Jumpstart the Global Travel Industry Using Self-Sovereign Identity for COVID-19 Immunity Credentials

by Subhajit Das,
Head, Productized Services, Blockchain Services, TCS

and

Justin Kersey,
Product Owner/Business Analyst, Blockchain Services, TCS

Key insights

Reviving trust in safe travel is possible using digital identity and immunity credentials.

- Travel bans, quarantines and lockdowns have negatively impacted the travel industry
- Restoring trust and safety is paramount for travel, tourism and hospitality industries to recover
- Self-sovereign identity (SSI) built on distributed ledger technology (like blockchain) and cryptography could be used to reinvigorate travel by allowing individuals to easily and securely demonstrate their immunity status

The health and safety precautions taken in response to managing the spread of COVID-19, including travel bans into many countries, has brought the travel industry to almost a complete standstill since February of 2020. Although signs show it is picking up slightly, multiple sources, including airlines and the Transportation Security Administration (TSA), state that passenger flight volumes are down 90%\(^1\) globally, and other forms of transport remain suspended. The International Air Transport Association (IATA) forecasts

---


that air traffic volume will not return to pre-pandemic levels until 2023\(^3\). At present, large amounts of data about COVID-19 transmission and mortality rates are helping health and government authorities decide how to best protect vulnerable populations and slow the spread of infection. In the near future, restoring social trust and enabling safe travel will become a priority as government lockdowns are lifted and people and businesses attempt to return to normality.

One approach to help restore trust and reinvigorate the travel industry is by using a combination of digital identity and immunity credentials that safeguards personal data. This approach offers many advantages, but the following requirements should first be considered.

### A coordinated government and industry response

Parallels can be drawn between the effect of the COVID-19 pandemic on the travel industry and the September 11 attacks, both of which generated a strong response of fear and loss of trust in aviation security. In the aftermath of 9/11, authorities and companies came together to implement processes and controls that restored traveler confidence and established a “new normal” by the creation of travel security agencies (such as the TSA in the US) and global mandates for tighter travel screening procedures. Although the circumstances and threats posed by COVID-19 are different from the 9/11 attacks, government and industry will inevitably follow a similar path of collaboration to combine policies, processes, and technology into a solution that reestablishes social trust and safety.

The International Civil Aviation Organization (ICAO), World Health Organization (WHO), and other multilateral groups are working with industry partners to develop technology-driven solutions to blunt the perceived risk of travel caused by the pandemic. Players in the travel industry ecosystem should be looking at how distributed ledger technology (DLT) (like blockchain) could be used to reinvigorate travel by allowing individuals to easily demonstrate their COVID-19 immunity status to airport authorities, airlines, immigration offices and other

---

\(^3\) [https://www.forbes.com/sites/suzannerowankelleher/2020/05/14/at-least-3-years-for-air-travel-to-recover-iata-chief-shares-boeing-ceos-pessimism/#769741c45714](https://www.forbes.com/sites/suzannerowankelleher/2020/05/14/at-least-3-years-for-air-travel-to-recover-iata-chief-shares-boeing-ceos-pessimism/#769741c45714)
relevant entities. At the heart of this technology-based approach is the role of self-sovereign identity and verifiable credentials. This combination would allow hospitals and testing facilities to issue digital COVID-19 immunity credentials to patients that could then be shared with and verified by the appropriate authorities.

**Self-sovereign identity explained**

Self-sovereign identity (SSI) blends principles regarding identity data ownership and management with technologies that implement those principles. Technological advancements include ways to store, share, and authenticate identity data and third-party credentials in a secure and privacy-preserving manner. SSI entrusts an individual with ownership and complete control of their identity without interventions by administrative authorities or centralized- or federated-identity providers (IDPs).

Verifiable credentials are the digital equivalent of the credentials an individual carries in their wallet or purse, such as driver’s license, work badge or passport. These digital credentials are stored in an identity wallet app on an edge device, like a smartphone, and can be shared with any other identity wallet that implements compatible standards and protocols.

**Exploring the user journey**

Let’s look at how this might work in our current and future post-pandemic scenario.

- Susan is a corporate executive who lives in London and frequently flies to New York for work. She has a US Global Entry credential that she uses to pass through US Customs and Border Protection (CBP).

- Susan recently booked a trip to New York and was advised that she would be required to present proof of having received a COVID-19 immunity test from an approved medical facility in order to gain entry to the United States.

- Susan books an appointment to receive the test from an approved medical facility.

- Prior to her appointment, Susan downloads a compatible self-sovereign identity wallet app on her smartphone and generates a decentralized identifier (DID) to serve as her identity shell.

