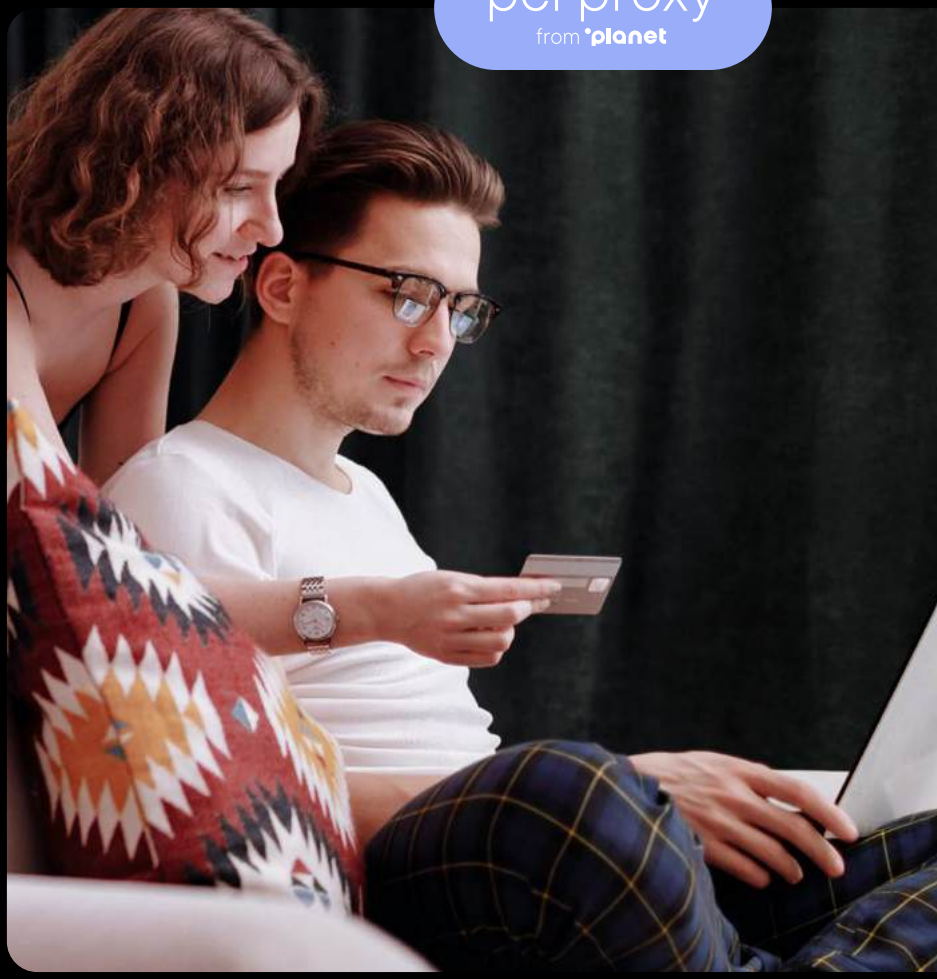
EBOOK

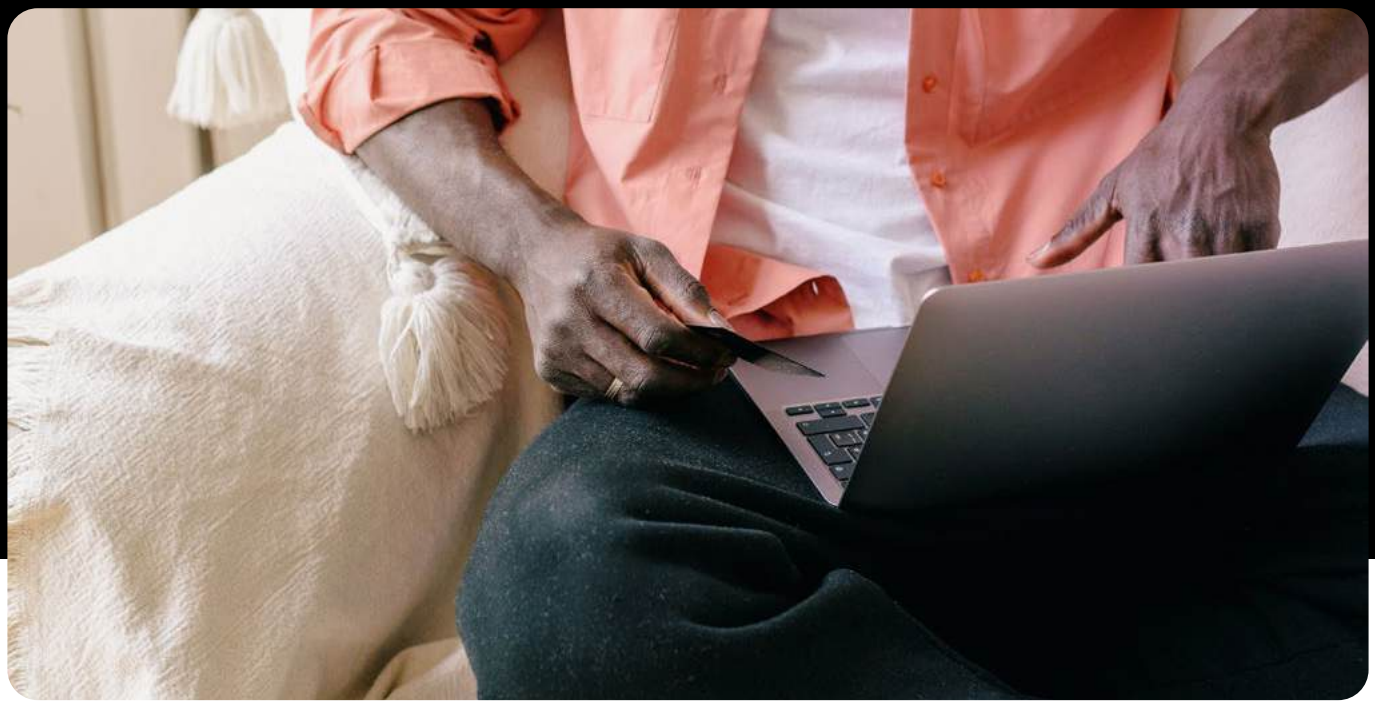
The Planet guide to **Payments and Tokenization for Airline Retailing**

pci proxy
from planet



Contents

Hello!



