IATA
GLOBAL
MEDIA DAY

Travel / Passenger Experience

Youn Kim
Manager Customer Experience

Yanik Hoyles
Director Distribution

Gabriel Marquie
Senior Manager Digital ID

IATA

Imagine a world of seamless, stress-free travel—where your journey is entirely digital, if you want it to be. Today, we'll show you that vision in action and how the industry is ready to deliver.

In a recent proof-of-concept in partnership with Cathay Pacific, Hong Kong International Airport and Narita Airport in Tokyo, and tech providers Branchspace, NEC, NeoKe, SICPA, Facephi and Northern Block; two passengers used digital wallets and travel credentials for a round-trip between Hong Kong and Tokyo.

The airport elements of this PoC were conducted in a live environment, meaning they were integrated in airport systems building on an initial PoC carried out in a test environment in 2023.

Journey: Hong Kong to Narita and Return

Customer 1

- Corporate traveler
- CX frequent flyer
- Visa not needed
- ePassport digital copy and live biometric image already stored in the wallet

Customer 2

- Corporate traveler
- No membership with CX
- Visa needed
- ePassport digital copy and live biometric image already stored in the wallet

- **Two travelers carried and used digital wallets with their ePassport copy, company ID, and frequent flyer credentials to book flights, apply for visas, check in, and manage airport processes.**
- **Biometric recognition streamlined the journey, eliminating the need for repeated document checks.**
- **Seven verified digital documents, two digital wallets, and a trust registry were seamlessly integrated in a live airport environment.**
- **Today, we'll walk you through this PoC, showcasing the passenger journey, and share the lessons learned.**

Step 1: Creating a Digital ID

- The first step is creating a digital identity—a secure, digital version of your passport or ID. It's your way to prove who you are digitally without carrying physical documents.
- Your details are securely stored on your phone in a tamper-resistant digital wallet, making it easy to share them only with relevant parties.
- Creating your digital passport is simple…

- Scan your passport using your phone, then complete a liveness check to verify it.
- These credentials stay fully under your control.

Step 2: Shopping and Booking

- Your digital wallet doesn't only store your passport. Other types of verifiable digital credentials can also be stored like frequent flyer status, student IDs, or employee cards—all under your control and selectively shared as needed.
- When booking flights, you can share preferences and credentials securely, enabling airlines to offer tailored, more relevant options.

Live Demo

- Now I am saving Order VC into my wallet – by doing so, I do not need to download a booking confirmation PDF or keep the booking reference separately.
- Legacy booking references and e-tickets can be replaced by a single order that can be stored in your Digital Wallet along with other Verifiable Credentials.

Step 3: Visa Process

- Now that I've booked my flight, it's time to apply for a visa to enter the destination country.

Visa Scan

- Instead of manually entering my details, I share my passport and flight information directly from my digital wallet.
- Once my application is approved, I receive a paper visa.
- I'll now create a digital copy of this visa to store securely in my wallet.

Step 4: Check In
Step 5: Contactless Experience
Step 6: Ready to Fly

- Now it's closer to departure, it’s time to check-in.

Live demo

- The airline informs me that I can enjoy a contactless experience at my departure airport. I want to learn more, including what information Hong Kong International Airport requires and how it will be used.
- At check-in, I use my digital order to access my booking and begin the process. The airline first requests my passport details, then my visa information. With a click, I share both digitally from my wallet, and check-in is complete.
- Check-in becomes effortless—your digital passport and order transfer seamlessly to connected systems, eliminating the need to manually enter details like reference numbers. It also removes the need for airline staff to swipe your passport to verify / correct any errors made while filling in your passport or visa information.
- The airline informs me that I can enjoy a contactless experience at my departure airport. I want to learn more, including what information Hong Kong International Airport requires and how it will be used.
- It tells me which of my information will be needed, whom I am sharing my information with and how my information will be used. I would like to share my consent and share my credentials from digital wallet. Now I am ready to travel.

