UNWTO World Tourism Organization

SUSTAINABLE DEVELOPMENT GOALS

COVID-19 RESPONSE

DIGITAL HEALTH PASSES COMPENDIUM

Digital Identity Initiatives emerged as a result of the digital transformation of the global economy. While naturally associated with international mobility, a wide array of solutions produced by corporations, entrepreneurs and public-private collaborations have been created over the past years to enable smoother identity verification and ensure the authenticity of information in health, finance, travel, and administrative procedures.

The implementation of such solutions has accelerated over recent months. This can help achieve two key goals: restoring confidence both among tourists and local communities, and facilitating seamless travel and tourism operations.

To this end, so-called **Digital Health Passes** are backed by innovative technologies including biometric matching, big data and machine learning. In most instances, they make use of blockchain technology - "a shared, immutable ledger that facilitates the process of recording transactions and tracking tangible and intangible assets in a network" (IBM, s.f.). This allows for the decentralized management of data for security purposes.

While the existing technology is already strong, there remains a need for stronger agreements on common principles such as **interoperability.** This will ensure different solutions are acceptable worldwide, "both with one another and across institutional and geographic borders (Good Health Pass Collaborative, 2021, p. 3), allowing travellers to integrate all their documents in just one application and avoiding repetitive processes for the sake of effectiveness and comfortability.

Likewise, the World Health Organization (WHO) Smart Vaccination Certificate Working Group, the International Civil Aviation Organization's Council Aviation Recovery Task Force (ICAO CART), the Digital Identity Alliance (ID 2020), the Covid-19 Credentials Initiative (CCI), the Vaccination Credential Initiative (VCI) and Good Health Pass Collaborative have highlighted the essential principles that a successful Digital Health Passes should take into account, namely:

• Privacy and data security
• User control over data
• Inclusivity and equity
• Open standards
• Interoperability
• Scalability
• Portability
• Sustainability

By complying with these principles, Digital Health Passes could help restore traveller confidence while at the same time increasing protection of both travellers and employees. Digitalized credentials open up a promising path towards reopening borders, above all if they can be used across different levels of government and the private sector.

With the objective of providing guidance to stakeholders all over the world, UNWTO offers a compendium of 16 solutions from Australia, Canada, Germany, Singapore, Spain, Switzerland, the United Kingdom, and the United States of America. UNWTO has collected information mostly from primary sources, for which most of the texts are direct quotes from the solutions' founding organizations or their official websites. Secondary sources were used to complement information only for examples of implementation cases. Hereunder, there is a detailed explanation of each solution, with a deeper description for those that were able to fill the UNWTO Digital Health Passes Collection Form (*).

1. Airside Mobile ID + Health Passport*
2. CommonPass*
3. CoronaPass
4. hi + Card*
5. IATA Travel Pass*
6. IBM Digital Health Pass
7. ICC AOKpass*
8. ilife*
9. IMMUVID*
10. myHealth Pass
11. ShareRing ID
12. Sherpa*
13. SimplyGo
14. VeriFLY
15. V-Health Passport*
16. Yoti Digital Identity*

Airside 🇺🇸

Name: Airside Mobile ID + Health Passport
Solution founded in: 2009
Founder(s): Airside Mobile
Country: United States of America
Website: airsidemobile.com
Contact: Amena Ali, CEO, amena.ali@airsidemobile.com

When it comes to identity information, individuals want convenience and privacy while organizations want access and ease. At Airside, we believe both are possible. Our Digital Identity Network empowers people with consent and control of their identity info while enabling organizations to verify identities in a cost-effective, compliant and secure way, and without ever holding sensitive information, such as biometric data, on their backend.

Added value: Airside, best known for the Mobile Passport App, recently launched the Airside Digital Identity Network to help people verify, share and manage personal information on a time-bound, consent basis while keeping individuals in control of their personal information. This includes collaboration with diagnostic labs to let individuals demonstrate their COVID status while protecting their data privacy. Airside offers a trusted, standards-based application of a digital Health Passport, linking biometric-based, source-verified mobile IDs to lab credentials, and enabling the sharing of these credentials with trusted organizations.