The air travel industry is rapidly evolving. Airlines process millions of transactions across direct and indirect channels every day. This makes airlines vulnerable to cybercriminals. So protecting passengers' payment data is critical to safeguarding brand reputation and revenue – and in gaining customers' trust.

Recent data breaches affecting major airlines such as Delta Airlines, Cathay Pacific, and British Airways highlight the importance of comprehensive and robust security measures.

The Payment Card Industry Data Security Standard (PCI DSS) is a framework designed to protect payment information. And the introduction of PCI DSS version 4.0 has given airlines 64 new technical and operational requirements to contend with.

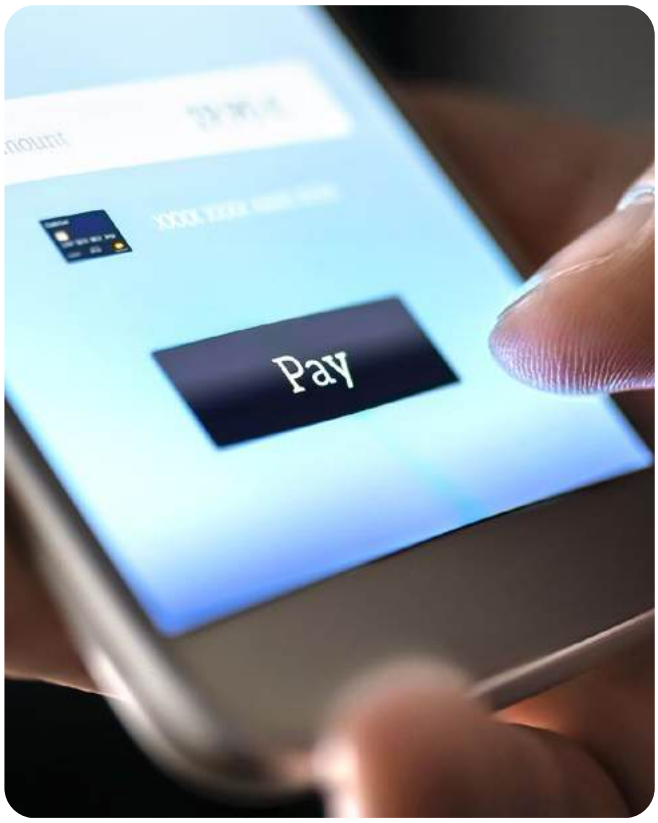
Payment compliance is becoming an increasingly complex area to navigate – and therefore needs a proactive approach from an entire organisation to safeguard sensitive data. Airlines also need to navigate a whole range of global and local regulatory requirements and adapt their data management strategies to comply with these mandates.

For example, the Reserve Bank of India's (RBI) data storage guidelines mandate the local storage of payment data within India, as well as other similar local legislation.

Maintaining data security is becoming even more complicated, due to the involvement of multiple third-party vendors or providers in payment processing. Each provider introduces additional layers of dependency – more stakeholders mean more chances the system could break, or not operate efficiently, which could make it vulnerable to attack.

An independent token system, or a token 'vault', offers a solution, shifting the responsibility away from airlines. This ensures managing card information from any channel is done in a PCI-compliant way on their behalf.

Tokens provide flexibility across various airline partners and applications, resulting in a more consistent, smoother process when managing card data from multiple online sources.



Tokens also make it easy and convenient to securely store payment details, by replacing sensitive payment data with a unique identifier, or token. This eliminates data from the airline's network, reducing the risk of data breaches and alleviating the time and resources associated with PCI DSS compliance assessments.

This payment security guide delves into the role of tokenization in airline retailing, with a focus on independent token vaults. We'll cover the various types of tokens available, how tokenization works, what a universal token vault is and how all this can help airlines with their payment security.

Payment tokenization 101

Tokenization is growing in popularity among global merchants and airlines. Around two-thirds of businesses globally now use some form of tokenization to strengthen payment security, reduce PCI DSS burdens and increase authorisation rates.

In this section we'll refresh the main principles of tokenization. Then we'll explore how it works, and the different token formats and uses. Plus, we'll explore the different types of token sponsors and vendors. Finally, we'll look at why companies are leveraging tokenization in today's payment landscape.

How it works

Tokenization is the process of substituting sensitive data, such as a customer's primary account number (PAN) or CVV code, with non-sensitive equivalents, known as tokens.

A centralised server, called a token vault, securely stores the original sensitive data. Then the de-tokenization process exchanges the token for the original sensitive data stored in the token vault.

Only the tokenization system that generated the token can perform the de-tokenization process. Whether that's managed by an external sponsor, or hosted by the airline operator itself. This upholds strict security measures for customers and the business.

What is a token?

Tokens are randomly generated strings of characters that serve as substitutes for sensitive data. But, unlike the original data, tokens aren't sensitive and have no intrinsic value. This makes it impossible to reverse the tokenization process without access to the tokenization server.

The most common distinctions are between single-use and multi-use tokens, and between format-preserving and non-format-preserving token formats.

Understanding these distinctions is key, as each serves different needs in today's complex payments landscape. Airline operators and businesses need to make sure tokens are compatible with existing applications and integrated third parties to minimise disruptions.

Token usage type:

Usage types refer to either single-use or multi-use tokens.

Single-use tokens are designed for one-time transactions. They minimise the risk of data exposure through limited validity, providing an extra layer of security. Single-use tokens are particularly useful for high-value or sensitive transactions, where security is paramount.

Multi-use tokens are valid over an extended period and businesses can use them for multiple transactions. These tokens offer convenience and continuity for customers making recurring payments.

For multi-use tokens, it's important to keep retention policies in mind. Retention policies refer to how long a business or service provider can keep sensitive card data in their systems. These policies are mainly defined by PCI DSS.

For primary account numbers (PAN), there are no specific retention policies defined by PCI DSS, whereas CVV numbers must be deleted after first use. So retention policies are important to consider, as different businesses will have different processes when it comes to payments, such as lead times, which require different policies. Plus, retention policies are needed to comply with PCI DSS assessments.