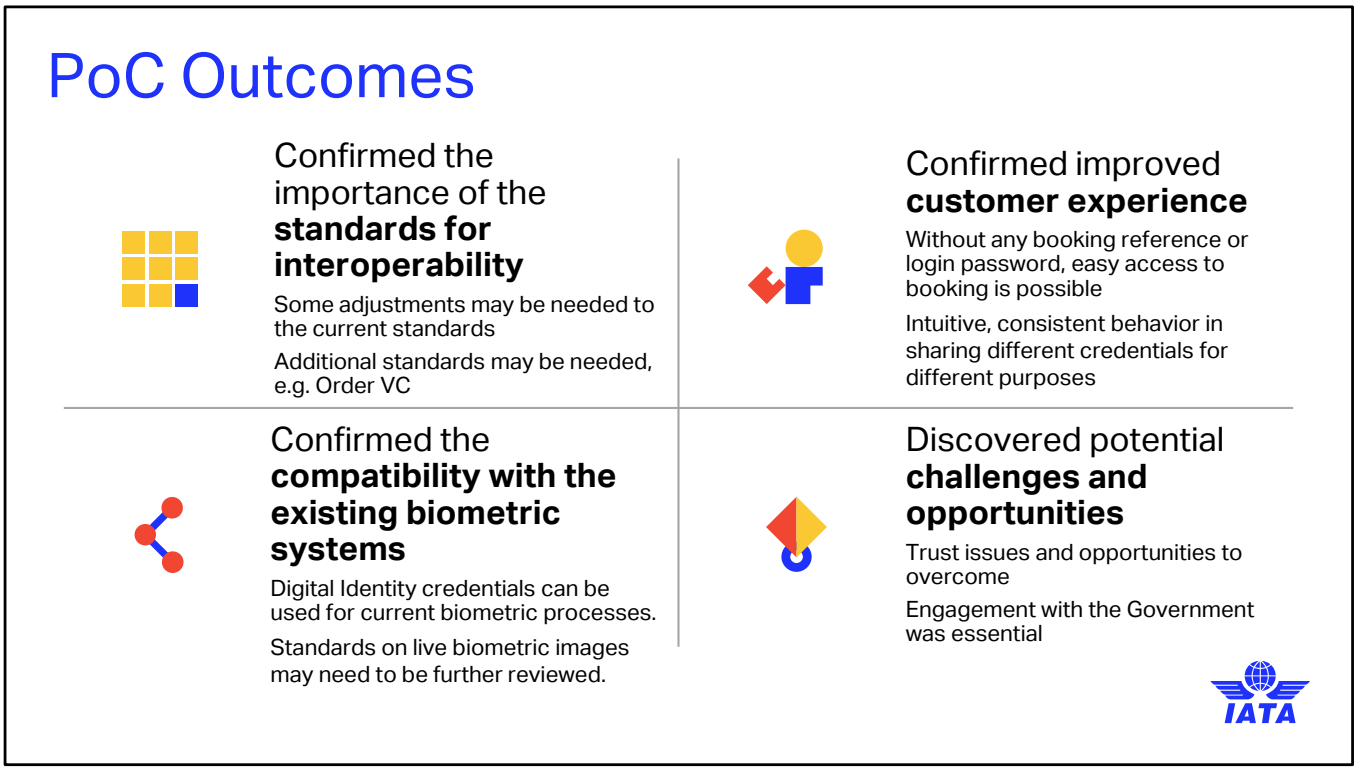
Lessons Learnt

Youn Kim
IATA Manager Customer Experience

Gabriel Marquie
Senior Manager Digital ID

Yanik Hoyles
IATA Director of Distribution

- Thanks Youn, very seamless!
- I'd now like to invite our other panellists (Louise, Yanik) to join me on stage to discuss key learnings from the POC and address some important points.



