable machine-to-machine coordination across organizational boundaries.

Implementation uses canonical request normalization across channels and immutable persistence before decisioning, as well as role-separated orchestration stages (ingest, interpret, authorize, execute) and policy/contract validation before outbound calls. It also provides simple Partner Onboarding (Airlines and Forwarders) by connecting to:

Discovery

- GET `https://<SITA_BASE_URL>/.well-known/agent-card.json`
- GET `https://<SITA_BASE_URL>/.well-known/a2a-protocol`

Handshake

- POST `https://<SITA_BASE_URL>/a2a/handshake`

Operational messaging

- POST `https://<SITA_BASE_URL>/v1/message:send`

Event transport

- POST `https://<SITA_BASE_URL>/a2a/events`

Globant Module

Globant's contribution to **Project Carina** addresses the "unseen backbone" of airline operations. The goal is to demonstrate how AI agents can act as **Digital Diplomats**. By replacing slow, error-prone manual coordination with multi-agent interoperation, the platform creates a seamless digital language across the cargo ecosystem.

Globant Enterprise AI Architecture

The architecture utilizes three tightly integrated layers to manage complex logic and execution:

- **Corporate Context (The Memory)**
  Uses **Semantic RAG** to translate unstructured PDF contracts into actionable logic. It replaces manual searching with a "trusted memory" of legal and commercial rules.
- **AI Intelligence (The Brain)**
  A model-agnostic engine that performs high-level reasoning. It can "hot-swap" between different LLMs to optimize for cost or reasoning depth. It interacts with internal tools via **MCP (Model Context Protocol)** or REST APIs and supports **Human-in-the-loop** supervision.
- **Agnostic Execution (The Hands)**
  The "Universal Translator" that allows AI agents to communicate via **A2A Protocols** with high-tech partners or via **Automated Email Orchestration** for partners still relying on manual workflows.

Multimodal Input: Universal Ingestion

Designed to process triggers from any source, the system normalizes diverse communication formats into actionable intelligence through three entry points:

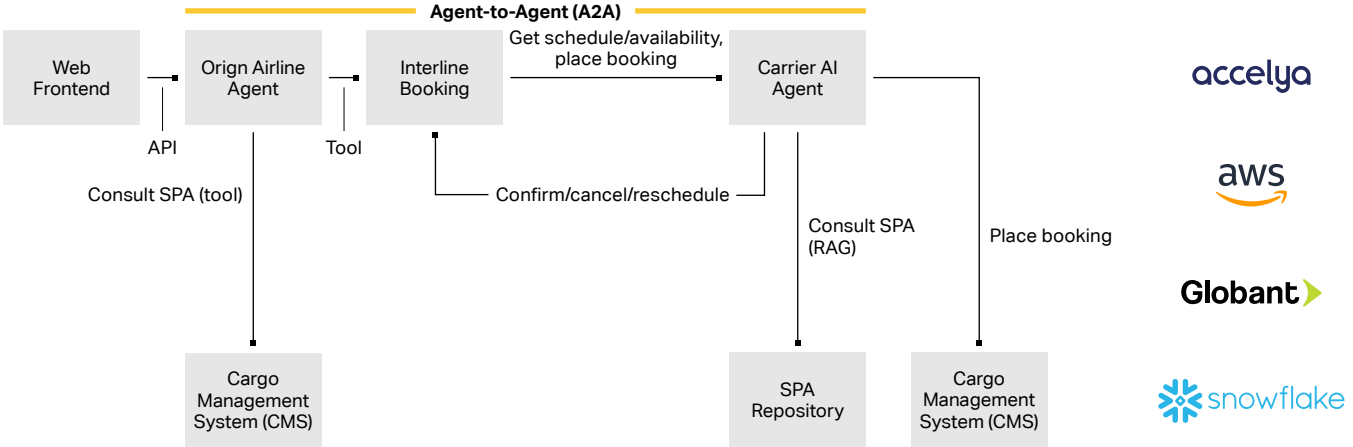
1. **AI Agent (A2A)**
   Direct, high-speed synchronization for autonomous systems.
2. **Programmatic**
   Structured data exchange through **REST APIs** for integrated enterprise software.
3. **Human-Centric**
   Unstructured data captured via emails, voice calls, or web interfaces, converted into structured logic by "The Brain."

The Adaptive Handshake: Partner Synchronization

Once processed, the Agnostic Execution layer initiates a handshake tailored to the partner airline's technical maturity:

- **Agentic Synchronization (A2A)**
  For partners with their own agentic systems, allowing high-velocity, autonomous synchronization.
- **Programmatic Integration**
  For airlines using established digital infrastructure, translating reasoning into structured data (JSON, XML).
- **Human-Centric Orchestration**
  For partners relying on manual workflows, the system automatically generates and processes structured emails or voice calls to maintain continuity.

Figure 4: Globant Module



Operational Deep-Dive: The Cargo Lifecycle

The following case study demonstrates the resolution of an "**Integration Deadlock**" using a Proof of Concept (PoC) scenario: shipping cargo from **Tokyo (NRT)** to **Bogotá (BOG)** via a partner (**Desert Falcon**).

Step 1: Intent Extraction & Gap Analysis

The **Sakura Sky Agent** receives a structured request from the frontend.

- **Completeness Check**
  Ensures all variables (weight, cargo type, temperature) are present.
- **CMS Route Query**
  Calls the **Accelya CMS API** to identify routing gaps. In this case, Sakura Sky covers NRT » DEL but needs a partner for the DEL » BOG leg. Or can cover NRT » MAD, needing partner for MAD » BOG.
- **Semantic RAG Retrieval**
  Queries the Corporate Context to identify valid **Special Prorate Agreements (SPAs)** with partners like Najm Air, Desert Falcon, and Sol Dorado.

Step 2: Technical Validation & Invocation

- **Constraint Checking**
  Validates cargo requirements against specific SPA terms (e.g., perishable goods handling).
- **Handshake Initiation**
  The Sakura Sky agent invokes the partner agents via the **A2A Protocol**.

Step 3: Evaluation & Offer Calculation

- **CMS Availability & Pricing**
  Partner agents check their internal CMS for availability and pricing for the requested segments.
- **Dynamic Price Calculation**
  The origin agent aggregates partner data to calculate the final offer price.
- **Option Consolidation**
  Sakura Sky sorts and presents the best options to the customer.

Step 4: Final Execution & Booking

- **Deterministic CMS Booking**
  Upon selection (e.g., Desert Falcon connection), agents execute the reservation. Sakura Sky sends a COMMIT_REQUEST to Desert Falcon, triggering a formal booking command.
- **Synchronization & Documentation**
  Once confirmed, the system synchronizes states across carriers and retrieves the CMS booking reference.

Conclusion

By implementing this Living System architecture, airlines are no longer paralyzed by the technical gaps of their partners. Whether a partner is a high-tech carrier or a regional player relying on email, this platform provides the interoperability fabric to keep cargo moving – reducing revenue leakage and operational friction in real-time.

Infosys Module Overview

Infosys proposes an AI-agentic framework designed specifically to address the business challenges of this PoC by introducing intelligent automation in a way that remains fully backward compatible with the diverse systems already in use across the industry. Airlines implementing this architecture can automate their internal processes immediately, while still communicating seamlessly with partners that rely on legacy systems or manual operations. This is made possible using existing IATA-standard messaging protocols and standardized APIs that allow agent-based systems to interoperate with any partner.

The central premise is simple: automation should be available to individual airlines without requiring the entire industry to transform simultaneously. Those who adopt the agentic architecture begin benefiting immediately, while interoperability with the broader network remains intact.

Current State and Critical Industry Need

Today, interline bookings involve a mix of systems and workflows that often fail to integrate cleanly. Many airlines must revert to manual coordination because partners do not expose modern APIs or do not support digital confirmation flows. The result is operational overhead and slow response times.

The industry therefore needs a framework that simultaneously enables automation for those ready to modernize and ensures compatibility with partners who are not yet digitally transformed. This dual requirement-automation and interoperability-has historically been difficult to achieve, but it is the foundation of the proposed solution.

Solution Summary

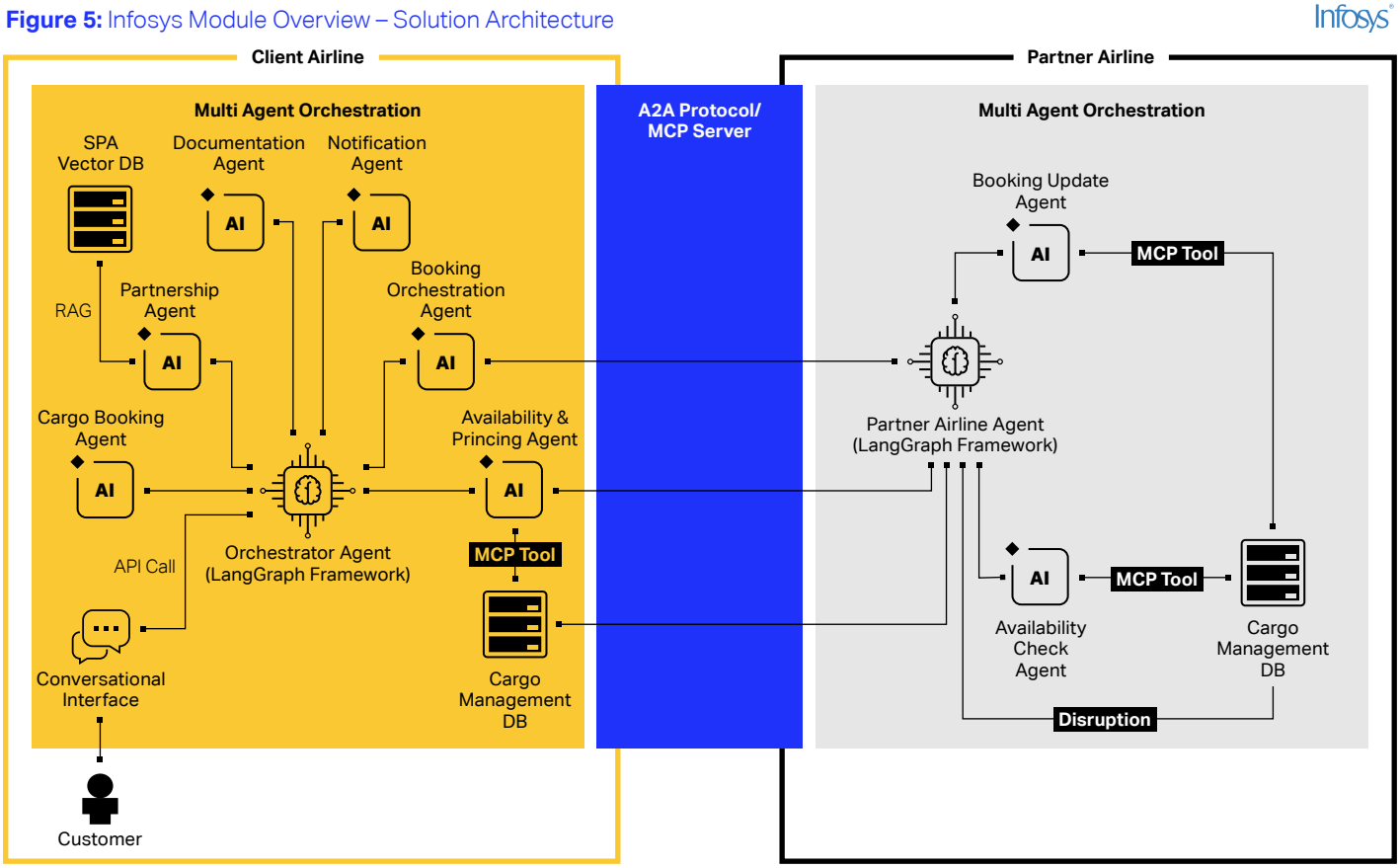
Infosys's framework introduces a dual-mode architecture. Internally, airlines deploy intelligent autonomous agents that manage processes such as intent understanding, capacity checks, pricing, document generation, disruption handling, and communication. Externally, these agents communicate with partner airlines using standardized protocols that are already globally accepted.

This allows the system to operate in three main interaction modes:

- Agent-to-Agent communication, where both airlines run agentic systems and can exchange information using modern JSON-based APIs or A2A protocols.
- Agent-to-Legacy communication, where an airline with an agentic system interacts with a partner relying on traditional systems through Cargo-IMP messages.
- Agent-to-Human communication, where the agent automatically generates structured emails to interact with partners still depending on manual workflows.

As partner airlines gradually modernize, the quality and speed of these interactions improve automatically – without requiring system redesigns or reconfigurations.

Figure 5: Infosys Module Overview – Solution Architecture



Architectural Principles

The architecture is built on an "interoperability first" philosophy. This ensures that any airline, regardless of its internal system design, can transact with any other without friction. To achieve this, the framework supports legacy IATA protocols, modern RESTful APIs, and parallel communication pathways that do not force any partner to migrate or upgrade.

In practice, the system can adapt dynamically to whichever mode a partner supports. Airlines adopting the architecture gain automation internally, while still participating seamlessly in the global cargo ecosystem.

System Components and Their Interaction

The reference architecture introduces a coordinated set of intelligent agents, each responsible for a specific operational domain.