Sensitive authentication data, such as CVV codes, must not be stored after authorisation under any circumstances, even if they are encrypted. The only exception to this rule applies to issuing entities. While these entities can store CVV codes, they are still bound by strict security requirements and must justify the business need for retaining this sensitive information.

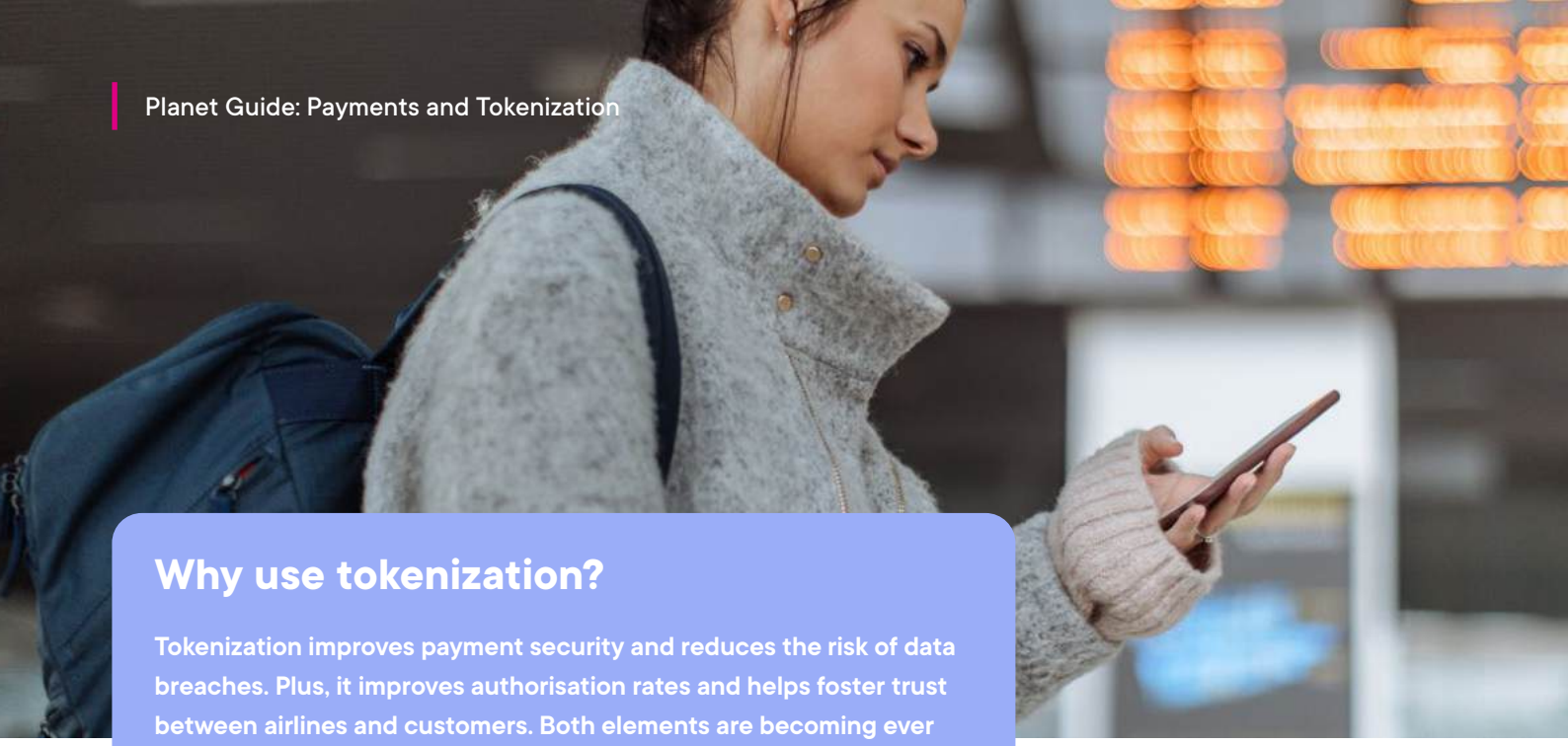
Format type:

Token format is another important consideration. This applies particularly to maintaining compatibility with existing applications and integrated third parties. There are plenty of possible token formats available, but two of the most common classifications are format-preserving and non-format preserving tokens.

Format-preserving tokens usually keep both the length and the specific structure or format of the original data. This makes them particularly suited for applications, which can easily handle this token format. Applications don't need to make significant changes to the existing systems or data structures, making implementation more efficient. Plus, it reduces the risk of errors or compatibility issues when working with tokenized data.

In contrast, non-format preserving tokens bear no resemblance to the original data. These tokens can incorporate a mix of alphabetic and numeric characters, as well as special symbols, and differ in length from the source data.

Creating a token that's entirely different to the original information offers enhanced security. This is because the resulting tokens are significantly more challenging to guess or reverse-engineer. This results in a higher level of data protection. But with increased security comes potentially more complex integrations with existing systems that expect data in a specific format.

