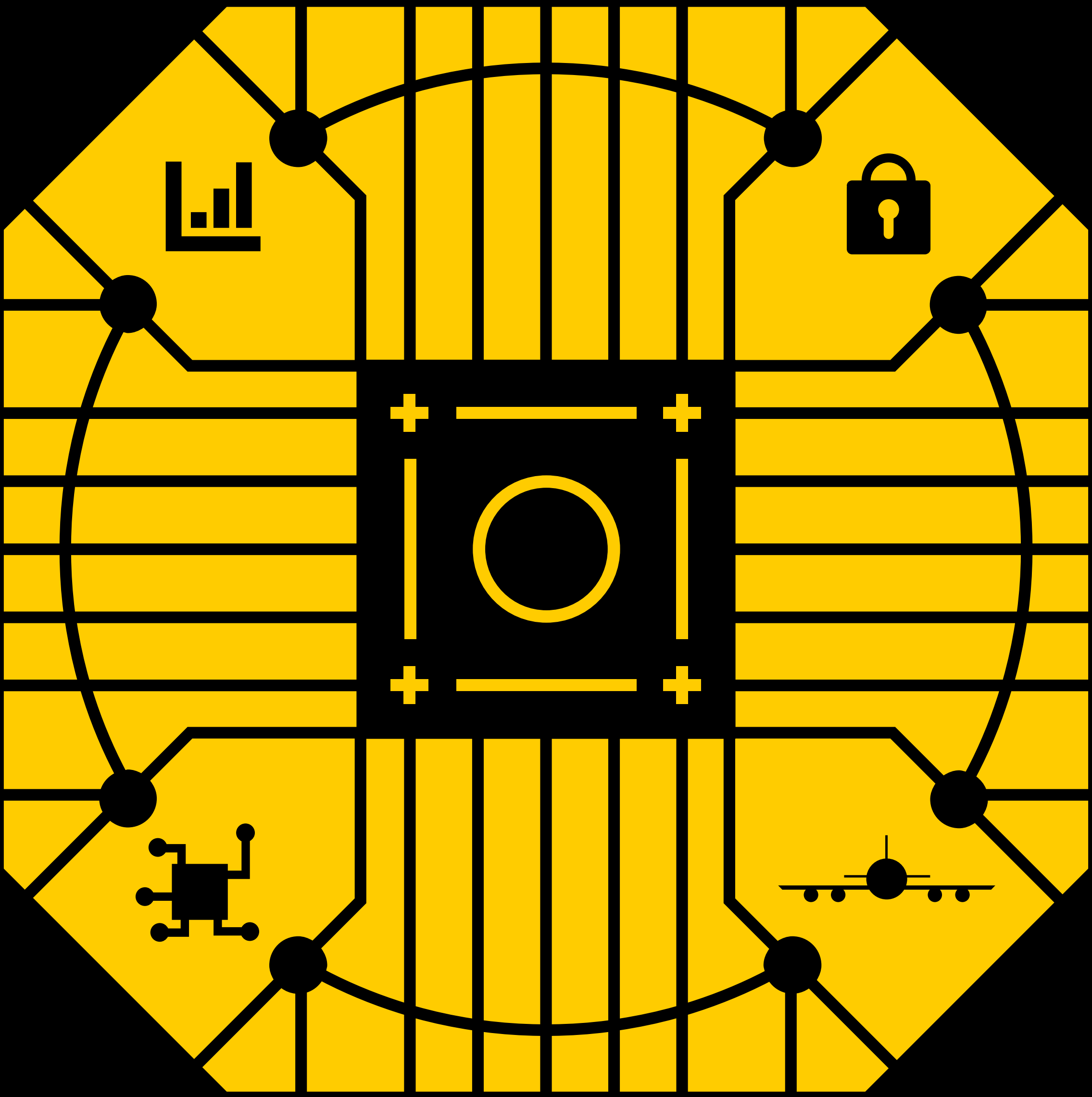
Exploring Artificial Intelligence and Digital Identity Use Cases in Aviation



IATA

Contents

Legal Disclaimer

All content in this paper, including text, graphics, research findings, and analysis, is and remains the intellectual property of IATA. Any reproduction, distribution, modification of the information and content contained herein without prior written consent of IATA, is strictly prohibited. Proper citation and attribution must be given when referencing this paper. Any third-party materials used within this paper remain the property of their respective owners and are cited accordingly.

While every effort has been made to ensure that the information in this paper is accurate and up-to-date at the time the paper issued, no warranty, express or implied, is given regarding its correctness, reliability, timeliness, or applicability. The content is provided on an 'as-is' basis, and IATA and the contributor(s) disclaim any and all liabilities for errors, omissions, or any consequences arising from the use of the content and information contained herein. Readers are advised to conduct their own due diligence and verification before making decisions based on the content of this paper.

This paper may contain forward-looking statements regarding potential technological advancements, industry innovations, market trends, or regulatory developments. These statements are based on current research, expert analysis, and reasonable assumptions but are inherently speculative and subject to change. Future advancements, regulatory shifts, economic fluctuations, and unforeseen events may materially alter the anticipated outcomes and projections. IATA makes no representations or warranties regarding the accuracy, reliability, or likelihood of these forward-looking statements. IATA disclaims any obligation to update or revise these statements in response to new information or future events. Readers are advised to conduct their own due diligence and verification before making decisions based on the content of this paper.

This paper may reference third-party sources, studies, or external websites for informational purposes. These references do not constitute an endorsement, nor does IATA assume responsibility for the accuracy, reliability, or completeness of third-party content. The inclusion of such references is intended to provide additional context and does not imply verification, endorsement or approval in any way of external viewpoints, data, or findings.

Introduction

The aviation industry is at a pivotal moment, with artificial intelligence (AI) emerging as a key enabler of efficiency, customer experience, and operational excellence. To harness its full potential, airlines and industry stakeholders must first establish a clear data strategy—one that aligns with their organizational vision and operational priorities. Everything related to AI is fundamentally data-driven, making it essential for organizations to understand their trajectory from a data perspective. Airlines need access to relevant data, robust data discovery capabilities, and a clear understanding of the highest-value use cases where AI can be effectively applied.

The use of Digital Identity technology is emerging as a critical enabler of efficiency, security, and personalization. As airlines and travel stakeholders embrace digital transformation, the adoption of Digital Identity solutions is reshaping the passenger journey—enhancing convenience while ensuring compliance with regulatory and security requirements.

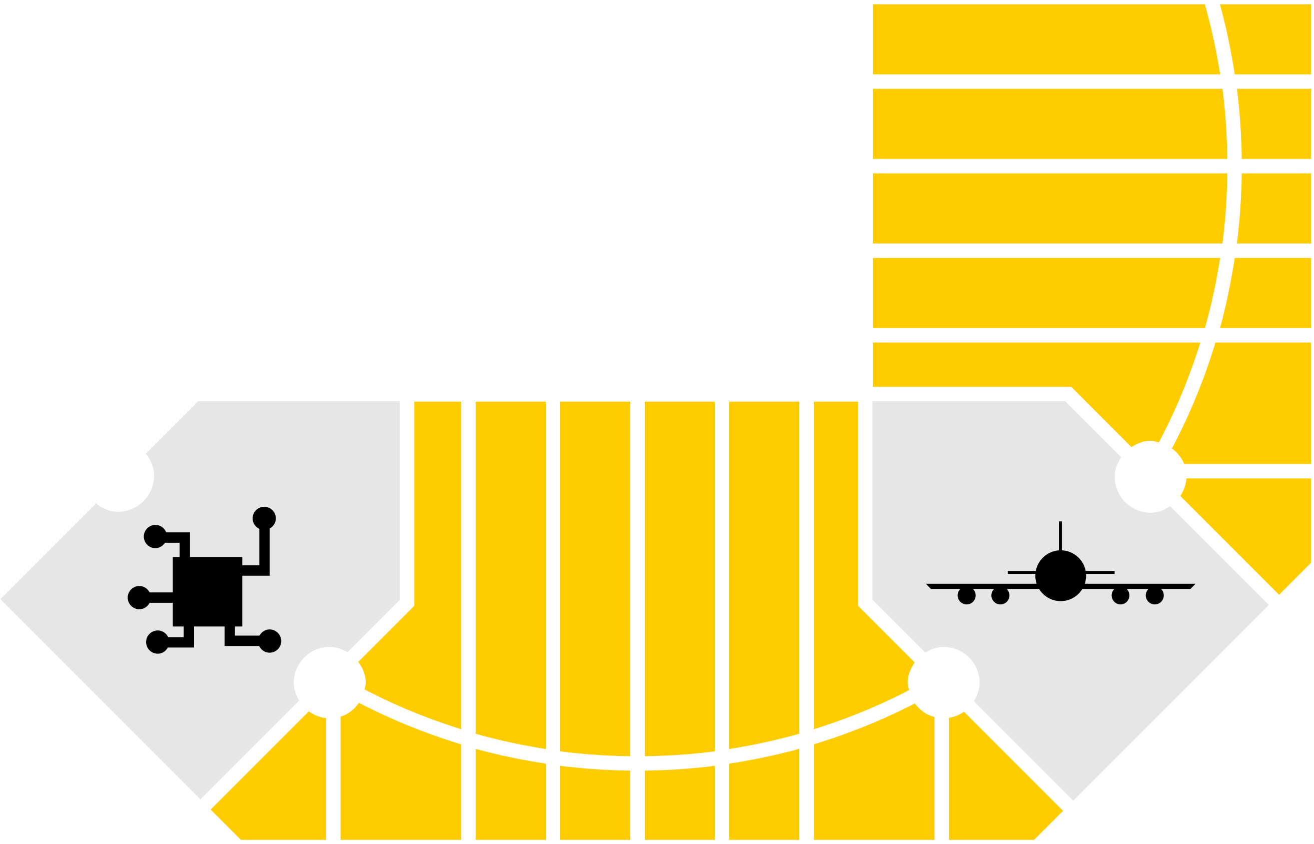
Member Airlines and IATA DAT PoC Strategic Partners (SPs) came together and have contributed in developing Proofs of Concept (PoCs) to address industry challenges and explore innovative solutions for both Industry Large Language Models (LLM) and Digital Identity.

This paper explores the key areas where AI can drive transformation and industry efficiency, the challenges that must be addressed, and the collaborative efforts needed to shape the future of data-driven decision-making in aviation. It also explores usecases related to Digital Identity on both B2B (Business-to-Business) and B2C (Business-to-Consumer) sides.

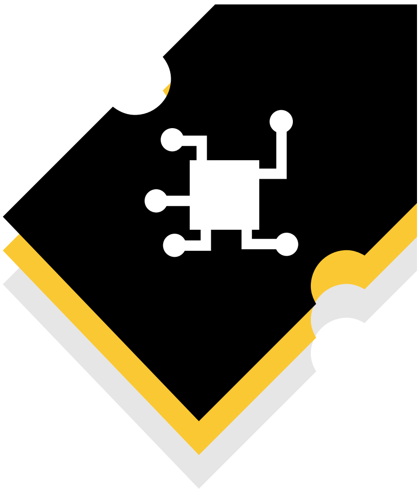
As always, I would like to especially thank the Data and Technology group who dedicate time and energy to tackle new challenges facing our industry.

Sincerely yours,

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



1. Project Industry LLM



Context

Large Language Models (LLM's) exploded into the mainstream in late 2022 with the release of OpenAI's ChatGPT-3.5—a seemingly all-knowing, human-like chat interface that captured the public's imagination. Early use cases may have focused on content creation, but LLM's are evolving rapidly and stakeholder across the aviation world are keen to understand their applicability to real-world challenges.

To this end, IATA has taken the lead by convening a Proof-of-Concept (POC) working group composed of representatives from IATA Member Airlines and strategic partners from the technology industry. This group was tasked with identifying, building and evaluating a use case to illustrate how LLM's could be harnessed to address real-world challenges in aviation beyond the obvious chat bot like solutions that most people imagine when hearing about an LLM.

In this paper we will outline the chosen use case, the approach taken to build solutions that leverages LLMs, and the learnings taken from the proof of concept.

While discussing potential directions for the POC, the group repeatedly encountered the challenge of navigating regulations—at global, local, and individual airline levels.

Given that an LLM-based solution excels at processing large volumes of text and extracting key insights, the group decided to focus the POC on simplifying regulatory compliance.

The next step was to identify a specific use case where the technology could be practically applied to demonstrate its effectiveness in addressing this challenge.

Cargo Acceptance Process

While regulatory compliance poses challenges across all departments within the airline industry, from flight operations to passenger handling, eventually the group decided to focus specifically on the cargo acceptance process, where documentation accuracy is paramount.

A significant pain point in cargo operations arises when shipments are delayed due to missing or inaccurate documentation. This leads to slow downs, increased costs, and dissatisfaction of air cargo stakeholders, and impact the end customer.

Our goal was to investigate whether LLMs could be leveraged to proactively identify and address potential documentation issues during the cargo acceptance process, preventing these costly disruptions. Going forward we specifically settled on the cargo acceptance process for perishable cargo (goods that have a limited shelf life and require specific conditions—such as temperature and humidity control—during transportation to prevent spoilage, decay, or degradation). This is a critical area due to the time and temperature sensitive nature of these shipments and the potential for significant loss if documentation is incomplete or inaccurate.

