

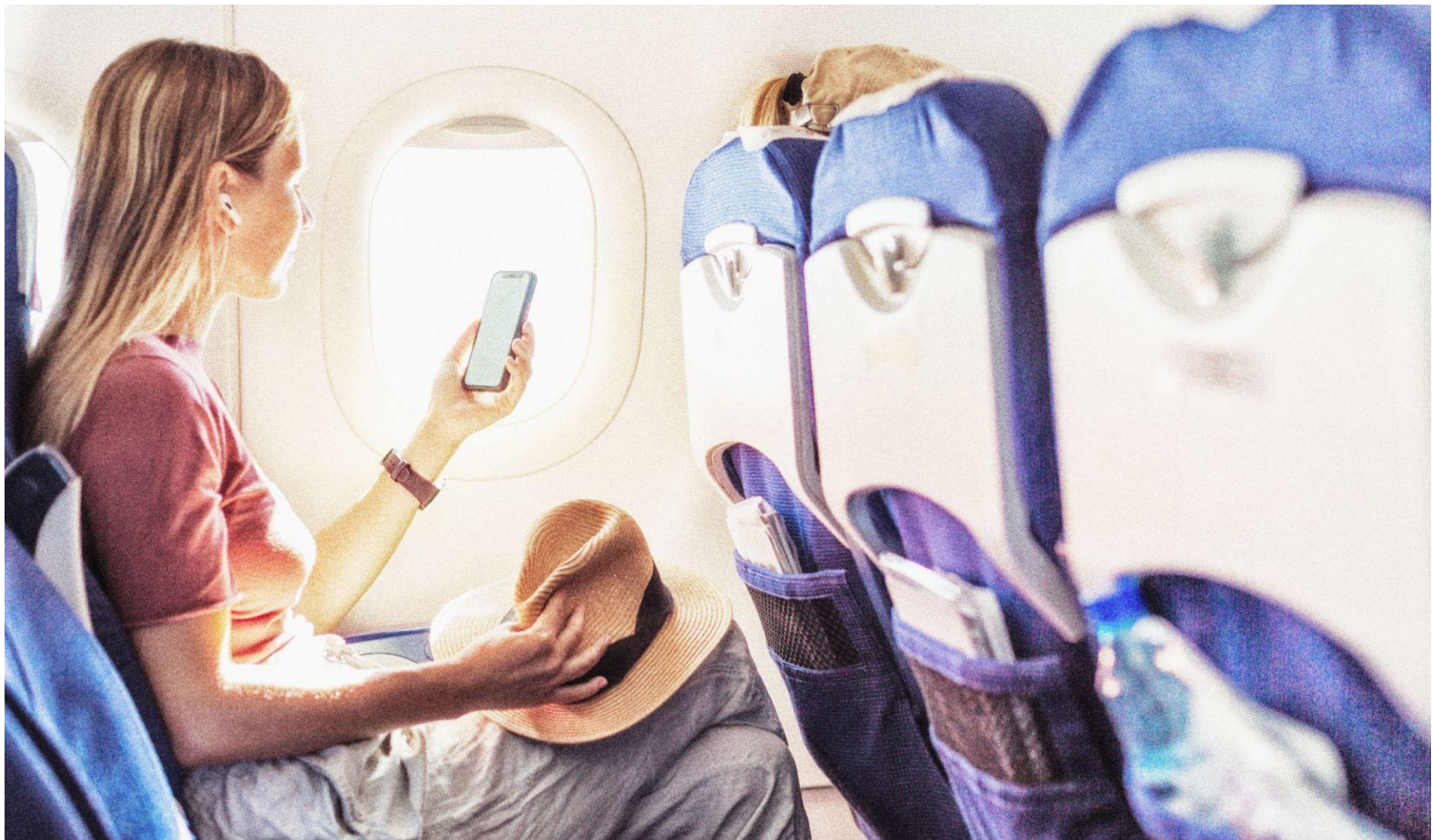
indicio[®]

AI, Chat, Decentralized Identity, and Digital Travel

Verifiable Credentials enable permissioned access, accurate data, and optimal, personalized performance from booking to boarding to hotel check-in and beyond

By Trevor Butterworth

November 25, 2024



You've got 25 minutes to make it to your connecting flight...