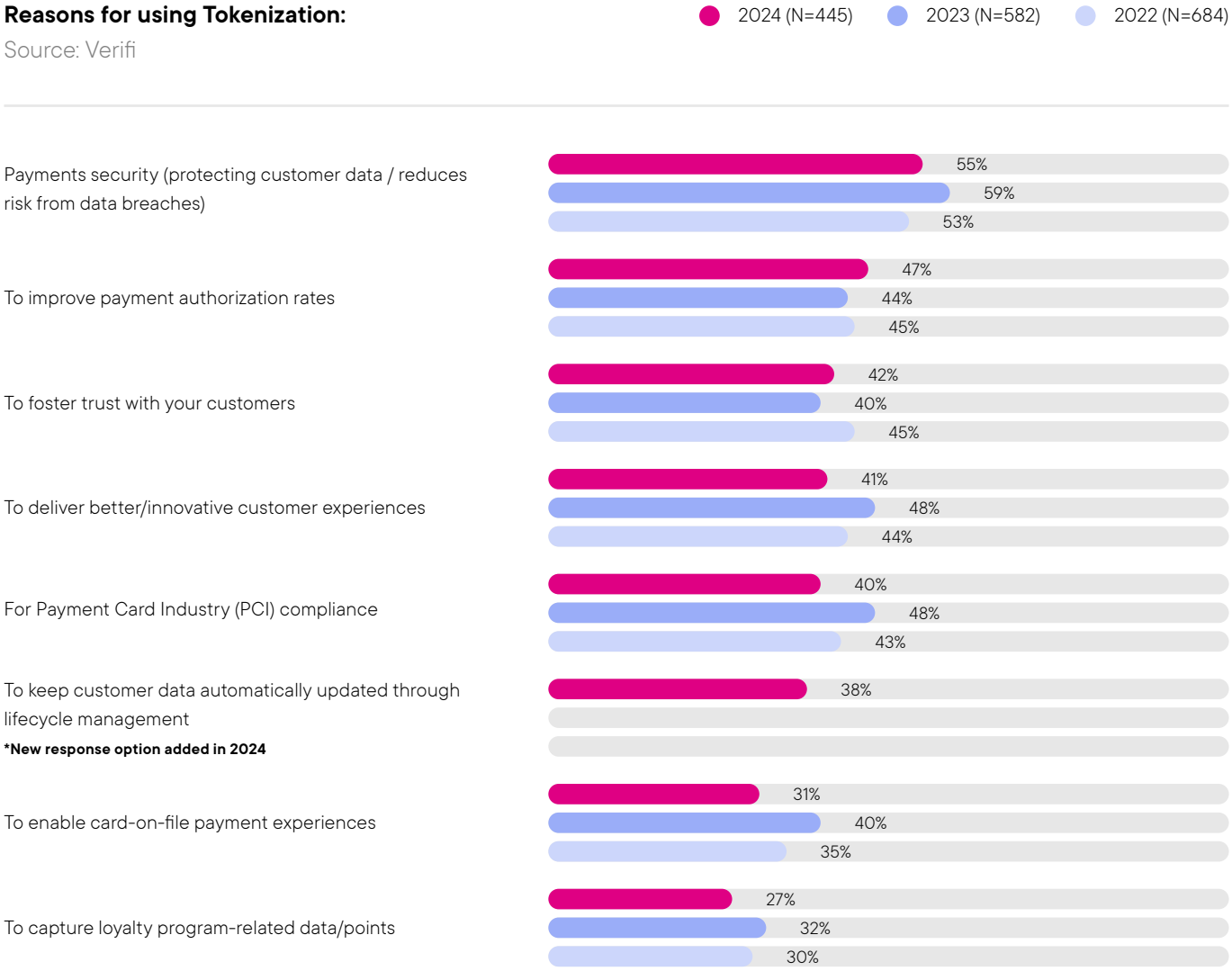


Why use tokenization?

Tokenization improves payment security and reduces the risk of data breaches. Plus, it improves authorisation rates and helps foster trust between airlines and customers. Both elements are becoming ever more important. According to the 2024 Global Fraud & Payments Report by Verifi, these trends are increasingly significant.

Reasons for using Tokenization:

Source: Verifi



Different token sponsor types:

We can categorise tokenization providers by the sponsor type. This refers to the entity responsible for issuing and managing the tokens. There are many sponsor types, including card schemes, issuers, acquirers, orchestrators, payment gateways and universal token vaults, as well as businesses hosting their own vaults. However, these are the three main types:

Payment gateways:

Most payment gateways offer built-in tokenization, so no need for extra development from the airline. This is great for both businesses and customers as it's usually straightforward to implement.

But, the payment gateway tokens work exclusively within that particular payment gateway's ecosystem. This restriction means that tokens generated by one payment gateway cannot be used or recognised by another. This lack of flexibility can leave airline operators locked in with a certain provider, finding it difficult to switch payment gateways or work with multiple providers.

Advantages	Limitations
Seamless integration: Built-in tokenization requires minimal additional development, reducing time-to-market.	Ecosystem lock-in: Tokens are confined to the specific gateway's environment, limiting flexibility.
Compliance simplification: Often includes PCI DSS scope reduction out-of-the-box.	Multi-gateway challenges: Using multiple gateways requires managing different token formats and integration points.
Unified solution: Tokenization is typically bundled with other payment services, simplifying vendor management.	Limited use cases: Typically focused on the collection via direct channels such as the website, may not support indirect channels.

Card schemes:

Card networks like Visa, Mastercard or American Express supply schemes or network tokens in cooperation with issuers. They offer enhanced security, higher approval rates and cost benefits, along with interoperability. Card networks offer more flexibility than payment gateway tokens, which means broader acceptance and usage across different applications and third parties.

But it's usually complicated to integrate network tokens, and requires certifications. Plus, businesses aren't usually allowed to integrate directly with the card networks. And the adaptation is still ongoing, which means that not all payment gateways are ready to accept network tokens.