Currently, the process involves a combination of manual and digital processes where acceptance staff must verify compliance by reviewing air waybills. attached documents, and navigating complex regulations related to the transportation of perishables. IATA Perishable Cargo Regulations (PCR) contain these requirements but additionally there may be requirements at the departure, arrival, or transit locations as well as airline specific ones. This acceptance process is time-consuming, prone to errors, and can easily lead to delays, especially for inexperienced staff. It's important to note that while airlines are not ultimately responsible for verifying every detail of the required documentation, they do bear the responsibility of ensuring the cargo is ready for carriage. This includes confirming that all necessary documentation is in order.

To address these challenges, the POC we delivered uses LLMs to streamline the cargo acceptance process for perishables. The actual user of our POC solution is the airline acceptance staff (or ground handling staff acting on their behalf) that checks for complete documentation. When done manually, this process can be time-consuming, in some cases taking upwards of 20 minutes for the most complex shipments to verify the necessary documentation, labelling and physical condition of the shipment. Other benefits relate to improvements in regulatory adherence and operational integration, elements which are crucial for trust and adoption in safety-critical environments.

The user interface (UI) part of our POC is a mobile based interface the staff can use to scan on the spot all the documents submitted for a consignment in case they are not already available in the system. Once transmitted to the back end of the solution, the LLM analyses the submitted documentation, including air waybills and attached documents, looks up the relevant regulations based on cargo type, location, etc., (in our case IATA PCR including State and Operator variations, embargo information, etc.), and instantly identifies any missing, incomplete or incorrect documentation and reports back to the user of the app that either the documentation is valid and complete or that it is not and the specific items that are missing or are incorrect. This allows acceptance staff to proactively notify shippers of issues on the spot and thus enable them to take corrective action in a timely manner. By improving compliance upfront, we can minimize delays, reduce waste, and maintain the integrity of these sensitive goods. This ultimately translates to more satisfied customers who can rely on timely and predictable deliveries. Beyond improving customer satisfaction and adherence to IATA and industry standards and regulations minimizing the risk of non-compliance and fines, this also contributes to a more sustainable cargo ecosystem by:

- **Reducing waste of perishable shipments**
  Preventing spoilage due to documentation issues avoids unnecessary disposal of valuable goods.

- **Optimizing cargo space**
  Ensuring only compliant shipments are transported optimizes the use of valuable cargo space.

- **Minimizing overall environmental loss**
  This encompasses the reduction of waste, efficient use of resources, and lower emissions, contributing to a more sustainable cargo industry.

Our POC has focused on the actual validation part, however, this could be just the first step. The same back end solution could be expanded to encompass supporting the entire cargo journey, from reservation to delivery, and to include a wider range of stakeholders. For instance, during the reservation process, shippers could be advised by the LLM on the required documentation based on their specific shipments. Furthermore, in the planning phase, shippers themselves could leverage the LLM enhanced with up-to-date, relevant and trusted regulations, such as the PCR in this case, to confidently explore and understand the necessary documentation, drawing from the same comprehensive knowledge base as the airlines.

This POC, while focused on cargo acceptance for perishables, could serve as a crucial stepping stone towards a future where LLMs can support regulatory compliance across the entire airline industry. By demonstrating the tangible benefits of LLM-powered solutions in this initial use case, we unlock the potential for wider adoption across all operational domains. Imagine a future where airlines can seamlessly navigate the complex web of regulations, ensuring compliance with unparalleled efficiency and accuracy. This not only benefits airlines by streamlining operations and reducing costs but also creates a smoother and more reliable experience for all stakeholders. By embracing LLMs and fostering industry-wide collaboration, we can usher in a new era of intelligent compliance for the aviation industry, paving the way for a safer and more efficient future.

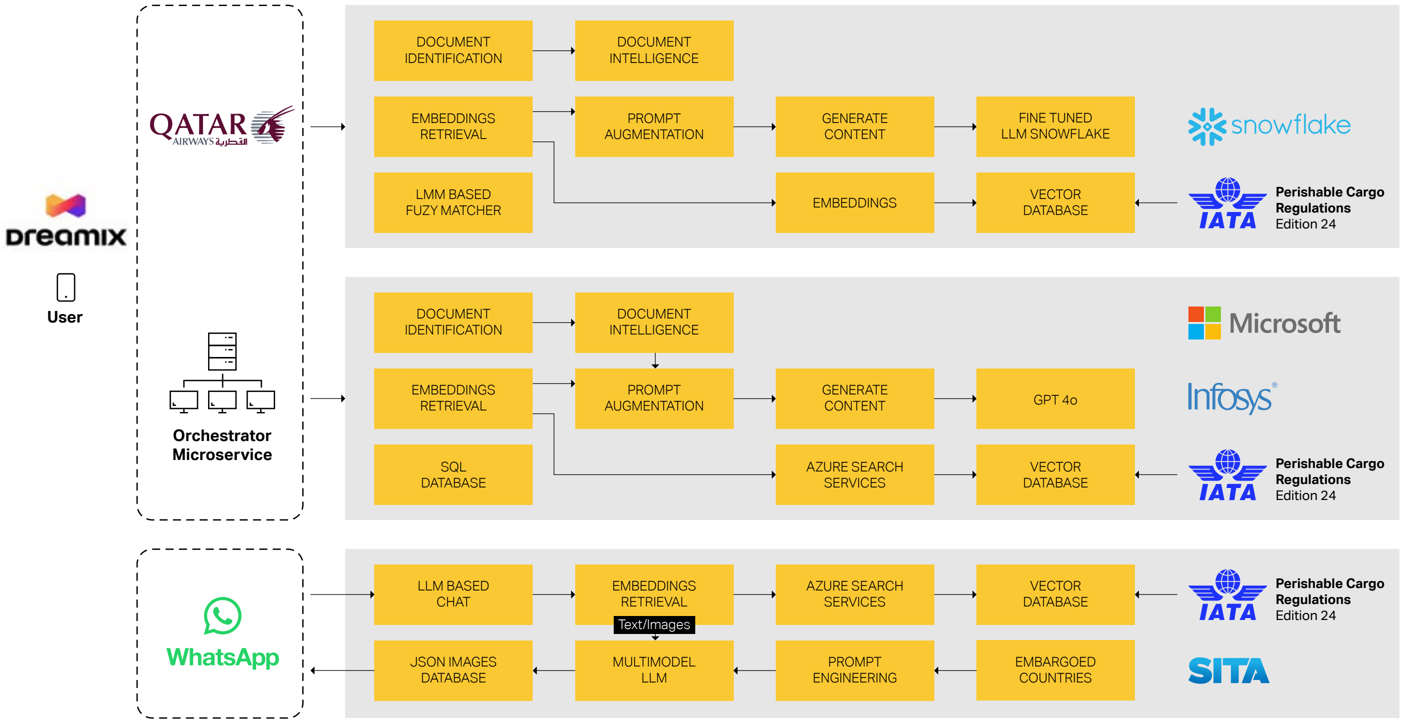
Technical Approaches and Results

Given the diverse range of IATA Strategic Partners contributing to this POC, the working group chose to develop multiple back-end modules to achieve the same functionality. This approach showcases the unique strengths of different cloud platforms while also demonstrating that the challenge is universal and can be addressed effectively using various technology stacks to achieve similar results.

In terms of contribution—Infosys, Microsoft, SITA and Snowflake each delivered a back-end component that performs the document ingestion through various channels for classification, information extraction, data validation, and compliance checking as well as a Retrieval Augmented Generation (RAG) like knowledge base approach on a subset of IATA PCR standards that are relevant to this use case as well as specific regulations prepared by the participating airlines (All Nippon Airways, LATAM and Qatar Airways).

In terms of user interaction we wanted to focus on a different LLM interaction paradigm that goes beyond the traditional chat screen. As such the front-end part of the POC was delivered by Dreamix and it is composed of a simple mobile app that allows the user to take pictures of documents and displays the validation status. A second user interface is a SITA delivered WhatsApp channel that allows for the same interaction but within the messaging app. The front end communicates with an integration layer delivered by Qatar Airways IT that dispatches the requests via a set of standard APIs between the different modules.

In a real-life scenario, successful adoption of any system as described in our POC will depend on direct connectivity with airline cargo management systems (CMS). The UI solution we described and put together is meant to be illustrative only in the context of POC, and while it could provide potential inspiration for some cases it is not meant to be definitive.



Infosys Module Overview

The Infosys backend provides a set of capabilities to implement the pipeline for streamlining air cargo document processing, regulatory compliance validation, and automated information extraction. The solution leverages Azure Document Intelligence as its core document processing engine, combined with Azure OpenAI's GPT-4o model and FAISS-based vector similarity search to deliver comprehensive information extraction and document validation capabilities. Through careful prompt engineering, the system achieves high accuracy in document validation, maintains efficient processing times for complex international cargo regulations while providing clear, actionable validation results.

The system's document processing pipeline begins with Azure Document Intelligence, which performs automated classification and multilingual information extraction from cargo export documents. This foundation enables accurate categorization of incoming documents while reliably extracting critical data points across various document types and languages. The solution implements Retrieval-Augmented Generation (RAG) with IATA PCR documentation and country specific document requirements. The system first converts the IATA PCR and country specific document requirements into vector embeddings stored in a FAISS database. During validation, these embeddings enable precise retrieval of relevant regulatory requirements using the vector similarity search technique against the prompt generated using information extracted using input document content, which the LLM then uses to verify compliance across multiple dimensions from PCR documentation.

The system exposes three primary APIs implemented using Python-Flask framework to enable the pipeline for document processing and validation on the mobile app. First API is related to document information extraction which processes base64-encoded Air Waybills, performing validation and returning structured JSON response. Second API analyses AWB details including source, destination, and perishable goods type to determine all mandatory documentation based on country specific regulations and return the list in JSON format. Third API performs comprehensive validation of multiple documents like AWB, Phytosanitary certificates, Invoices, packing list, etc., against each other (to ensure documents are related) along with PCR requirements and return the validation results in JSON format.

To maintain high accuracy and responsible AI practices (avoid hallucination from LLMs), the system continuously monitors key quality matrices including Groundedness (Ensuring responses align with source documentation), Coherence (Maintaining logical consistency in extracted information), Fluency (Delivering clear and understandable outputs) and Relevance (Providing pertinent information for the specific cargo context). This is to ensure that RAG and prompts can be optimised for desired results as accuracy and compliance are the key requirement for cargo document validation process.

Microsoft Module Overview

Microsoft's design goal in the delivered solution has been to blend the best aspects of agentic and deterministic AI design patterns into a cohesive "agentic determinism" architecture. This hybrid approach ensures a balance between adaptability and reliability, addressing the inherent challenges in conventional AI agent systems while meeting the rigorous requirements of mission-critical workloads.

While regular AI agents excel in autonomy, capable of planning, reasoning, and adapting to new problems, this flexibility often comes at the cost of unpredictability. Such behavior is unsuitable in domains where consistency, reliability, and compliance are paramount. To bridge this gap, the agentic determinism design combines dynamic, autonomous decision-making (agentic) with structured, rule-based processing (deterministic), ensuring both adaptability and adherence to predictable processes.

At the heart of this system is OpenAI's GPT-4o multimodal LLM, capable of processing both visual and textual information, acting as a versatile engine for document classification, analysis, and validation. By employing a structured workflow, the solution processes user-provided documents against a predefined set of validation rules, while dynamically selecting appropriate rules based on the analyzed information. This design not only enhances operational efficiency but also provides the flexibility to accommodate evolving regulatory and business requirements.

Additionally, the following features have been implemented to increase trust, adaptability, and extensibility:

- **Explainable AI (XAI)**
  Every decision point and data extraction is accompanied by clear justifications, enabling full auditability and building trust in the system.

- **Rule Modification Capability**
  The solution allows for seamless updates to validation rules, ensuring adaptability to evolving regulatory contexts.

- **Rule Set Switching**
  Multiple validation rule sets are supported, enabling the system to tailor processes for different air carriers or business needs efficiently.

SITA Module Overview

The SITA backend is a self-contained, monolithic Python application that simplifies air cargo document processing, regulatory compliance, and validation. The POC incorporates Multimodal Large Language Model to analyse images, extract structured data, and conduct real-time regulatory and embargo checks. To ensure seamless user interaction, the solution integrates with either a WhatsApp-based interface or a web UI.

The POC harnesses state-of-the-art LLM (OpenAI's GPT-4o model as at January 2025) for advanced reasoning and context-aware responses. The AI-driven functionalities include structured data extraction from Air Waybills (AWB) and other supporting documents, retrieval-augmented generation (RAG) for precise regulatory insights, and compliance validation against country-specific trade laws. Additionally, the system processes free-text queries, allowing users to receive AI-powered responses for seamless support.

To maintain up-to-date compliance with country-specific trade laws, the system automates regulatory document ingestion like the IATA PCR. It continuously scans designated databases and documents for supported file formats (.pdf, .txt, .docx, etc.). The extracted content is then segmented into manageable chunks, converted into vector representations, and stored in a FAISS-based vector database for efficient retrieval. When a user queries regulations, the system retrieves the most relevant sections and processes them through another LLM model, ensuring precise, context-aware responses that reflect the latest regulatory requirements.

In this system, large language models are harnessed to automate the extraction and validation of cargo shipping documents by leveraging carefully crafted prompts. When a document image is received, the system encodes the image and passes it along with detailed instructions to the language model, directing it to extract specific information, such as shipment details, party information, and cargo metrics, in a structured format. This precise prompt engineering ensures that the output aligns with the expected data schema, enabling downstream processes to easily validate the document's completeness and compliance with regulatory requirements. The system returns the data in a precise JSON format that matches a predefined schema. A separate prompt asks the model to classify an uploaded document by matching it against a list of expected document types, instructing it to respond with a clearly formatted output.

