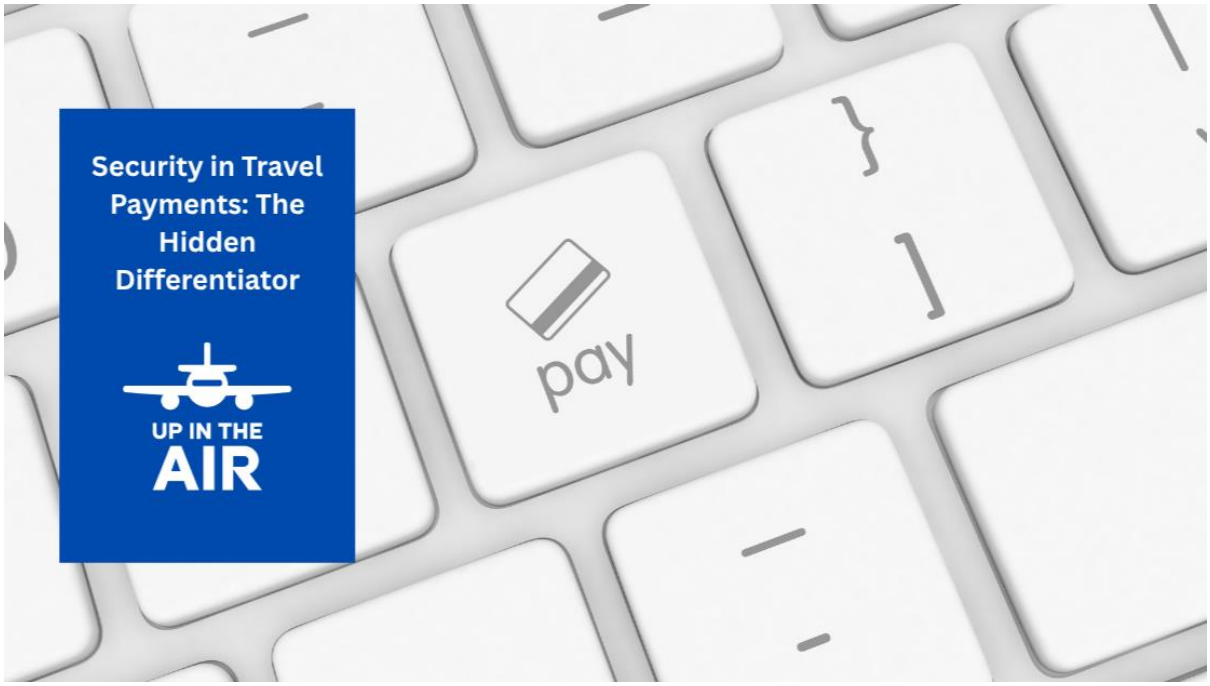
Up in the Air Travel Fintech Newsletter - Special Edition - Security in Travel Payments: The Hidden Differentiator



A special edition of the **Up in the Air | Consultancy** Travel Fintech newsletter introducing a new infographic, this time covering one of the 'hygiene factors' in Travel payments: Data Security and more specifically **Tokenization** of sensitive card details.

The challenge: 'How can the industry securely store card information for a wide range of payment touch points whilst limiting exposure to data breaches?'

Tokenization 101

Let's start with the definition of a 'card payment token': it is a substitute for an actual credit or debit card number, used to secure transactions and reduce fraud risk. It is a randomly generated string of numbers or characters that replaces a real card number during a payment transaction.

Card data is typically tokenized using one of three different techniques (for single or multi use):