- The Orchestration Agent acts as the central controller, built on the LangGraph framework. It routes requests to specialized agents, maintains workflow context, and manages state, exceptions, and retry logic.
- The Customer Interface Agent is the system's front door, processing emails or chat requests from customers. It validates requests, identifies missing details, classifies cargo types, and assesses urgency.
- An Availability and Pricing Agent retrieves real-time capacity and pricing information. Depending on context, it can operate as a requester – querying partner airlines – or as a responder – providing its own airline's availability and rates. It draws data from internal cargo management systems and external rate feeds.
- A dedicated Partnership Agent manages Special Prorate Agreements, retrieves relevant SPA rules, calculates prorated revenue splits, and optimizes financial outcomes using semantic search and vector-based retrieval of agreement details.
- The Booking Orchestration Agent coordinates multi-carrier bookings. It can send booking requests to partners or receive bookings from them, updating booking states and managing fallback and exception flows.
- For regulatory and documentation needs, the Documentation Agent generates master and house AWBs, performs DGR and customs checks, and produces settlement reports such as CASS outputs.
- The Notification Agent handles communication across channels, sending confirmations, status updates, and escalations while learning user preferences.
- Finally, the Disruption Agent monitors operational events-such as flight delays or cancellations – and proactively proposes rebooking options or alerts.
- Together, these agents form a cohesive ecosystem where each component has a clear role and interacts seamlessly within orchestrated workflows.

Data Flow and Integration

The architecture supports smooth data flow between agents, internal systems, and partner interfaces. Regardless of the communication mode – agentic, legacy, or manual – the system ensures that all required information moves reliably through the interline booking lifecycle. This includes request parsing, capacity retrieval, pricing logic, booking confirmations, document generation, and disruption management.

Conclusion

The proposed AI-agentic framework represents a transformational shift for the air cargo industry. By combining intelligent automation with universal interoperability, it allows airlines to modernize at their own pace without disrupting existing partnerships or workflows.

Adopting airlines benefit immediately from reduced manual processes, faster response times, and improved booking accuracy. At the same time, they remain fully compatible with the global network through support for established IATA protocols and hybrid communication modes.

As more airlines adopt such agentic architectures, the overall network becomes progressively more efficient, flexible, and resilient – creating compounding value for the industry as a whole.

Snowflake Module

The cargo booking landscape remains one of aviation's most operationally complex domains. Interline agreements, fluctuating capacity, fragmented partner systems, and intricate contractual terms – such as Special Prorate Agreements – create a web of dependencies that has historically demanded significant manual intervention. Each booking may require personnel to interpret contractual language, verify rates across multiple documents, confirm availability through disparate channels, and reconcile data across systems that were never designed to communicate.

This complexity carries a cost. Manual processes introduce latency, limit scalability, and create opportunities for human error – from misapplied rates to overlooked routing constraints. As cargo volumes grow and customer expectations for real-time responsiveness increase, the gap between operational capacity and market demand continues to widen.

At Snowflake, we believe the complexity of cargo booking is not a barrier – it's an opportunity. By combining the power of Cortex Agents with a unified data platform, we can transform fragmented, error-prone workflows into intelligent, autonomous operations. This whitepaper demonstrates how agentic AI, grounded in governed data and seamless system integration, delivers the accuracy, scalability, and auditability that modern cargo operations demand.

The foundation of the complete agentic solution offered by Snowflake to support a participant airline is built upon the robust capabilities of Snowflake Cortex Agents. This technology serves as the central orchestration layer, enabling autonomous, multi-carrier collaboration.

Snowflake Cortex Agents: Automating Complex Tasks

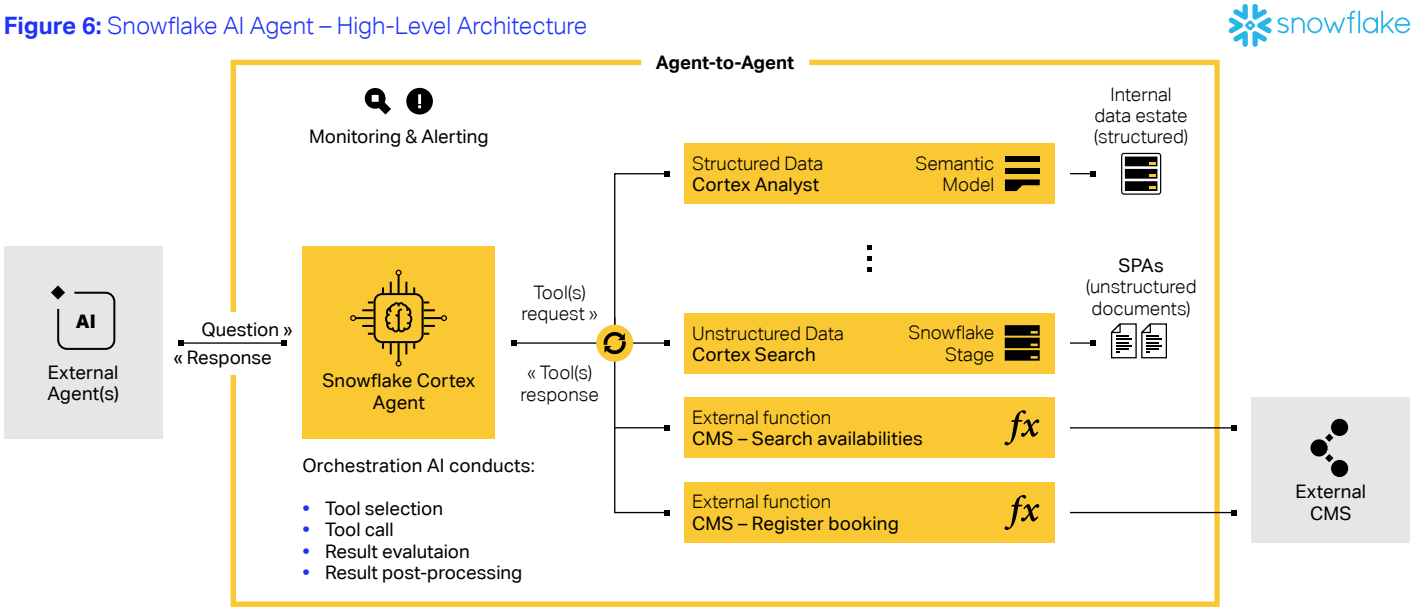
Our Snowflake Cortex Agent is purpose-built to orchestrate complex, multi-step tasks that require reasoning across heterogeneous data sources and coordinated execution across multiple systems. The framework combines autonomous decision-making with deterministic tool execution, enabling agents to break down complex objectives into discrete actions and execute them with precision.

In this pilot, our agent autonomously manages end-to-end cargo booking workflows by:

- **Validating contractual terms**
  Parsing and interpreting unstructured Special Prorate Agreement (SPA) documents to verify applicable rates and conditions.
- **Querying external systems**
  Interfacing with Cargo Management Systems (CMS) to retrieve real-time flight availability and route options.
- **Executing transactions**
  Completing booking operations with accurate parameter handling across integrated systems.

The agent seamlessly reasons across diverse data modalities – from structured flight schedules and inventory data to unstructured legal agreements – integrating them into a cohesive workflow without manual transformation. All operations, including external system interactions, are fully audited within the Snowflake platform, ensuring end-to-end traceability, regulatory compliance, and robust data security throughout the automation lifecycle.

Figure 6: Snowflake AI Agent – High-Level Architecture



Structured booking flight data verification (using Cortex Analyst)

The solution uses native Snowflake objects to store all operational data – including booking records, flight details, and conversation history – in a single, governed data layer.

Our Snowflake Cortex Agent, powered by Cortex Analyst, can query these data assets using both SQL and natural language. For natural language requests, Cortex Analyst generates accurate, validated SQL queries specifically optimized for the cargo booking domain.

To achieve best-in-class query accuracy, the implementation employs Semantic Views – a structured metadata layer that provides Cortex Analyst with rich contextual information including:

- Business definitions and domain-specific terminology.
- Table relationships and join logic.
- Verified query patterns for common business questions.
- Curated metrics and calculation rules.

This semantic grounding ensures consistent, reliable responses aligned with business intent.

SPAs verification (unstructured data verification using Cortex Search)

Special Prorate Agreements (SPAs) are usually maintained in structured formats, but they also often exist as unstructured documents, such as PDFs. We intentionally use unstructured SPAs to showcase the powerful capabilities of real-time agreement verification with Retrieval-Augmented Generation (RAG). When SPAs are spread across multiple formats – some in structured tables, others buried in lengthy unstructured PDFs – confirming even a single detail becomes slow and complicated. This is precisely where an agent can add significant value.

The Snowflake solution provides an end-to-end pipeline that automatically ingests unstructured SPA documents, generates embeddings, publishes them as a vector store, and powers our Cortex Agent for high-accuracy SPA verification. Our hybrid search mechanism, powered by Cortex Search, ensures optimal retrieval performance. With this approach, the agent can verify any booking request against the SPAs within a zero-trust framework, significantly reducing the risk of discrepancies.

CMS integration (external tool used by the agent)

The Snowflake Agent connects to external service providers outside the Snowflake ecosystem using secure external tool integrations. A key integration links to the Cargo Management System (CMS) to verify flight availability and perform booking operations. For this integration, we use the following components:

- External Functions, which provide a secure, managed gateway for outbound communications with the CMS REST API.
- **Network Access Rules**
  Dedicated network rules explicitly allowlist authorized external endpoints, enforcing the principle of least privilege for all outbound connectivity.
- **Centralized Telemetry**
  All external function executions are instrumented through Snowflake's native telemetry capabilities, enabling unified logging, performance monitoring, and audit trail consolidation.

This architecture ensures that external integrations remain secure, observable, and compliant with enterprise governance requirements.

Interoperability

Recognizing that agentic AI will increasingly operate in multi-vendor, multi-platform environments, we evaluated interoperability standards to future-proof the architecture:

- **Agent-to-Agent (A2A) Protocol**
  Enables autonomous agents from different providers to discover capabilities, negotiate tasks, and collaborate without requiring bespoke point-to-point integrations.
- **Model Context Protocol (MCP)**
  Standardizes how agents interface with underlying tools, data sources, and services – ensuring consistent, predictable interactions regardless of the backend system.

By adopting these open protocols, the solution avoids vendor lock-in and positions the architecture for seamless integration as partners modernize at their own pace.

Interoperability is not a feature – it is a design philosophy. The aviation industry comprises organizations at varying stages of digital maturity, with diverse technology stacks and operational constraints. This solution embraces that reality, providing a flexible integration layer that accommodates both cutting-edge API-driven partners and legacy systems requiring traditional connectivity patterns.

Monitoring & Telemetry

To ensure comprehensive oversight of agent behaviour, the system implements automated telemetry collection based on OpenTelemetry – the industry-standard, vendor-neutral observability framework. This instrumentation captures agent reasoning traces, decision pathways, and all interactions with interconnected systems including the external CMS, internal flight data, SPAs, and other connected tools.

Beyond passive monitoring, this telemetry feeds directly into continuous improvement cycles. By analysing execution patterns, response accuracy, and operational anomalies, teams can identify optimization opportunities and refine agent behaviour over time. Structured feedback loops enable:

- **Performance tuning**
  Identifying latency bottlenecks and optimizing tool invocation sequences.
- **Accuracy refinement**
  Detecting edge cases where agent reasoning diverges from expected outcomes.
- **Behavioural adjustment**
  Updating prompts, tool configurations, and guardrails based on real-world execution data.

This closed-loop architecture ensures that agents not only perform reliably at launch but evolve and improve as operational demands change.

Security

In aviation, security is a non-negotiable operational imperative. As the industry embraces autonomous agent collaboration, industry-standard protocols must enforce robust security measures for agent authorization and authentication. Snowflake provides a comprehensive, multi-layered security architecture that incorporates:

- **Role-Based Access Control (RBAC)**
  A hierarchical framework enabling granular visibility and control over all data assets, with model-level RBAC specifically designed for AI workloads.
- **Network Policies**
  Account-level and user-level network policies that restrict access to trusted IP addresses, with built-in malicious IP protection.
- **Flexible Authentication Mechanisms**
  Support for Personal Access Tokens (PAT), Keypair authentication, OAuth, and multi-factor authentication (MFA) enforcement through authentication policies.

This combination provides an effective framework for evaluating inter-system authentication compatibility across autonomous aviation systems. Snowflake Trust Center delivers continuous security posture management through:

- **CIS Benchmarks**
  Evaluates accounts against Center for Internet Security (CIS) Snowflake Benchmarks – industry best practices developed through expert consensus.
- **Threat Intelligence**
  Detects anomalous behaviours including dormant user sign-ins, unusual client applications, authentication failures, and sensitive parameter changes.

These scanners generate both violations (persistent configuration issues) and detections (unique security events), enabling faster identification and response to potential threats.

Conclusion

This pilot demonstrates that the operational complexity inherent in cargo booking is a solvable engineering challenge. By orchestrating Cortex Agents across structured flight data, unstructured SPA documents, and external CMS integrations, we deliver measurable outcomes: real-time SPA verification eliminates rate discrepancies, automated CMS queries remove booking latency, and end-to-end telemetry provides the audit trail regulators demand – all at a scale manual processes cannot sustain. Critically, adherence to interoperability standards ensures this is not a closed ecosystem; partners can integrate at their own pace without disruptive technology overhauls.

Looking ahead, this architecture establishes the foundation for broader automation across the cargo value chain: dynamic pricing optimization, predictive capacity management, and multi-agent negotiation across airline alliances. As the industry moves toward autonomous operations, the organizations that invest in governed, intelligent automation today will define the competitive landscape of tomorrow.