The system also leverages a prompt that combines extracted shipment data with pre-loaded country-specific regulations, instructing the model to summarize or reformat the relevant regulatory requirements in a clear and concise manner for further validation. Each of these instructions is carefully crafted to guide the model toward a specific, structured output, ensuring that subsequent processing steps can reliably validate and act on the information. For checking embargo status and proximity risks, the prompt directs the model to evaluate whether the importing country has close borders with any embargoed country and if so it will verify if any shipment items are restricted due to this proximity, thus producing an alert message if risks are detected. By dynamically adjusting prompts based on the document type and processing stage, the system achieves a high level of accuracy and efficiency in validating cargo shipping documents while adhering to complex international shipping regulations.

Snowflake Module Overview

Snowflake offers a comprehensive solution that combines Retrieval-Augmented Generation (RAG) with Cortex Search, general purpose and task-specific LLM functions with Cortex AI, and document extraction capabilities with Document AI. This powerful combination optimizes cost, accuracy, and performance at every step, streamlining the process of searching and retrieving relevant documents.

Document AI, a key capability of Snowflake, is utilized to extract information from AWBs, invoices, and phytosanitary documents with high accuracy. It leverages the Arctic-TILT large language model, a proprietary multimodal LLM developed by Snowflake specifically for document understanding and extraction tasks. This component significantly increases the accuracy of information extraction from documents compared to using a general purpose LLM. In addition to Document AI, Snowflake employs Cortex task-specific functions to handle classification, chunking, and extraction of data from various documents, including AWBs, invoices, and phytosanitary certificates. These specialized functions ensure that the system accurately identifies document types, extracts relevant sections, and organizes content into manageable chunks for further processing in the RAG process.

To enhance the search and retrieval of AWB-related information, this solution utilizes Cortex Search for RAG. It is a fully managed, low-latency hybrid search service which is used to identify the required documents associated with the processed AWB by searching regulatory documents. By leveraging Cortex Search, Snowflake ensures that critical data can be retrieved on demand, saving time and improving operational efficiency. For the response generation part of RAG service, several LLM options hosted in Snowflake were tested, and it was determined that even a small model like Llama 3.1-8b is sufficient to generate high-quality results for this use case.

To enhance regulatory compliance and real-time insights, the system automates the ingestion of country-specific trade laws and industry regulations (e.g., IATA Perishable Cargo Regulations). Extracted data is vectorized and stored within Snowflake's scalable infrastructure, ensuring efficient retrieval for AI-driven decision-making. Whether validating cargo classifications, embargo risks, or proximity restrictions, the platform ensures accurate, auditable, and real-time regulatory adherence, transforming how perishable cargo is processed and reducing costly delays in global logistics.

Qatar Airways Integration Module Overview

The integration module manages all integrations between the UI and the backend modules (Snowflake, Microsoft, Infosys). It exposes standardized APIs to consumers and, based on the request, invokes the different backend modules. Some key features of the integration module are maintaining the interaction session between UI and LLMs, managing the lifecycle of the digitalized document and handling the complexity of integrating multiple LLM solutions

Further integration with the airline cargo systems will play the critical role in a production like future of such a solution as described in our POC. Some use cases that could be handled by the integration module:

- Capability to directly fetch digital AWB data and more. The module could fetch the AWB data and any available documents from airline cargo management systems directly, allowing users to query with an AWB number instead of scanning it. Upon verifying the AWB and supporting documents, this module can synchronize the digitalized AWB and supporting documents to airline cargo systems, along with any additional information provided by the LLM during the document validation process.

- REST API Connectivity: In a hypothetical multi-tenant world different airline cargo systems can connect to this solution via REST APIs built on OpenAPI specifications. Cargo systems can use these APIs to upload AWBs and supporting documents in real-time for validation. This module will maintain all LLM subscriptions and use them based on the airline utilizing the service.

Cost Implications

The implementation of an LLM-based solution in general involves various cost factors that are crucial for budgeting and strategic planning. Beyond the obvious licensing, security, development and operational costs, the infrastructure ones can be significant as the LLM inference is still in its infancy and does not benefit yet from full economies of scale. Efficient management of infrastructure costs without compromising the quality of the cargo document validation process can be achieved through:

- Optimizing input to reduce unnecessary LLM inquiries, focusing on precise and relevant queries to decrease token usage and processing time.

- Batching Requests: Handling multiple documentation checks in a single batch to maximize throughput and minimize per-transaction processing costs.

- Memory Management Techniques: Implementing strategies such as data summarization to handle large documentation and sections within documents efficiently (e.g. PCR or sections of PCR).

- Model Distillation: replacing complex models with smaller ones purposefully fine-tuned for a specific task that will reduce computational demands, especially beneficial in scaling operations, while providing better results.

While generic solutions (using available LLMs like OpenAI in market with language understating but lacking knowledge of regulation of international cargo export) may offer cost benefits through scalability, the complex and varied nature of international cargo regulations often necessitates tailored solutions (fine tuning model for domain specific information and jargons), which might be more resource-intensive to start with but crucial for compliance.

The adoption of cost-saving strategies must be judiciously balanced with the imperatives of accuracy and compliance in the cargo industry. The potential financial and operational impact of documentation errors in cargo acceptance necessitates a focus on maintaining high-quality outputs from AND inputs (up-to-date accurate regulations and other sources) into the LLM. Investments in advanced LLM capabilities (RAG, finetuned model, etc.), though initially more costly, can prevent significant losses due to non-compliance and enhance overall operational efficiency.

By strategically implementing these cost optimization strategies and carefully considering the trade-offs, cargo operators can ensure that the adoption of LLM technologies not only supports cost-effective operations but also robustly meets the stringent requirements of cargo documentation and compliance. This approach ensures an efficient and compliant cargo acceptance process that can adapt to the evolving demands of the industry.

Finally, we end this section acknowledging that these are the very early stages of the technology and that many opportunities for further optimization and cost savings lie ahead. Just as this paper was going to “press” DeepSeek R1 shook the AI world with a reasoning engine significantly cheaper to train and perform inference on versus the established players. Maybe the most relevant recommendation we can come up with is to build loosely coupled solutions to easily swap models as cheaper, more effective ones come along.

Results

To validate the approach and focus the POC on a "provable" outcome within the limited time available, the group designed approximately 30 test cases. These cases targeted key routes and perishable commodities relevant to the three participating airlines—all Nippon Airways, LATAM, and Qatar Airways.

The test set included sample documents, such as AWBs and supporting materials, for both valid cases (correctly labeled sets) and invalid cases (with missing or incorrect information, along with detailed explanations). This approach enabled testing a range of edge cases, including poor-quality documents and mismatches between AWBs and supporting files.

The results were promising. The LLM-based modules developed by the Strategic Partners correctly 90% of the test cases. While this accuracy may seem high or low depending on perspective, the limited sample size and its bias toward edge cases—uncommon in real-world scenarios—suggest that the POC successfully demonstrated the technology's real-world applicability.

Lastly, while IT-driven automation is often expected to deliver 100% deterministic results (e.g., an accounting system must close accurately), the bar for automating certain processes is not absolute perfection but rather exceeding human performance. LLMs are probabilistic systems that will never produce identical outputs consistently. Instead of aiming for flawless execution, the goal should be to outperform human capabilities in efficiency and accuracy.

Conclusion

The POC's AI-driven compliance validation serves as a real-world demonstration of how technology can help support wider compliance with key aviation standards information and access, connecting to IATA's long-term roadmap. It shows how LLMs can extract insights from IATA standards and industry regulatory texts while maintaining information integrity and secure access through digital channels. Airlines, cargo operators, and technology partners increasingly demand automated, scalable compliance tools, and IATA is well positioned to support the delivery of structured regulatory data and information.

Beyond compliance validation, IATA's vision together with industry extends to broader AI applications in regulatory operations that support people in conducting their work—enhancing automated risk assessments, preemptive compliance checks, and seamless integration with airline workflows.

The API-first model is central to this vision, eliminating outdated distribution methods such as PDFs and ensuring that all regulatory content is securely accessed through structured, value-added API services or AI-driven tools. This controlled access preserves data integrity and aligns with the evolving needs of airline IT teams and regulatory partners.
As AI adoption accelerates, IATA remains committed to continuous innovation in regulatory access, ensuring that its datasets remain authoritative and trusted for industry compliance, and not at the cost of critical human factors and knowledge of standards application. This POC serves as a foundational step toward a fully digital regulatory ecosystem, where AI and APIs streamline airline operations together with human intelligence, while helping to safeguard industry standards and safety compliance.

At the start of our industry LLM POC journey, our goal was to explore innovative applications of this emerging technology in the air transport industry beyond the common chat-based interfaces that dominated early demonstrations. While we focused on regulatory compliance in the air cargo sector, we hope this work has sparked new ideas and excitement for how LLMs could transform other areas of aviation and beyond.

2. Project 777

from **7**
Business days
to registration

to **7**
Seconds
to registration

with **7**
new
workflows

Vision

In the short to medium term both customers and ecosystem actors will have digital identities. There are use cases already defined to verify agencies' identity but managing agency users' identities is crucial for preventing fraud and simplifying onboarding and management processes.

The travel industry can benefit by implementing a secure, efficient, and seamless digital identity management system that ensures the integrity and trustworthiness of travel agency operations worldwide. Leveraging Digital Wallet and Digital employee ID agents will be able to instantaneously onboard.

Vision description

This project seeks to expand on the previous year's B2B use case—Agency Onboarding Pilot. As a prerequisite, the agency must obtain an IATA code, select a digital wallet, and register its cryptographic identifier along with its IATA code in a directory.

We aim to create an eco-system that addresses the critical challenges of identity management and fraud prevention in the travel industry. By leveraging the power of issued Digital Credentials, we will provide travel agencies and airlines with a robust digital identity framework that not only enhances security but also streamlines operational processes. This shift will move the industry towards a more secure and efficient future.

Our vision includes the creation of a unified authentication framework that will eliminate the need for multiple logins and credentials across different airline B2B portals. This consolidation will enhance efficiency when enabling and deactivating user access, reducing fraud risk and increasing overall operational effectiveness. The standardized approach to identity verification and fraud prevention will not only protect sensitive data but also build a more resilient and connected travel ecosystem. To achieve this vision, we propose to leverage:

- The capability for agencies to issue and manage employees' digital credentials
- Digital identity wallet for credential storage
- Open standard solution

By integrating digital identity management into travel operations, we aim to ensure a secure, efficient, and user-friendly experience for the airlines' agencies partners.

Current situation

As airlines expand direct distribution and new distribution channels, many agencies are now moving towards a direct distribution model. With this new model, agencies must register into each airline's direct B2B platforms. Today, there is no standard way to validate that the person triggering the registration in the airline portal is legitimately representing the agency they declare, which raises concerns about fraud. Due to airlines' focus on preventing fraudulent activities, the agency onboarding process remains highly manual, often taking several days or weeks.

This extended time is attributed to the absence of data linking agents to agencies, which is essential for ensuring the legitimacy of requests. Consequently, human analysis and intervention are required for each request, often requiring back-and-forth communication with the agency for approval. The current process is inefficient, unreliable, and unsustainable for both airlines and agencies, adversely affecting cost.

The staff deactivation process is more cumbersome as the agency manager must remove the staff from each airline portal. The airline does not have any standard way to know about the departure of staff from an agency. If the agency manager did not action, then the staff who had left an agency can still gains access to the valuable information thus resulting in data leaks or even financial losses.

Fraud types

- **Impersonation**
  Fraudsters use a legitimate IATA number to book through BSP Cash, charging the agency that did not sell the ticket resulting in financial loss.

- **Willful misconduct**
  A former employee uses their active credentials to cancel customer reservations, with the aim of maliciously impacting agency operations and integrity. This highlights the importance of promptly revoking access for departing staff. This situation can be more difficult to manage when agencies use shared credentials (same username and password used by multiple employees in the same agency).

Proof of Concept

Scope

This Proof of Concept (PoC) validates the 7 workflows outlined in the table below, focusing on an agency employee interacting with 4 different airline B2B portals. Three of these portals are implemented directly by airlines and integrated with Verifiable Credential (VC) verification services provided by multiple technology providers. The PoC demonstrates interoperability across multiple end-to-end workflows, combining credential issuance (by travel agencies), wallets (mobile and web), and verification capabilities from multiple independent technology implementers.

#	Workflow	Description
1.	Agent Digital employee ID issuance	Agency to issue agent credentials
2.	Agency registration (not all airlines use it)	Application form information generated from digital wallet data attribute
3.	Agency approval (not all airlines use it)	Automatic approval triggered for application triggered with an agent Digital Identity linked to a partner agency profile
4.	User self-registration in airline portal	Upon first login to airline portal, all necessary information about an Agent is presented to the Airline. Upon submission of the information the qualification is automatic, and user profile is automatically created in the airline portal
5.	Agent authentication via mobile app	Mobile authentication for agent login
6.	Agent authentication via desktop app	Desktop authentication for agent login
7.	Agent digital ID revocation	Agency to revoke agent digital credential

This PoC introduces a governance stack alongside the technology stack. The trust framework addresses questions, such as whether the issuer's DID corresponds to a trusted travel agency (linked to their IATA code via the Trust Registry) and whether the entity is authorized to issue specific credential types. Airlines, as relying parties, can implement validation policies that leverage Trust Registry lookups to verify issuer legitimacy and credential authorization.