Before you're down the airbridge, your airline has messaged you with the location of the next flight and, using the GPS on your phone, is sending you directions and showing you where you are on a map. It asks whether you want to share your location data with the gate.

You say "yes," and the gate agent can track your progress — maybe holding that door for those vital final seconds it takes you to make the flight.

Some airlines are already close to delivering this kind of customer service. At the leading edge of airline apps, passengers are being sent push notifications via text or in-flight wifi for every step of the trip, from the time it will take to get to the gate to how to store their luggage, to bag claim details before landing. If a flight is delayed, airline apps can push alternative flight solutions.



Some apps have also begun to push boarding passes into the home screen of a phone, so it's easy to scan when the passenger arrives. When checking in, some passengers now have the option of using the credit card they purchased their flight with to pay for in-flight snacks.

These customer interactions are not without friction. Passengers still have to juggle their phones to present their boarding passes or manage interactions. Credit card data needs to be stored and managed in data compliant and fraud resistant ways. Help from chatbots requires passengers to manually enter Flight Confirmation Numbers, Loyalty Program, Name, Date of Birth and Passenger Name Record, which inevitably means they have to toggle across the reservation screen and chat. A mistaken input means starting over. These systems are optimized to work with data that passengers, typically, do not commit to memory and have to manually retrieve outside of chat.

And what about a joined-up chatbot experience, where your airline could seamlessly redirect you to another airline chatbot or an airport chatbot for transit or onward travel? Or just help you find the nearest Starbucks — and submit and pay for your order?

Chat is “optimized to work with data that passengers, typically, do not commit to memory and have to manually retrieve outside of chat.”

Know your passenger

There are two obstacles to delivering frictionless and optimized customer interaction through apps, chat, and AI: passenger identity and data integrity. So much of the friction in customer interaction is generated by trying to be certain that the passenger is who they are supposed to be and ensuring that the information they present is authentic.

These obstacles work against the idea of seamless processes that need to ingest data instantly in order to deliver real time value. So, how do we make apps, chat and AI work in a way that delivers a dazzling, integrated customer experience?

Permissioned access; precise data; optimal, personalized performance

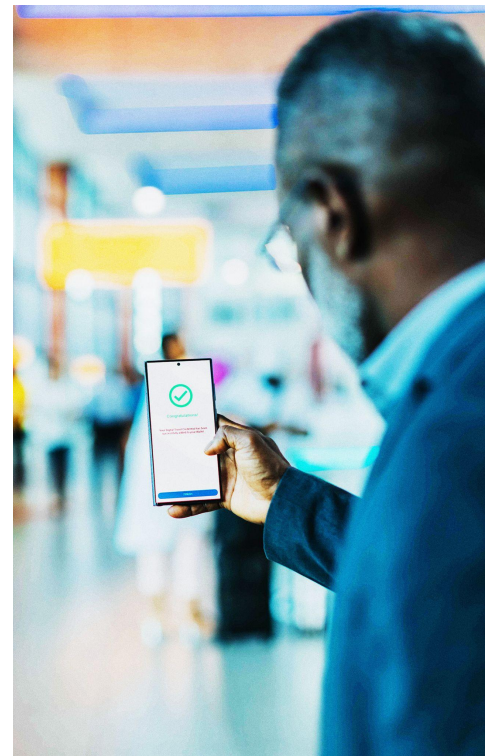
Verifiable Credentials are a simple way to generate seamless authentication. They can be used to permit a chatbot or AI agent to access a set of personal data on a person's phone. To understand how this works, a little background on decentralized identity, a specific and very powerful form of digital identity.