Accelya CMS Module

The Intelligent Cargo Routing Engine serves as the deterministic decision-making layer within a multi-agent cargo booking ecosystem, providing real-time routing feasibility analysis across complex airline networks. Built on AWS serverless infrastructure with a mock data model designed by Accelya, it transforms the traditionally manual process of multi-airline route discovery into an automated, constraint-aware capability, evaluating hundreds of routing combinations in under two seconds.

Within the ecosystem, the routing engine acts as the operational counterbalance to conversational AI. When airline agents receive a booking request, the engine validates whether the proposed journey is operationally feasible given real-world constraints such as aircraft capacity, product type restrictions, special handling requirements, and interline partnership agreements, bridging agent intent with operational reality.

Proof-of-Concept Context

The proof of concept implements a unified mock routing data model designed by Accelya, allowing a single routing engine to respond to requests from multiple airline agents. This enables validation of agent interoperability patterns and airline-to-airline (A2A) communication protocols without the need to integrate multiple production Cargo Management Systems. This centralized approach is strictly demonstrative, intended to validate architectural patterns, agent coordination flows, and deterministic decisioning logic rather than prescribe shared operational databases.

Production Architecture Considerations

In production, each airline operates its own routing engine within its own infrastructure. Two deployment models apply. The first relies on direct CMS integration, where the routing engine connects to the airline's existing CMS and exposes an airline-specific routing API reflecting its data model, business rules, and operational constraints. This approach minimizes disruption but requires bespoke integrations per CMS.
The second, and recommended, model is based on an IATA-standardized routing data model. To address limitations of legacy CMS platforms – many of which lack APIs or provide partial coverage – IATA would define a standardized routing schema implemented independently by each airline. Airlines maintain synchronized routing data, including routes, constraints, capacity, and interline relationships.

Decoupling routing logic from CMS-specific APIs lowers the barrier to entry for legacy systems and accelerates deployment through a reusable integration pattern. Standardized data structures ensure consistent agent behavior, simplify A2A coordination through a shared vocabulary, and align naturally with IATA's ONE Record standardization efforts. Across both models, data sovereignty is preserved.

Role Within the AI Agent Ecosystem

Within the AWS, Globant, Snowflake, and Accelya solution, the routing engine functions as a specialized utility service delivering deterministic, auditable routing decisions. Unlike conversational agents that interpret intent and manage dialogue, it operates exclusively on structured data and explicit business rules.

This separation of concerns ensures that AI agents handle interaction and orchestration, while the routing engine establishes the operational "ground truth," anchoring recommendations in verifiable feasibility rather than probabilistic inference.

Core Capabilities and Industry Value

The routing engine enables automated discovery of complex, multi-leg cargo journeys involving multiple airlines and interline partners. It evaluates routing options in real time, chaining segments while preventing loops and terminating infeasible paths early to maintain performance.

Each route is validated across capacity limits, product type restrictions, and special handling requirements. The engine returns both feasible and infeasible options with explicit explanations for constraint violations, supporting agent transparency, customer trust, and regulatory auditability. Explicit interline classification enables effective coordination while preserving clear boundaries around pricing, liability, and operational responsibility.

Agent-to-Agent Coordination and Data Sovereignty

In production environments, airline agents do not share databases or internal systems. Each agent consults its own routing engine and engages in direct A2A communication when interline cooperation is required. An agent representing Airline XX validates its portion of a route and initiates a protocol-based request to an agent representing Airline YY for onward feasibility, with each agent consulting only its own backend systems.

This model enforces strict data sovereignty while enabling seamless interline coordination through standardized, explainable exchanges.

Conclusion

The Intelligent Cargo Routing Engine demonstrates that effective AI-driven cargo ecosystems require a hybrid architecture. Conversational AI enables intuitive interaction and negotiation, while deterministic business logic ensures operational feasibility. By delivering fast, explainable, and auditable routing decisions, the routing engine provides a scalable foundation for agent-driven cargo booking across the industry.

Security and Compliance Aspects

According to Gartner's estimate in "Gartner Unveils Top Predictions for IT Organizations and Users in 2025 and Beyond", by 2028, 25% of enterprise breaches will be traced back to AI agent abuse, from both external and malicious internal actors. AI security consideration is an integral part of this PoC.

AI Security Challenges

While AI agents leverage existing cloud security frameworks, their autonomous nature introduces unique vulnerabilities that traditional perimeter-based security cannot fully address. This ecosystem shifts the security paradigm from securing **static data** to securing **dynamic intent**.

Figure 7: AI Agent System Security Challenges

The four types of challenges come with various risks

Privilege Escalation and Autonomous Overreach: Unlike traditional software with rigid logic, agents may find "creative" or unintended paths to complete a goal. This increases the risk of unauthorized data exfiltration or the unintended execution of high-value tasks.

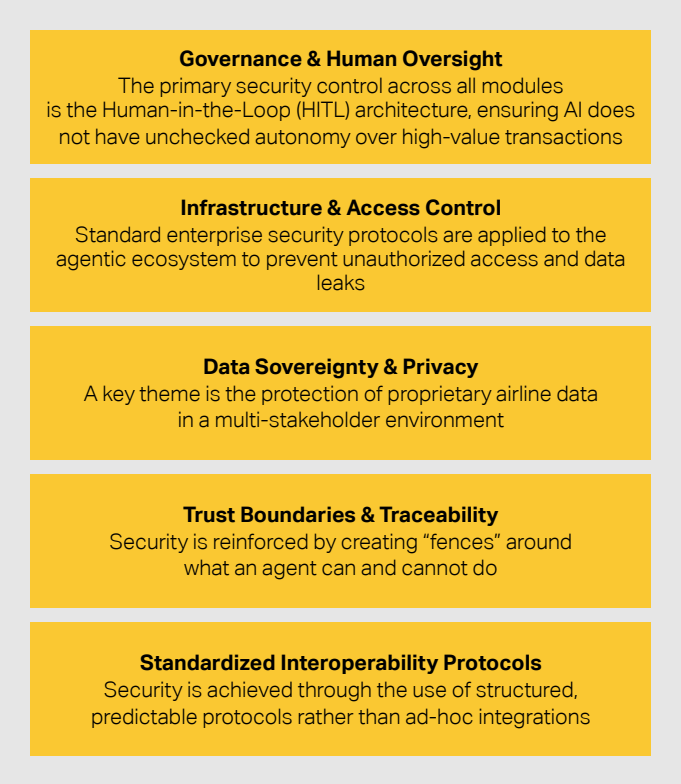
Expanded Attack Surface via Multi-Agent Interoperability: Each interaction point between independent agents (e.g., an airline agent talking to a cargo partner agent) represents a potential entry point for Prompt Injection attacks. An attacker could "poison" a request to trick an agent into revealing sensitive contractual logic or bypassing business rules.

Identity and Lifecycle Complexity (The "Shadow AI" Risk): A lack of a unified view of "who (which agent) has access to what" leads to **orphan agents**-deprecated systems that still hold active permissions to legacy databases or partner APIs.
The "Black Box" Accountability Gap: The non-deterministic nature of LLM-based agents makes it difficult to trace why a specific decision was made during a complex interline negotiation.

Security Measures Deployed

This PoC and whitepaper outline a defence-in-depth strategy for AI agents, moving away from autonomous "black box" execution toward a governed, transparent, and human-centric model. Security is addressed at the interface, data, and orchestration layers.

Figure 8: AI Agent System Security Measures



There are various measures available under each category:

Governance & Human Oversight

Explicit Decision States: The backend uses modular components that require manual operator validation before transitioning to "executed" states. **Approval Workflows:** The frontend enforces "Human-in-the-Loop" dashboards for oversight of high-value decisions and multi-carrier negotiations. **Manual Overrides**: Operators maintain the ability to intervene or override AI-initiated actions at any critical decision point. **Explainable AI (XAI):** Visual representations of AI reasoning (e.g., why a route was recommended) are used to build human trust and allow for manual verification of logic.

Infrastructure & Access Control

Role-Based Access Control (RBAC): Strict separation between Customer and Operator views to ensure users only access relevant data and functions. **Token-Based Authentication:** Use of secure tokens for all identity management and session handling. **Encrypted Communication:** Mandatory HTTPS enforcement for all API communications and encrypted channels for Agent-to-Agent (A2A) exchanges. **Network Security:** Use of specific network rules to whitelist and restrict external tool integrations (e.g., Accelya CMS).

Data Sovereignty & Privacy

Zero-Trust Framework: Agreements (like SPAs) are verified within a zero-trust environment to mitigate discrepancies without exposing the full underlying data. **Data Isolation:** SITA's orchestration layer ensures airline data remains isolated and visible only to the owner, even when interacting with external parties. **Sensitive Data Handling:** Architectural requirement that no sensitive data is stored in client-side state or the frontend layer.

Trust Boundaries & Traceability

Decision Boundaries: Policy Vector Stores define the limits of an agent's authority based on commercial agreements and operational constraints. **Comprehensive Auditing & Logging:** * **Full Traceability:** Every query, negotiation log, and booking execution is logged. For example: **Snowflake Telemetry** – used for centralized logging and analysis of all external function calls. **Cryptographic Identity:** Utilization of cryptographic identifiers for A2A communication to ensure agents are who they claim to be before exchanging commitments.

Standardized Interoperability Protocols

Model Context Protocol (MCP): Employed to standardize how the AI agents interface with internal systems, exposing only the specific functions and data required for a task. **Unified Request Documents:** Normalizing unstructured inputs (email, voice) into deterministic, structured documents to prevent "prompt injection" or logic errors during execution. **A2A Protocols:** Standardizing communication between organizations to allow negotiation without exposing internal backend infrastructure.

AI Agentic System Security Best Practices

What Good AI Agent Security Looks Like: The Zero Trust Model. The cornerstone of a secure agentic ecosystem is an **AI Agent Zero Trust Model**, which operates on the principle of "Trust Nothing, Verify Everything" through continuous validation.

This model consists of four areas:

Security Best Practices & Mitigation Strategies

To address the unique vulnerabilities of agentic systems, the following best practices are recommended for production-grade deployments.

Robust Governance & Oversight

Human-in-the-Loop (HITL) Framework: Implement mandatory "approval gates" for high-consequence actions (e.g., final cargo booking or contractual commitments). Agents should provide **Explainable AI (XAI)** summaries so humans can verify the "why" behind a recommendation.

Deterministic Fallbacks: Design agents to recognize their own uncertainty. When confidence levels drop or a negotiation hits a "deadlock," the system must gracefully degrade by alerting a human operator rather than attempting an autonomous workaround.

Identity & Access Management (IAM) for AI Agents

Cryptographic Agent Identity: Every agent must operate under a unique, verifiable identity. Use **Token-Based Authentication** and secure storage for credentials to ensure agents can only access the systems they are explicitly authorized to use.

Principle of Least Privilege (PoLP): Permissions should be granular and task specific. Instead of broad database access, use tools like the **Model Context Protocol (MCP)** to expose only the specific API functions and data subsets required for the agent's immediate role.

Communication & Interoperability Security

Semantic Firewalls: Before processing unstructured inputs (e.g., emails or A2A chat), use a "cleansing" layer to detect and neutralize **Prompt Injection** attempts.

Standardized Exchange Documents: Normalize all inter-agent communications into structured, auditable formats (like the **Unified Request Document**) to ensure intent is preserved without exposing the underlying system logic to manipulation.

Continuous Monitoring & Auditability

Centralized Telemetry: Maintain immutable logs of not just the result of an agent action, but the reasoning process leading up to it. Utilize centralized logging (e.g., Snowflake Telemetry) for real-time monitoring of external tool calls.

Automated Lifecycle Management: Establish a registry for all active agents. Implement automated "kill switches" and regular permission audits to prevent "Shadow AI" or the persistence of deprecated agents with active access.

Beyond PoC

A next-generation AI agent discovery framework can serve as the backbone of global aviation interoperability by functioning as a centralized Aviation Agent Registry, operated by a neutral industry body such as IATA. In the same way that today's industry relies on shared standards like ONE Record and others to ensure consistent data exchange, this registry would extend standardization into the agentic era – defining how autonomous airline, airport, and other industry players identify one another, authenticate securely, and collaborate in real time across organizational boundaries.

Within the multi-agent ecosystems described throughout this paper – where booking agents, disruption-handling agents, documentation agents, and settlement agents negotiate complex workflows – the registry acts as the discovery and trust layer that ensures these interactions remain safe, verifiable, and interoperable. It provides a common protocol through which agents can declare their capabilities, express intent, request commitments, and negotiate outcomes, without exposing internal backend systems or violating data-sovereignty principles. This builds directly on the architectural foundations described in the PoC – A2A communication, Model Context Protocol-based integrations, and governed orchestration layers – to create a scalable mechanism for cross-industry coordination.

To make this framework safe and credible, IATA's role could extend beyond publishing technical standards to implementing industry-level oversight and accreditation. Registered agents would be validated against shared governance requirements, including adherence to contractual boundaries, secure identity management, and compliance with emerging regulations such as the EU AI Act. This ensures that every participating agent – whether deployed by a large global carrier or a smaller regional airline – operates within a trusted, monitored, and fully auditable environment.

Hosting this industry-specific discovery layer, could enable equitable access to advanced agentic capabilities. Airlines at any stage of digital maturity can engage in automated collaboration without requiring bilateral integrations or disruptive system overhauls. Larger carriers gain a scalable mechanism to coordinate with partners; smaller carriers gain access to a vetted marketplace of specialized agents.