Scenario

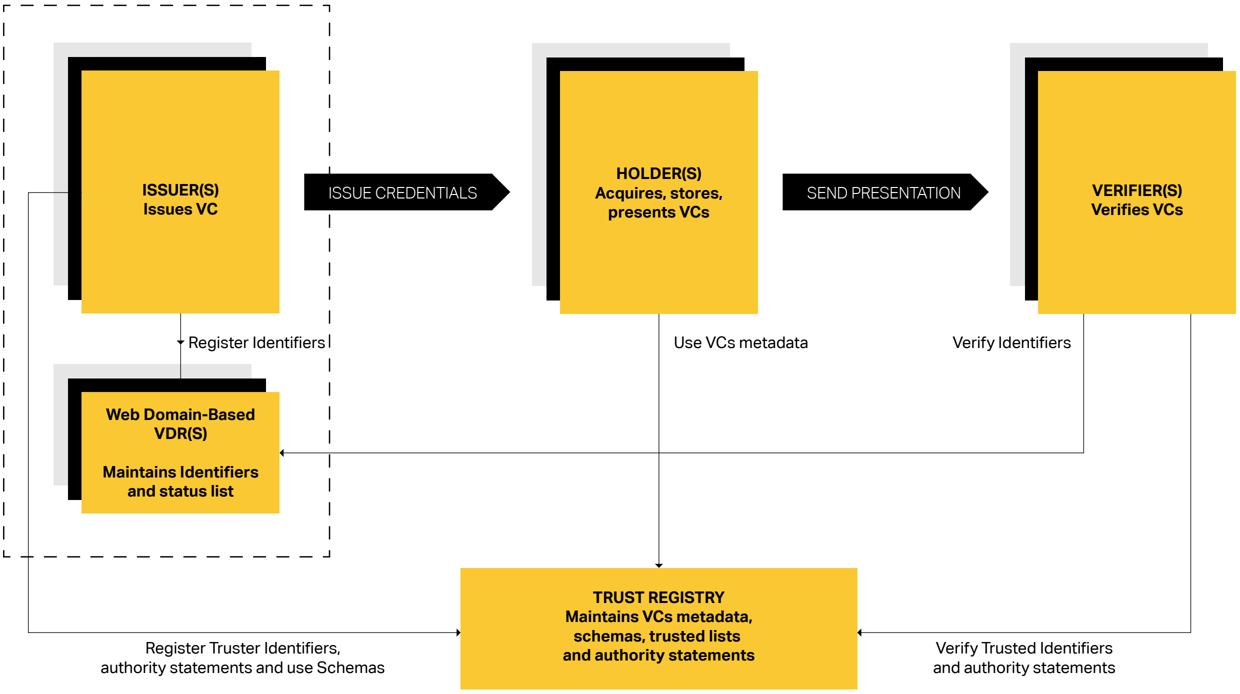
The PoC validates the following interactions:

- Digital Employee ID Issuance: A travel agency issues digital employee IDs (Verifiable Credential) to 3 employees, each using a different digital wallet (mobile or web-based).
- Cross-Airline Registration & Login: Each employee registers and logs in on 4 different airline B2B portals using their digital wallet, demonstrating interoperability across airline systems.
- Revocation: The agency revokes the digital employee ID of one travel agent triggering deactivation of their access across all 4 portals.

Decentralized Identity Implementation & Standards
This Proof of Concept leverages the principles of decentralized identity by adopting standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). These standards ensure a secure, interoperable framework for managing digital identity, allowing individuals and organizations to establish trust without relying on centralized authorities. By leveraging these standards, which form the backbone of a modern digital identity ecosystem, the PoC establishes a robust foundation for secure and trusted interactions within the travel industry.

For this PoC, the decentralized identity ecosystem relies on the following roles and responsibilities:

- **Issuer(s)**
  Travel agencies create and issue Employee Verifiable Credentials (VCs) to their travel agents.
- **Holder(s)**
  Travel agents securely store Employee VCs in a digital wallet and present them as required when onboarding or logging into airline portals.
- **Verifiers(s)**
  Airlines validate Employee Verifiable Presentations (VPs) during interactions with travel agents to confirm their authenticity.
- **Verifiable Data Registry(s)**
  Maintains identifiers and status information needed to verify the validity and revocation status of Employee VCs, based on each travel agency's web domain. Each travel agency manages its own web-domain-based VDR.
- **Trust Registry**
  The Trust Registry maintains VC type metadata, schemas, a trusted list of issuers, and credential issuance authority statements. VC type metadata and schemas define the rules, structure, and display requirements for specific types of Verifiable Credentials (VCs), guiding issuers, verifiers, and wallets on how to manage and validate credentials. The trusted list of issuers and credential issuance authority statements supports airlines (verifiers) by enabling them to implement validation policies that ensure only trusted travel agency issuers and authorized credentials are accepted.


ISSUER(S)
Issues VC
ISSUE CREDENTIALS
HOLDER(S)
Acquires, stores, presents VCs
SEND PRESENTATION
VERIFIER(S)
Verifies VCs
Register Identifiers
Use VCs metadata
Verify Identifiers
Web Domain-Based VDR(S)
Maintains Identifiers and status list
TRUST REGISTRY
Maintains VCs metadata, schemas, trusted lists and authority statements
Register Truster Identifiers, authority statements and use Schemas
Verify Trusted Identifiers and authority statements

Interop profile

This Proof of Concept (PoC) has developed and implemented an Interoperability Profile as a central approach to implement decentralized digital identity standards across different technology providers.

An Interoperability Profile is a set of specific guidelines and requirements designed to ensure that different vendors can work together seamlessly. It defines how core components such as VC formats, VC exchange protocols, identifiers, and security mechanisms should be implemented, reducing complexity and variability. By standardizing these elements, the profile ensures consistent, and reliable interactions across the ecosystem.

This table summarize the different standards use in this PoC:

Component	Standard	Purpose
VC issuance	OpenID for Verifiable Credential Issuance Implementors Draft v1 https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html	Defines how an Issuer and a Wallet perform the issuance flow (pre-authorized code flow, credential offer/response).
Holder binding	SD-JWT VC	Ensures the Verifiable Credential is bound to the holder's wallet.
VC presentation	OpenID for Verifiable Presentations OID4VP 20 https://openid.net/specs/openid-4-verifiable-presentations-1_0-20.html	Describes how a Holder presents credentials (Verifiable Presentations) to a Verifier, including request and response flows.
Data format and validation rules to express VC	SD-JWT VC draft-ietf-oauth-sd-jwt-vc-07 https://datatracker.ietf.org/doc/html/draft-ietf-oauth-sd-jwt-vc-07	Enables selective disclosure and cryptographic binding of claims in a Verifiable Credential.
VC Revocation	OAuth 2.0 Credential Status List draft-ietf-oauth-status-list-05 https://datatracker.ietf.org/doc/html/draft-ietf-oauth-status-list-05	Defines a status list mechanism for revocation checks (active/revoked) so Verifiers can ascertain a credential's validity.
Decentralized Identifiers	did:web https://w3c-ccg.github.io/did-method-web	Specifies a method for hosting DID documents on HTTPS web domains, enabling domain based DID resolution for key material.
Cryptographic Suites	P-256 (secp256r1) ES256 (JWT)	Establishes Elliptic Curve Digital Signature (ECDSA) requirements for signing and signature validation (SHA-256 hashes).
Trust Registry	Ad-hoc	Enable airlines to implement validation policies that ensure only trusted travel agency issuers and authorized credentials are accepted in the ecosystem. Link DID to an IATA code.

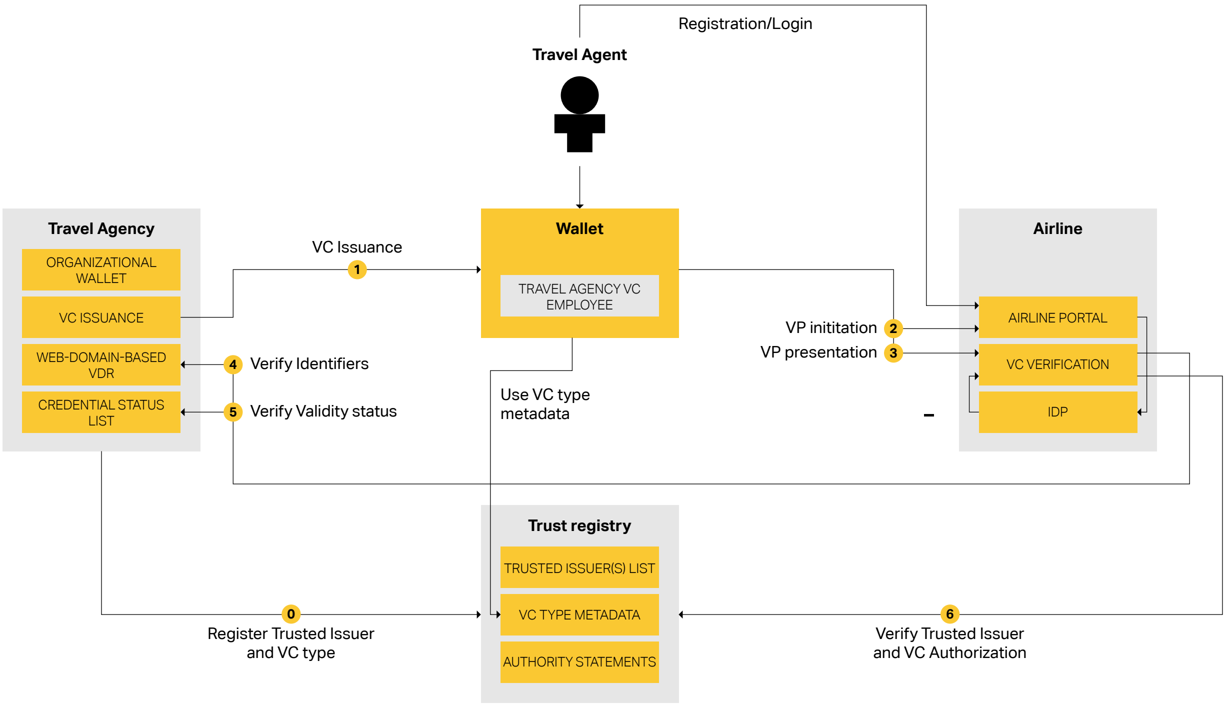
Component Implementation overview

Based on the interoperability profile, multiple independent implementations have been developed to demonstrate interoperability within a standards-based setup. The table below highlights the different implementations for each component.

Component	Implementation
Issuer	2 Technology providers
Wallet	3 Technology providers: 2 native mobile wallets and a web-based (cloud) wallet
Verifier	4 Technology providers
Trust registry	1 Technology provider

Ecosystem Blueprint

The diagram below illustrates the high-level PoC ecosystem, highlighting how travel agencies issue credentials to their employees and how airlines verify these credentials.



Prerequisites

Before issuing and managing Verifiable Credentials, travel agencies must first onboard the ecosystem by registering with the trust registry. This enables their partners to rely on the credentials they issue without a bilateral set up with each airline partner.

Travel Agency

Travel agencies play a critical role in managing the lifecycle of Employee Verifiable Credentials (VCs) issued to their travel agents. In the diagram, three key components represent the capabilities required to fully manage the VC lifecycle:

- **VC Issuance**
  Enables travel agencies to create and issue credentials to employees' digital wallets.

- **Web-Domain-Based VDR**
  Anchors the DID document associated with the travel agency's DID to a web domain controlled by the agency, allowing verifiers to resolve the DID document and access verification keys.

- **Credential Status List**
  Maintains the validity of all credentials issued by the agency, enabling actions such as revoking credentials as needed (e.g., when an employee leaves the agency).

For the PoC, a Travel Agency Employee VC has been designed to include the following information: salutation, given name, surname, phone number (including country code and local number), employee ID, email, and job title.

Travel agencies issue these credentials to verified employees' digital wallets, enabling travel agents to share this verifiable information with airlines, which can then instantly confirm the information's authenticity.

Travel agent and Wallet

Travel agents can choose between a mobile or web-based digital wallet, where a Travel Agency Employee VC is issued. The PoC explores both form factors to address different use cases, including scenarios where mobile devices are available and those where they are not accessible in a corporate setup (e.g., due to place of work restrictions).

Once the digital wallet is fully provisioned, it enables authorized travel agency personnel to gain access to the airline's booking platform efficiently and securely. This is achieved by sharing verifiable information requested by airlines during the onboarding process for instant verification or by using the credential as an authentication mechanism during the login step.

For this PoC, one of the proposed improvements for wallet implementation is the harmonization of how Verifiable Credentials are displayed in wallets, including graphical elements and translation-based artifacts. This ensures that wallets can present credentials in a way that aligns with the intent of the provider of the VC visualization rules, which in this PoC is a standardization body such as IATA.

Airline

Airlines provide three key components as part of this PoC. First, an airline portal is used to consume Verifiable Credentials during the onboarding process of travel agents or the login process, enabling instant verification of employee data. Second, the airline's existing Identity Provider (IDP) is enhanced to register travel agent information as it does today, but now with authentic, error-free data. Third, the IDP integrates a new authentication mechanism to enable users to log in using VCs.