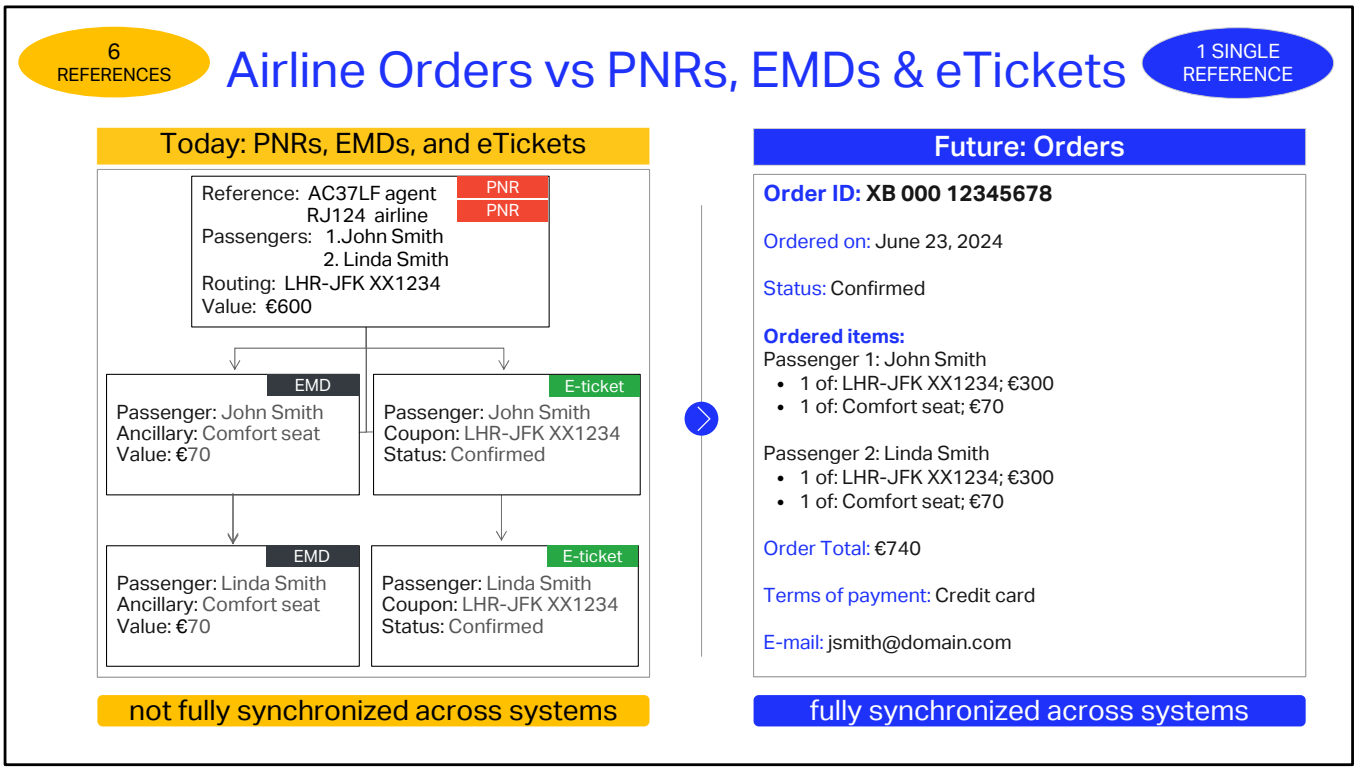
Q. What were the main outcomes of the PoC?

1. We confirmed the importance of the standards to achieve global interoperability. IATA and the industry have made significant progress in developing the standards but thanks to the lessons learned, we will adjust and enhance the current standards and continue to work on completing the standards.

2. We confirmed improved customer experience throughout the journey; The customer didn't need to juggle with different forms of data and information and could make transactions only by clicking 'share from wallet' and 'save to wallet'. The customer experience was consistent and intuitive.

3. We confirmed the compatibility with the existing biometric systems – given that we already have numerous biometric implementations in place across the globe, this is good news to prove the compatibility.

4. Lastly, we discovered potential challenges and opportunities. Airlines and airports would need to know how to trust the credentials in the first place and IATA is looking at this space whether IATA can play a role in this. Engaging governments will be essential as well to get their support.



- In the POC, we noticed the customer received an 'Order' instead of a PNR or booking reference. Could you provide more detail on this?
- Things will be clearer and simpler. For example, today, a family of 2 on a direct flight, with a seat each means they will have 2 PNRs, 2 e-tickets and 2 EMDs – so 6 references. And this is 6 references that are not automatically synchronized when there are changes (voluntary/ disruption).
- Why is this? Because the PNR is what you have reserved / booked; the ticket is when you have paid and the EMD is for what you have booked and paid and that is not the flight, so a seat for example. It's been like this for over half a decade!
- Tomorrow, all these items will be held in 1 single Order! – that you can add to, remove from, or change – just like a regular shopping basket (Click for pop up) – and all will be automatically synchronized.
- This will be much simpler for the customer and they will benefit from a much better service: for example the Customer will technically be able to service their Order through any channel they want (agent, airline website, call center) wherever they booked the ticket from.

Data Security

- **Encryption**: Your data is locked with advanced codes (encryption) so only you can access it.
- **Secure Storage**: Digital wallets store your data in a secure part of your phone or device, separate from everything else.
- **Tokenization**: Instead of storing the real details, they use fake numbers or codes to protect your actual information.
- **Authentication and Authorization**: You need to prove it's really you to access the wallet, using things like fingerprints, face scans, or passwords.
- **Share Only What's Needed**: If you need to show your passport or visa info, the wallet only shares the necessary details, not everything.
- **Secure Connections**: When your data is sent somewhere (like an airport), it travels through secure, private channels so no one else can see it.
- **Updates to Stay Safe**: Wallets are updated regularly to stay protected from new threats.
- **Privacy Rules**: Digital wallets follow strict privacy laws to ensure your personal data is handled properly.