For digitally seamless interaction, we need a very high level of identity assurance. In the manual world, we rely on physically checking and manually scanning passports to meet this requirement. In the digital world, we need the same level of identity assurance; and the best way to do this is to create a digital version of a passport that delivers the same or better assurance. The International Civil Aviation Organization (ICAO), which governs the rules for physical passport documents has specifications for their digital equivalents, and specifically, a [specification](#) as to how a passenger could create a digital equivalent of their passport. This is called a DTC — Digital Travel Credential — Type 1.

A DTC extracts the digital information in a passport chip and combines it with **1) cryptographic authentication** of the passport issuer and **2) a real-time liveness check**. You take a selfie in real time and that is compared with the digital version of your passport photo.

What makes a DTC so powerful is that it is a Verifiable Credential. This is a specific kind of digital credential that enables you to:

- Cryptographically prove who issued the credential (e.g., a government or airline).
- Prove that any information in the credential is authentic and hasn't been tampered with.
- Prove that the credential is bound to the person presenting it.
- Allow the person hold their data on their device and share it by consent. There is no need to centrally store any personal data or rely on third parties for authentication (hence, decentralized identity).



A passenger adds a Digital Travel Credential to their digital wallet in Aruba.

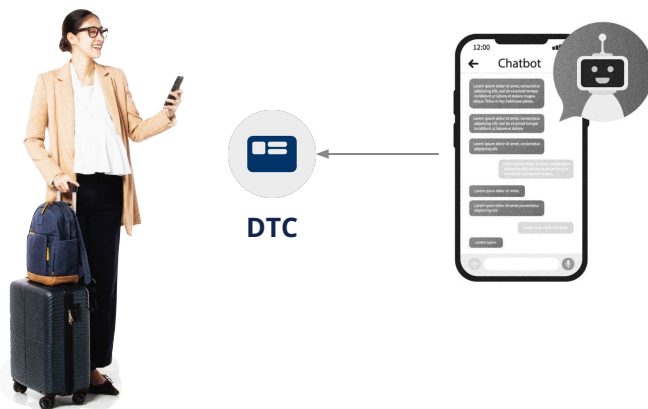
“Find my gate, lounge, ground transportation...”

As the DTC allows passengers to hold their own data and consent to share this data (and in various privacy-preserving ways), this radically simplifies compliance with data protection regulation such as GDPR.

A person can also hold many different types of credentials, thereby holding all kinds of information for consent-based sharing; these credentials and their information can also be combined in different ways, effectively turning a person, a passenger, into their own data sharing platform.

This means that, an AI agent or chatbot can immediately verify the identity of the passenger, request access to their flight data, and instantly deliver helpful information based on:

- 1) Direct consent or pre consent.
- 2) The specific data in the DTC and electronic ticket.



1. Authenticates DTC
2. No manual text input is needed, leading to improved data quality.
3. Obtains consent to access personal and flight details
4. authentication and permissioned access enables autofill direct from the credential
5. Provides assistance — connecting flight, lounge location, ground transportation details, etc.

No manual data entry is needed. No complex backend verification is needed. No direct integration between databases is needed. All the relevant data is portable, cryptographically bound to the passenger, cryptographically authenticatable, and instantly accessible to the chatbot.

What this means for the passenger: The point of a chatbot is to solve someone’s problem without first creating a data entry challenge for the passenger and a data quality problem for the airline. Whether implemented as voice, swipe or pre consent, the passenger doesn’t have to input any details when they use a Verifiable or Digital Travel Credential. Authenticated information is automatically ingested in a stress free way.