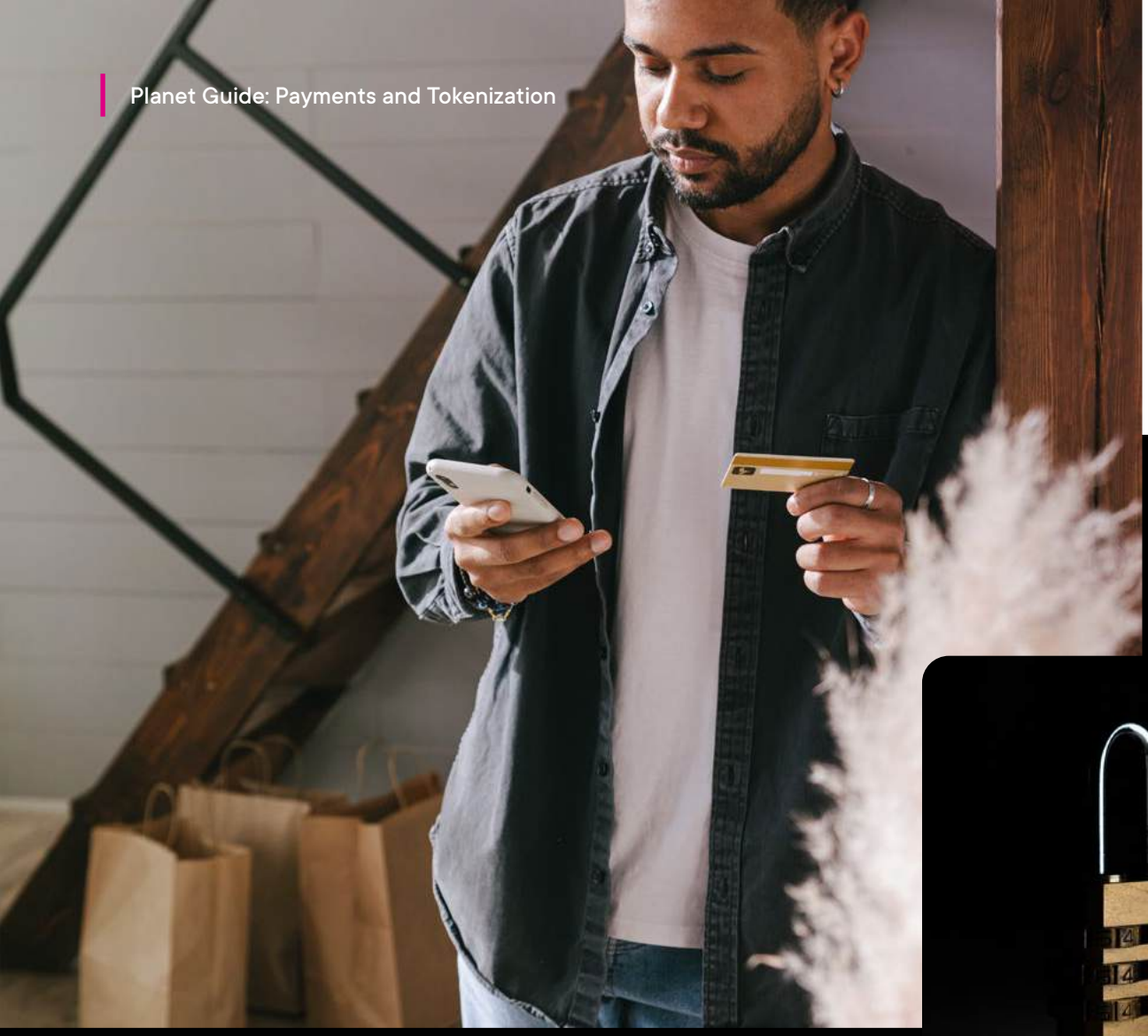
Advantages	Limitations
Improved authorisation rates: Network tokens often lead to higher approval rates and lower fraud.	Complex integration: Requires significant technical resources and often involves lengthy certification processes.
Interoperability: Usable across different acquirers and gateways that support the scheme.	Indirect access: Most businesses must access network tokens through third parties, adding a layer of complexity.
Update management: Automatic updates of card details (e.g. expiry dates) can reduce declines.	Regional variations: Adoption and functionality can vary significantly across different global regions.

Universal token vaults:

Universal token vaults are versatile solutions for managing payment information. They are agnostic, so tokens can be used across various payment gateways and third-party services. This reduces vendor lock-in and enables seamless integration across platforms.

With features of both network tokens and payment gateway tokens, universal tokens offer security and compliance. And they give businesses the flexibility to switch providers or work with multiple gateways without the hassle of managing different token formats. However, implementing universal token vaults can be more complex and may require additional technical resources and expertise. Despite this, their scalability and adaptability make them an attractive option for airlines looking to streamline their payment processes.

Advantages	Limitations
Vendor agnostic: Tokens can be used across multiple payment service providers, reducing lock-in.	Integration complexity: May require significant initial development effort to implement effectively.
Omnichannel support: Facilitates consistent tokenization across various sales channels and partners.	Additional cost layer: Introduces another vendor and potential cost centre in the payment stack.
Centralised management: Offers a single point for token management, simplifying operations.	Potential performance impact: Adding another layer to the payment process may affect transaction speed.



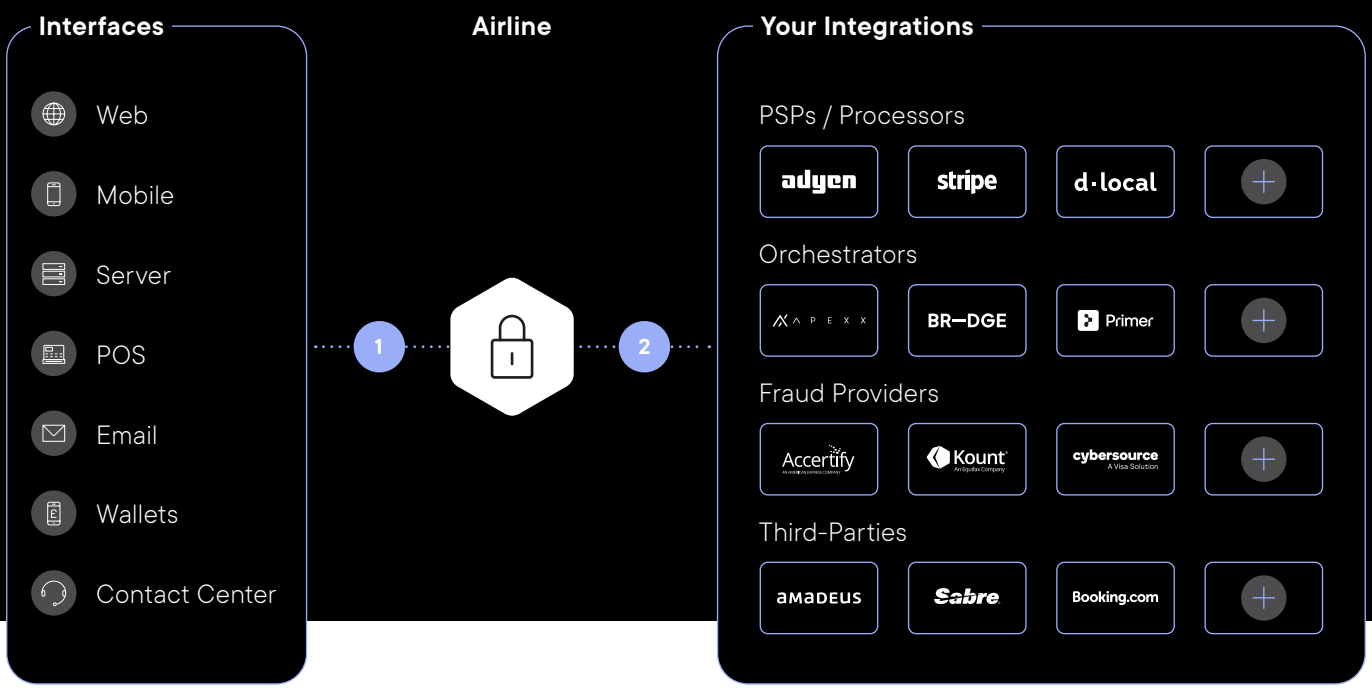
Understanding universal token vaults

Leveraging tokenization technology is generally consistent across different sponsor types, but the term 'universal' introduces a significant distinction. In the context of vaulting, 'universal' implies that providers can collect payment data through various methods. And that the resulting tokens can be transmitted to any provider with the same level of flexibility. Unlike a payment gateway, where tokens are restricted to the gateway's specific environment, universal tokens offer complete flexibility in their usage.