Q. How is sensitive data, like passports and visas, protected within digital wallets?

Sensitive data, such as passports and visas, is protected within digital wallets through a combination of advanced security technologies and best practices. Here's how:

- Encryption: Sensitive data is encrypted both at rest and in transit using strong encryption standards. This ensures that even if data is intercepted, it cannot be accessed without the appropriate decryption keys.
- Secure Storage: Digital wallets store your data in a secure part of your phone or device, separate from everything else.
- Tokenization: Tokenization replaces sensitive information with a randomly generated token that has no exploitable value. This ensures that actual passport or visa details are not exposed during transactions or when sharing information.
- Authentication and Authorization: Digital wallets require strong user authentication methods, such as biometrics (fingerprint, face recognition) or multi-factor authentication (MFA), to ensure that only authorized users can access sensitive data.
- Secure Connections: When your data is sent somewhere (like an airport), it travels through secure, private channels so no one else can see it.
- Updates: Wallets are updated regularly to stay protected from new threats.
- Privacy Rules: Digital wallets adhere to strict international standards and privacy laws to ensure your personal data is handled properly.
- Backups: Your data is backed up securely so you can recover it if your phone is lost or damaged.

Q. Who owns the data—the traveler or the companies enabling the technology?

- The traveler retains ownership of their personal information. It's their data, and they decide who to share it with.
- Companies enabling the technology can only use the data with the traveler's explicit permission. This means travelers control when and how their information is shared, such as when passing through airport security. After the data has been used for the purpose it was needed for, it is deleted and not retained.
- Companies must comply with data protection laws (like GDPR or similar), which emphasize that the traveler has the right to know how their data is used and to request its deletion.

Strong interest in digital wallets but what if I don't want to use one?

20%

state a digital wallet as (one of) their preferred payment options

77%

interested in using a digital wallet that is loaded with a payment card, digital ID and loyalty cards.

Interest highest in Africa, Asia Pacific and the Middle East.

Q. For travelers, convenience is key. What happens if someone loses their phone or the system goes offline?

Losing a phone or facing an offline system doesn't mean travelers are stranded. Digital wallets often have encrypted backups that can be restored to a new device, and many offer remote locking to protect lost devices. Key data is stored locally, so it can still be accessed without an internet connection, and authorities usually have fallback processes like manual verification. Travelers are also encouraged to carry their physical passport, as an extra safeguard.

Q. And for those without access to smartphones, what alternatives will be available?

Yes, alternatives will always be available for those without smartphones. Travelers can use physical copies of their travel documents, such as passports or visas. Airports and checkpoints also offer manual verification processes through kiosks or assistance desks to ensure smooth travel for everyone.

What is next?

Digital Identity is ready for travel today

- One ID standards
- IATA guidance and services

> Ready for implementation

Government support is crucial

- Government's lead in issuing digital identity credentials that will enable travel and providing the trust framework
- Removal of obstacles

Q. What are the next steps? Yanik over to you to talk about the booking and payment part?

Work on booking and payment comes under IATA's MAR initiative which is helping our members become more customer centric by adopting the capabilities that typical retailers have. We will continue working on the standards supporting One Order and testing these in a live environment. It will mean better servicing, more choice of products and more choice of payment solutions, aligned with customer expectations.

Q. When will we see airlines start to use "orders"?

Through a consortium we are working with many value chain players, including airlines and IT providers to make this happen. We hope to see the first orders in 2026.

And the transformation will continue. In the paper that was shared with you – you may have read that the Consortium is working on further benefits that could be delivered thanks to all these new standards: why do you need to check in? It's just an extra step, and extra hurdle … why do you need another document such as a boarding pass that suggests you are ready to board? All this can be streamlined and be part of your Order which is simply updated along the journey… watch this space!

Q. And on the passenger experience side?

Through the PoC this year, we demonstrated enhanced interoperability with multiple issuers, verifiers and wallet providers and with existing live biometric systems, enabled by improved IATA standards. This proves that digital identity is ready for travel today. We hope this PoC helps move the industry closer to more implementations and adoptions.

Now that the industry is getting ready, government support is crucial. The most trusted digital identity is coming from the government. IATA believes that Government's lead in issuing digital identity credentials for travel and providing the trust framework will accelerate the adoption. Also, it is important that regulatory obstacles are removed for the industry to use digital identity for travel.

Access the white paper:
bit.ly/Orders-DigID