Main technology used: ID source-verification, biometric matching, diagnostic matching

Support secured: Authorized by the U.S. Department of Homeland Security and U.S. Customs and Border Protection. Endorsed by the Airports Council International - North America (ACI-NA), Airlines for America, and Kantara Initiative.

Implementation cases: Airside is currently piloting a biometric bag drop solution with a major airline at two domestic airports in the U.S., and we are putting the final touches on our Mobile ID + Health Passport app for various use cases in travel and beyond.

Compliance of WHO Recommendations: Yes. During the COVID-19 pandemic, Airside is gearing our Mobile ID + Health Passport solution for the immediate, high-need travel population (i.e. emergency and and humanitarian actions), knowing that as countries gradually resume international travel, the imperative must be on the introduction of risk mitigation measures aiming to reduce transmission of the virus while enabling safe travel and the reopening of borders and economies.

Compliance of ICAO CART requirements: Yes. Our solution is focused on safety, security, and efficiency to promote public health and confidence among travelers and the workforce. Our mission is to harness the power of private digital identity management to help organizations and society recover and advance with integrity. We believe our privacy-first approach to digital identity has never been more needed to help reopen borders, economies, and opportunities for humanity.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**Depends**
COMPLIANCE EXPLANATION	Airside has always believed that data privacy is a human right and over the past few years we have affirmed our conviction that no one should have to choose between convenience and privacy in the digital exchange of their personal information. We build technology that protects personal information and meets privacy regulations around the world while bringing value to businesses and consumers.	Taking the perspective of the individual (not Big Tech or Big Brother), our privacy-based business model is the key to our innovative solution. We have shown that it is possible to store, protect and share sensitive data with a self-sovereign and decentralized architecture that is both consumer-centric and scalable. That is a win-win-win for people, organizations and society.	Our services are available globally for immediate application across a variety of sectors, such as travel, tourism, health, finance and more. They are also designed to be open and interoperable across existing providers and locations.	We acknowledge the still evolving development and adoption of standards and the limited opportunity, mobility, and interoperability of digital technology, making individuals, businesses, and governments more vulnerable to identity theft, data breaches, and cybersecurity scams and fraud. That said, depending on what components of the API governments need and how their existing infrastructure is set up, we can provide technical resources to help customize the technology for their implementation. Overall, it's a fast process and we're eager to help with a fast conversion.

CommonPass

Name: CommonPass*
Solution founded in: 2020
Founder(s): The Commons Project Foundation
Country: Switzerland
Website: commonpass.org
Contact: Khadija Rejto, Managing Director, International Policy and Government Affairs, khadija@thecommonsproject.org

At the core of the CommonPass platform is the recognition that the COVID-19 crisis is fundamentally a health crisis that impacts travel as well as many other sectors - entertainment, employment, education.

In order for any and all of these sectors to reopen, a common protocol is necessary- the operators of entities in these sections need to have a way to ensure that the health status of people visiting their facilities and utilizing their services in person are compliant with their health requirements and have therefore been recognized as sufficiently safe from a public health perspective as befits the operating context of the entity and commensurate to the risks it faces.

As important to those protections for operators are the protections for people- people need to have confidence that their demonstration of this compliance occurs with their privacy foremost in mind, so that the sharing of their compliance does not require sharing of their health records.

CommonPass has designed this common protocol, leveraging both existing and also emerging technical and health standards to:

1) Articulate in computer-readable form the health entry and participation policies of operators/commercial entities/jurisdictions

2) Provide for standards- and privacy-based integration with the health and lab systems that people trust and are directly engaging with

3) Determine for the individual person whether their health records comply with the health entry requirements

4) If they do comply, allow that compliance to be shared with the operator without any additional conveyance of private health or other personal information

Added value: CommonPass is first and foremost designed to empower individuals with access to their personal health data so that they can get back to work, school and life. By connecting directly into trusted data sources of test results and vaccination records using existing health data interoperability standards, the source of the health information is verifiable. Facilitating international air travel is a prime example of one user case in which an individual can leverage their health data to improve their lives, but everyone will be best served by an interoperable solution focused on the person and not on a specific airline use case. Direct API integrations into third party apps and services allows for a seamless experience for people and organizations.