In this section we'll explain the concept of a universal token vault, how it works and how it addresses the main challenges airlines are facing when it comes to PCI DSS compliance, preventing data breaches or avoiding lock-ins.

How it works

Universal token vaults enable airlines to collect, store, and use payment data in the form of non-sensitive tokens, with full flexibility. This includes collecting and accepting payment data through a wide range of interfaces, and the use and exchange of data across any of the integrations the airline has in place.



01 Collect

Universal token vaults offer a comprehensive suite of methods for collecting sensitive payment data. They ensure airlines never directly touch or handle the sensitive data they collect.

Besides the usual web and mobile checkout components, this often includes server-side APIs or reverse proxy servers that sit between the airline's server, and the indirect channel partner. They tokenize sensitive credit card data within the reservation or booking messages on the fly, before they hit the airline server.

02 Use

During payment processing, the airline's system uses the generated token instead of the actual card information. The token vault has the capability to reconvert this token back to the original card details.

This conversion process is facilitated through a reverse proxy server, which functions as an intermediary between the airline's server (which initiates the request) and the receiving entity (which receives the request). By serving as an intermediary, the universal token vault performs a real-time substitution, replacing the token with the original card data before forwarding the request to the receiving entity. This sophisticated procedure ensures seamless compatibility with any payment system the airline has integrated with.

Top challenges in airline retailing that universal token vaults can solve

Taking the pain out of PCI compliance

For airlines, PCI DSS compliance is not just a regulatory obligation but a critical component of their overall security strategy. It's a set of security standards designed to ensure that all companies that accept, process, store, or transmit sensitive card information maintain a secure system or environment.

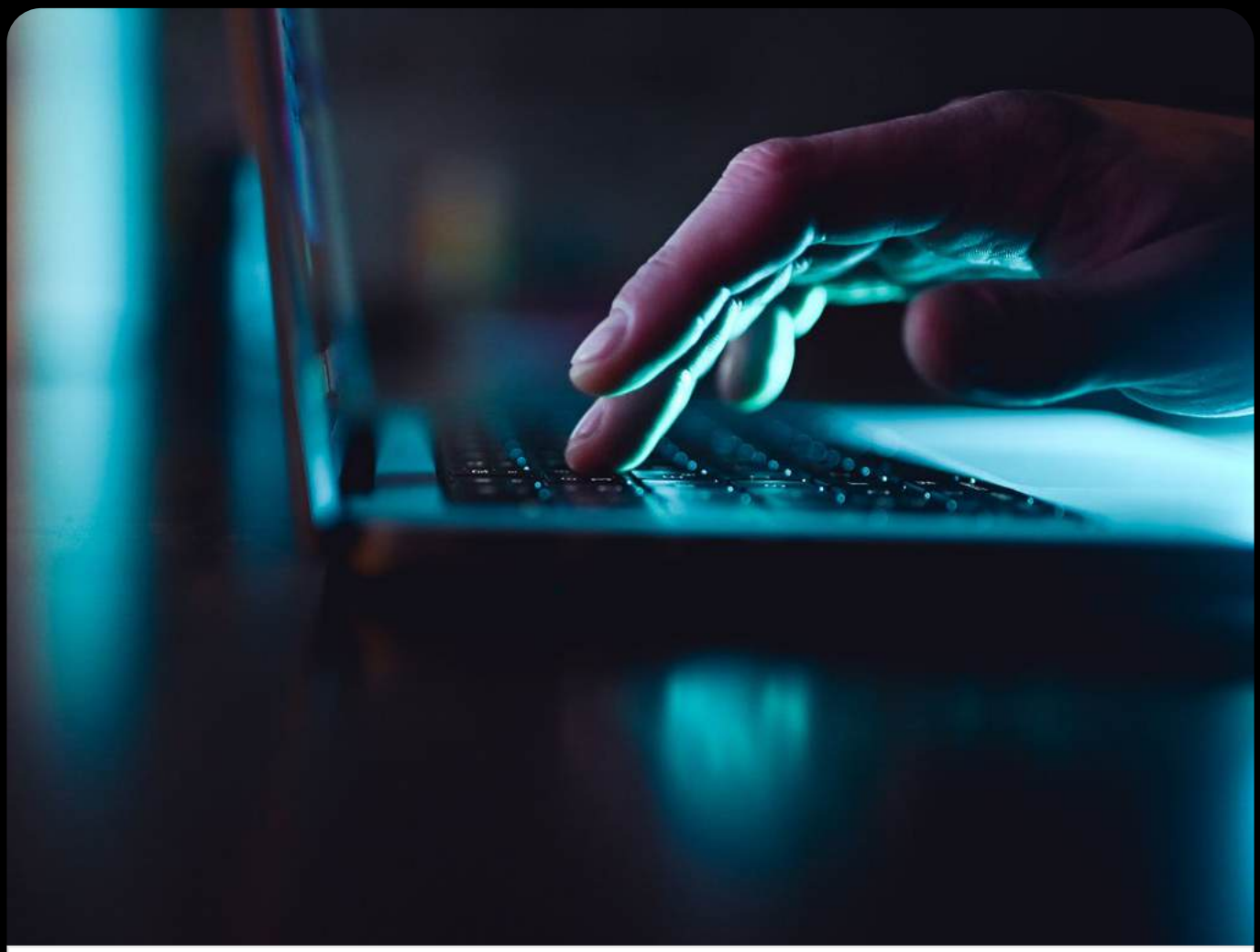
Achieving or maintaining PCI compliance can be extremely complex, taking some airlines months, or even years.