- Susan arrives at her appointment and fills out the required patient in-take forms via an application running on a Wi-Fi connected tablet.
Susan is required to share her DID with the application. This triggers an authentication process, allowing the medical facility to reliably link Susan with the DID.

- The medical facility administers the COVID-19 immunity test to Susan.
- Next, the medical facility accesses their enterprise identity wallet app, selects a COVID-19 credential template, and fills it out with the relevant information about Susan and her test results.
- The medical facility then issues the COVID-19 immunity credential to Susan that shows she is asymptomatic and has antibodies.
- Susan receives the credential in her identity wallet. She reviews the credential’s contents and taps Accept, which adds it to her smartphone’s local storage.
- Susan can now share her COVID-19 immunity credential, along with her US Global Entry credential, at US CBP in New York.
- The US CBP verifies the authenticity of Susan’s COVID-19 immunity credential through a cryptographic process. Susan is now cleared to enter the United States.
- Susan can share her COVID-19 immunity credential with other countries’ immigration authorities as long as they operate identity wallets that implement compatible standards and protocols.

This image shows the user’s digital journey for immunity credentials.
Why self-sovereign identity makes sense for the travel industry

Privacy and security

Strong data privacy and security characteristics are embedded into self-sovereign identity implementations at the distributed ledger layer, which stores decentralized identity (DID) information and the communication layer where identity wallets and cryptographic messaging reside. These characteristics facilitate compliance with some of the most stringent data protection laws like the European Union’s General Data Protection Regulation (GDPR) and California’s Consumer Privacy Act (CCPA).

The decentralized nature of SSI prevents user account data from accumulating in honeypot environments. As such, only individual accounts are at risk of hacking attacks rather than hundreds of thousands or millions of accounts, as might occur with centralized- and federated-identity systems.

The travel industry is global in nature, with tens of millions of people accessing airports and other transport hubs on a daily basis. It could greatly benefit from an identity management solution that aligns with the strictest privacy controls and minimizes any threat of attack to individual identities only, not large groups.

Globally scalable

Self-sovereign identity implementations adhere to open source standards and protocols, so any organization can develop SSI solutions and tools running on top of these standards and protocols, enabling global portability and interoperability of identity. The benefit to an open source approach is that it allows self-sovereign identity to organically scale across countries and regions without the need to create a patchwork of systems connected to one another through APIs.

Cryptography, credential proofs, and an immutable registry of decentralized identifiers (DID) stored in blockchain or other DLTs facilitate a “trust-triangle pattern” that gives authorities the ability to verify an individual’s credentials without having to electronically communicate with the issuers of those credentials, as shown in the following image.

5. https://www.eff.org/deeplinks/2020/05/no-california-bill-verified-credentials-covid-19-test-results
A trust-triangle pattern enables the ability to verify an immunity credential without having to access an API to view the data from the medical facility.

Conceptually, this means that an immigration official in New York could verify a foreign traveler’s COVID-19 immunity credential without having to call an API to access data from the medical facility that issued the credential.

SSI adoption: advantages and challenges

Self-sovereign identity is one of many technologies that could potentially help restart the global travel industry. Although SSI offers many self-evident benefits, successful adoption requires an understanding of the following technical and non-technical challenges:

Technical

- Key management (which is conceptually similar to password management) and identity recovery are difficult to implement. The user experience is complex and may ultimately require individuals to rely on a centralized service provider.

- SSI standards and protocols are nascent. There will be limited uptake of self-sovereign identity systems until the required standards and protocols are thoroughly validated. This process may extend beyond the timeframe required by the travel industry.

Non-technical

- At present, verifiable credentials are best suited for fixed data such as date of birth, name, and academic and professional achievements. Currently, there is no evidence showing that individuals with COVID-19 antibodies will not become symptomatic at a future date. Thus, any credential issued for antibodies or vaccinations, when they come to market, does not guarantee that an individual will not become sick or transmit the virus to others.
A significant percentage of the global population will reject COVID-19 immunity tests and vaccinations. Many will seek exemptions or simply evade compliance. The adage, “code is easy, humans are hard” clearly applies to this use case.

**Getting ahead of the travel curve**

Government and industry participants are already collaborating to develop policies, processes, and solutions to help restart the travel industry. Self-sovereign identity (including verifiable credentials) could provide a secure, privacy preserving, highly scalable identity system; however, its readiness in the near term as a solution for the travel industry to the challenges presented by COVID-19 is unclear. SSI still requires market validation, and support for its implementation is currently limited to a relatively small group of technologists and enthusiasts. However, the implementation of SSI in the travel industry at a future point in time, especially once the standards and protocols are production ready and existing user experience challenges have been resolved, is something that all travel industry stakeholders should be watching, waiting and ready for.
About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com