Main technology used: Direct connections with labs and other health data sources via HL7 FHIR.

Support secured: Support from 47 governments and international organizations on every continent.

The Commons Project is working with national, regional and global organizations implementing their own health passes and safe travel standards as part of our Common Trust Network initiative built in collaboration with the World Economic Forum.

Implementation cases: CommonPass is in full production between Germany and the US with Lufthansa[1] and between the US and Aruba[2] with JetBlue. By the end of March 2021, routes to and from Singapore, Hong Kong, London, New York, Frankfurt, Tokyo, Darwin and Los Angeles will have also been completed with Cathay Pacific, United Airlines, ANA, JAL and Qantas.

---

1. Lufthansa. (s.f.). Check in faster: The CommonPass app. Retrieved from https://www.lufthansa.com/xx/en/common-pass

2. CommonPass. (s.f.). JetBlue invites you to travel safely to Aruba with CommonPass. Retrieved from https://commonpass.org/aruba

Compliance of WHO Recommendations: CommonPass complies with all WHO international health regulation standards and guidelines.

Compliance of ICAO CART requirements: Implemented in a multi-layer approach commensurate to the risk level and shall not compromise aviation safety and security;

-CommonPass is a highly targeted tool that addresses the new, very specific operational pain-point the COVID crisis created- the need for the aviation or travel partner to verify the health status of their customers and travelers, to answer the question is this traveler safe to travel? CommonPass supports a variety of configuration, integration and verification methods to support the specific operational workflows of the travel and aviation partner, so the points where that question has to be answered, it can be.

Able to capitalize on the sector's longstanding experience and apply the same principles used for safety and security risk management. This includes monitoring compliance, reviewing the effectiveness of measures at regular intervals, and adapting measures to changing needs as well as improved methods and technologies;

-CommonPass is a targeted tool that can be deployed by aviation partners as part of their own safety and security protocols. Use and acceptance of CommonPass does not create a new security risk surface for airline partners, and in fact shields partners from exposure to and management of highly sensitive personal health records. Analytics available from use of the CommonPass platform can facilitate monitoring compliance and effectiveness of evolving health safety measures, while preserving individual traveler privacy.

Able to minimize negative operational and efficiency impacts while strengthening and promoting public confidence and aviation public health;

-CommonPass is specifically designed to positively impact aviation partners' operational efficiency with regard to COVID-19 related health screening. At present many new manual procedures have had to be introduced. CommonPass is intended to facilitate a return to largely automated processing for routine cases.

Consistent and harmonized to the greatest extent appropriate, yet flexible enough to respond to regional or situational risk-assessment and risk-tolerance. The acceptance of equivalent measures based on shared principles and internationally recognized criteria will be a fundamental enabler to restore air services on a global level; Supported by medical evidence and consistent with health best practices;

-CommonPass is working actively with commercial and health partners to arrive at consistent and harmonized standards for health status attestation- there should be a relatively universal standard for what it means to "be vaccinated"- while recognizing that in individual contexts, jurisdictions / venues / events may have very specific and custom requirements and guidelines.

Non-discriminatory, evidence-based, and transparent;

-Our mission is to unlock the full potential of technology and data to improve people's lives. We have architected our product to ensure that it will be accessible to all with transparency and openness.

Cost effective, proportionate and not undermining to the equal opportunity to compete;

-CommonPass is intended to be free for people to use. Commercial participants who verify the health status of their visitors/travelers/clients/customers pay a small fee for that verification, a fee that drops at larger scale.

Highly visible, and communicated effectively and clearly to the aviation community as well as the general public;

-CommonPass is intended to be a universally recognized international consumer brand facilitating back-to-X use cases not only in aviation but across diverse other sectors as well.

Consistent with international requirements, standards, and recommended practices applicable to aviation and public health.