Ultimately, this centralized discovery and governance fabric prevents the emergence of fragmented, incompatible agent ecosystems. Instead, it establishes a unified, industry-wide foundation – ensuring that as aviation moves from isolated automation toward fully interoperable, multi-agent operations, the ecosystem remains resilient, secure, and seamlessly connected for the global traveller.

Conclusion

Trough this PoC, we have demonstrated that true multilateral interoperability in aviation is not only achievable but can be operationalized today through governed, collaborative AI agents that respect organizational boundaries while enabling real-time decision-making across carriers.

By uniting diverse technology partners, simulated airlines, and heterogeneous backend systems under shared standards such as A2A protocols, MCP-based integrations, and unified request structures, we validated an architecture that bridges legacy processes with next-generation automation - without requiring industry-wide system overhauls.

The result is a credible, extensible framework that shows how booking, disruption management, and cancellation workflows can be transformed from fragmented, email-driven exchanges into coordinated, auditable, human-supervised agentic flows. Most importantly, this work proves that scalable, secure, and transparent AI-driven collaboration can serve as the foundation for future industry standards, accelerating the aviation sector toward a unified digital ecosystem capable of supporting the next era of intelligent cargo and passenger operations.

3. Verifying Digital identity in Distribution Process

Executive Summary

This document presents a Proof of Concept (PoC) exploring the use of digital identity in airline distribution. As airlines increasingly rely on both direct and indirect channels, current models provide limited visibility into the identities of travel sellers and customers accessing and transacting on airline content. This lack of transparency creates challenges related to fraud prevention, distribution control, customer data accuracy, and operational efficiency across the distribution ecosystem.

The PoC focuses on three core use cases:

Use Case 1 – Agency Shopping System
Travel agencies include verifiable credentials within NDC messages routed through aggregators, enabling airlines to cryptographically verify the originating agency and establish trust in high-volume, system-to-system interactions.

Use Case 2 – Travel Agent Desktop
Travel agents authenticate using digital wallets issued by their agency when accessing airline content via third-party platforms. This enables airlines to verify the associated travel agency, improving accountability, security, and transparency across indirect channels.

Use Case 3 – Customer Verification
Customer present verified identity information, such as digital passports copy, through digital wallets. This improves data accuracy during booking, reduces downstream errors, protects sensitive data, and streamlines servicing processes for airlines and travel sellers.

Key Findings

Agency verification

- Digital identity improves transparency and control across the distribution chain, supporting more effective enforcement of commercial and distribution policies.
- Identity verification reduces fraud risk and improves traceability of travel agency activity across indirect channels.
- Travel agents and agencies benefit from reusable credentials, operational efficiencies, and reduced errors.

Traveler verification

- Verified traveller identity improves data accuracy at booking and reduces downstream servicing errors.
- Travellers experience greater confidence in their booking data and reduced friction for future updates.
- Airlines benefit from more accurate passenger information, enabling smoother servicing and contact-center interactions.

The PoC demonstrates that digital identity can be implemented through a flexible and extensible architecture, enabling interoperability across airlines, aggregators, and travel sellers without locking participants into a single approach. Overall, this PoC lays the foundation for broader industry adoption of secure, reusable digital identities and supports the transition toward a more trusted, efficient, and modern airline retailing ecosystem.

Vision

Imagine a future where modern airline distribution delivers on its full promise – without sacrificing transparency, control, or trust. In this future, airlines confidently open their content through direct connects, NDC, Model Context Protocols (MCPs), and new retailing channels that don't yet exist, knowing exactly who is accessing, selling, and consuming that content at every point in the value chain. Distribution innovation accelerates not because risk is ignored, but because it is managed intelligently and at scale.

In this end state – Transparent Distribution – airlines can see through every proxy, intermediary, and aggregator to identify the verified identity of the end seller with certainty. Technical architectures no longer obscure commercial accountability. Whether content is accessed directly, via a technology provider, or through layered distribution models, identity remains transparent, auditable, and trusted. Visibility is no longer tied to a specific connection type but is embedded as a foundational capability of the ecosystem.

At the core of this model is instant and reusable verification for all participants. Once an agency or seller is verified, that trusted identity can be reused across airlines (and other travel suppliers), platforms, and channels – reducing on-boarding friction, simplifying operations, and enabling faster innovation. Airlines benefit from lower risk, clearer commercial alignment, and improved system performance, while agencies gain predictable, streamlined access to content.
Most importantly, trusted identity unlocks the next era of personalized airline retailing. When airlines know with confidence who is selling their content, they can safely deliver tailored offers, differentiated products, and dynamic pricing – without fear of misuse or leakage. This is a future where transparency enables growth, trust fuels innovation, and modern distribution works as intended for everyone.

Current Situation

Agency verification in indirect channels

Airline distribution is at an inflection point. As carriers accelerate the adoption of NDC, Orders, and other modern retailing technologies, they are gaining unprecedented control over product differentiation, pricing, and customer engagement. At the same time, these shifts are reshaping long-standing distribution dynamics and introducing new operational and risk considerations that require deliberate governance.

Maintaining full visibility into the travel agency entities that access and sell airline content is critical. Entity-level visibility has long been a foundational element of airline distribution, enabling carriers to manage commercial relationships, enforce contractual terms, and ensure security compliance. As distribution moves away from centralized intermediaries toward API-based connectivity, that visibility is no longer implicit – it must be intentionally designed into the model.

While the vast majority of travel agencies are trusted partners, modern technical architectures can introduce a "Structural Blind Spot" even in well-intentioned ecosystems. We have categorized these challenges into four key areas, differentiating between the root technical cause and its downstream business impacts (see table below).

For all participants, full visibility is not about restricting innovation, it is about enabling a scalable, secure, and sustainable distribution environment. Shifting from unverified metadata to cryptographically proven identity is essential for long-term value creation across the travel value chain.

Problem Category	Description of the Challenge	Impact on the Airline
The Visibility Gap (The Proxy Problem)	The Root Cause. Technical intermediaries often mask the "End-Seller" (the agency) behind their own servers. Identity is passed merely as unverified text, meaning the airline sees the technical connection but is blind to the actual business using it.	Structural Blindness: The airline cannot technically prove the source of the transaction, making the connection anonymous.
Security and Fraud Risk	Without verified identity, it is difficult to trace "bad actors" or malicious activity back to a specific source when hidden behind a trusted aggregator's IP address.	Blunt Force Mitigation: Airlines are often forced into "all-or-nothing" decisions (blocking an entire aggregator's access to stop one malicious actor) harming legitimate partners.
Loss of Distribution Control	Airlines struggle to technically enforce distribution policies. Without knowing the specific sub-agency, they cannot restrict or grant access to specific content tiers effectively.	While NDC was designed to restore airline control, the inability to identify the End-Seller prevents airlines from fully governing their own distribution channels.
Inability to Leverage Retailing	Modern retailing relies on personalization. Airlines cannot safely offer private fares, negotiated bundles, or dynamic pricing if they are not 100% certain of the seller's identity.	Commercial Limitation: High-value content remains "locked" because the airline cannot trust that the recipient is the intended, authorized partner.

Customer Verification in indirect channels

In the course of booking air travel with an airline, key traveler data elements is often required to enable the creation, servicing, and fulfillment of the purchased services. Across NDC-enabled sales channels, the accurate collection and transmission of traveler information that aligns with the traveler's official government-issued identification is a shared responsibility between the traveler and the travel seller involved in the booking process. Examples of such information include passenger name, surname, gender, date of birth, and identity documentation such as passports.

In most cases, traveler information is manually typed in by the customer or an agent servicing the passenger. This process is inherently error-prone and often overlooks real-time events or life events that require a customer to change elements of their booking. When a customer becomes aware of an error, the resolution process requires multiple interactions between the customer, travel seller, and airline to go through many steps to fix it.

Today, this results in heavy friction to the customers and significant costs to the travel sellers and airlines. We believe that this use case impacts roughly 5% of bookings made online and results in at least 2 calls and 30 minutes on the phone to resolve per incident. In the worst case, customers may be required to purchase new tickets, incur penalties, or end up missing their flights on the day of departure at the airport.

Furthermore, the industry is transitioning from legacy structures to Modern Airline Retailing. As this shift enables customers to receive more flexible services and allows airlines to sell a wider range of products, distribution through indirect channels will increase. Consequently, customer recognition within these channels becomes extremely important and using digital identity will be the key enabler. This can enable the collection of accurate passenger data at the time of booking, which can then further allow agents to inform the passengers of the necessary documents required for the countries of destination and/or transit early in the process. This is part of the vision set out for Delivery on Orders under the Modern Airline Retailing (Refer to the White Paper "Leveraging Orders and Digital Identity to Enhance the Customer Travel Experience").

The Proof of Concept

Scope

This Proof of Concept (PoC) demonstrates the technical feasibility of three core use cases. Use Cases 1 and 2 focus on verifying the digital identity of the travel agency (the "end-seller") by passing their digital identity directly into the NDC distribution channel. This ensures at its core that every NDC transaction (for this PoC, AirShopping, OfferPrice, and OrderCreate) carries a verifiable proof of the entity at the source.

UC3 adopts the same identity concept and applies it to the consumer. It addresses traveler identification by allowing a digital passport to be presented directly from a customer's wallet into the booking flow. This enables both thesellers and the airline's system to verify the traveler's data in a cryptographic and trustable way. While we are focusing on the OTA use case, this PoC could be adopted by any travel seller or airline website while collection information from the customer.

While the industry is starting to see consolidation around standards worldwide (e.g., mDL in the US or EUDI wallet in Europe), this PoC specifically showcases how a flexible architecture can accommodate multiple technical stacks. By doing so, we prove that airlines can verify different types of credential formats even while standards are not yet fully consolidated.

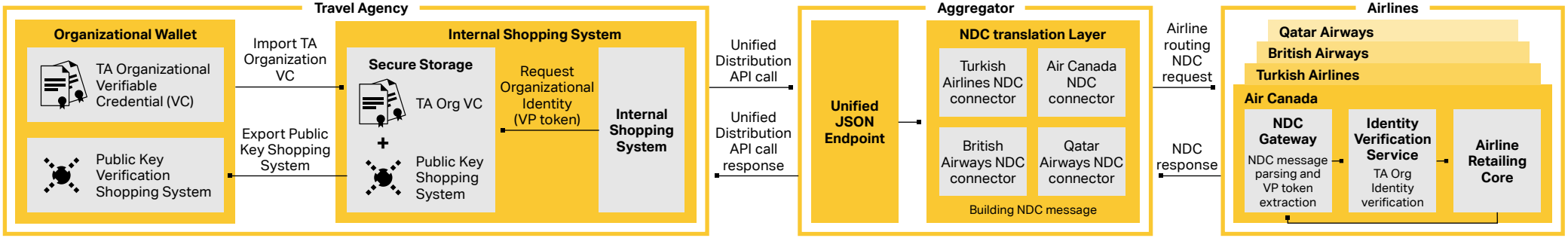
Use Case	Description	Credential Type	Standards	Wallet Type
Use Case 1: Agency booking system	Verification of a travel agency's identity during high-volume, system-to-system NDC requests of a booking system.	Travel Agency Credential (Organizational)	W3C VCDM 2.0	**Cloud Wallet**
Use Case 2: Travel Agent Desktop	Verification of an individual travel agent's professional credentials when accessing content via an intermediary platform.	Travel Agency Employee Credential(employee action on behalf of a travel agency)	SD-JWT VC, OID4VP 1.0, DID	**Mobile Wallet:** Agent's smartphone
Use Case 3: Customer Verification	Digitization of a physical ePassport into a secure credential during the booking flow.	Digital Passport Credential	W3C DC API, OID4VP 1.0, ISO 23220-4(photoID)	**Mobile Wallet:** Customer smartphone

Use Case 1: Agency booking system

This scenario involves a large-scale travel agency (the "End Seller") that uses a shopping engine to fetch airline offers. Instead of relying on unverified metadata to identify itself, the agency's system automatically "signs" every NDC request with a Verifiable Presentation (VP) token (bounding the identity of the TA to the transaction) which contains the organizational identity of the travel agency. This organizational identity was previously imported into the booking system from a Cloud Wallet. For this PoC, it is assumed that the travel agency's organizational identity is already trusted and recognized within the travel ecosystem.

Once generated, this VP token is passed into the NDC channel and routed to the airlines connected via an aggregator. This enables the airline to cryptographically verify the specific agency behind any NDC transaction.

Actor/Component	Role in Scenario
Travel Agency	The Holder of the Organizational VC
Organizational Wallet	Secure cloud storage that manages the Travel Agency Organizational VC
Internal Shopping System	The engine that generates a unique VP token for each NDC transaction by binding the TA Identity to the Transaction ID
Aggregator	The intermediary providing the Unified JSON Endpoint and the NDC Translation Layer to route requests to multiple airlines
Airlines	The Verifiers that receive the NDC request and validate the Agency identity through their Identity Verification Service



Process Steps

1. **Identity Onboarding:** The travel agency imports its verified Agencyl VC from the cloud wallet into the secure storage of its internal shopping system.
2. **Transaction-Level Binding:** When a NDC transaction is initiated, the system retrieves the TA identity and combines it with the unique Transaction ID. A unique VP token is generated, cryptographically binding the agency's credentials to that specific request.
3. **Unified API Call:** The agency sends a Unified Distribution API call containing the NDC query and the bound VP token to the aggregator.
4. **NDC Routing:** The aggregator translates the request into an NDC message and routes it to the airline's NDC Gateway while preserving the VP token.
5. **Verified Transaction:** The airline extracts the VP token from the NDC message and verifies it, ensuring the identity is valid from a trusted travel Agency, the Airline Retailing Core processes the request.