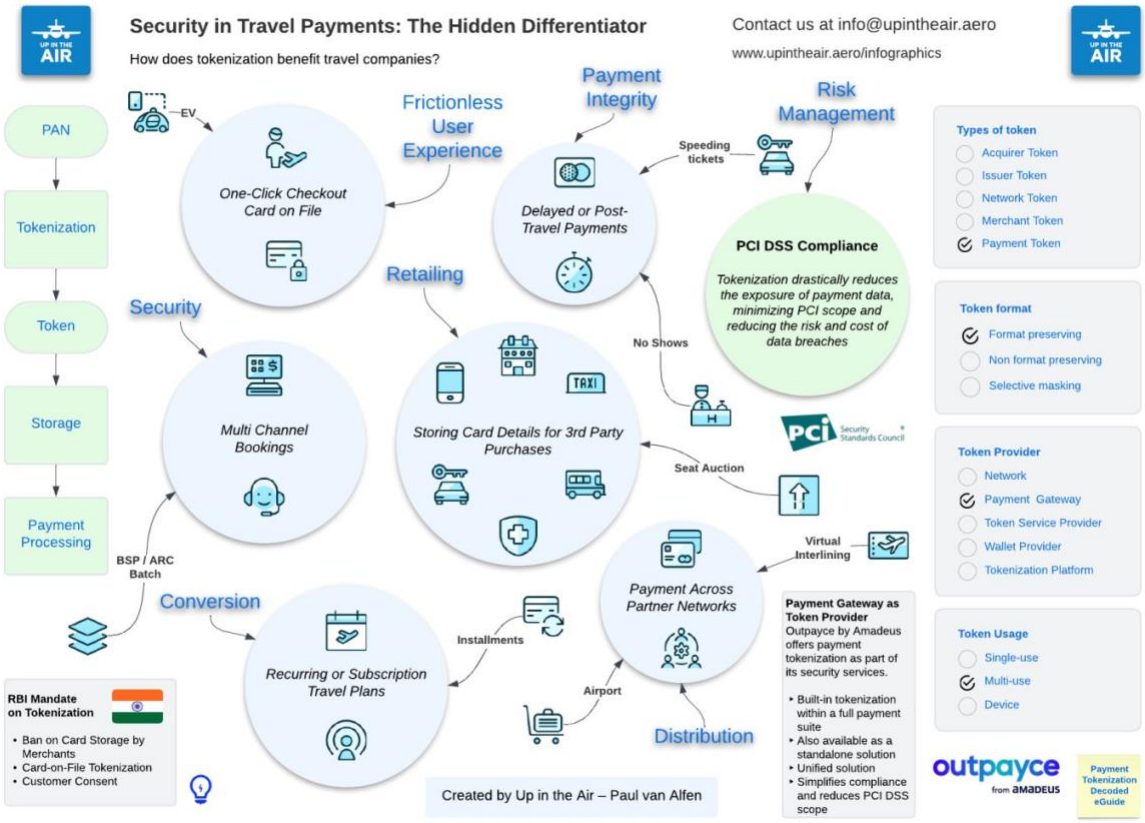
1. Non-format preserving: card data is replaced by a string of alphanumeric characters.
2. Format preserving: the token retains the format of the card number but scrambles the ordering of the numbers.
3. Masking: some of the card numbers remain the same, which can help with verification, while some others are replaced.

To reduce the scope for this article and to spare non technical stakeholders, I'm focusing on payment tokens supported by payment gateways and token service providers (including 'token vaults') for merchant processing.

Whilst tokenization is common across all different types of travel merchants, airlines with their many sales channels and technology partners, are a one of the most complex categories. Securing card data and avoiding card scheme fines resulting from data breaches is therefore a top priority for airlines, but tokenization is about more than that, it's also a sales generator.

Airline & Travel use cases

In my below infographic I try to visualize actual day to day use cases where tokenization can be used, typically in the background, to exchange payment details in a secure manner both internally and with partners.



Click on image to download the PDF version

One-Click Checkout

'One-Click', a frictionless checkout based on, with customer consent, stored and tokenized payment credentials is ideal for regular purchases from loyal customers, as proven by the likes of **Amazon** and **Uber**. This 'Card on File' method is an alternative for a 'guest checkout' whereby payment details need to be entered manually for (non mobile wallet) card transactions.

Multi Channel Bookings
Designing a payment architecture based on one tokenization process across sales channels and payment touch points is preferred. For airlines, especially card transactions originating from the travel agency channel and received in offline batch files are especially hard to manage. Exchange of sensitive details with tokens needs to happen 'upstream', before the airline receives the files from **International Air Transport Association (IATA)** and **Airlines Reporting Corporation (ARC)**.