The VC verification service performs three key functions: first, it cryptographically verifies the validity of the credential, second, it ensures the trustworthiness of the proof by confirming the issuer is a trusted travel agency (linked to their IATA code via the Trust Registry) and that the credential type is authorized within the ecosystem, and third, it ascertains the credential's ongoing validity by checking its revocation status through a status list mechanism.

Trust Registries

The Trust Registry enables airlines to verify that a credential originates from a trusted agency by providing a mapping between the issuer's DID and their IATA code. While the registry also validates whether issuers are authorized to issue specific credential types, this capability is secondary in the current PoC, as only one credential type (Travel Agency Employee VC) is in use.

Additionally, the Trust Infrastructure is responsible for managing Verifiable Credential (VC) metadata, schemas, and type definitions, serving as a centralized repository for credential specifications. It hosts detailed descriptions of each credential type, including mandatory and optional claims, data formats, and display requirements. By ensuring uniformity in how credentials are issued, presented, and validated, the Trust Infrastructure provides an interoperable, and scalable foundation for the ecosystem.

Process Steps

Below is a high-level overview of the steps in the ecosystem, illustrating how Travel Agencies issue credentials, how Travel Agents present them, and how Airlines verify them against the Trust registry.

Prerequisite

The Travel Agency (issuer) must be fully provisioned:

- Signing keys: Cryptographic keys are generated and associated with the issuer.
- DID and DID Document: A DID using the did:web method is anchored, and a DID Document containing the Travel Agency's public keys and metadata is accessible via the internet.

Step 0: Register Trusted Issuer and VC Type

Before issuing any credentials, the Travel Agency must register with the Trust Infrastructure:

- The Travel Agency's DID and IATA code is added to the Trusted Issuers List maintained by the Trust Registry.
- The issuer (travel agency) request for credential issuance authority from the Trust Registry to issue a Travel Agency Employee VC.

Step 1: VC Issuance

The Travel Agency issues a Verifiable Credential (VC) to the Travel Agent's wallet:

- The Travel Agency Employee VC is cryptographically signed using the issuer's private key.
- The credential includes a status claim pointing to a Credential Status List, allowing verification of whether the credential is active or revoked.
- The VC is bound to the Travel Agent device and securely delivered to their wallet.

Step 2: VP Initiation

When the Travel Agent wants to access the Airline's B2B portal (e.g., for login or registration), the following occurs:

- The Airline Portal displays a QR code. The QR code can be scanned, or the QR code content can be copied for a manual proof request transfer to the web wallet. The QR code encodes a URL containing a proof request.
- The Travel Agent either scans the QR code using a mobile wallet or copies and pastes it manually into a web wallet, which triggers the wallet to initiate the Verifiable Presentation (VP) process.

Step 3: VP Presentation

The Travel Agent's wallet responds to the proof request:

- The wallet prepares a Verifiable Presentation, which may include selective disclosure, ensuring only the necessary claims are shared.
- The cryptographically signed presentation is sent to the Airline's verification service.

Step 4: Verify Verifiable Presentation

The Airline's verification service validates the Verifiable Presentation:

- It resolves the issuer's DID using the did:web method.
- The service retrieves the issuer's DID Document to access the associated public key.
- Using the public key, the verifier cryptographically checks the integrity and authenticity of the Verifiable Presentation.

Step 5: Verify Credential Status

The verifier consults the Credential Status List (referenced in the credential's status claim):

- The verifier retrieves the Status List from the issuer's specified URL.
- It checks the status bit corresponding to the credential to confirm whether the credential is active or revoked.

Step 6: Verify Trusted Issuer type

The verifier ensures the issuer and credential type are trusted:

- The verifier checks that the issuer's DID is listed in the Trusted Issuers List in the Trust Registry, confirming the Travel Agency is onboarded.
- The verifier checks that the issuer is authorized to issue the Travel Agency Employee VC by consulting the Trust Registry, which contains the necessary credential issuance authority statements. The trust registry returns the Travel Agency's IATA code associated with the issuer DID. Airlines can use this IATA code retrieved from the trust registry to match it against the list for agency partner recorded in their systems
- If the validation process pass, the verifier confirms the information is authentic and trustworthy, allowing the Airline to proceed with its business processes.

Benefits

Benefits	Agency/Employee	Airline
Increased Security and Fraud Prevention Only verified and authorized individuals can access the airline's booking platforms, limiting fraud risk and impersonation.	✓	✓
Enhanced Operational Efficiency Seamlessly linking agency profiles with agent access, supporting immediate agency registration, with reduced administrative overhead.	✓	✓
Enhanced User Experience Unified authentication mechanism for all platforms, simplifying the management of multiple credentials.	✓	
Authorization Policies Credentials revocation is managed centrally, blocking user access to all airline platforms.	✓	✓
Flexibility Option to use mobile and web wallet authentication	✓	
Industry Standardization Promoting consistency and trust across all stakeholders.	✓	✓

By establishing this comprehensive ecosystem model, we aim to create a secure, efficient, and trustworthy digital identity management system that will drive the travel industry towards a future of enhanced security and operational excellence.

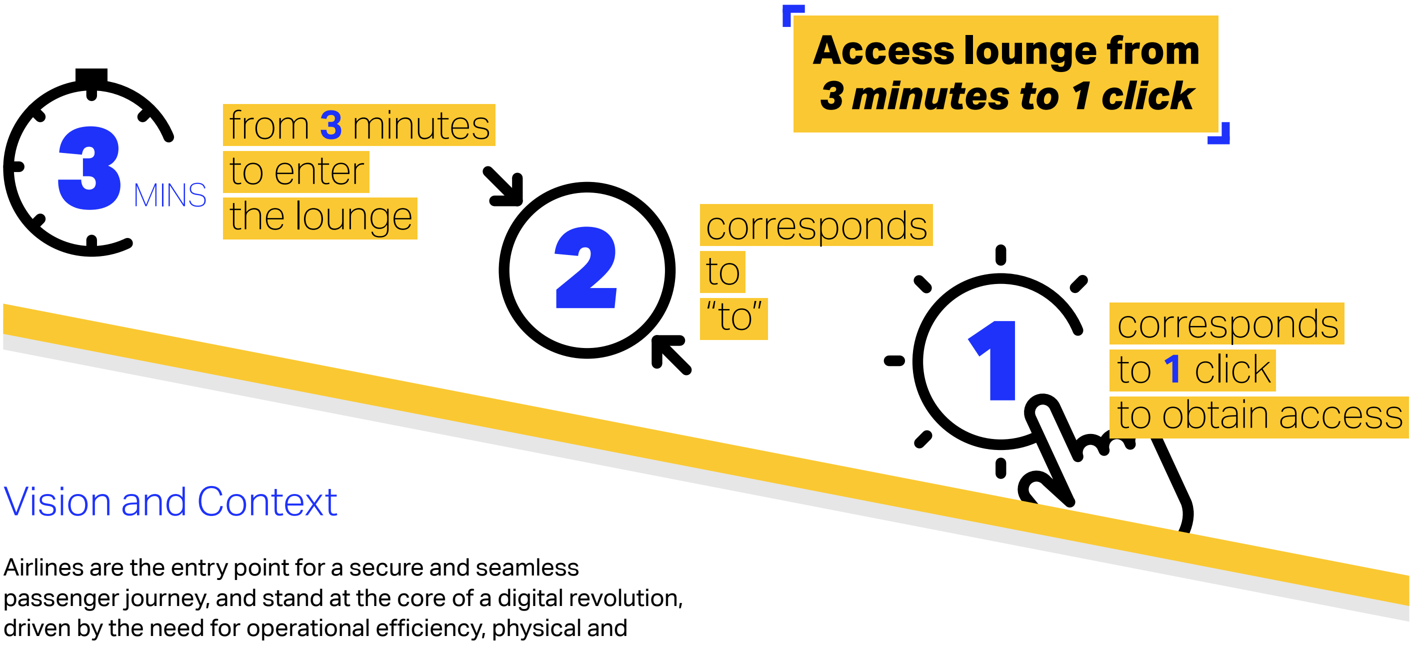
Implementing Agency digital employee ID, the onboarding process can become automated, linking agency profiles with agent access seamlessly. This framework will ensure secure and reliable identity verification, significantly reducing the time and effort for onboarding "from 7 business days to 7 seconds".

Next Steps

The 2024 777 project recommends that IATA and/or its Member Airlines:

- **Develop a standard schema for digital employee ID (Verifiable Credential).**
- **Develop an implementation guide for onboarding and log in with a digital employee ID (Verifiable Credential).**
- **Explore solutions to improve the UX for web wallets implementations.**
- **Explore the usability of such digital employee ID to enable airlines to authenticate the agency or sub agency in intermediated distribution via the airline NDC channel.**
- **Set up a trust registry to allow easier adoption at scale.**
- **Set up an interoperability test bed to help implementers.**
- **Support the development of reference implementations in the most popular technical stacks to ease interoperability.**
- **Explore the usability of such digital employee ID in the distribution of corporate deals.**
- **Advocate for private and government issued Digital Wallet to support standard digital employee ID when available.**

3. Project 321



Access lounge from *3 minutes to 1 click*

3 MINS
from 3 minutes to enter the lounge
2
corresponds to "to"
1
corresponds to 1 click to obtain access

Vision and Context

Airlines are the entry point for a secure and seamless passenger journey, and stand at the core of a digital revolution, driven by the need for operational efficiency, physical and digital security, and seamless passenger experiences. As global travel is back to pre-pandemic levels, airlines feel again the need for improved efficiency to handle passenger volumes, airports introduce changes in their infrastructure for achieving operational efficiencies (e.g. biometric kiosks), and customer expectations on digital experiences rise. The integration of Verifiable Credentials (VCs) emerges as a groundbreaking solution to address long-standing challenges. These cryptographically secure, tamper-proof digital credentials offer a decentralized and privacy-preserving way to verify identities, and travel documents, eliminating inefficiencies tied to traditional paper-based processes.

From streamlining passenger onboarding to enhancing compliance with international regulations, VCs with Digital Identity Wallet are poised to reshape how travelers and airlines interact. By fostering trust across stakeholders and empowering passengers with greater control over their personal data, this technology also builds a foundation for future innovations in on-device security, biometrics, digital identity ecosystems, and contactless travel. Together, Airlines, Airports, and Immigration can establish a Trust Framework—a unified ecosystem where verifiable credentials are recognized and trusted across borders, and across these stakeholders.

Verifiable Credentials issued as a derivative of a Know Your Passenger (KYP) process amplifies the value proposition for adopting this travel framework. By incorporating KYP into it, airlines and airports can conduct secure, real-time identity verification of passengers before they even reach the airport. This proactive approach enhances security, reduces the risk of fraud, and creates a personalized experience by tailoring services to individual passengers' needs. For travellers, KYP provides peace of mind, as their credentials are securely verified once and can be reused across multiple interactions, all while maintaining strict control over how and when their data is shared, building an Identity Trust Framework where Passenger becomes also part of it.

Additionally, the implementation of Selective Disclosure of Identity Attributes of the Passengers lets the Airlines build status such as "ready to travel"—a state where passengers have all the required documents, such as passports, visas, health certificates, and boarding passes, verified and readily accessible before arriving at the airport. By leveraging Verifiable Credentials, this vision becomes a reality, enabling travellers to securely store, manage, and share their identity attributes beforehand in a seamless and secure manner. Airlines, airports, and governments (i.e. Digital Identity Trust Framework) can instantly verify these documents, reducing bottlenecks at check-in, security access, and boarding, and providing passengers with a frictionless journey. The adoption of digital ID can significantly reduce the reliance on physical documents and the cumbersome processes associated with them. Decreasing the time spent by both staff and customers on administrative tasks. This shift towards a more digital-centric approach aligns with global efforts to promote eco-friendly operations within the aviation sector. By embracing Verifiable Credentials and a Digital Identity Trust Framework (Airlines, Airports, and Immigration), the aviation industry can deliver a transformative travel experience—one that prioritizes speed, security, and passenger convenience in an era of increasing demand for contactless and privacy-first solutions.

The Data & Technology PoC team has targeted three pain points to resolve. Since these issues are purely service-related and not driven by regulatory and compliance requirements, they present unique challenges to improving the customer experience. As a consequence, this PoC does not focus on biometrics and passport check as part of compliance requirements.

Current State

Challenges in Identity and Entitlement Management

The B2C identity landscape is hindered by inefficiencies, security risks, and fragmentation, preventing a seamless and contactless travel experience for passengers. The key challenges include:

- **Fragmentation of Identity Systems**
  Consumers interact with multiple stakeholders (airlines, airports, lounges, and service providers), each managing identity independently. This leads to redundant data collection, inefficiencies in user verification, and a fragmented experience, particularly for customers not existing in an airline's database.

- **Privacy Concerns and Over-Sharing of Data**
  Traditional identity management relies on centralized systems and PNR data exchanges, often resulting in over-sharing of Personally Identifiable Information (PII) like passport details and dates of birth. Meanwhile, critical entitlement-related information is frequently missing, limiting personalized service delivery.

- **Inefficiencies in Centralized Systems**
  Current systems require passengers to create multiple accounts and repeatedly share personal data across services, which are stored in silos. This leads to repeated identity verification, long queues at check-in and security, and inefficiencies in entitlement validation for services like lounge access and Wi-Fi.

- **Complexity in Verifying Entitlements**
  Eligibility verification for entitlements such as lounge access, onboard Wi-Fi, and other ancillary services is increasingly complex. Entitlements are tied to multiple criteria, including credit card partnerships, high-tier loyalty status, paid programs, and agreements beyond the airline's control, leading to inefficiencies in the verification process.