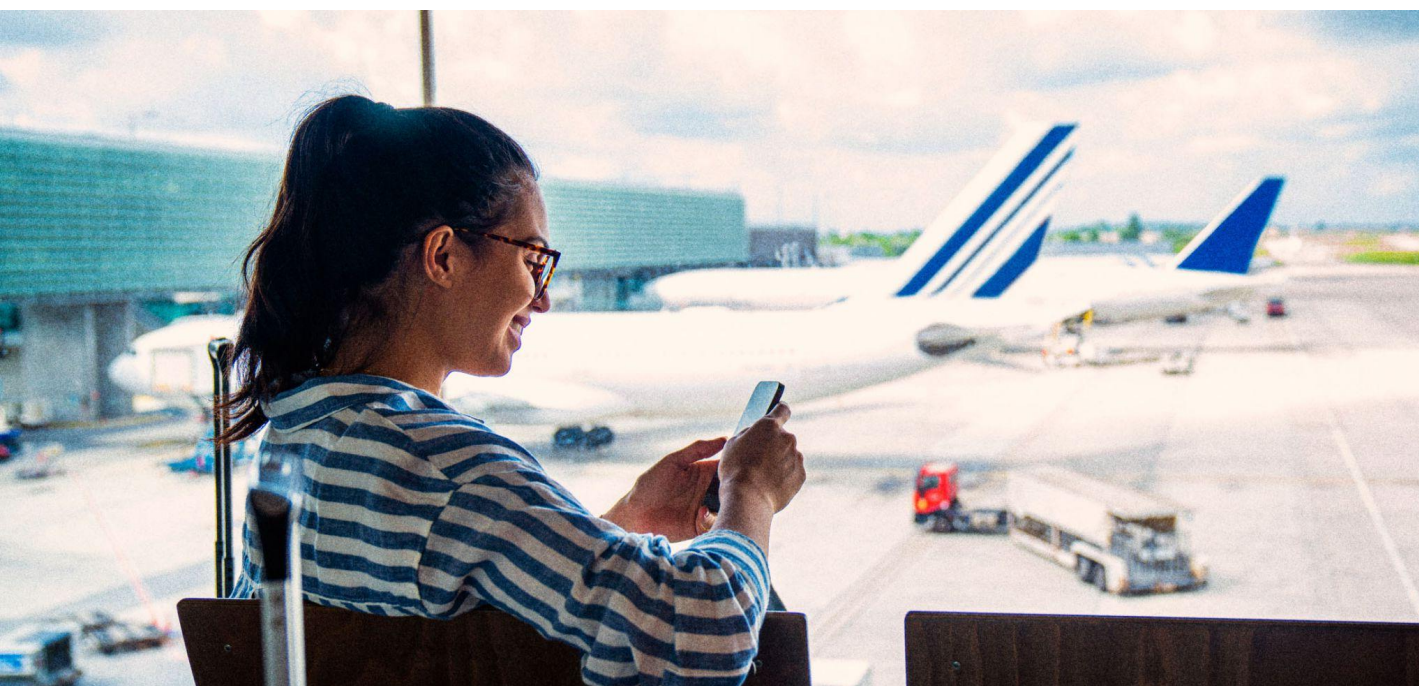
What this means for the airline: It can immediately know that the interaction is with an authenticated passenger, reducing fraud. It can know that the information ingested is accurate, speeding up customer engagement.

The passenger is now their own data platform

Now that you have an instant, permissioned way to access authenticated data from a verified identity, the fun begins.

Verifiable credentials can be configured so that people can hold all kinds of useful data — and credentials can be combined to leverage the credential with the most identity assurance. For example, I can present data from a DTC and a Loyalty Program Credential and a verifier can know that both were issued to the same person.

This expands the scope of customer engagement. A passenger can seamlessly access an airport lounge by generating a QR code from the right credential; or, a passenger whose flight has been delayed and who may not have the status to use a lounge can be asked in chat whether they want to pay using airline miles or by using a credit card. Everything can be auto-filled through real-time consent and they can be issued with a QR code for instant access when they get to the lounge.



The airline has the assurance it's dealing with an authentic customer and it can request access to the information needed to deliver superlative engagement. Think about all the steps required to log into onboard wifi. No codes, no links, just swipe or even pre consent for automatic access.