-CommonPass is working closely with all major international organizations to encourage standards-setting, interoperability and to ensure compliance with international regulations.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**No**
COMPLIANCE EXPLANATION	The core of the CommonPass platform is preserving privacy and security. All personal health data is stored only on the person's phone or at the original source and is not captured in the cloud or in any centralized server.	The user is the only one in control of their own health data in the CommonPass platform.	The Commons Project is building CommonPass to ensure that it is available in an offline mode, both in case of a power or connection failure on a mobile device and for those individuals without a smartphone. In later releases in 2021 of CommonPass, individuals will be able to print out a CommonPass health pass with a QR code that can be read by airline or border control staff to verify compliance with entry rules.	There is no fee charged to governments for using CommonPass.

![CoronaPass Powered by Bizagi]

Name: CoronaPass
Solution founded in: 2020
Founder(s): Bizagi
Country: United Kingdom
Website: coronapass.org/home
Contact: bizagipr@walkersands.com

CoronaPass™ is an app to support COVID-19 policy implementation and risk management.

With this powerful solution, organizations can quickly create different pass types, such as a Vaccine Passport. Through this, businesses, employees and citizens will be able return to normal activity more quickly, with the lowest possible levels of risk.

Added value: Protect the Front-line: Health professionals' CoronaPass applications are prioritized to get them back to work safely to help those in need.

Global Solution: The solution offers the technology to validate the CoronaPass on a global basis and can be configured in multiple languages. Data centers are in the jurisdiction of each country thus ensuring compliance.

Comprehensive: CoronaPass manages the complete lifecycle from applying for different types of passes, based on vaccination or other criteria, to creating and validating the CoronaPass.

Main technology used: N/A

Support secured: N/A

Implementation cases: N/A

hi +
card
Health Identification Card

Name: hi + Card*
Solution founded in: 2020
Founder(s): Health Identification Card SL
Country: Spain
Website: hicard.travel
Contact: Antonio López de Avila, CEO, antonio.lopezdeavila@hicard.travel

App works as International Health Identification Card. Users will travel with more security as they will have all their medical information at hand in case of emergency (in several languages).

As well, any medical certificate or document - emitted by an Authorized Health Entity- can be uploaded to the system and be shared when necessary.

European-based Blockchain technology, high level encryption codes and double authorization to assure Data User Protection.

Added value: hiCard can be used as a Health Digital Passport, since it can store vaccine or PCR certifications in a very secure way. Blockchain avoids fake certificates and users are the only owners of their data (safe and in privacy).

Main technology used: Blockchain/encryption codes/doble authorization process

Support secured: Canarian Regional Government (Spain), beta test of the technology in July 2020; Cabo Verde, letter of interest; Uruguay, letter of interest; Chile, letter of interest; Consell de Ibiza (Spain), expression of interest; Madeira (Portugal), expression of interest; Qatar, expression of interest.

Implementation cases: The app will be ready in April 2021. The pilot project took place last July 2020 with the support of the Canarian Government (Spain) and the UNWTO, tracking 100 international journalists in a fam trip to the Canary Islands within the "Safe Destination" project.

Compliance of WHO Recommendations: Yes. The solution has been developed taking WHO recommendations in mind, since back in April 2020 we set up a working group consisting of public and private health entities, labs and private health groups. Blockchain technology avoid fake profiles and certifications, so hi+Card guarantees safer travels.

Compliance of ICAO CART requirements: Yes. The solution has been developed taking the ICAO´s requirements in mind, since back in April 2020 we set up a working group consisting of airlines, IATA, AENA and others and from then the Aviation sector has been always in the center of our work.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**No**
COMPLIANCE EXPLANATION	The combination of: *Blockchain platform *High-level encryption codes and a *Dual authorisation system enables the operation and ensure full protection of user data in accordance with the EU (GDPR). The system creates profiles by patient that include all their medical info referenced by all the centres they have been through and are in the network. Only those within the network will be able to upload new information to the patient's medical record and only with his or her previous authorization.	The App is built on a blockchain platform, high-level encryption and a dual authorisation system, so that the patient controls his or her information at all times, following EU guidelines on health data.	Yes. The user can publish his or her medical info in the phone´s wallet and show it whenever and wherever they want.	No, since the user is the one who pays to download the app. But, we have found a deep interest in some Governments to implement hi+Card at a national level. Both, to digitize the medical records of their citizens and give them the opportunity of having their medical information when traveling around the world.