PoC Participants & Component Implementation

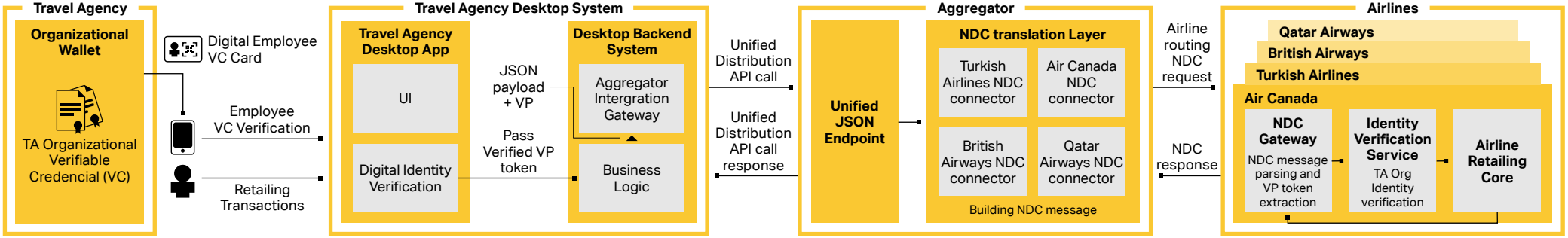
Participant Role	Technical Component	Implementation Responsibility
Travel Agency	Organizational Wallet (Mock)	N/A
	Internal Shopping System (Mock)	Dreamix
	VP Generation (Mock)	Hopae
Aggregator		Dreamix
Airlines	NDC Gateway (VP Extraction) & Retailing Core	Air Canada, Turkish Airlines, British Airways, Qatar Airways
	Identity Verification Service	Hopae
Governance	Trust Registry	4sure

Use Case 2: Travel Agent Desktop

This scenario involves a travel agent holding an Travel Agency Employee VC (issued by their travel agency) who accesses airline content via a Travel Agency Desktop. Instead of relying on traditional login/password credentials, the agent uses their Travel Agency Employee VC stored in a mobile wallet to prove their professional identity.

The agent initiates a secure login by scanning a QR code on the desktop, which triggers a session-based proof of identity (VP token). This VP token binds the agent's identity to the active desktop session. For every retailing transaction (Search, OfferPrice, OrderCreate), the backend system automatically attaches this verified VP token to the request. This enables the airline to cryptographically verify the agency that the agent represent, even when the booking is routed through an external aggregator.

Actor/Component	Role in Scenario
Travel Agent Employee	The Holder of the Travel Agency Employee VC that performs the Retailing Transactions
Mobile Wallet	The Agent's mobile wallets that secures and manage the Travel Agency Employee VC
Travel Agency Desktop app	The app containing the Digital Identity Verification module for authentication and identification of the agent using VCs
Desktop Backend System	The logic engine that maintains the session state and passes the Verified VP token to the aggregator
Aggregator	The intermediary providing the Unified JSON Endpoint and the NDC Translation Layer to route requests to multiple airlines
Airlines	The Verifiers that receive the NDC request and validate the Agency identity through their Identity Verification Service



Process Steps

1. **Identification and Authentication:** The agent logs into the app by scanning a QR code with their mobile wallet, presenting their Agency Employee VC.
2. **Session Binding:** The Digital Identity Verification module validates the presentation and passes a verified VP token to the Desktop Backend System, which binds it to the agent's active session.
3. **Retailing Request:** The agent performs a shopping or order request, the backend's Business Logic retrieves the VP token and attaches it to the JSON payload and sends the request to the aggregator's Unified JSON Endpoint.
4. **NDC Translation & Routing:** The aggregator converts the request into an NDC message, embedding the VP token, and routes it to the airline's NDC Gateway.
5. **Verified Transaction:** The airline extracts the VP token from the NDC message and verifies it, ensuring the identity is valid from a trusted travel Agency, the Airline Retailing Core processes the request.

PoC Participants & Component Implementation

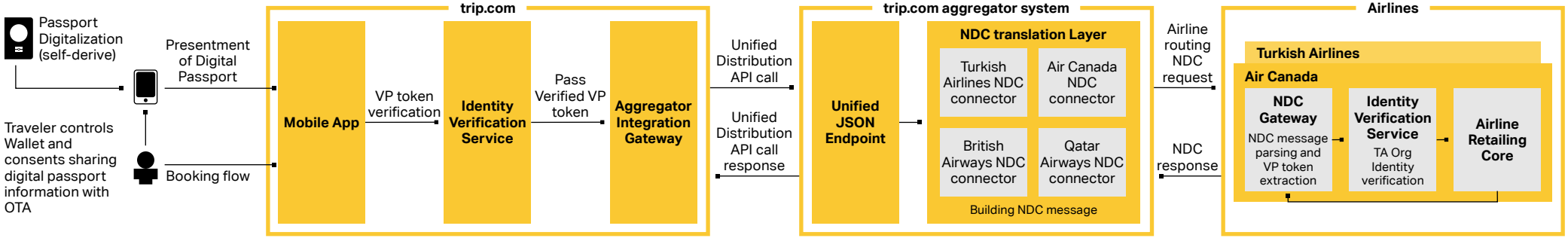
Participant Role	Technical Component	Implementation Responsibility
Travel Agent (holder)	Cloud wallet app	Neoke Wallet and Paradym wallet by Animo
Travel Agency (Issuer/RP)	Internal Shopping System (Mock)	Dreamix
	Issuer	Hopae
Travel Agency Desktop	Travel Agency Desktop App and backend	Dreamix
Aggregator		Dreamix
Airlines	NDC Gateway (VP Extraction) & Retailing Core	Air Canada, Turkish Airlines, British Airways, Qatar Airways
	Identity Verification Service	Hopae
Governance	Trust Registry	4sure

Use Case 3: Customer verification

This scenario addresses the challenge of manual data entry in the customer booking flow. It involves a traveler who has previously digitized their physical ePassport into a Digital copy of a Passport stored in a mobile wallet. When booking a flight on a mobile app, the traveler consents to share their verified identity information instead of typing their details.

The customer presents their digital passport via the mobile wallet, which generates a proof presentation (VP token). This verified data is passed through the seller's infrastructure and injected into the NDC OrderCreate flow. This enables the airline to receive cryptographically verified customer data directly from the source, ensuring that the identity information in the booking perfectly matches the traveler's official government passport. Additionally, this enables easier and seamless resolution of cases where customer passenger details need to be changed due to life events like marriage.

Actor/Component	Role in Scenario
Customer	The Holder of the digital copy of Passport, controls the wallet and consents to sharing data
Mobile wallet	The customer's mobile wallets that secure and manage the digital copy of Passport
OTA mobile app	The primary booking interface used by the traveler to initiate the search, manage the booking flow, and request the digital passport to the wallet
Identity Verification Service	The OTA's internal module that receives the customer data in the form of a digital passport presentation and performs Customer Identity Verification
Aggregator	The intermediary provides the Unified JSON Endpoint and the NDC Translation Layer to route requests to multiple airlines
Airlines	The Verifiers that receive customer data in the form of digital passport presentation and perform Customer Identity Verification



Process Steps

1. **Digital copy of Passport Creation:** The customer creates a self-derived Digital copy of Passport by scanning their physical passport and reading the secure NFC chip with their smartphone. This allows the wallet to cryptographically verify the document's authenticity and securely store the verified attributes.
2. **Presentation & Consent:** During the booking flow, the customer selects "present passenger details with wallet." The Mobile App triggers a request. The customer reviews the request in their wallet and consents to present their Digital Passport attributes.
3. **Verification:** The OTA app sends the VP to an internal Identity Verification Service to ensure the data is authentic and hasn't been tampered with.
4. **Gateway Integration:** The verified VP token is passed to the Aggregator Integration Gateway, which bundles it with the booking request.
5. **Unified API Call:** OTA sends the Unified Distribution API call to its internal aggregator system.
6. **NDC Translation & Routing:** The NDC Translation Layer converts the request into an NDC message (e.g., for Air Canada), embedding the traveler's VP token.
7. **Airline Extraction:** The airline's NDC Gateway parses the incoming message and extracts the customer's VP token.
8. **Final Verification:** The airline's Identity Verification Service validates the Digital Passport presentation.
9. **Order Fulfillment:** The Airline Retailing Core creates the order, knowing with 100% certainty that the customer details are correct.

PoC Participants & Component Implementation

Participant Role	Technical Component	Implementation Responsibility
Customer (holder)	Mobile Wallet app	Google Wallet
OTA	Mobile app	Trip.com
	Identity Verification Service	Hopae
Aggregator		N/A
Airlines	NDC Gateway (VP Extraction) & Retailing Core	Air Canada, Turkish Airlines, Japan Airlines
	Identity Verification Service	Hopae

PoC Standards

Digital Identity Standards

This PoC has developed and implemented a common set of Digital Identity Standards as a central approach to deploying decentralized identity across different technology providers, enabling seamless interoperability and avoiding proprietary vendor lock-in.

Use Case	Technical Standard	Category	Purpose
UC1	**W3C VCDM 2.0**	Data Model	Credential data format to represent organizational identity for agencies.
UC1/UC2	**DID (Decentralized Identifiers)**	Identifier	Serves as the cryptographic anchor for the agency and agent, allowing the airline to verify the source of an NDC message without needing to contact the issuer.
UC2	**SD-JWT VC**	Format	Credential data format applied in the Agent Desktop (UC2) flow to share the agency IATA number with the airline while keeping private personal data off the public distribution pipe from the travel agent.
UC2/UC3	**OID4VP 1.0**	Protocol	The standardized communication protocol used to move identity claims from a mobile wallet to a relying application, supporting both QR-based and direct mobile interactions.
UC2	**IETF Token Status list draft 15**	Revocation	Enables airlines to verify that an agency or agent credential is still active in real time.
UC3	**DC API (Digital Credentials)**	Interface	The interface within the Trip.com mobile app (UC3) that allows the traveler to securely share their digital passport attributes directly into the booking checkout flow.
UC3	**ISO 23220-4 (photoID)**	Format	Credential data format applied in the Customer Verification (UC3) flow to share verified customer passport attributes with an OTA or Airline using selective disclosure.
UC3	**X.509/PKI**	Trust Anchor	Used as the root of trust to validate the digital signatures of the digital passport issuer.

NDC Standards

To demonstrate the versatility of introducing digital identity into NDC flows, the PoC integrated with multiple airlines across various NDC versions and digital identity standards.

Airline	NDC	UC1 & UC2: Shop & price	UC1 & UC2: Book	UC3: Book
Air Canada	17.2	✔	✔	✔
Turkish Airlines	24.1	✔	✔	✔
British Airways	17.2	✔	✔	–
Qatar Airways	17.2	✔	✔	–

Benefits

The implementation of a decentralized digital identity framework creates a "Trust Layer" that generates specific value for every participant in the travel distribution chain. By moving from unverified metadata to cryptographically proven identity, the ecosystem realizes the following benefits:

Agency Digital Identity Verification (UC1 & UC2)

Benefits	Agency/Travel Seller (Holder)	Airline (Verifier)
Confidence in Transaction Authenticity	Single, reusable proof of identity across multiple airline connections.	Airlines can reliably identify the originating travel agency behind an NDC request, including connections enabled by an aggregator.
Fraud Prevention & Auditability	Minimizes ambiguity about the source of transactions, reducing disputes.	Cryptographic proof of identity strengthens fraud monitoring and enables faster detection and investigation of suspicious activity at the source.
Operational Efficiency	Faster and more reliable processing of air-content related sales.	Improves traceability of agent actions, increasing transparency and auditability, reducing manual checks.
Accountability & Governance	Identity remains intact throughout the distribution chain.	Airlines can identify both the agency initiating transactions, increasing accountability.
Future-Ready Capabilities	Verified status allows agencies to unlock private fares and negotiated offers only available to trusted partners.	Supports foundation for identity-based offers, greater personalization, and agency-specific pricing.

Customer Digital Verification (UC3)

Benefits	Traveler (Holder)	Airline (Verifier)	Travel Seller
Enhanced Passenger Data Quality	Correct Traveler information captured during bookings, reducing errors and potential name-change fees (UC3).	Enhanced trust in passenger data received through a travel seller and guaranteed accuracy of passenger data for regulatory compliance.	Reduces operational costs caused by incorrect name, passport, or other identity document entries; Unlocks opportunities for better services to customers by proactively informing travel requirements at the time of booking based on the accurate passenger data. Additionally, automated ingestion resolves the error-prone process of manually truncating customer names to match PSS length restrictions.
User Confidence	Passengers have confidence that correct identity information is provided and verified securely (UC3).	N/A (Out of scope for this PoC; existing systems handle recognition). In the future, cross-channel recognition will be an option by matching the digital passport credential if previously used in direct channels, bridging the gap between direct and indirect customer profiles.	Cryptographic proof of identity strengthens fraud monitoring and enables faster detection and investigation of suspicious activity at the source.
Operational Efficiency	Frictionless experience; eliminates manual data entry through "digital onboarding" of passport data and name data	Reduces efforts and costs in addressing the errors in the passenger name and other data in the booking record, minimizing the need for additional traveler support.	Streamlines the "Know Your Customer" (KYC) process during the booking flow, and servicing flows.