Decentralized identity and Verifiable Credentials enable a seamless trust network between an airline and a passenger — one that can easily be expanded to cover partner organizations and service providers and everything a passenger might need for their flight or trip.

Example — “Change my flight”



1. Authenticates DTC and Loyalty Program VC
2. **“Change my flight”**
3. Obtains consent to access
4. Accesses PNR without passenger having to input their PNR or ticket number
5. Provides flight options
6. **Passenger chooses flight**
7. Chatbot facilitates change*

*The workflow will depend on the sophistication of the Chatbot: it may transfer the passenger over to a Virtual booking agent for executing the change and the booking agent will send updated travel details to the passenger.

“Change my flight and pay with points”



1. Authenticates DTC and Loyalty Program VC
2. Compares liveness check with verified biometric in DTC*
3. **“Change my flight”**
4. Obtains consent to access
5. Accesses travel details
6. Provides flight options
7. **Passenger chooses flight**
8. Chatbot facilitates change**

* If required by security policy

**The workflow will depend on the sophistication of the Chatbot: it may transfer the passenger over to a Virtual booking agent for executing the change and the booking agent will send updated travel details to the passenger.

AI and concierge-level service

This is where small-language model AI comes in. First, it can, in a permissioned way, learn passenger preferences so that it can “know” that they usually want a Starbucks at certain hours of the day, direct them to the nearest location, and take, place, and pay for the order — all from within the airline in-app partnership with Starbucks.

Flight delayed or canceled? “Chat, help me out here, I need to be in X by Y time, what are my options?” Yes, some apps can push this kind of response if they detect your flight has been delayed. But how about “find me a hotel room ASAP within these budget parameters, book, pay, and complete advanced check-in using my DTC?”

This is where small-language models tied to specific information domains really deliver value, not least because they are vastly more efficient and effective at search. And there’s no need for a hotel employee to photocopy your passport at reception.

It’s like you have your own personal concierge or gate agent. And if it can talk to you, it can talk to other chatbots or agents either to retrieve the information you need or pass you onto a different system — all without passengers having to manually input customer and flight information.

“...how about “find me a hotel room ASAP within these budget parameters, book, pay, and complete advanced check-in using my DTC?”



AI elevates chatbot interaction from clunky to clever because it is narrowly focused on specific use cases. When trained on small language models with contextually-relevant parameters, these AI agents deliver better accuracy, efficiency, and performance, while being smaller and requiring fewer resources to deploy.

This is all unlocked with authoritative, authenticatable digital identity. It represents a leap forward in customer engagement; it meets the expectations of digitally-native customers for everything to be manageable through their phones, and it meets the needs of airlines with finite resources, tight margins, and constantly increasing passenger numbers.

The protocol that makes seamless, secure payments possible

Verifiable Credential technology is the perfect way to implement seamless in-app payment facilitated by chat. It provides a way to:

- Authenticate the passenger through a government-grade digital identity.
- Enable the passenger to authenticate that their airline is their airline and not a phishing website.
- Incorporate a liveness check and verify it against an authenticated biometric for added identity proofing if required.
- Conduct the transaction directly over a secure channel.
- Conduct the transaction without having to store either the passenger's personal or account information, or only store what is necessary for the duration of regulations.
- Populate form details automatically and provide invoice and receipt credentials for proof of purchase.
- Integrate seamless workflows with Apple/Google payments, tokens, and crypto.
- Integrate the transaction into loyalty program benefits.

For airline credit cards, virtual credit card numbers could be issued to customers as credentials further simplifying transactions.