Recurring or Subscription Travel Plans
When airlines and OTA's offer subscription plans to their customers, payment details are captured during the check out / at time of 'onboarding'. When individual follow up payments are due, the stored card is charged according to the agreed terms, making use of tokenization. The same applies to platforms like **Airbnb**, Tour Operators and Cruise lines taking a 'down payment' at the time of booking and a 'remainder payment' close to departure.

Delayed or Post Travel Payments
These are probably the best known and 'historic' use cases, both because they have been around for a long time and have proven to be a challenge from a payment processing and card scheme compliance point of view. Two examples:

- The infamous 'no show' charge for 1 night when a hotel reservation is not cancelled in time
- The car rental company that keeps your card on file in case of any 'post return charges' for damages, speeding / parking tickets and refueling

Storing Card Details for 3rd Party Purchases
When travel companies sell 3rd party products or services (from e.g. hotel stays to ground transportation, insurance and eSIM's), typically 1 of 2 models is applied: agency or merchant. In case of the agency model, customer card details are passed through at the time of booking so that the card can be charged (later) with the supplier as Merchant of Record. Tokenization of payment card data during this exchange is key, not only to streamline the process but also to protect the data from fraud.

Payment Across Partner Networks
The travel payment value chain is long and diverse with many partner links that need to be considered for handling and securing payment data. How for instance to address virtual interlining, when legacy carriers and Low Cost Carriers are combined in a single booking, making use of different flows (e.g. GDS and API)? Ideally the customer only checks out once, with a single authentication and 2 transactions in the background, making use of tokenization.

NDC and Tokenization

What's the role of tokenization when airline bookings are made based on the IATA NDC standard? Well, in the traditional GDS booking flow the authorization and settlement steps for card payments are completely decoupled, with agents and airlines not directly connected and the GDS taking care of the authorization directly on the 'schemes'.

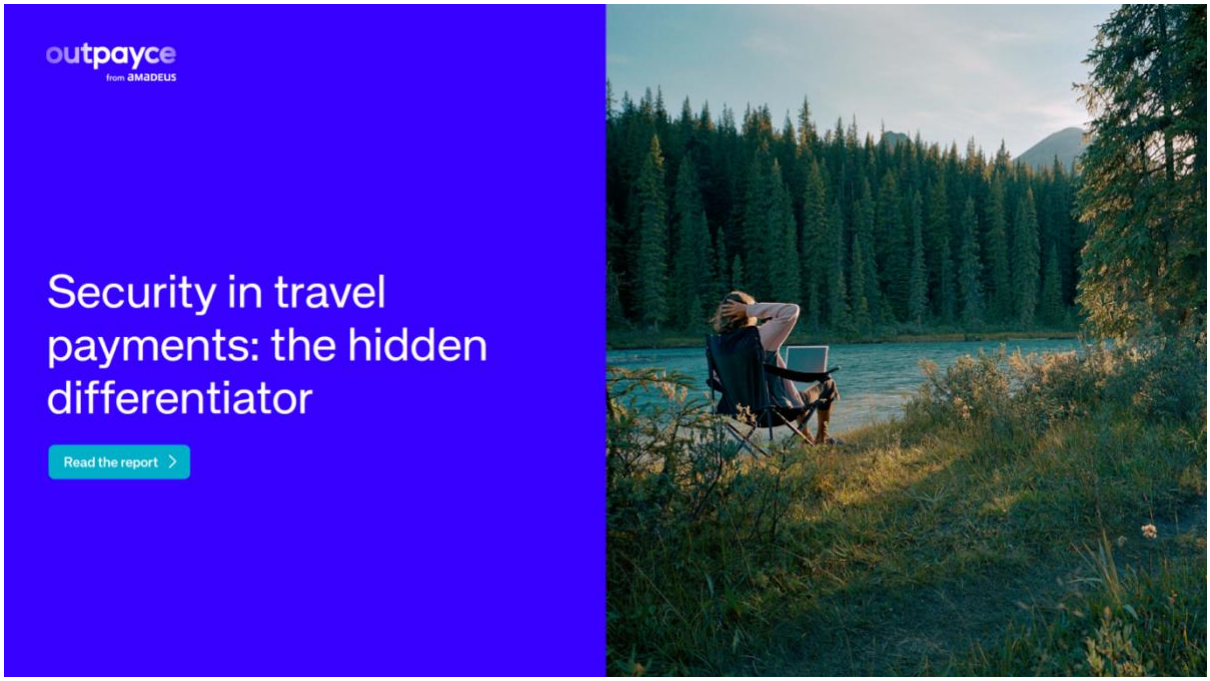
With NDC, the agent in most cases still collects the card details (both for 'customer' and 'agent's own' card) and performs the 3DS authentication step (where applicable) before passing on the tokenized card details (via the NDC aggregator) to the airline for authorization and settlement.