Name: IATA Travel Pass*
Solution founded in: 2020
Founder(s): International Air Transport Association
Country: Switzerland
Website: iata.org
Contact: Alan Murray Hayden, Head Airline, Airport and Security - Compliance and Operational Solutions, murrayhaya@iata.org

The IATA Travel Pass solution is an end-to-end decentralized solution enabling passengers to:

1. Create a digital identity
2. Inform passengers of regulations for their upcoming flight
3. Receive test/vaccine results from laboratories enrolled in the IATA Ecosystem, as a verifiable credential. Link the results to their identity ensuring everyone can have faith in the data.
4. Verify the test meets the COVID regulations for their itinerary.
5. Share their Ok to Travel status with airlines enabling processing off airport avoiding the need to queue at the airport to prove their identity, and that they meet COVID regulations.

Added value: The IATA Travel Pass solution is uniquely positioned to help restart aviation as:

1. Identity Management – The solution is based on the creation of passenger's identity using the ICAO DTC. This ensures that everybody can have confidence in the identity of the passengers and that the test results belong to that passenger. This is central to governments having the confidence to open up their borders. Secondly the passengers will be given the option to share their passport and biometric photo with the airlines in advance of travel so that they can take advantage of contactless travel – their face becomes their passport and boarding pass.

2. Timatic COVID Rules database and engine is the most comprehensive database of immigration regulations. The sourcing network has over 1500 sources with over 200 regulation updates per day. In 2019 Timatic AutoCheck was used to process over 800m international passengers.

3. Decentralized identity management – The IATA Travel Pass puts passengers in control of their own data using decentralized identity management technologies and principles. All of the passengers' data remains on their phone and is not stored in any central IATA database. The passengers are prompted to share their data with airlines and can choose to do so or not. There is an overwhelming desire by airlines around the world to adopt such principles for all data interactions with passengers which is reflected in various industry resolutions.

4. Based on open standards and networks – The IATA Travel Pass solution is based on the W3C standards and works on the publicly permissioned Sovrin network. This ensures interoperability and means that no one party controls the passenger's identity, the network or standards.

5. Designed by airlines with the needs of airlines and passengers by utilizing existing airline systems and processes ensuring the solution will be the most effective at restarting the industry.

6. Cost Effective Industry Solution which is critical to for airlines who are struggling to survive financially.

Main technology used: There are 4 modules within the IATA Travel Pass Ecosystem:

1. IATA Travel Pass Application – Developed using the Soverin network based on W3C standards, and decentralized identity principles. Identity creation based on ICAO Digital Travel Credential standard.

2. IATA Lab App – Interacts with IATA Travel Pass App to exchange and verify passenger's identity and issue their test results as a verifiable credentials using the Soverin network.

3. IATA Lab Registry – Lists labs who are accredited to provide testing services accepted by airlines.

4. Timatic COVID – Existing industry solution

Support secured: Several international and regional bodies do support the IATA Travel Pass concept. At national level, strong support from several Government agencies such as Transport, Health, Home Affairs, Tourism and External Affairs mainly.

Implementation cases: A limited trial of the solution is underway with Singapore Airlines since December. A full pilot of the solution was launched in March[3,4]. Furthermore, we have trial projects launched with 25 airlines, with others lined up to join the ecosystem.

Compliance of WHO Recommendations: IATA Travel Pass will accommodate to the standard digital vaccination certificates specifications to be issued by WHO.

IATA is actively engaged and sits on the relevant WHO standard setting bodies.

Compliance of ICAO CART requirements: Yes. The digital identity element is adhering to the principles of ICAO Digital Travel Credentials.

IATA Travel Pass accommodates the standard content for test certificates, issued by ICAO.

IATA Travel Pass also paves the way for contactless travel processes, a key ICAO CART biosafety recommendation to reduce the risk of virus transmission when documents need to be exchanged in the travel process.

---

3. Singapore Airlines. (8 March 2021). Singapore Airlines First In World To Pilot IATA's Travel Pass App. Retrieved from: https://www.singaporeair.com/es_ES/es/media-centre/press-release/article/?q=en_UK/2021/January-March/ne0921-210308 and IATA. (17 March 2021).