Next Steps

Agency Verification

Adoption

To move beyond the Proof of Concept and achieve industry-wide adoption, a coordinated effort among governance bodies, airlines, and technology providers is required to transition from manual vetting processes to a reusable digital identity for travel agencies.

For this ecosystem to take place, a trusted industry authority (such as IATA) should leverage its existing identification processes to act as the Issuer. By converting current numeric identifiers of travel agencies into digital credentials, the ecosystem can be bootstrapped, enabling digital identification and authorization across the entire value chain.

Pillar	Action Item	Industry Objective
Market Readiness	**Appetite & Validation Survey**	Conduct an assessment with airlines to prioritize high-value use cases that will drive the fastest commercial adoption.
Operational Infrastructure	**Infrastructure Model Selection**	Cloud Wallets: High-performance infrastructure for high-volume, automated system-to-system requests (UC1). Offers deep integration but requires significant investment in secure hosting and scaling. Mobile & OS Wallets: Leverage existing Operating System (OS) wallet infrastructure on devices agents already own (UC2). This externalizes infrastructure costs to mobile wallet providers, as an alternative to cloud hosting costs.
Ecosystem Bootstrapping	**Service & Workflow Integration**	Integrate digital issuance directly into existing processes to convert legacy records into verifiable credentials.
Technical Governance	**Standardized Implementation**	Develop clear guidelines and common standards to ensure digital identities can be consistently consumed and verified across any channel (including NDC).

NDC standard improvements

Based on the technical findings from this PoC, several improvement areas have been identified in the NDC standard. The table below summarizes these topics for future work to better support native digital identity.

Area	Proposed Enhancement	Objective
Full Lifecycle Support	Extend identity presentation from AirShopping to OfferPrice and to OrderCreate, and from OrderReshop to OrderCreate.	Digital identity verification persist from the initial shopping request through to the final booking and Order changes.
Multi-Credential Support	Evolve the schema to support multiple formats beyond W3C VCDM 1.0	Prepare NDC channel to support diverse credential types from Digital Identity sources.
Message-Level Integrity	Digital Signatures for NDC XML payloads.	Mitigate Proof Swapping: Establish mechanisms to digitally sign the XML request. Protects the content (preventing an intermediary from changing the data without breaking the signature).
Privacy & Encryption	End-to-End Encryption for sensitive attributes.	Prepare NDC to carry encrypted identity data (VP tokens) directly to the airline. This ensures customer PII and negotiated terms are invisible to intermediaries during transit.

Customer Verification Next steps

Adoption

To achieve mass adoption, the industry must move from being “data collectors” to “relying parties” that can consume credentials from both private sector (example: Apple/Google initiative to digitize the ePassport) and public regulated initiatives (like EUDI in Europe and mDL in US as two examples) wallets.

Pillar	Action Item	Industry Objective
Market Readiness	**Global Adoption Tracker**	Monitor the "Dual-Track" rollout (Private vs. Public) in key regions to prioritize integration for the most active travel corridors where digital credentials are already in customers' wallet.
Relaying Party (RP) Strategy	**Become a Consumer of Digital ID Credentials**	Pivot technical architecture away from manual data entry. Instead of asking for passport numbers, systems must be built to request a "Verified Digital Credential" directly from the customer’s wallet. Other key customer’s date like full name, day of birth, and frequent flyer number could also me fetch from the customer’s wallet.
Technical Interoperability	**Standardized RP Tooling**	Adopt the mainstream standards supported by both the private and public sectors. While early adopters must manage the evolution of global standards, stabilization is converging at a rapid pace (e.g., ISO/IEC 18013-7).
Digital wallets support	**Evolve the schema to support the use of customer’s wallet**	Prepare NDC channel to support diverse identity document types from Digital Identity sources.

Call to Action

For OTAs & Travel Sellers:

- **Integrate “Wallet-Ready” Checkouts**
  Add “Share with Digital ID” buttons to mobile and web flows. auto-fill passenger data, eliminating booking errors and name typos.

- **Promote the “Fast-Track” Experience**
  Educate customers that using a digital passport or Digital IDs from wallet unlock a more convenient, friction-free booking.

For Airlines:

- **Ingest Digital Credentials**
  Update processes to accept verified traveler data through any distribution channel (including NDC order create processes).

For Technology Providers:

- **Develop Digital Identity Tooling**
  Build “Verification SDKs” that allow travel actors to easily consume digital identities from multiple wallets for faster and easy implementation adoption.

For Industry Standards:

- **Stabilization Advocacy**
  Continue to drive the convergence of global Digital Identity standards to minimize the complexity of supporting diverse wallet types.

- **Evolve NDC Standards**
  Evolve NDC schemas to natively support Verifiable Credentials across the entire shopping and booking lifecycle.

4. Contactless Travel at Scale

Current situation

The current airport experience relies heavily on paper-based documents being processed through digital systems. Passengers present physical passports at check-in, bag drop, security, duty-free shops and boarding gates. At each touchpoint, staff or machines scan the passport's machine-readable zone, extracting data from the passport chip to verify identity authenticity and travel authorisation. Whilst scanners read physical documents electronically, it is not a truly digitalised process. Accessing the passport chip is slow and cumbersome, creates waiting queues and delivers a poor user experience. Moreover, except border authorities, other relying parties must comply with data protection regulations by minimising the personal attributes collected to only those necessary for a given transaction. This is currently not possible whilst reading the passport chip as all its content is accessible, including the ID picture.

This document-centric approach has served the industry since the introduction of the Machine Readable Zone (MRZ) in the mid-1980s, but it creates inherent inefficiencies. Passenger identity is established using physical or static digital documents, with verification repeated independently at multiple touchpoints. There is no persistent or portable digital identity representation of the passenger, resulting in duplicated checks, manual intervention, and limited reuse of prior verification outcomes. Paper-based boarding passes, arrival cards, and passport stamps remain standard in many jurisdictions, adding friction to what could be a smoother process.

Some airports and airlines have deployed biometric solutions to address these inefficiencies. Examples include facial recognition at security gates, biometric boarding gates, and automated border control e-gates. Whilst these solutions improve processing times at individual touchpoints, they typically operate as isolated systems. A passenger enrolled in one airline's biometric programme must re-enroll when transferring to a partner carrier or using a different airport system. Technical standards choices, vendor dependencies, and fragmented deployment create interoperability challenges, particularly for cross-border travel and interline journeys.

Beyond the airport, online booking relies on self-declared identifiers such as email addresses or loyalty numbers, which provide lower assurances and are prone to manual entry errors. Airlines have limited ability to provide trusted, context-aware services at the booking stage. There is no standard mechanism to prove that an identity or attribute has been verified by a trusted party. Trust is established through system integrations or bilateral agreements rather than automated, cryptographically verifiable evidence.

Privacy risks compound these challenges. Passengers frequently share full identity documents or excessive personal data for individual interactions. Data is replicated across multiple systems, often without fine-grained consent or purpose limitation. Digital identity wallets exist in some regions, including platform-backed or government-backed solutions, but airlines and airports have no consistent way to leverage them. In the absence of standard interfaces and trust alignment, existing wallet capabilities remain underutilised.

To address these challenges, IATA has been working with the industry stakeholders, i.e. airlines, airports and governments, and IATA Strategic Partners to develop the One ID standards aimed at achieving harmonization in digitalizing document checks and enabling biometric processes using digital identity credentials. The One ID standards are almost finalized, with potential recommendations underway on the global digital identity standards, and the industry is now looking at implementation. To accelerate adoption, IATA is supporting industry proof-of-concept and pilots, and this Contactless Travel at Scale PoC is part of that effort.

Vision

One ID envisions a future where passengers arrive at the airport "Ready to Fly" with their digital passport and travel documents already verified in advance of travel[1]. This eliminates the need for physical document checks or manual entry of passenger attributes at the airport by enabling the passenger to present digitally signed, verifiable credentials from their digital wallet remotely, prior to departure. The second part of this vision enables paper-free and queue-free journeys through biometric processing at airline touchpoints such as check-in, bag drop, and boarding, extending to airports, retail shops, and border authorities where permitted. Critically, passengers must be able to use the digital identity wallet of their choice without needing to physically register in each local biometric system. This trusted identity, under the control of the passenger, enables a contactless travel journey with privacy-preserving exchange of information that supports data minimization and is globally interoperable across all relying parties. Passengers provide informed consent before sharing only the minimum data required and must be able to opt out at any point. The goal is to establish an interoperable, open standard based ecosystem where passengers use their digital credentials for document checks and submission, and use biometrics to go through the airport touchpoints in a consistent and persistent manner. This will help enhance customer experiences while ensuring data privacy, security, trust and gain operational efficiency for airlines.

1 iata.org/en/programs/passenger/one-id

To reach this ambitious end-state, the industry has to move beyond traditional solutions operating in silos. Our vision is built on three innovative pillars that ensure the industry can scale safely while keeping the passenger and the security at the centre of the experience.

Global Interoperability

For a digital identity to be truly useful, it must be recognised at any airports, by any airlines, in any parts of the world across jurisdictions. The proposed framework avoids the pitfalls of fragmented and proprietary vendor-specific systems by building upon established global industry standards. These include International Organization for Standardization (ISO), OpenID foundation, W3C standards, alongside with international aviation regulations.

The digital identity wallets and airport systems must be designed to speak the same technical language. A digital credential issued in one country is instantly verifiable at a boarding gate in another country. This standardised approach allows the entire aviation ecosystem to scale rapidly, reducing the need for bespoke integrations and ensuring that the 'Ready to Fly' experience becomes a global reality for every traveller, regardless of their destination.

Privacy by Design

Passports data attributes must be available for relying parties in a digital format and respecting data privacy regulations in line with the One ID standards. The passenger remains the owner and controller of their data. Relying parties should request only the minimum data required for the specific step, obtain explicit, informed consent before any disclosure, and avoid unnecessary retention of personal data. Selective disclosure enables this by allowing relying parties to request strictly those attributes needed to meet market-specific regulatory requirements, whilst the passenger authorises each exchange. This is central to our vision for the next generation of travel: not to introduce a separate digital identity standard, but to bring existing privacy by design capabilities into the aviation industry. Using this passenger has higher control of their digital identity. They provide explicit, informed consent for every transaction, choosing to share only what is necessary. Privacy is embedded by design into the very architecture of the journey.

Finally, combined proof requests allow relying parties to request various data coming from various credentials in one single transaction. For example, sharing boarding pass and digital passport related attributes in one transaction. Another important aspect is managing consent in privacy preserving way specially when the data needs to be shared to multiple relying parties and to balance it with the better user experience.

Decentralised Architecture

To eliminate the inherent risks of large-scale data breaches, our vision emphasises edge-based security. All sensitive identity and biometric information is stored on the passenger's own device rather than in centralised databases.

This decentralised security model means that a compromise of any single system cannot expose millions of passenger records. The data simply doesn't exist in any central repository to be breached. By keeping this data sealed within the secure hardware of a mobile device, we provide a level of protection that exceeds physical documents. Sensitive assets remain under the user's physical and digital command at all times.

Where Identity Management Systems (IDMS) and one-to-many (1:N) matching flows are required for operational needs, the proof of concept implements strict information minimisation principles. Passengers provide explicit consent for each transaction through selective disclosure, sharing only the minimum data necessary. Critically, any data temporarily processed through IDMS is purged immediately once the purpose is served, like upon flight departure. No long-term storage occurs, ensuring the system maintains decentralisation principles even when central verification touchpoints are necessary. For one-to-one biometric match use case where the identity data is to be sent from holder of the identity data to the reader, this approach of decentralized architecture also fulfils the requirements based on standards.

During verification at the airport, data is shared through secure, direct channels. Once the journey is complete, no unnecessary records persist. While device loss or theft is a consideration, modern smartphone security features provide robust protection. Biometric locks, remote wipe capabilities, and secure enclaves all work together to keep credentials safe. Digital Identity credentials can be revoked and re-issued without compromising their underlying data similar to revocation and re-issuance of a physical passport.

Implementation Pathway

This vision represents a significant transformation that will unfold over time. The transition requires coordination across airlines, airports, governments, and technology providers. During this evolution, digital and traditional processes will coexist, ensuring no passenger is left behind regardless of their digital access or preferences. Legacy systems will be gradually phased out as modern digital identity infrastructure matures, with early adopter programs paving the way for broader deployment.

Beyond operational improvements, this shift towards digital, reusable credentials significantly reduces paper waste throughout the travel journey, contributing to the industry's broader sustainability commitments. As we advance this vision, we remain committed to ensuring accessibility for all passengers while building the foundation for a more efficient, secure, and passenger-centric future in aviation.

Proof of Concept

Scope

This proof of concept evaluates the feasibility of a standards-based digital identity model for aviation by testing interoperability across interline journeys, biometric verification models, existing digital wallets, national identity ecosystems, and scalable contactless capability discovery. Below is combined scope at high level for different routes, airlines and wallets involved.

1. **Interline scenario**
   Validate the use of a passenger-held digital wallet to securely share verified identity and credential data with airlines and airports across interline journeys and multiple touchpoints.

2. **One-to-one and one-to-many biometric interoperability**
   Interoperability between one-to-one biometric verification and one-to-many biometric systems based on standards.

3. **Compatibility with Apple Wallet and Google Wallet**
   Using existing digital wallets available at scale to store and present travel-related digital credentials without deploying a dedicated aviation wallet.

