Self-sovereign: the new dawn of digital identity in travel

Giving identity storage and control back to the passenger is the next step, but how can organisations ensure customer relationships are not lost?

Organisations are spending huge sums in efforts to protect sensitive identity data and meet consumer demand for both next-level data privacy and frictionless experiences where a secure digital ID is used to access interconnected services.

The self-sovereign identity (SSI) approach continues to gain traction, recentring the notion of identity around the individual. Put simply, the individual owns and controls access to their identity data, and can use it to access goods and services from different organisations. But with identity data moving out of the corporate environment and into the hands of the consumer, how can organisations ensure their customer relationships remain intact?

Here are four considerations to bear in mind:

> **Travel companies have become a hotbed of personal identity data**

4.4bn

individual passenger flights globally in 2019

8bn+

individual identity transactions involving sensitive personal data including biometrics

10k+ years

annually spent on processing and verifying identity across global air travel

Airportwatch

1. Identity data is dangerous

Data is constantly under attack. Identity, credit and cyberfraud costs an estimated £190 billion a year in the UK alone, according to think tank the Royal United Services Institute.

At the same time, stricter privacy regulations heighten the risk of huge financial and reputational loss. For example, 9.4 million Cathay Pacific passengers were impacted in aviation's largest known data breach, leading to a government inquiry and a £500,000 fine.

As the requirements for identity data increase, which in travel now include other sensitive data such as biometrics, current health status and visas, travel companies have become a hot bed of personal identity data.

Given the coronavirus pandemic, there is the additional challenge of inextricably linking a customer's health status to a secure verified identity at the point of travel.

Organisations need an approach that allows them to set up a singular, persistent verified digital identity for each customer. They must also be able to orchestrate and configure the use of that identity while not storing or controlling the data themselves.

To enable this, Zamna has created a unique decentralised approach it calls Identity Rails. Similar to how open banking has transformed financial services, Zamna's Identity Rails are set to transform the way in which identity data is managed, stored, shared, connected and controlled between organisations and individuals.

"The strength in our approach lies in how companies can create valuable partnerships within their commercial ecosystems with verified identities at the centre," says Zamna chief executive Irra Ariella Khi. "Giving identity storage and control back to the customer, without losing them to your competitor, is paramount; our Identity Rails infrastructure solves this."

2. Bad data, bad decisions

Quality data is at the heart of every business decision, from assessing risk and allowing access to services, to crafting personalised marketing campaigns at scale. But how accurate, and how verifiable, is identity data flowing through these systems? The truth is it's neither, yet.

"The foundation of identity data needs to change. You need a way to validate whether it is correct and establish if it's been seen before, while also removing the need to control or store," says Khi.

"Zamna enables organisations to create super smart verification 'signals' that allow recognition and validation of identity data previously seen but not stored. From this, clients can remove the need to store sensitive data, aggregate verifications and work towards cleaning up identity data at scale. A single version of truth is the starting point."

With airports empty due to the pandemic, travel companies are rapidly transforming the way in which they can service and monetise passengers

3. Trust and privacy are everything

Trust is a huge challenge for organisations. Millions are invested in tools to trust that people are who they say they are and yet identity fraud is at an all-time high, says UK fraud prevention service Cifas. Given low adoption rates and privacy challenges, it is evident there's no silver bullet consumer app that will single handedly solve digital identity at scale. So how can organisations create trust and privacy at scale?

> **Self-sovereign gives identity storage and control to the customer, but not losing them to your competitor is paramount; our Identity Rails infrastructure solves this**

"We use permissioned distributed ledger technology to harness the power of a curated network at scale and in real time. The immutability of this type of system means once a verification event has happened it can never be altered or reversed, but it can be recalled," explains Khi. "From this base, companies can enable their customers to create persistent identities secured by both biographic and biometric identity attributes."

"Putting secure identity at the centre of your business, together with trust, extends new commercial opportunities and business models."

Airlines are exploring this to solve the challenge of verifying and servicing vast numbers of passengers to enable frictionless travel. Zamna has been instrumental in the development of the International Air Transport Association's One ID framework, which is set to harmonise the way identity is managed across a notoriously fragmented travel ecosystem.

4. Connecting the dots

The dream for the post-pandemic traveller is a joined-up experience, where they can control and prove their identity only once before even booking a trip, and seamlessly share this with airline, rental car and hotel systems. But allowing identity data, and the trust in that data, to flow freely through the travel ecosystem in this way has, until now, been an insurmountable problem, exacerbated further by increasing data privacy concerns.

"Our Identity Rails are the next generation of corporate infrastructure for individuals and organisations to trust, orchestrate and control identity data without the limitations of existing self-sovereign identity technology. Organisations can put their customers back in control, but maintain operational and commercial value," says Khi.

The development of next-generation privacy and security strategies is now a non-negotiable for organisations dealing with identity data. Tools that orchestrate identity within an organisation, and with chosen commercial partners, while moving storage and control of this valuable, yet dangerous, data to the hands of the customer are where we are heading.

We've already seen the financial services industry move to the open banking framework to enable easy exchange of financial data transactions. Zamna believes its Identity Rails are the future for securely managing and orchestrating identity across organisations, and it has the travel ecosystem in its sights. Solving identity in travel is the holy grail. If this is Zamna's starting point, it may be the most important company in digital identity that you've never heard of.

For more information visit zamna.com

Zamna.