4. IATA. (17 March 2021). IATA Travel Pass Successfully Trialed on First International Flight. Retrieved from: https://www.iata.org/en/pressroom/pr/2021-03-17-04/

KEY FACTS

|	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**Depends**
COMPLIANCE EXPLANATION	IATA Travel Pass is based on decentralized identity principles and complies with the highest data privacy standards and regulations. The IATA Travel Pass does not store any data centrally. It manages and facilitates the passenger to share their data with the entities that need verification (airlines and governments) with test or vaccination data when travelers permit.	Travelers always remain in complete control of their data with their privacy protected and upon consent, decide with whom they are sharing the data and what data they are sharing. Sovereign identity is governing IATA Travel Pass. The passenger can access the share data logs on application.	The solution is designed so that passengers can share their data with airlines ad governments before the arrive at the airport. As such it does not matter of the passenger arrives at the airport and does not have internet access as all the work has been done already.	Authorities can link their systems to IATA Travel Pass for which IATA will provide a Software Development Kit to authorities. As such the only costs for the government is the cost of implementation.

IBM
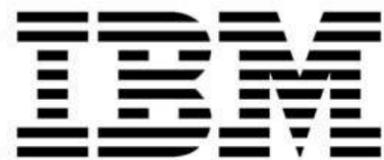
Name: IBM Digital Health Pass
Solution founded in: N/A
Founder(s): IBM Watson Health
Country: N/A
Website: ibm.com/products/digital-health-pass
Contact: N/A

Digital Health Pass, part of IBM Watson Works, is designed to provide organizations with a smart way to bring people back to a physical location, such as a workplace, school, stadium or airline flight.

Built on IBM Blockchain technology, the solution is designed to enable organizations to verify health credentials for employees, customers and visitors entering their site based on criteria specified by the organization.

Privacy is central to the solution, and the digital wallet can allow individuals to maintain control of their personal health information and share it in a way that is secured, verifiable, and trusted. Individuals can share their health pass to return to the activities and things they love, without requiring exposure of the underlying personal data used to generate the credential.

Added value: Trust and transparency: individuals can manage their information through an encrypted digital wallet on their smartphone, so they control what they share, with whom and for what purpose.

Data-driven: organizations design the rules for configuring a health status that fit a fluid situation based on any number of data sources.

Flexible and agile: the versatile platform is designed to help address multiple use cases and can be incorporated into existing ecosystems.

Main technology used: IBM Blockchain technology

Support secured: IBM Watson Health and Salesforce are partnering to help organizations as they strive to safely reopen physical locations. Integration of the IBM Digital Health Pass with the Salesforce Work.com Workplace Command Center is designed to give organizations a single hub to help make data-driven decisions as they look to minimize risk, take action where needed and communicate effectively. These decisions can help organizations bring employees back to offices, visitors back to hotels, concert goers back to music venues and sports fans back to stadiums[5].

Implementation cases: United Airlines, JetBlue and Lufthansa[6].

5. IBM. (18 December 2020). IBM and Salesforce join forces to help deliver verifiable vaccine and health passes. Retrieved from https://www.ibm.com/blogs/watson-health/partnership-with-salesforce-verifiable-health-pass/
6. The New York Times. (13 December 2020). Vaccinated? Show Us Your App. Retrieved from https://www.nytimes.com/2020/12/13/technology/coronavirus-vaccine-apps.html

AOKpass

Name: ICC AOKpass*
Solution founded in: 2020
Founder(s): AOKpass, International Chamber of Commerce & International SOS
Country: Singapore
Website: aokpass.com
Contact: Darren Toh, CEO, darren@aokpass.com

ICC AOKpass supports a safer and more efficient return to work, travel and play.

Our technology is built upon 3 core principles - privacy, security, and portability - to enable you to present your health status without ever losing control of your medical information. Built on the principle of privacy by design, AOKpass provides you with a digitally authenticated, secure and portable copy of your medical records. With this, you can prove compliance with health requirements without compromising your right to strict health data privacy.