- **Settlement and Reconciliation Issues**
  Entitlement validation often requires settlement between multiple service providers (e.g., airlines and lounge operators). The lack of integrated systems and real-time capabilities results in manual processes, increased costs, and inefficiencies.

- **Security and Trust Concerns**
  Traditional centralized systems, relying on passwords and manual processes, are vulnerable to phishing attacks, data breaches, and unauthorized access. The lack of privacy safeguards and reliance on single points of failure harm customer trust and brand reputation.

- **Lack of Interoperability**
  Existing identity management systems lack standardization and interoperability, forcing passengers to repeatedly provide and verify their information across platforms, regions, and industries. This results in inconsistencies in service delivery and operational inefficiencies.

Existing Systems and Gaps

Existing Systems

1. **Centralized Identity Systems**
   Airlines and service providers rely on centralized databases to manage passenger identity and entitlements. These systems are functional for basic operations but struggle to accommodate modern complexities like loyalty partnerships, joint ventures, interline agreements, and perks tied to credit cards or paid programs.

2. **PNR-Based Data Exchange**
   The exchange of PNRs via EDIFACT messages remains the backbone of passenger data sharing between airlines and service providers. While this method includes sensitive PII such as passport details, it often lacks critical data like precise loyalty tier mapping or partner-program entitlements. This over-sharing of PII creates privacy concerns and compliance challenges, especially with modern data protection regulations such as GDPR.

3. **Loyalty Program Integration**
   Airline alliances have implemented centralized databases for tier mapping and benefit sharing, yet these databases are incomplete and lack a standardized framework for querying data. This results in delays and inefficiencies, particularly when recognizing entitlements for high-value customers across interline or codeshare agreements. Alternatively partner airlines exchange subset of loyalty data bases that beyond the above requires extensive work to protect customer PII and airline confidential information.

4. **Lounge and Wi-Fi access systems**
   Passengers must frequently present physical credentials, such as boarding passes or membership cards, to gain lounge access. This process introduces inefficiencies, as frontline agents must manually verify entitlements based on a mix of booking class, frequent flyer status, credit card partnerships, and paid subscriptions. Human errors in verification can lead to customer frustration, delays, and inconsistencies in access.

5. **Onboard Wi-Fi Authentication Systems**
   Onboard Wi-Fi services often require passengers to log in using loyalty account credentials. However, nearly 30% of passengers forget their loyalty account passwords, creating a significant barrier to access. Current systems do not offer seamless authentication alternatives, leading to frustration and a subpar customer experience.

6. **Manual Entitlement Validation**
   Eligibility for entitlements, such as lounge access or extra baggage, is often tied to complex criteria from loyalty tiers, bank programs, or partner agreements. These are frequently decoded manually by frontline staff, leading to inefficiencies and increased risk of errors.

Gaps

1. **Customer Experience Challenges**
   Forgotten loyalty account credentials, fragmented service delivery, and delays in entitlement recognition degrade the passenger experience. High-value customers expect seamless and personalized services, which current systems struggle to deliver

2. **Onboard Service Accessibility**
   The absence of real-time, user-friendly authentication systems for onboard services, such as Wi-Fi, results in lost opportunities to enhance passenger satisfaction and generate ancillary revenue.

3. **High-Value Customer Recognition**
   Incomplete or missing data in shared systems, such as loyalty tier mapping or partner airline entitlements, hinders airlines' ability to prioritize high-value customers. This not only impacts service delivery but also increases the risk of losing these customers to competitors due to poor recognition or experience.

4. **Data Privacy and Security Risks**
   Sharing customer data across airlines and partners involves sensitive Personally Identifiable Information (PII), including high-value customer profiles and loyalty program details. Current methods lack robust privacy safeguards, exposing data to risks such as breaches, unauthorized access, and misuse. Ensuring compliance with global privacy regulations, such as EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), remains a significant challenge. Over-sharing of data, often beyond what is needed for entitlement validation, exacerbates privacy risks.

5. **Interoperability and Standardization**
   Existing systems are not designed for seamless integration of identity and entitlement data across multiple stakeholders, including airlines, airports, and third-party providers. The lack of interoperability leads to fragmented passenger experiences and operational inefficiencies.

6. **Cost and Operational Inefficiencies**
   Sharing and managing data across loyalty partnerships and interline agreements increases IT costs. Airlines and partners must continuously update systems to accommodate new agreements and evolving criteria, creating ongoing operational challenges. Manual processes further contribute to inefficiencies.

Case for Change

To address these challenges, decentralization of identity management, along with secure storage and controlled access to identity data, is key. This is where we see significant potential in leveraging digital identity technologies that are built around decentralized identity and interoperability concepts. By adopting these principles, the industry can enable seamless, secure, and privacy-compliant passenger authentication, reducing inefficiencies and enhancing the overall travel experience.

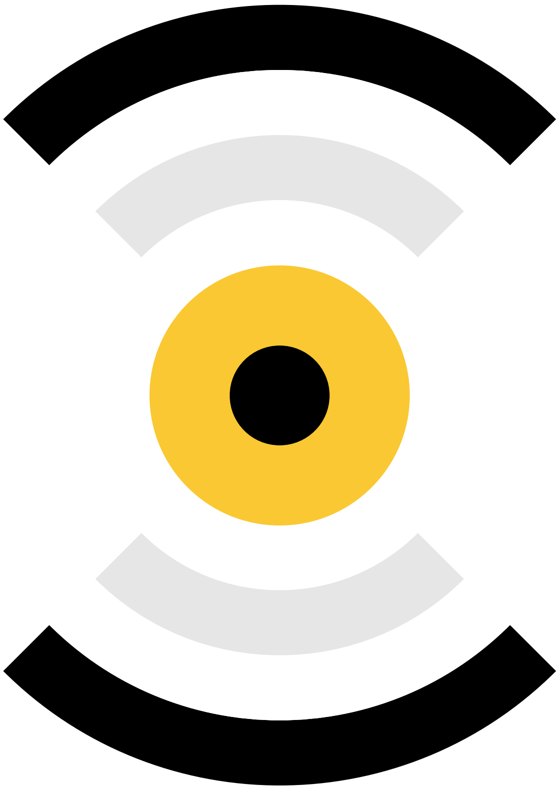
The PoC

Use Cases

The Data & Technology PoC team has targeted three paint points to resolve. Since these issues are purely service-related and not driven by regulatory and compliance requirements, they present unique challenges to improving the customer experience.

Digital Identity for Seamless Wi-Fi Access on the Ground

Getting access to Wi-Fi network in the terminal is often conditioned by agreeing to local government rules for internet access such as accepting term and conditions and providing certain personal information data entry can be simplified, and government authorities can obtain trustworthy data by leveraging digital identity.



PoC Steps
Athena Airlines and Kronos Airlines are partner airlines. Top tier customers with Athena Airlines can access Kronos Airlines lounge even when traveling in economy with Kronos Airlines.

As a pre requisite to the PoC steps:

- Athena issues a top tier loyalty credential to the customer mobile wallet.
- Kronos issues a boarding pass credential to the customer mobile wallet (without entitlement for lounge access in boarding pass).
- A trusted party issues a passport copy credential to customer mobile wallet.

1. The passenger locates a static QR code displayed near the lounge entrance.
2. The passenger scans the QR code using a mobile device.
3. The **Kronos Airlines Wi-Fi captive portal** opens on the passenger's device.
4. The passenger is prompted to provide **first name, last name, passport number, and nationality** for Wi-Fi access.

   Two options are available:

   - **Option 1**
     Share the required details securely from the **Digital Wallet**.
   - **Option 2**
     Manually input the required details using the **traditional login method**.
5. The passenger chooses to share credentials via the **Digital Wallet**.
6. The passenger Digital Wallet contains **verifiable credentials (VCs)** for **frequent flyer program (FFP), boarding pass, and ePassport**.
7. The passenger consents to share the required data elements of the passport directly from the **Digital Wallet**.
8. The **passenger's identity is verified** in real time leveraging the **trust registry** in the background.
9. Upon successful verification, the passenger is granted **Wi-Fi access** and is redirected to the **Wi-Fi welcome page**.
10. The **welcome page** also provides an **option obtain access to the lounge**, leading to the next use case.

Verifiable Credentials for Effortless Lounge Access

Full-service carriers, service providers and even Airport authorities operate lounges across the globe, serving as an ancillary revenue stream, but not without management and operational complexities.

This is due in part to the many profiles of customers who are authorised to access the facility:

- Premium cabin passengers (First and Business Class).
- Top Tier Frequent Flyer programme holders (applicable to interline, codeshare and joint-venture agreements between carriers).
- In the case of involuntary upgrades resulting from overbooking, customers are often not permitted lounge access—Conversely, those were downgraded from a premium cabin, maintain lounge access eligibility.
- Complimentary access holders (such as service recovery options).
- VIPs and CIPs (Very Important and Commercially Important Persons).
- Paid access for those willing to pay a fee to access the facility.
- Credit Card and Banking customers who have specialized agreements in place with lounge providers (such as Priority Pass and Revolut).

The complexity of access management is compounded by operational challenges:

- Overcrowding and visitor tracking.
- Invoicing and settling of funds for visits.
- Card or physical identity-based access systems.
- Local and State regulations.
- Manned vs. Automated access controls.

Using VCs as a form of identification for access affords benefits to lounge operators and guests alike:

- Faster, automated access for guests without cumbersome eligibility checks.
- Dispense with the exchange of data between carriers, complying with the protection of personal information.
- Integration with loyalty programs, without the need to check against a registry (which is often outdated and inaccurate).
- Smoother and more efficient billing and back office functions, avoiding revenue leakage for lounge providers.
- Allows for the adoption and expansion of automated access control, improving manpower efficiencies and related overheads.

PoC Steps

1. The passenger selects the **Lounge Access option** on the **Wi-Fi welcome page**, but in the same item 1: This web page is managed by Kronos Airlines who operates the lounge.
2. The passenger is prompted to share verifiable credentials (VCs) from the **Digital Wallet** to validate lounge eligibility.
3. The passenger consents to share the **boarding pass (issued by Kronos Airlines)** and **FFP (issued by Athena Airlines) credentials** with Kronos Airlines.
4. The **Kronos Airlines** verifies the credentials in real time, cross-checking lounge eligibility based on **ticket class, frequent flyer tier**, and **airline entitlements**.
5. The passenger is notified of successful authentication and authorization to access the Kronos Airlines lounge.
6. A **new QR code, to be used as lounge access pass, is generated** and displayed to the passenger.

Digital Identity for Seamless Wi-Fi Access Onboard/In-Cabin

Similarly to Wi-Fi access on the ground, in plane access can be conditioned by agreeing to local government rules for internet access such as accepting term and conditions and providing certain personal information data entry can be simplified, and government authorities can obtain trustworthy data by leveraging digital identity.

When entitlements are based on Frequent Flyer status, the specific tier needs to be identified and verified. This can be achieved by offering passenger to log in into their account. Even though many travellers do not remember their password this is a viable option when the traveller is part of the airline own program. This is usually not an option when the traveller is part of the frequent traveller program of a partner airline.

For this use case the Digital Wallet solution should be able to operate without internet access, by only connecting to the local wifi network.

PoC Steps

1. The passenger initiates the onboard Wi-Fi access process by either **selecting the onboard Wi-Fi SSID** from the mobile phone's Wi-Fi settings.

2. The **Kronos onboard Wi-Fi captive portal** opens on the passenger's device.

3. The passenger is prompted to provide **first name, last name, passport number, nationality** and loyalty tier status for Wi-Fi access. Two options are available:

   – **Option 1**
   Share the required details securely from the Digital Wallet.

   – **Option 2**
   Manually input the required details using the traditional login method.

4. The passenger chooses to share credentials via the **Digital Wallet**.

5. The passenger consents to share the required data elements from the passport verifiable credentials and loyalty card directly from the **Digital Wallet**.

6. The passenger's identity and Wi-Fi entitlement as part of loyalty offering is verified in real time over the aircraft's **onboard connectivity**, with verification happening against the **trust registry** to ensure the authenticity of the loyalty verifiable credentials.

7. Upon successful verification, the passenger is granted **Wi-Fi access** and is redirected to the **Wi-Fi welcome page**.

8. The **welcome page** confirms successful authentication and provides access to in-flight services.

Decentralized Identity Implementation & Standards

This Proof of Concept leverages the principles of decentralized identity by adopting standards such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). These standards ensure a secure, interoperable framework for managing digital identity, allowing individuals and organizations to establish trust without relying on centralized authorities. By leveraging these standards, which form the backbone of a modern digital identity ecosystem, the PoC establishes a robust foundation for secure and trusted interactions within the travel industry.

For this PoC, the decentralized identity ecosystem relies on the following roles and responsibilities:

- **Issuer(s)**
  Airlines, immigration authorities, or trusted government bodies issue Verifiable Credentials (VCs) (e.g boarding passes, loyalty status, or passport-derived credentials) to passengers.

- **Holder(s)**
  Passengers securely store their VCs in a Digital Identity Wallet (e.g., mobile driver's license wallets or airline-branded apps) and selectively present them during check-in, lounge access, or Wi-Fi authentication.

- **Verifiers(s)**
  Airlines, airports, lounges, and onboard service providers validate Verifiable Presentations (VPs) to confirm eligibility (e.g., lounge access, Wi-Fi entitlements). By leveraging Verifiable Credentials, they can verify eligibility by cryptographically checking the integrity and authenticity of the VPs while minimizing unnecessary personal data exposure through selective disclosure.