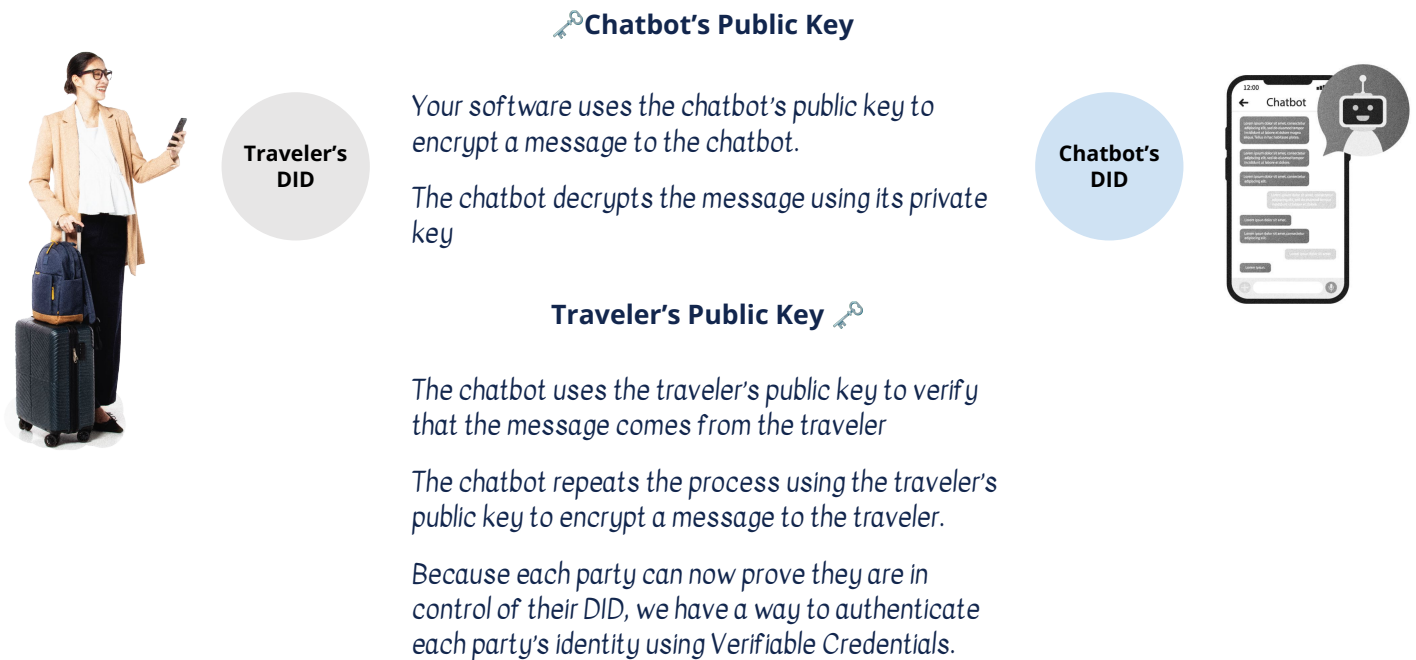
This is all made simple and secure by a protocol called DIDComm, which refers to "Decentralized Identifier Communication." To accept and hold a Verifiable Credential, the software in a person's digital wallet app creates a piece of code called a Decentralized Identifier or DID. It's like an address but it allows you to use a communications protocol to connect with other DIDs (hence "DIDComm").

The DID owner's app also creates public cryptographic key pairs, where a private key is paired with a public key for encrypting and decrypting information.

This is really powerful as it enables people and organizations and chatbots to know who they are interacting with before sharing data — and to do so instantly.