AOKpass is decentralized, meaning your medical records are stored only on your device and will not be shared or stored elsewhere. You have exclusive control of when and where to share your information. Only you have access to your information and the ability to display your unique AOKpass QR code for verification.

ICC AOKpass is co-founded by AOKpass, the International Chamber of Commerce and International SOS.

Added value: ICC AOKpass has an unparalleled global network of partners, including access to nearly 90,000 accredited clinics, 45 million businesses and a growing alliance of airlines and airports, including: ADP Group, TAV, Rome Airport, San Francisco Airport, Air France, Alitalia, Etihad, Frenchbee, Air Caraibes and Corsair.

Main technology used: Blockchain hash technology and verification

Support secured: ICC AOKpass has directly partnered (or engaged via the ICC and partners) with international bodies including: the ACI, IATA, ICAO, ISO, G20/B20, OECD, WHO, WEF, WTTC & UNWTO. We also actively engaged with other regional multilaterals such as SICA, SIECA and UN ESCWA.

Implementation cases: ICC AOKpass is being actively implemented for pilots involving the following countries: Italy, France, Japan, Pakistan, Philippines, Singapore, Spain, Switzerland, Thailand, US and UAE.

Airport and airline partners include: ADP Group, TAV, Rome Airport, San Francisco Airport, Air France, Alitalia, Etihad, Frenchbee, Air Caraibes and Corsair.

Compliance of WHO Recommendations: ICC AOKpass has actively sought to ensure it incorporates the WHO recommendations as they have evolved from initial development to operational implementation. The dynamically adaptive certificate-based framework employed by ICC AOKpass ensures that it is able to comply with medical science, standards and regulations as they evolve.

Compliance of ICAO CART requirements: ICC AOKpass has actively sought to ensure it complies with ICAO requirements as they have evolved from initial development to operational implementation. The dynamically adaptive certificate-based framework employed by ICC AOKpass ensures that it is able to comply with any standard for authentication, verification or interoperability as they evolve.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**Depends**
COMPLIANCE EXPLANATION	ICC AOKpass does not handle, store or otherwise process any personal data of users. All such data is stored exclusively in the mobile device of users and under their control at all times. This is achieved through the use of blockchain technology and hashing systems to enable secure verification without compromising data privacy.	All personal data is stored exclusively in the mobile device of users and under their control at all times. Only they can choose when and where they want to share their data with third parties.	N/A	Not upfront establishment costs are imposed. However, a small per user fee based on a scaling tiered pricing structure, which decreases in cost with volume is required to ensure the app and system remain operational and sustainable.

Name: iLife*
Solution founded in: 2016
Founder(s): ConnectedLife
Country: Spain
Website: connectedlife.es
Contact: Ángeles Rodríguez Silván, CEO, angeles.rsilvan@connectedlife.es

International vaccination certificate with digital ID. Health data storage, emergency services. A 360-degree solution. Creation of digital care and security and protection against possible situations where life may be at risk.

Added value: Creation of verified and certified ID and health data and storage of health data available in emergency situations for the different professionals with the aim of improving the quality of the care provided. It is capable of working in offline mode by facial recognition.

Main technology used: Facial recognition.

Support secured: We are in negotiations with the Government of Spain and the Autonomous Communities. Emergency services support.

Implementation cases: Castilla y León Emergency Services, REALE, Axa, El Molar Municipality, Unidad Militar de Emergencias (Military Emergencies Unit, Spain).

Compliance of WHO Recommendations: N/A

Compliance of ICAO CART requirements: Not yet, but it is prepared for it.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**No**
COMPLIANCE EXPLANATION	Yes, with a Data Protection Delegate who is an expert in the oversight structure for compliance with the LOPD and RGPD regarding the data it stores.	Yes, they are the ones who decide what information they upload or is uploaded to the app itself.	Through face recognition and an app for professionals that is able to read offline even when the mobile has been lost or damaged or simply is out of battery.	No, the platform is divided into two apps, one for users and the other for professionals. ConnectedLife grants the use of the app (key) to governments to restart the economy, digitize citizens and protect them in situations of vital risk. And the user app is acquired through B2B2C or B2C.