- **Verifiable Data Registry(s)**
  Maintains identifiers and status information needed to verify the validity and revocation status of Employee VCs, based on each travel agency's web domain. Each travel agency manages its own web-domain-based VDR.

- **Trust Registry**
  The Trust Registry maintains VC type metadata, schemas, a trusted list of issuers, and credential issuance authority statements. VC type metadata and schemas define the rules, structure, and display requirements for specific types of Verifiable Credentials (VCs), guiding issuers, verifiers, and wallets on how to handle and validate credentials. The trusted list of issuers and credential issuance authority statements supports airlines (verifiers) by enabling them to implement validation policies that ensure only trusted travel agency issuers and authorized credentials are accepted.

Interop profile

This Proof of Concept (PoC) has developed and implemented an Interoperability Profile as a central approach to implement decentralized digital identity standards across different Technology Providers.

An Interoperability Profile is a set of specific guidelines and requirements designed to ensure that different vendors can work together seamlessly. It defines how core components such as VC formats, VC exchange protocols, identifiers, and security mechanisms should be implemented, reducing complexity and variability. By standardizing these elements, the profile ensures consistent, and reliable interactions across the ecosystem.

This table summarize the different standards use in this PoC:

Component	Standard	Purpose
VC issuance	OpenID for Verifiable Credential Issuance Implementors Draft v1 https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html	Defines how an Issuer and a Wallet perform the issuance flow (pre-authorized code flow, credential offer/response).
Holder binding	SD-JWT VC	Ensures the Verifiable Credential is bound to the holder's wallet.
VC presentation	OpenID for Verifiable Presentations OID4VP 20 https://openid.net/specs/openid-4-verifiable-presentations-1_0-20.html	Describes how a Holder presents credentials (Verifiable Presentations) to a Verifier, including request and response flows.
Data format and validation rules to express VC	SD-JWT VC draft-ietf-oauth-sd-jwt-vc-07 https://datatracker.ietf.org/doc/html/draft-ietf-oauth-sd-jwt-vc-07	Enables selective disclosure and cryptographic binding of claims in a Verifiable Credential.
VC Revocation	OAuth 2.0 Credential Status List draft-ietf-oauth-status-list-05 https://datatracker.ietf.org/doc/html/draft-ietf-oauth-status-list-05	Defines a status list mechanism for revocation checks (active/revoked) so Verifiers can ascertain a credential's validity.
Decentralized Identifiers	did:web https://w3c-ccg.github.io/did-method-web	Specifies a method for hosting DID documents on HTTPS web domains, enabling domain-based DID resolution for key material.
Cryptographic Suites	P-256 (secp256r1) ES256 (JWT)	Establishes Elliptic Curve Digital Signature (ECDSA) requirements for signing and signature validation (SHA-256 hashes).
Trust Registry	Ad-hoc	Enable airlines to implement validation policies that ensure only trusted airlines, banks, commercial partners issuers and authorized credentials are accepted in the ecosystem.

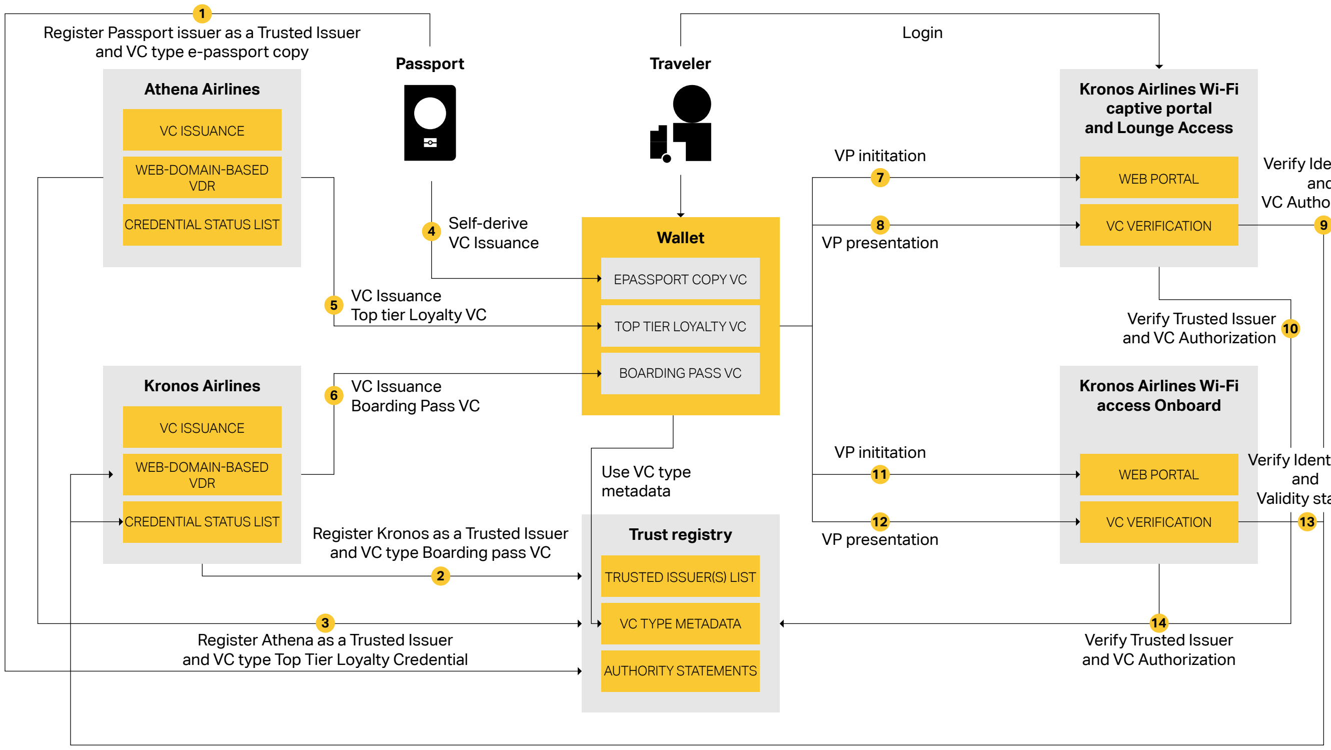
Component Implementation overview

Based on the interoperability profile, multiple independent implementations have been developed to demonstrate interoperability within a standards-based setup. The table below highlights the different implementations for each component.

Component	Implementation
Issuer	1 Technology provider
Wallet	2 Technology providers: 2 native mobile wallets
Verifier	2 Technology providers
Trust registry	1 Technology provider

Ecosystem Blueprint

The diagram below illustrates the high-level PoC ecosystem, highlighting how a traveler can obtain verifiable credentials (VCs) from Kronos Airlines and self-derive an e-passport VC.


1
Register Passport issuer as a Trusted Issuer and VC type e-passport copy
Passport
Traveler
Login
Athena Airlines
VC ISSUANCE
WEB-DOMAIN-BASED VDR
CREDENTIAL STATUS LIST
Kronos Airlines Wi-Fi captive portal and Lounge Access
VP inititation
7
WEB PORTAL
Verify Identifiers and VC Authorization
8
VP presentation
VC VERIFICATION
9
4
Self-derive VC Issuance
Wallet
EPASSPORT COPY VC
5
VC Issuance Top tier Loyalty VC
TOP TIER LOYALTY VC
Verify Trusted Issuer and VC Authorization
10
BOARDING PASS VC
Kronos Airlines
VC ISSUANCE
6
VC Issuance Boarding Pass VC
Kronos Airlines Wi-Fi access Onboard
WEB-DOMAIN-BASED VDR
CREDENTIAL STATUS LIST
Use VC type metadata
VP inititation
11
WEB PORTAL
Verify Identifiers and Validity status
12
VP presentation
VC VERIFICATION
13
Register Kronos as a Trusted Issuer and VC type Boarding pass VC
2
Trust registry
TRUSTED ISSUER(S) LIST
3
VC TYPE METADATA
14
Register Athena as a Trusted Issuer and VC type Top Tier Loyalty Credential
AUTHORITY STATEMENTS
Verify Trusted Issuer and VC Authorization

Prerequisites

Before issuing and managing Verifiable Credentials, all actors (Athena Airlines, Kronos Airlines, and the self-derived e-passport issuance authority) must first onboard the ecosystem by registering with the trust registry. This allows participants to rely on credentials issued within the ecosystem without requiring a bilateral setup with each airline partner. In our PoC, this applies to Kronos Airlines as a consumer of Verifiable Credentials within the ecosystem.

Self-derived e-passport copy issuance authority

A foundational digital identity credential is created by securely capturing a traveler's physical passport data through MRZ scanning and NFC chip reading, while performing liveness and document authentication to derive a foundational credential. Once verified, a e-passport copy verifiable credential is issued and stored in the traveler's digital wallet.

Athena and Kronos Airlines (Issuers)

Athena Airlines manage the lifecycle of Top Tier Loyalty Verifiable Credentials issued to their frequent flyer members and Kronos manage the Boarding Pass Verifiable Credential issued to travelers after check-in. In the diagram, three key components represent the capabilities required to fully manage the VCs lifecycle:

- **VC Issuance**
  Enables Athena and Kronos Airlines to create and issue credentials to their frequent flyer members and travelers' digital wallets.

- **Web-Domain-Based VDR**
  Anchors the DID document associated with the Athena Airlines DID to a web domain controlled by the airline, allowing verifiers to resolve the DID document and access verification keys.

- **Credential Status List**
  Maintains the validity of all credentials issued by Athena Airlines, enabling actions such as revoking credentials as needed (e.g., fraudulent Activity or Misuse).

Passenger and Mobile Wallet

The passenger, using a mobile digital identity wallet, has full control over their travel credentials: boarding passes, loyalty cards, and e-passport copy data are securely stored on their mobile device.

This wallet enables seamless access to services such as lounge entry and onboard or terminal Wi-Fi through instant verification, sharing only the necessary data via selective disclosure. As a result, passengers enjoy enhanced data privacy and control while establishing real-time trust and streamlined interactions across airlines, airports, and service providers.

For this PoC, one of the proposed improvements for wallet implementation is the harmonization of how Verifiable Credentials are displayed in wallets, including graphical elements and translation-based artifacts. This ensures that wallets can present credentials in a way that aligns with the intent of the provider of the VC visualization rules, which in this PoC is a standardization body such as IATA.

Kronos Airlines (Verifier)

Kronos Airlines, acting as the verifier in this PoC, provides two key components.

The portals
First, its airline Wi-Fi captive portal is designed to consume Verifiable Credentials during passenger authentication for on-ground Wi-Fi access. After successful Wi-Fi login, the portal also facilitates lounge access verification, enabling instant credential validation for the first and second use cases. For the third use case, Kronos Airlines' onboard Wi-Fi captive portal is used to consume Verifiable Credentials, ensuring seamless authentication for in-flight connectivity.

The verification Service
The VC verification service performs three key functions: first, it cryptographically verifies the validity of the credential, second, it ensures the trustworthiness of the proof by confirming the issuer is a trusted issuer and that the credential type is authorized within the ecosystem, and third, it ascertains the credential's ongoing validity by checking its revocation status through a status list mechanism.

Trust Registries

The Trust Registry enables airlines to verify that a credential originates from a trusted actor in the ecosystem. While the registry also validates whether issuers are authorized to issue specific credential types (in our PoC, Top Tier Loyalty VC, Boarding Pass VC and e-passport copy VC)

Additionally, the Trust Registres is responsible for managing Verifiable Credential (VC) metadata, schemas, and type definitions, serving as a centralized repository for credential specifications. It hosts detailed descriptions of each credential type, including mandatory and optional claims, data formats, and display requirements. By ensuring uniformity in how credentials are issued, presented, and validated, the Trust registry provides an interoperable, and scalable foundation for the ecosystem.

Process Steps

Below is a high-level overview of the steps in the ecosystem, illustrating how Airlines and trusted authorities issue credentials, how travelers present them, and how Airlines verify them against the Trust registry.

Prerequisite

The Airlines (issuer) and e-passport copy issuance authority must be fully provisioned:

- Signing keys: Cryptographic keys are generated and associated with the issuer.
- DID and DID Document: A DID using the did:web method is anchored, and a DID Document containing the issuer's public keys and metadata is accessible via the internet.

Steps 1, 2 and 3: Register Trusted Issuer and VC Type

Before issuing any credentials, Athena and Kronos Airlines must register with the Trust registry:

- Both Airline's and E-passport copy issuance authority DIDs are added to the Trusted Issuers List maintained by the Trust Registry.
- The issuers request credential issuance authority from the Trust Registry to issue each of them the Top Tier Loyalty VC, Boarding Pass VC and e-Passport copy VC.

Steps 4: Self-derive e-Passport copy VC

- MRZ Scanning: The traveler scans the Machine Readable Zone (MRZ) of their physical passport using their mobile device.
- NFC Chip Reading: The system reads the passport's embedded chip via NFC to extract biometric and biographic data.
- Liveness and Document Authentication: Liveness detection and document authentication verify that the traveler is present and that the passport is genuine and unaltered.
- Credential Derivation: A foundational digital identity data is derived from the validated passport data.
- The VC is cryptographically signed using the issuer's private key.
- The credential includes a status claim pointing to a Credential Status List, allowing verification of whether the credential is active or revoked.
- The VC is bound to the Traveler device and securely delivered to their wallet.