The airline (or travel agent) can then use the token for (e.g):

- Adding ancillaries
- Issuing refunds
- Processing a no-show fee
- Handling post-booking exchanges

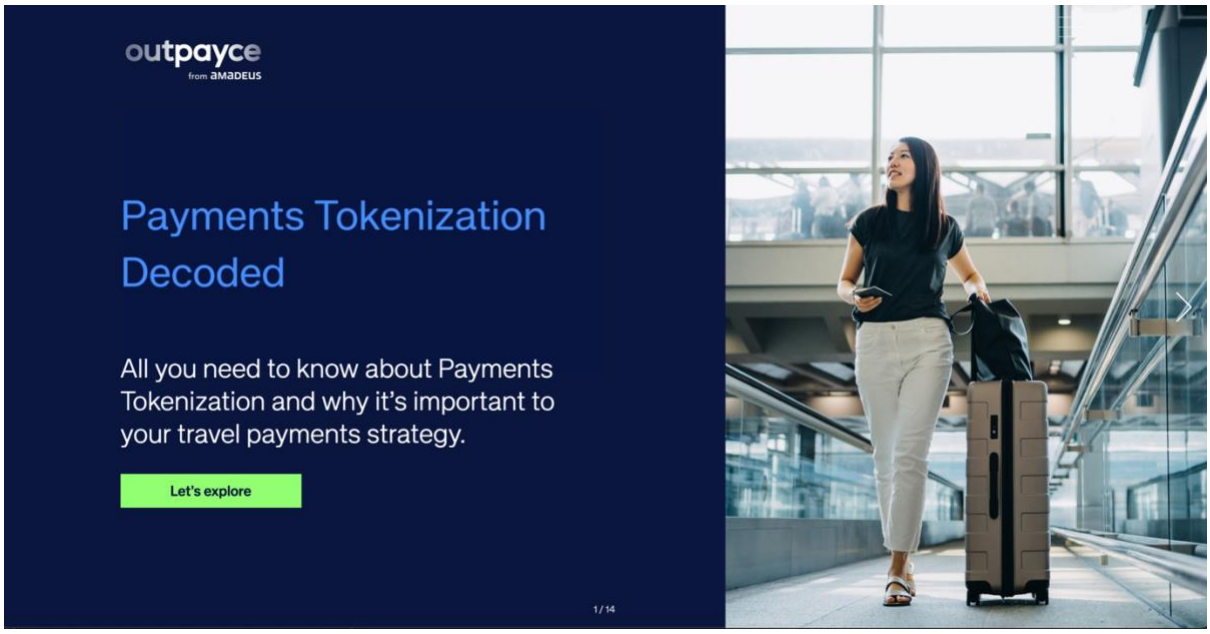
Outpayce from Amadeus: Security in travel payments: the hidden differentiator

This report, commissioned by **Outpayce from Amadeus**, draws on a multi-market survey with 4,500 travelers which shows that our industry's customers are increasingly security conscious and have come to expect high levels of security from their travel provider.



Click on image to download the white paper

Payment Tokenization Decoded, all you need to know about Payments Tokenization and why it's important to your travel payments strategy.



Click on image to access the eGuide

ℹ Follow us for more news and information

Subscribe to this newsletter to automatically receive it!

LinkedIn:

Paul van Alfen

Up in the Air | Consultancy

Airline Retailing Payments Up in the Air's Airline Retailing (Offer/Order/Settle/Deliver, NDC) page for the Airline & Travel Payments community

Think Travel Payments Webinar Series

YouTube:

UpintheAirPay

Would you like to suggest content for this newsletter? Contact me at paul@upintheair.aero