In the past, many airlines looked to do this all in-house, which is a considerable drain on time and resources. New staff must be recruited, or existing employees need to shift their focus away from other projects. And the team must invest time in training to understand all the details and PCI compliance processes, as well as their impact on the airline's systems, products, employees, and overall infrastructure.

Once this is understood and the team are up to speed, requirements must be implemented. And it doesn't stop there. Businesses must be re-certified for PCI compliance on an annual basis.

For airlines, using a universal token vault is likely the most effective measure to reduce PCI DSS headaches. As tokens replace sensitive card data, and airlines have no access to this, many questions and requirements in the PCI assessment simply won't apply. Airlines reduce their PCI scope and audit costs to the absolute minimum.

As opposed to payment gateways, universal token vaults not only host the card data collection on web and mobile applications but also provide a wide range of other collection tools, ensuring that the full payments stack remains out of scope. For example, universal token vaults can act as a proxy layer between the airline and indirect sales channels, usually sending reservation messages via HTTPS or SFTP protocols to the airline servers. By intercepting those requests on the fly, universal token vaults can ensure that sensitive data gets tokenized before arriving on the airline's servers.



Data breaches and fraud: How safe are tokens against hackers?

Airlines are prime targets for cyberattacks due to the vast amount of personal and financial data from passengers they handle. In the worst case, a data breach can compromise thousands of passenger details, leading to financial losses and reputational damage, which has been seen in recent years with major airlines such as Delta Airlines, Cathay Pacific, and British Airways.

In addition, airlines often face attacks due to their infrastructure, operational complexities, and reliance on interconnected systems. This makes them vulnerable to various threats, including ransomware, phishing, and other sophisticated attacks aimed at disrupting services or stealing information.

Using a universal token vault mitigates this risk by ensuring that even if data is intercepted, it's rendered useless to cyber criminals. Tokenization replaces sensitive account data with a unique and non-sensitive identifier – a token. These tokens are meaningless to anyone who gains unauthorised access to them, as they cannot be reverse-engineered to reveal the original data. So airlines can significantly reduce the risk of data breaches, protect their passengers' information, and maintain their reputation and trustworthiness in the industry.

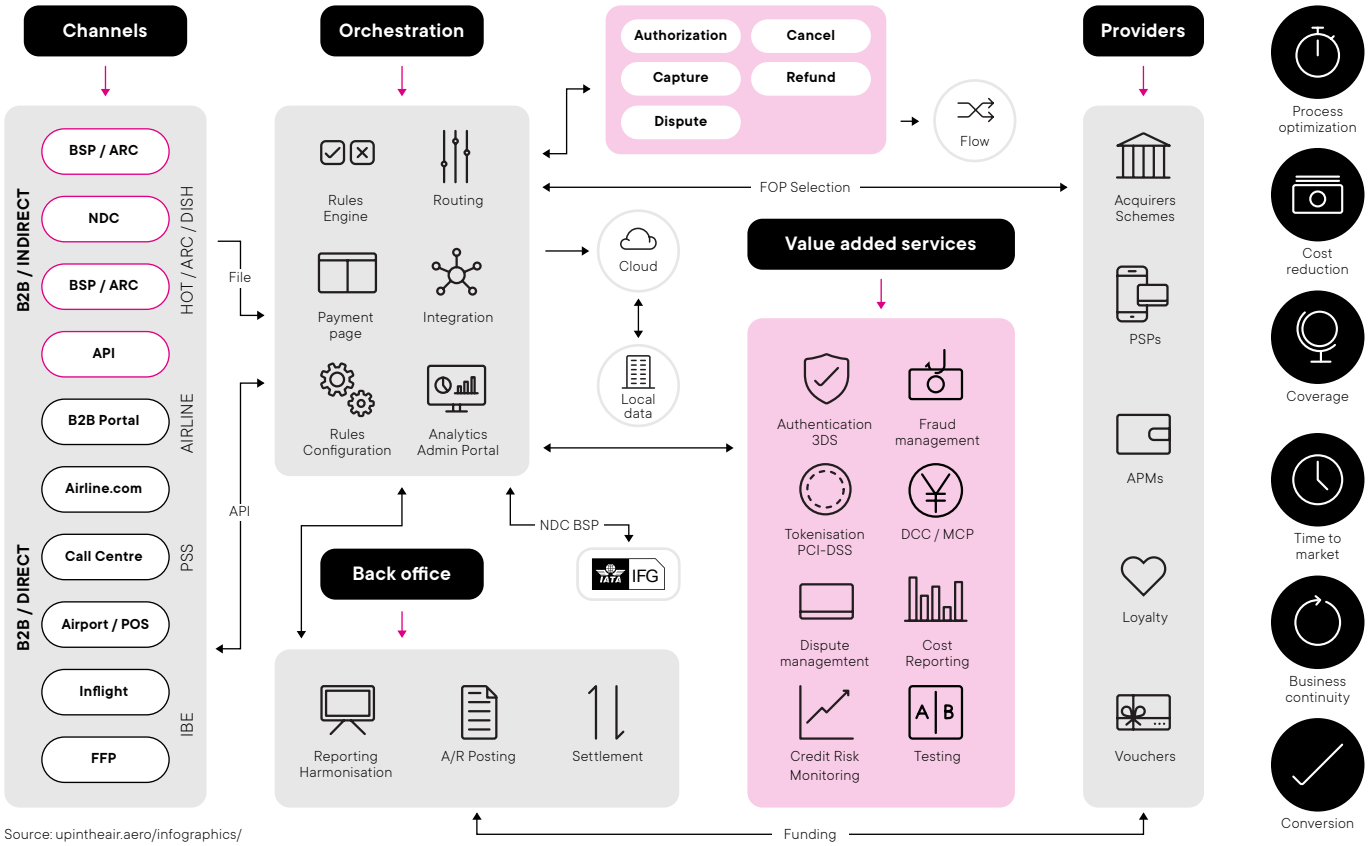
Complex airline payments - how to keep it simple across multiple channels

A payment transaction can be as simple as collecting passengers' payment details at checkout – ideally hosted by a payment gateway – authorising the details, and, if approved, transferring the funds to the airline's merchant account.