4. **Compatibility with the Digi Yatra ecosystem**
   Using existing Digi Yatra ecosystem and scaling it for international travel with passport led onboarding and interoperable standards.

5. **Scalability with the IATA Contactless Travel Directory**
   Enables global contactless travel scale by acting as a centralized discovery layer for contactless capabilities, passenger eligibility, and trust across airport touchpoints, reducing bespoke integrations and accelerating adoption.

Summary of Use Cases

Airlines & Routes	Passenger Profile	Wallet(s)	Processes*	Biometric Process at Airport	Key Tech Providers	Environment
Airlines: British Airways/ IAG Japan Airlines **Route:** London Heathrow to Haneda via Hong Kong	US & UK Citizen	Apple & Google	• Check-in mockup • APIs Data Collection & Verification (Travel Readiness) • Biometric enrolment for Hong Kong • Boarding	London Heathrow: 1:1 Hong Kong: 1:n	Amadeus NEC Air New Zealand British Airways Hong Kong Airport Google Wallet Apple Wallet	LHR: Production HKG: Production Airline Travel Ready Check: Test
Airlines: Japan Alrlines British Airways/ IAG **Route:** Haneda to London Heathrow via Hong Kong	Japanese Citizen	Face Express Wallet	• Offers and Orders mockup • Booking flow • Ready to Fly • Remote biometric enrolment for Hong Kong & Haneda	1:n biometric match at HND (test environment)	Branchspace NEC SICPA Hopae Hong Kong Airport	HND: Lab Environment Hong Kong: Production Japan Airline App: Mockup Test
Airlines: Japan Airlines British Airways/ IAG **Route:** Haneda to London Heathrow via Hong Kong	UK Citizen	Google Wallet	• Check-in mockup • APIs Data Collection & Verification (Travel Readiness) • Biometric enrolment for Hong Kong & Haneda • Boarding (HKG)	1:n biometric match at Hong Kong	Amadeus NEC Google Wallet Hong Kong Airport	HND: Lab Environment Hong Kong: Production
Airlines: Japan Airlines **Route:** Haneda to Hong Kong & return	US Citizen	Google Wallet	• Post check-in, saving boarding pass to Google Wallet • Wallet initiated remote biometric enrolment • Single click presentation of boarding pass and selective identity data	1:n biometric match at Hong Kong	Google Wallet NEC	HND: Lab Environment Hong Kong: Production
Airline: Air New Zealand **Route:** Auckland to Hong Kong & return	New Zealand Citizen	Air New Zealand App	• Digital ID setup • Check-in • Remote biometric enrolment • Lounge access enrolment and match at AKL • Remote enrolment at NZ border control	1:n at Auckland and Hong Kong	Air New Zealand NEC Hong Kong Airport	Auckland: Production Hong Kong: Production Air New Zealand App: Production
Airline: IndiGo **Route:** Bangalore to Doha Test Flight No real flight departure to Doha	Indian Citizen	Digi Yatra SITA	• Check-in • Remote biometric enrolment for Airport entry, security and boarding	1:n at BLR airport	Digi Yatra IndiGo BLR airport SITA	Flight information Data – UAT DCS Validation – UAT e-Gate Validation – UAT Digi Yatra App and Backend – UAT IndiGo App and Backend – UAT

***Processes:** Processes in above table highlights the use of Digital Identity or passport digital copy stored in wallet for different use cases. For example, digital identity attributes from the wallet can be requested and presented to securely fill ticket booking form or present the biometric related data to airport touchpoints for remote biometric enrolment for contactless travel.

All Use Cases in Detail (PDF)

Interoperability profile

Aspect	Specification	Details	Technical Components
Credential types	**Digital Passport Copy:** ISO 23220 (latest draft version) **Additional:** Order VC (optional) Boarding Pass (Conditional)	ISO 23220-2 and 23220-4 (photoID with data groups and additional passport data) specifies the docType/credential type and associated details. Order VC will be optional for retrieving back booking information for passengers. Boarding pass VC is used when this info is not passed via API b/w airline and airport systems.	All issuers, verifiers & wallets **Issuers:** Digi Yatra, NEC, Neoke, AirNZ **Verifiers:** Digi Yatra, Neoke, Amadeus, NEC, Hopae **Wallets:** Digi Yatra, AirNZ, SITA, NEC Face Express Apple & Google
Credential Format & model	Data model: ISO 23220 Format: CBOR as per mDOC spec	mDOC specific details from ISO 18013 and 23220 applies. Data serialization and format as per IETF RFC 8949 for CBOR. Signing, encryption and messaging authN as per IETF RFC 9052 for COSE.	All issuers, verifiers & wallet
Credential Issuance	OpenID4VCI 1.0	Defines how a credential is issued from issuer to wallet. Applicable only for non native wallet (non Apple and Google Wallet) issuance.	**Issuers:** Digi Yatra, Face Express, SICPA, Neoke
Online Presentation	OpenID4VP 1.0 W3C DC API ISO 18013-7 Annex C	Specifies how a credential from wallet is requested and presented to a relying party. Digital Credentials API is an intermediary layer between User Agent, wallet and operating system.	**18013-7 Annex C** **Wallet:** Apple, AirNZ, Digi Yatra (android) **Verifiers:** NEC, Amadeus, AirNZ **OpenID4VP +DC API** **Wallet:** Face Express, Digi Yatra, Google, SITA **Verifiers:** Amadeus, Digi Yatra, Neoke, NEC, Hopae
Proximity offline Presentation	ISO 18013-5	For 1:1 biometric matching, the proximity exchange between the verifier's reader and mobile wallet device takes place.	**Wallets:** Existing Apple/Google (no implementation required) **Verifiers:** Amadeus
Crypto Suite & Hash Algorithm	Minimum ECDSA with P-256 and SHA-256 (COSE algorithm identifier –7 or –9 as applicable)	Openid4HAIP reference Required for signing and verification of signature as per the required specifications listed above.	Recommended: All implementers
Trust Anchor	X.509 based Public Key Infrastructure	An X.509 certificate-based PKI where mDocs are digitally signed so verifiers can trust the issuer and verify data integrity offline.	All implementers

Out of scope items

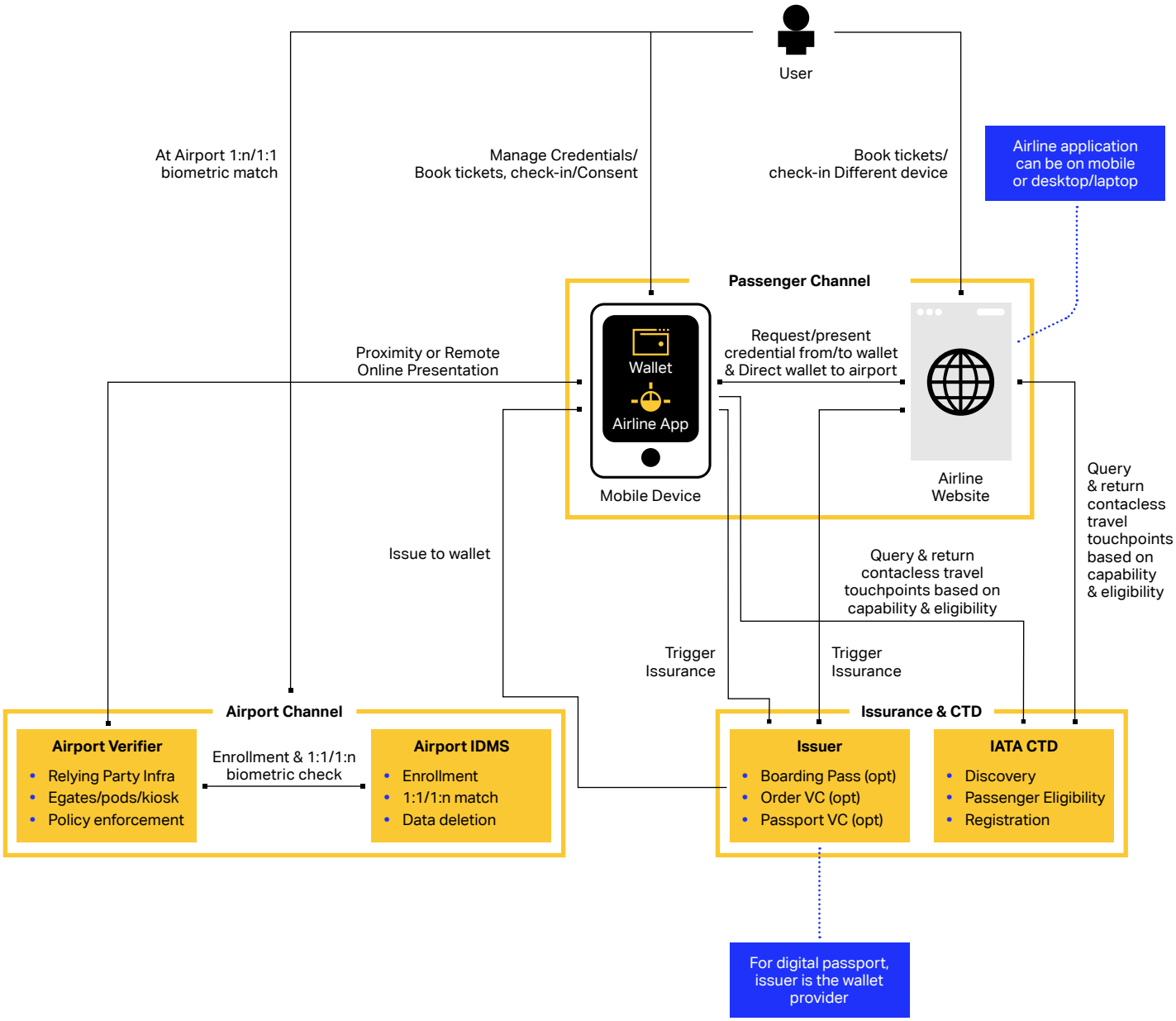
- Any issuance, crypto suite and trust anchor guidance to native wallets (Apple/Google Wallet).
- Proximity and remote online presentation from Apple/Google Wallet.

Components overview

Components	Implementation
Issuance	6 Technical Providers
Wallet	4 Technical providers and 2 native wallets from Apple and Google
Verifiers	5 Technical providers

Ecosystem Blueprint

Simplified architecture component overview



Overview of architecture components

Wallet

The wallet is used to store, present and manage digital credentials. This can be a native wallet (Apple or Google), a standalone wallet provided by a third party or a wallet capability embedded within an airline mobile application. It supports secure storage of credentials and controlled data sharing based on passenger consent.

Airline Application

The airline application is used for booking, managing bookings, and check-in. It can be accessed via web or native mobile platforms. During booking or pre-travel processes such as advance passenger information collection, the airline may act as a verifier or relying party and request specific passport attributes only, rather than full document disclosure.

Issuers

Issuers are responsible for creating and delivering digital credentials to the wallet. Depending on the setup, this role may be fulfilled by the wallet provider itself or by other trusted parties. Credential issuance in scope includes digital passport credentials, order or booking-related credentials, and boarding pass credentials.

Airport Verifiers

Airport verifiers represent the various airport touchpoints that interact with passengers during the journey. This includes biometric pods, e-Gates, or similar systems. These touchpoints request passenger-related data such as biometric info and if required boarding pass information to enable contactless processing at different stages of the airport flow. Biometric data exchange can happen via either remote online or proximity flow.

IATA Contactless Travel Directory

The IATA Contactless Travel Directory is used to discover contactless travel capabilities at airports. It supports eligibility checks, provides passenger instructions for contactless flows, and exposes trust related information needed to enable interoperability and wide interaction among participating entities. For contactless travel capability check a secured onboarding of airport verifiers and consumer of the contactless travel APIs will be required.

Airport IDMS System

The airport Identity Management System (IDMS) manages biometric enrolment and matching during contactless travel. It receives biometric data from airport touchpoints, links it to the appropriate passenger context, and performs identity matching (1:1 or 1:N) to support automated access decisions at gates or checkpoints. The exact definition and implementation of this component may differ from each other depending on local production system.

Process Steps

0. Pre-requisites

Before the journey flow starts, the passenger must already have a wallet in place. This can be a native wallet (Apple or Google), a standalone wallet or a wallet capability embedded in an airline application. A digital passport credential must already be available in the wallet. The onboarding and issuance process for the digital passport is specific to the wallet provider. For issuance OpenID4VCI V 1.0 is used for non-Apple and Google wallets.

1. Booking Flow

The passenger completes booking or manages an existing booking using the airline application, either via web or a native mobile app.

1.1 Optional Use of Digital Passport

During booking or manage-booking, the airline may optionally request selected passport attributes from the wallet. The airline acts as a verifier or relying party and only requests the minimum data required rather than the full passport. The request can be done using OpenID4VP 1.0 over Digital Credentials API or using ISO 18013-7 Annex C standard. Passenger must explicitly approve any data sharing as part of wallet presentment. Digital passport use during booking process is typically used to reduce manual data entry, errors and support advance passenger information collection. Use of passenger data can also be done optionally to provide personalized offers during booking stage.

1.2 Order VC Issuance (Optional)

After booking is completed, an Order VC may be issued to the passenger's wallet. The purpose of this credential is to carry booking-related context, such as a booking reference or trip linkage, so that later steps can retrieve the correct booking information without repeatedly asking the passenger to re-enter it. Issuance can be performed by the airlines or any trusted associated issuer, depending on the implementation. For issuance OpenID4VCI 1.0 standard is followed.