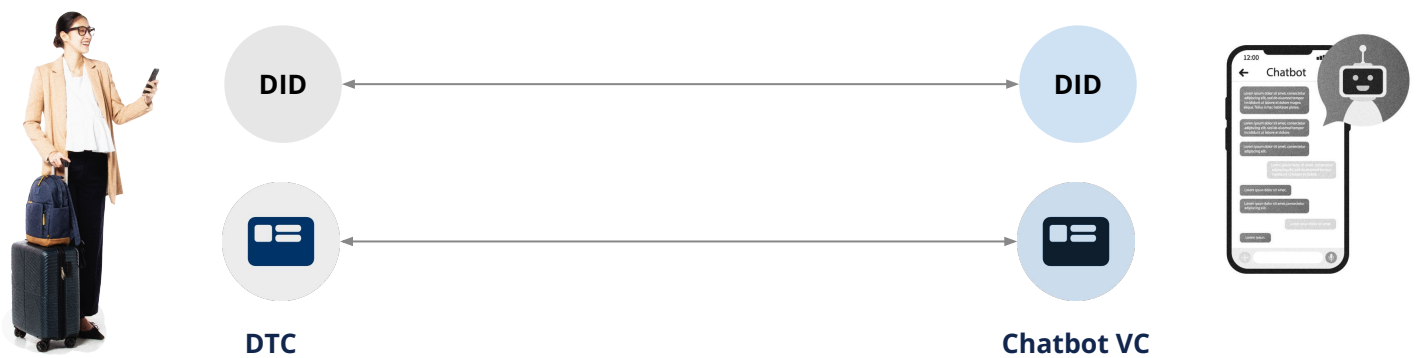
Technical note: DIDComm is able to work with OpenID for VC. See [here](#) and [here](#), which means this protocol works with European Union digital identity standards.

DIDComm enables direct, secure communication between credential holders



This end of the communication channel is controlled by a verifiable identity

This end of the communication channel is controlled by a verifiable identity



The Verifiable Credential (DTC) provides information about who or what controls their DID.

The Verifiable Credential (Chatbot VC) provides information about who or what controls their DID.

The source of the credential can be proven (by cryptography), and the contents of the credential are digitally signed so they cannot be tampered with without breaking the credential

The source of the credential can be proven (by cryptography), and the contents of the credential are digitally signed so they cannot be tampered with without breaking the credential

Freedom from intermediaries...

If someone is going to allow an AI chatbot access to their data, their account details, and facilitate payments, **they must be absolutely confident of its identity**. Similarly, the chatbot — or rather, the organization behind it — wants to be absolutely confident in the identity they're interacting with, too.

The magic of a frictionless, joined-up travel and tourism ecosystem is not going to happen unless every party in the ecosystem can be identified and can communicate in this secure, bidirectional way. Getting this right from the start is the key to rapid scalability.

DIDComm is a very powerful communications protocol. It effectively allows a mobile device to leverage the capacities of an API but in a highly secure and mobile way. It removes the need for a client (in this case, your phone) to be highly available to a server for interaction; it removes the need for firewalls; and it encrypts the data shared.

You can develop protocols on DIDComm and other newer technologies like Object Capabilities to enable permission for complex information flows between airlines, airline partners, banks, and credit card providers. Each message doesn't have to be verified or require an API call because each message has effectively been pre-verified by the architecture and is only accessible to its intended recipient. Information flows can be monitored securely, and permission revoked easily.

AI agents can be trained on the specifics of travel — booking flights, cars, hotels — and the entire data held by tourist boards, accreditation agencies, and information sites. With AI performing better at search than traditional search, all of this can be seamlessly networked and accessible within a tourist app.

This combination of AI and Verifiable Credentials connected by DIDComm is able to remove a significant market blocker for e-commerce and meets consumer expectations for seamless digital experiences. It also enables permissioned data access for customer personalization without the headaches of data privacy compliance. **But possibly most significant of all, it removes the need for intermediaries from the booking process.**

Airlines, hotels, hospitality, restaurants, and tourism operators of every kind dependent on booking no longer need to be dependent on web search and third-parties, all of whom extract a high cost relative to low margin businesses.

For tourism-dependent countries, this technology provides the path to an economic windfall: a simple, low cost technology that can drive down booking fees.

This is the technology we're building and deploying — now. If you want to change your world, [contact us here](#).

“The magic of a frictionless, joined-up travel and tourism ecosystem is not going to happen unless every party in the ecosystem can be identified... Getting this right from the start is the key to rapid scalability.”

”