However, the airline retailing landscape is more complex when it comes to payments. There are many different channels, applications and providers involved in the process. When it comes to channels, flight bookings can come via travel agencies and booking platforms such as GDS or NDC, mobile and website channels, call centres or in-flight purchases via a point of sale, to name just a few.

After collection, data passes through multiple internal applications before the actual transaction gets processed across payment gateways, processors, acquirers, card schemes, and more. And this simplified diagram below only scratches the surface.

With direct and indirect channels and multiple providers involved in the payment process, using a universal token vault can be an effective measure to streamline operations and reduce dependencies on certain providers. Universal token vaults provide omnichannel support, ensuring a consistent tokenization process across direct and indirect channels. This means that airlines can easily share tokens freely across multiple payment service providers or any integrations they have. This also means that airlines can implement automated failover rules. If one Payment Service Provider (PSP) experiences downtime, transactions can be rerouted to another PSP without interruption, ensuring continuous payment processing.



Source: upintheair.aero/infographics/

Conclusion

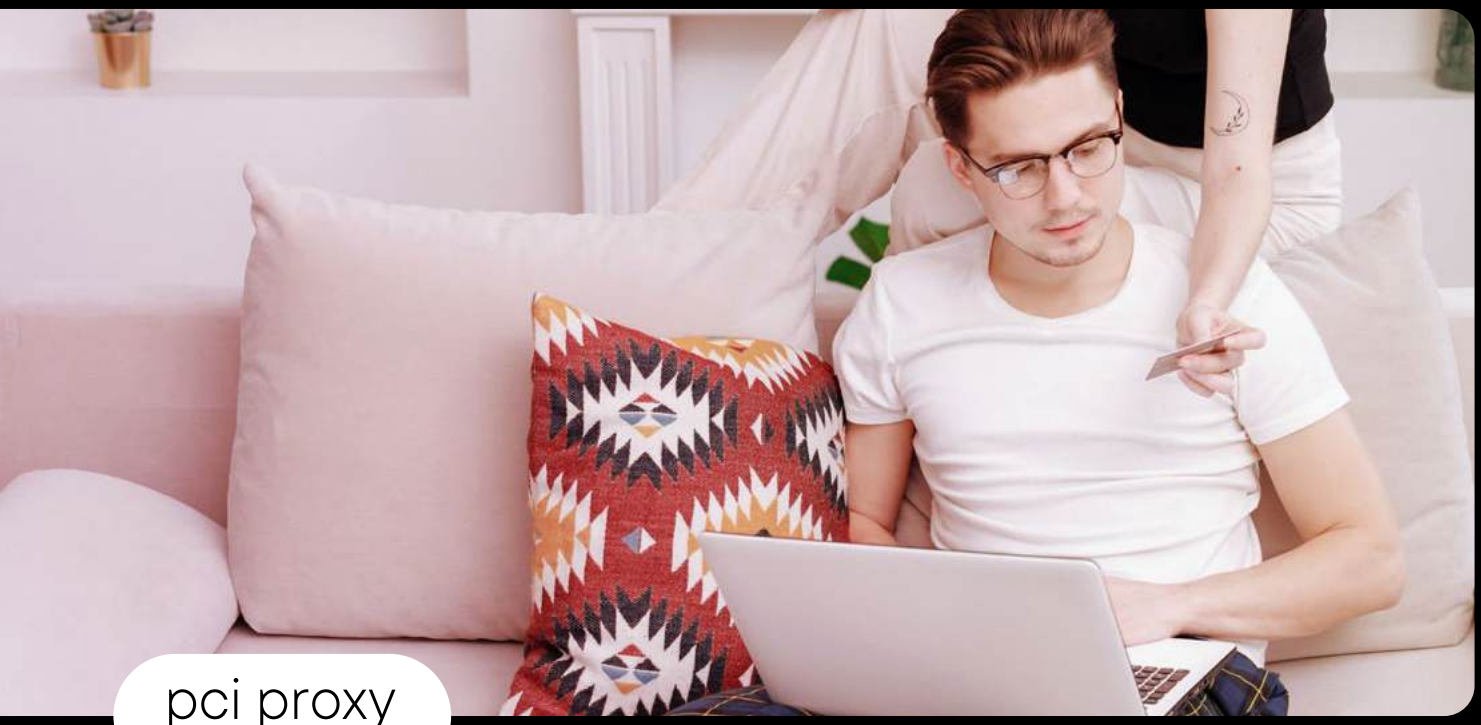
A universal token system provides airlines with a comprehensive solution for protecting sensitive payment data while maintaining flexibility in their operations.

By centralising tokenization, airlines can reduce their PCI DSS compliance scope, protect against data breach risks, and simplify payment data management across multiple channels and partners. The token vault's ability to securely store and collect payment data, and distribute tokens to any provider, allows airlines to work seamlessly with various payment service providers (PSPs) and acquirers, improving security and reducing compliance burdens.

While a universal token vault offers many benefits, its suitability depends on an airline's specific needs, existing infrastructure, and strategic goals. Each airline should evaluate its size, geographic reach, and payment processing setup to determine the most appropriate approach when it comes to its tokenization requirements.

About Planet

Planet is a leading global provider of financial services including payment tokenization. Its fully provider-agnostic tokenization system, PCI Proxy, empowers businesses such as airlines, hotels, retailers, platforms, or financial service providers to simplify compliance, minimise risk and develop and maintain control over their payment flows, allowing the use of tokens with payment service providers, card network, orchestration platforms, fraud providers and more.



pci proxy
from planet

PCI Proxy is part of Planet, one of the leading software and payment providers. PCI Proxy empowers organisations such as airlines, hotels, retailers, platforms, or financial services, to securely protect the payment data they store, process and transmit through a universal token vault solution.

With this approach, businesses can minimise their PCI compliance scope and ensure they retain the flexibility to work with any payment service provider, such as payment gateways, orchestrators, and acquirers.

Leading brands worldwide use PCI Proxy to enhance their payment flexibility, improve the security of transactions, and reducethe significant burden and cost of PCI DSS compliance

For more information, visit:

weareplanet.com

LinkedIn