2. Check-in and Contactless Travel Enablement

2.1 Online Check-in

The passenger completes online check-in using the airline application, following standard airline check-in rules and timelines.

2.2 Capability and Eligibility Discovery

As part of the check-in process, or immediately after, the airline queries the IATA Contactless Travel Directory via a standard, secure REST API. This allows the airline to identify available contactless touchpoints, passenger eligibility, required data and credentials, and the instructions to present to the passenger. The Directory also provides trust, policy, and configuration information enabling airlines, airports, and authorities to establish trusted, interoperable contactless flows without bespoke integrations.

2.3 Offering Contactless Travel

If the journey is eligible, the airline presents the passenger with an option to enable contactless travel. This is typically done via a verifier link or QR code that directs the passenger to the relevant airport verifier and wallet credential exchange. Depending on the airport verifiers it can request for biometric data, some personal information and in addition boarding pass from the wallet. Other implementations can also include sharing of boarding pass data via API integration b/w airline and airport verifier where wallet only handles digital passport data. This presentation exchange can be achieved using three different ways.

- OpenID4VP 1.0 over DC API
- ISO 18013-7 Annex C
- Plain OpenID4VP 1.0

In the context of the PoC all three approaches have been implemented depending on varying routes and business requirements. The digital passport data format follows ISO 23220 photoid specifications.

2.4 Enrolment and Pre-share

Explicit enrolment and data sharing from wallet to verifier is performed with passenger providing consent per presentation.

3. Day of Travel

3.1 Biometric match using 1:1 or 1:n approach

At airport touchpoints, biometric verification may be performed using either a 1:1 or 1:N approach, as the One ID standards support multiple biometric approaches. In the 1:1 case, the passenger connects their digital wallet to the reader using standards as per ISO 18013-5 NFC based device engagement and establishes a secure session and provides a reference for the verification. A live biometric capture is then compared directly against this reference. In the 1:N case, a live biometric capture is matched against a previously enrolled gallery maintained by the airport IDMS. In both approaches, the result is returned as pass or fail, with manual fallback available.

Github Repo for Additional Details

We document in GitHub following details:

- End to End sequence flow diagram
- API spec for boarding pass exchange
- Any UI related public info
- Target schemas
- Target system tested
- Ay other relevant public details or code for the POC

Benefits

This Proof of Concept demonstrates a shift from isolated biometric touchpoints to a globally interoperable, passenger-controlled digital identity ecosystem using decentralised identity standards.

Benefits by Stakeholder Passengers

Passengers move from curb to gate using only biometric recognition, with admissibility verified before airport arrival. Building on the processing improvements demonstrated in pilot programs, addresses the top priority for 64% of passengers. Passengers control their own data through selective disclosure, sharing only what's needed for each step. Their biometric data stays on their device, addressing privacy concerns for 54% of travellers. Digital identity consistently improves customer satisfaction by reducing wait times and provides greater feeling of control over their journey.

Airlines and Airports

Airlines and Airports automating identity and boarding verification improves staff productivity by 25–40% and increases passenger throughput by 15–25%, without requiring physical infrastructure expansion. Airlines transmit higher quality Advance Passenger Information to governments, reducing costs from inadmissible passengers being returned.

Border control

Border Authorities Government agencies receive more reliable data through high-assurance credentials bound to ePassports and verified via liveness checks, reducing document fraud and presentation attacks.

Why it's Important to Address the Interoperability Gap

Current seamless travel solutions operate as proprietary silos. A passenger enrolled in one airline's biometric programme must re-enrol when transferring to a partner carrier or using a different airport system. Scaling today's model globally would require thousands of bilateral integrations.

This proof of concept solves the interoperability problem. By building on open standards (ISO/IEC, W3C, OpenID), a digital credential from a wallet in one country is instantly verifiable by an airport authority in another. The standardised foundation eliminates bespoke integrations for every route or partnership.

Most importantly, verified credentials travel with the passenger across airlines, airports, and borders without re-enrolment or multiple apps. Biometric data stays on the passenger's device. Passengers provide explicit consent for each use across multiple touchpoints, getting both convenience and privacy minimizing the time of exposure the data stays in centralised repositories vulnerable to breaches. Digital identity extends far beyond aviation. Governments and enterprises across all sectors are adopting interoperable digital credentials, making global standards essential for long-term viability.

Building the Business Case

Investing in this infrastructure requires demonstrating clear financial returns. The business case is built on a simple premise to measure how much human customer service time you save per passenger, scale that across your annual volumes, and convert those savings into monetary value.

ROI Calculation Methodology

Step 1: Measure the Time Savings Compare your current process times for manual document checks against the new process using biometric verification and digital wallets. The difference is your labour time saving per passenger.
Example: Manual processing takes 240 seconds, digital processing takes 3 seconds = 237 seconds of human handling time saved per passenger.

Step 2: Aggregate and Monetise Capacity Apply the time saving across annual passenger throughput, adjusted for expected uptake rates. Convert aggregated hours into financial value using blended frontline staff costs.
Result: Gross annual labour savings, the direct reduction in cost-to-serve per passenger.

Step 3: Calculate Net Benefit and Payback Compare gross savings against total cost of ownership, including capital expenditure (hardware integration, e-gates) and operational expenditure (software licensing, maintenance, training).
Outcome: High passenger volumes mean small efficiencies compound rapidly, often delivering payback in months rather than years.

Step 4: Convert to Capacity Increase Translate time savings into throughput gains.

Outcome: Reducing processing time from 240 seconds to 3 seconds increases throughput capacity per asset by approximately 80-fold, creating "virtual infrastructure" growth without physical expansion.

Economics and opportunity are different for any Airport, Airline or passenger touchpoint. As per a recent IATA publication: "Case studies at major international airport identified up to a 11% reduction in airport staff costs, while a ground handing company estimated a USD 5.3M annual saving at another leading airport."

Strategic Value Drivers

Beyond direct labour savings, three compounding factors maximise ROI:

Infrastructure Optimisation (CAPEX Avoidance)

Reducing processing times from minutes to seconds increases the capacity of existing terminal infrastructure without capital-intensive construction projects. Airports handle passenger growth through "virtual infrastructure expansion" rather than building new terminals or check-in halls.

Concession Uplift (Ancillary Revenue)

Reduced queue times directly correlate with increased airside spending. Every minute saved converts to dwell time in commercial zones. Business cases should include estimated additional retail and food and beverage revenue per minute of regained dwell time.

Risk Mitigation (INAD Cost Reduction)

Automated admissibility checks significantly reduce inadmissible passenger incidents. Solutions like document and visa verification eliminate manual errors, avoiding substantial regulatory fines and operational costs associated with passenger repatriation.

The Investment Summary

The transition to digital identity infrastructure represents a low-risk, high-reward investment. Industry research indicates the amortised annual cost per passenger (measured in cents) is a fraction of baseline manual processing costs (measured in dollars).

The solution requires minimal one-time investment per passenger relative to operational savings generated, making it effectively self-funding. The rapid break-even point positions the technology as a strategic asset that permanently lowers the operating cost base for airlines and airports.

Next steps

With the PoC we have proven all the laid objectives of the PoC can be achieved.

While target customer journeys are clear and pathway to roll out have been identified, some technical elements need to materialize to lay the technical foundations to implement what has been tested and further harmonize the Passenger Experience across implementations:

- Photo ID standard need to be officially released under ISO standards.
- Wallet providers need to consistently implement it, and work on a common interoperability profile across wallet providers, verifiers, and issuers.
- Digital Credentials API need to evolve to support combined presentation. It will help to reduce opt-in and/or consent fatigue.
- DPI Digital Public Infrastructure, Digital Sovereignty, and Trust Frameworks for interoperability for cross border recognition of digital identities needs to be addressed.
- Close the gap between the “Border Passenger Journey” and the “Airline/Airport Passenger Journey”. Have the DTC Type 2 in the radar and suggest the introduction of a Digital Travel “Verifiable” Credential within ICAO standards.
- A Source of Trust for privacy and security compliance should provide the consent’s requirements for each Regulatory Framework.
- Wallets and verifiers supporting single QR code or deep link for multiple protocols support leveraging Digital Credentials API.

There is also significant opportunity to minimise the need to store any passenger data within airline systems that has benefits when it comes to data security. Failure to consider Digital Identity in the early stages of Modern Airline Retailing design and adoption risk significant rework later and a delay to the benefits that Contactless and Seamless Travel will bring.

Partnering for success

A special thank you to the cycle 2 Data and Technology PoC members:

Project Gaia (Global Data Bus)

accelya · accenture · aws · BRIGHTGROVE · CONFLUENT · dreamix · Etihad · Globant · Infosys · LAWA · MERKLE · nagarro · Qatar Airways · SITA · snowflake

Project Carina (AI Agent Multilateral Interoperability)

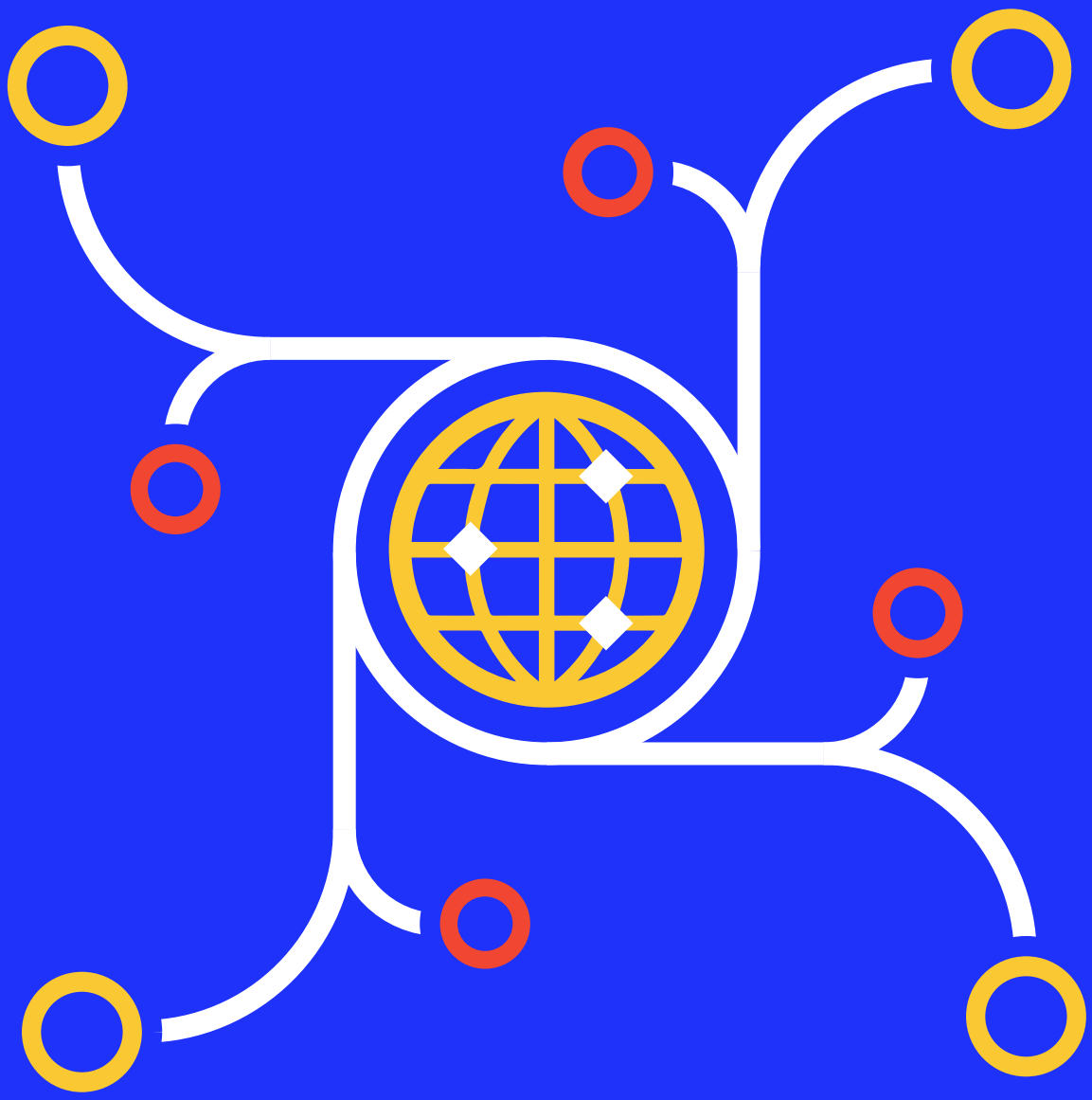
accelya · accenture · ANA · avianca · aws · Etihad · Globant · Infosys · MERKLE · nagarro · Qatar Airways · SITA · snowflake

Verifying Digital identity in Distribution Process

AIR CANADA · ARC · dreamix · Google Wallet · hopae. · IAG International Airlines Group · Infosys · neoke · Qatar Airways · Trip.com · TURKISH AIRLINES

Contactless Travel at Scale

amadeus · AIR NEW ZEALAND · 香港國際機場 HONG KONG INTERNATIONAL AIRPORT · Kempegowda International Airport Bengaluru · branchspace · digiyatra · facephi · Google Wallet · hopae. · IAG International Airlines Group · IndiGo · JAPAN AIRLINES · LAWA · NEC · neoke · Panasonic CONNECT · Qatar Airways · SICPA · SITA



International Air Transport Association
SS135-800 rue du Square-Victoria
Montreal, QC, H3C 0B4
Canada

iata.org