Step 5 and 6: VC Issuance

Athena and Kronos Airlines issues a Verifiable Credential (VC) to the Traveler's wallet:

- Top Tier Loyalty data and Boarding Pass data is obtained from Airline data sources
- The VC is cryptographically signed using the issuer's private key.
- The credential includes a status claim pointing to a Credential Status List, allowing verification of whether the credential is active or revoked.
- The VC is bound to the Traveler device and securely delivered to their wallet.

Steps 7: VP Initiation

When the traveler wants to access to the on the ground Wi-Fi network, the following occurs:

- The Wi-FI Captive Portal displays a QR code. The QR code can be scanned or via deep link in case of mobile navigation. The QR code encodes a URL containing a proof request.
- The traveler either scans the QR code using a mobile wallet or clicks the deep link, which triggers the wallet to initiate the Verifiable Presentation (VP) process.

Step 8: VP Presentation

The Traveler Agent's wallet responds to the proof request:

- The wallet prepares a Verifiable Presentation, which may include selective disclosure, ensuring only the necessary claims are shared.
- The cryptographically signed presentation is sent to the Airline's verification service.

Step 9a: Verify Verifiable Presentation

Kronos Airlines' verification service validates the Verifiable Presentation:

- It resolves the issuer's DID using the did:web method.
- The service retrieves the issuer's DID Document to access the associated public key.
- Using the public key, the verifier cryptographically checks the integrity and authenticity of the Verifiable Presentation.

Step 9b: Verify Credential Status

The verifier consults the Credential Status List (referenced in the credential's status claim):

- The verifier retrieves the Status List from the issuer's specified URL.

- It checks the status bit corresponding to the credential to confirm whether the credential is active or revoked.

Step 10: Verify Trusted Issuer type

The verifier (Kronos Airlines) ensures the issuer and credential type are trusted:

- The verifier checks that the issuer's DID is listed in the Trusted Issuers List in the Trust Registry, confirming the Athena is onboarded in the ecosystem.

- The verifier checks that the issuer is authorized to issue the Top Tier Loyalty VC by consulting the Trust Registry, which contains the necessary credential issuance authority statements.

- If the validation process pass, the verifier component confirms the information is authentic and trustworthy, allowing the passenger to gain Wi-fi access.

Step 10, 12 13 and 14:

Same process as steps 7–10 but for the Wi-Fi Access Onboard/In-Cabin use case.

Benefits/Costs Analysis

3 new business benefits are identified today from a future eligibility credential (example for Lounge access)

1 Enable 100% self-service check for customers not known in our departure control system as eligible, including complex local business rules (upgrade/downgrade, priority in case of lounge full, paid access).

2 Track all customers and their guests who accessed lounges including the reason for entitlement, and keep proof of access for further invoicing/settlement with the issuer of the entitlement.

3 Support staff with smartly clearing doubts for "unofficial" (i.e. non tier based) proprietary eligibility (like Royal family, VIPs).

This will result for airlines in:

- Cost savings by reduced workload for staff.
- Improved operational efficiency.
- Enhanced brand loyalty.

All this without sharing sensitive personal customer information with competitors, as legal consent for data is always taken into account ("privacy by design", "privacy by default").

On top of these, once personal identification will become a standard way of connecting, Airlines will benefit from a higher login rate on their Digital touchpoints. This would enable further opportunities for revenue increase through personalized offers.

These benefits must be available for a reasonable cost

When governments issue electronic documents, these will have to be recognized: airlines have no choice and will have to implement such capabilities for regulatory reasons. No need for a business case to be presented: it is compulsory, and in the best case, part of the costs will be shared with State, Immigration, Airport authorities, Banks, Telco operators, or a combination of these.

The story here is different: the purpose of this PoC is to cover how to generate new commercial airline benefits: implementation, and use, have to be profitable.
Actually, there will be probably -limited- new costs associated to the technology.

Today, the download of a wallet is often free for the customer, and so is the upload of electronic documents. The costs come from the use of the wallet, namely the verification of the credential.

Who will pay? The technology vendors will make their business by charging a fee for each identification. Most probably the costs will be proportional at start, keeping them very low at the beginning when overall volumes are still low, in order to ease adoption by airlines. Analysis shows that, depending on complexity, some identification costs can be very actually start low (even "no use- no charge" is possible under certain solutions) and grow proportionally of usage.

These costs might drive reasons why some airlines could still be reluctant today to accelerate or broadly implement such identification:

1. During transition, a "classical" double check – e.g. 6 digit code sent by email or text message-, currently implemented or soon to be implemented, will have to continue for all other customers who do not have yet their Digital ID. So a double infrastructure will run for a while, creating a temporary increase in complexity and costs.

2. Airlines do not want to pay eventually more than they pay today for such authentication processes.

No further elaboration is possible for this Industry position paper. Competition guidelines prevent any guidance at IATA for this field, only bilateral confidential discussions are allowed. However industry players are well aware of this cost/benefit aspect, and that the fee has to be adapted (read "low enough").

Next Steps

Pathway to adoption:

- **Regular day-to-day usage (depending on countries) will make passengers very familiar with identifying themselves with their mobile phone, using VC, held in one of their wallet . Airlines just have to follow the stream, and the idea here is that airlines will leverage this natural trend to simplify the life of their customers, not only for regulatory Passport and Identity control, but also in less sensitive situations.**

Additional potential Benefits to be explored:

- **Systematic usage of a VC by passengers to interact with the airline can bring a huge increase in "login rate", enabling personalized offers, marketing activities ("couponing"), etc.**
- **Easier implementation of links with other Loyalty programs (enabling "double dipping" agreements).**
- **Eeasier authentication to loyalty account open options for payment with miles at more touch points and via more channels.**

The 2024 Customer Digital Identity project recommends that IATA and/or its Member Airlines:

- **Ensure industry awareness of the various experimentations adjacent to this PoC.**
- **Work on defining a solution for a neutral and affordable "Trust registry".**
- **Establish a standard framework to guarantee the interoperability of the different solutions involved.**
- **Identify possible existent and potential technology gaps that may prevent widespread adoption of VCs.**
- **Work on a set of shared tools that bridges the technology gaps that may exist and that may make it difficult for airlines to adopt the standard framework and offer VCs to their customers.**
- **Establish a benchmark for the usage of Verifiable Credentials during air travel to help airlines assess passengers' readiness.**
- **Launch solutions based on Wallets and VC for selected pain points.**
- **Advocate for technology providers to propose low cost, scalable solutions for simple "eligibility checks" (as opposed to "strong biometric identification", which is explored already, and requires higher level of security).**
- **Explore the feasibility of developing cost benchmarking solutions?**
- **Further explore with technology providers high quality solutions for branding of verifiable credentials and wallets, enabling airlines to guarantee their brand presence (logos, colors, look and feel at every step).**
- **Advocate for the development of open and flexible solution for regulatory passport check so that they can easily accommodate adjacent use cases such as the ones show cased in this PoC.**

Conclusion

IATA realizes the importance of the industry leading addressing AI and Digital Identity. Through programs like the Data and Technology PoC, IATA and participating organizations are leading and supporting the industry in the path towards the future. With a focus on innovation with speed, our industry needs to move full speed forward. The airlines and other stakeholders participating in the Data and Tech PoC are also leaders and fully onboard with the shared vision.

It is important that more airlines join the effort, through the Data and Technology PoC. IATA encourages more airlines and partners to get involved in 2025 and help us drive these ideas into initiatives and potential projects.

Partnering for success

A special thank you to the 2024 Data and Technolgy members.

Project Industry LLM

Conor McMenamin
Head of Data & Analytics

Aer Lingus

Keiichi Ueda
Vice President, Innovation, Digital Transformation

ANA

Venkatesh Attinti
Solution Architect

QATAR AIRWAYS القطرية

Boniface Naickar
Partner, Services

Infosys

Vishal Parikh
Enterprise Architect

Infosys

Bhanumurthi Tellapati
Technology Architect

Infosys

Sergey Chernykh
Senior AI Technical Specialist

Microsoft

Sid Ryan
Senior Lead Data Scientist

SITA

Karol Tarčák
Solutions Architect

snowflake

Bogdan Pasol
Head Data Engineering and Operations

IATA

Project 777

Lisa Bourque
Senior Manager B2B Products

AIR CANADA

Kurt Zuo
Product Manager

AIR CANADA

Lukman Hakkim Abdul Rahuman
Technical Lead

QATAR AIRWAYS القطرية

Tamilarasu Saravanakangeyan
Technical Lead

QATAR AIRWAYS القطرية

Hilal Demirtaş
Director, Distribution and Sales Solutions

TURKISH AIRLINES

Özgür Kayalar
B2B Sales and Marketing Solutions Manager

TURKISH AIRLINES

Gary Kenny
Head of Aviation Solutions

Dreamix A Synechron Company

Miguel Santos Luparelli Mathieu
Product Innovation Director

facephi

Sebastian Honores Espejo
CPO and Co-founder

neoke

Vikas Bhola
CEO

neoke

Mathieu Glaude
CEO

4SURE TECHNOLOGY SOLUTIONS

Gabriel Marquie
Head Digital Identity, Innovation and Identity Services

IATA

Project 321

Fréderic Gonnaud
Portfolio, Architecture,
Programs

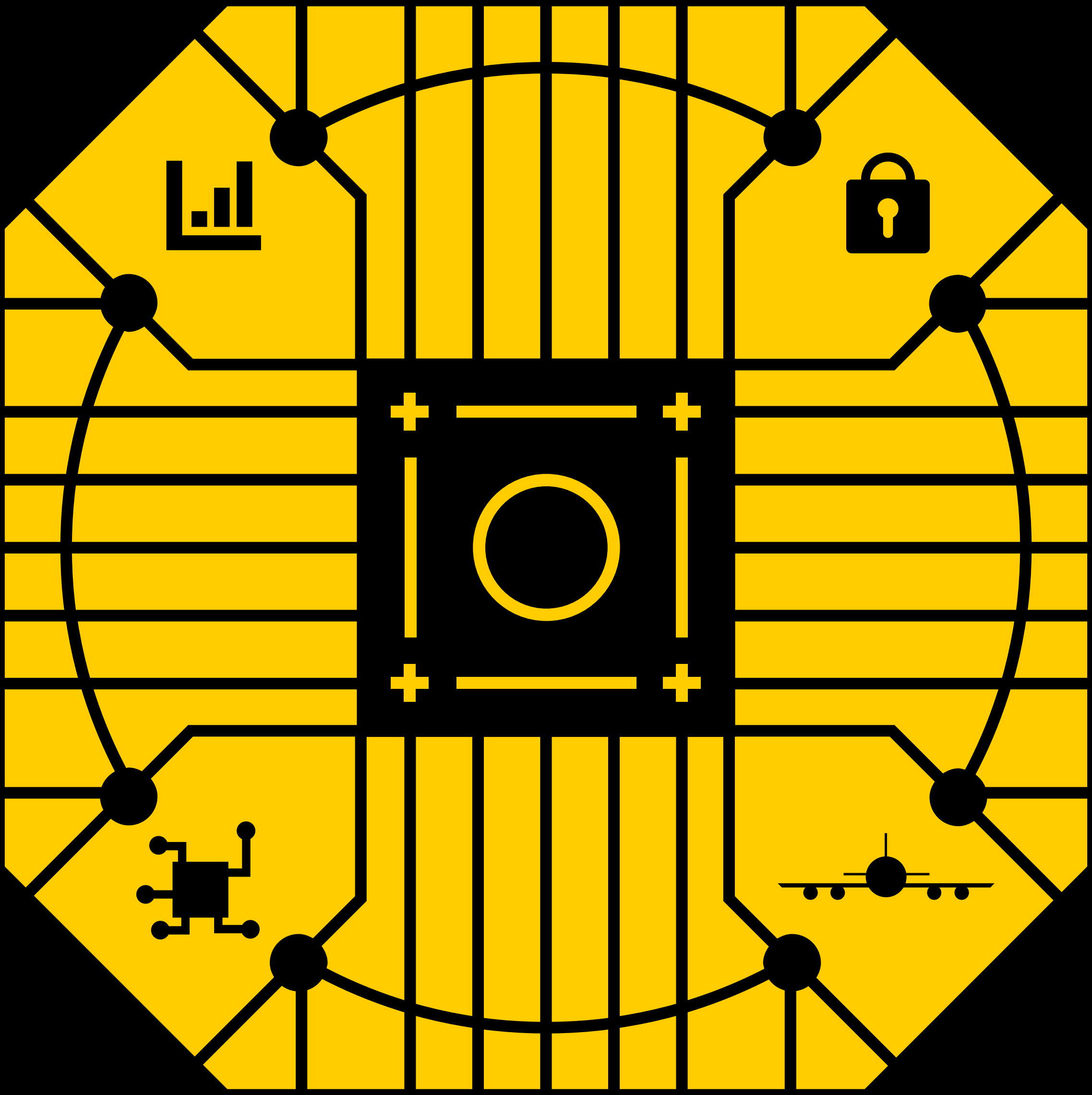
Sajith Abdul Salim
Manager Enterprise
Architecture

Jaepyo Jung
Senior Manager,
Data Architect Team

Havva Yıldız
Expert Business Analyst

Alex Hervet
Director Innovation,
Customer and Product

Gabriel Marquie
Head Digital Identity, Innovation
and Identity Services



International Air Transport Association
800 Place Victoria, PO Box 113
Montreal, Quebec, Canada H4Z 1M1
Tel +1 (514) 874 0202

iata.org