IMMUVID

Name: IMMUVID*
Solution founded in: 2020
Founder(s): Nexplain Solutions SL
Country: Spain
Website: immuvid.com
Contact: Pieter Louw, Co-founder, pieter.louw@nexplain.es

ImmuvID is a solution that enables economic activity in a sustainable way DURING the pandemic. It is an ecosystem of technological products that promotes mobility and the control of people in COVID times with solutions for:

- Individuals (COVID testing/COVID vaccine, where to find laboratories, connected to shops - e.g. COVID Protect hotels).

- Industry (access control of employees, tourists, customers with guarantees of "green" COVID status to create protected COVID spaces).

- Governments:
    a) Integration of COVID controls in border control systems at airports, seaports, land borders with various mobile reading options to fixed facilities.
    b) COVID standards management/verification system.
    c) Health Passes test validation/verification system from around the world.

- Airlines:
    a) Integration of COVID control into an airline's usual boarding/control systems at an airport.
    b) COVID standards management/verification system.
    c) Health Passes test validation/verification system from around the world (in collaboration with major laboratories internationally).

Added value: We focus on ore areas that will be crucial to reactivating tourism:

1. Connecting the multitude of travel passes that will soon flood the market with testing labs, official vaccination results.
2. We are capable of issuing a Guarantee of test/vaccine results that cannot be forged (veracity by design).
3. Our solution starts before the journey begins, accompanies through border control and flights as well as in the destination: travellers receive the information they need and have access to the tests they need to keep travelling and get home safely.
4. Our technology is based on interoperability with any other system. There will be no reactivation of tourism if solutions operate in silos.
5. ImmuvID is not another travel pass: it is an ecosystem that consists of various products and services for all parts of the industry.

Main technology used: Mobile phone app.

Support secured: We have signed collaboration agreements with universities, testing laboratories (the largest private group assembled globally with coverage in more than 150 countries around the world), test manufacturing companies

Implementation cases: - Proof of Concept: employee COVID test and access control with the Spanish Healthcare Company Quirón Prevención.
- Tourism Innovation Summit: core technology used for all access control.

Compliance of WHO Recommendations: Yes - the entire platform is developed to allow a risk-based management of mobility.

Compliance of ICAO CART requirements: Yes:

1. We provide a platform and a service to integrate COVID-19 test controls into passport controls at border crossings.
2. We provide a platform to local government, connected to a vast network of testing laboratories that allows them to develop a safe corridor strategy.
3. We have developed a verification app that allows us to control access based on COVID status as reflected in government issued regulations in real time. This allows us to emit a guarantee that legislation is being adhered to at all times.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**Depends**
COMPLIANCE EXPLANATION	All of our processes are in strict adherence to the GDPR. Users keep all relevant data on their mobile devises, and we do not have any database of either identity or medical information.	Users have full control of their data, ImmuvID does not have access to their identity or health data. Users decide to share specific credentials with one time only identifiers	Yes, the Digital Health Certificate functions offline completely.	Yes, but the level of the cost depends on the part of the solutions chosen by the government to implement. These are the modules: -Health Status Control Integration for Border Agencies and Airlines -Digital Health Certificates with Guarantee of authenticity -Tests & Vaccine integration -Health Status Access Control to create Safe Spaces -Digital Platform for COVID Protected hotels, restaurants, museums, bars to showcase and connect -Travel app for tourists The business model is an annual, volume-based license.

Name: myHealth Pass
Solution founded in: N/A
Founder(s): SICPA
Country: Switzerland
Website: sicpa.com/MyHealthPass
Contact: N/A

Pitch: myHealth Pass is a tool enabling real-time health status management and safe mobility. It is specially designed to meet the highest levels of data security and personal privacy protection. It ensures secure and anonymous issuance, use and verification of certified data.
This flexible technology can support the return to social and economic activity in accordance with national and local policies and conditions.

Added value: Powered by the CERTUS™ technology, myHealth Pass is easy to set up and can be immediately operational. Full automation and integration with existing IT processes can be achieved thanks to the simple and REST API standards.

Looking beyond the immediate crisis, myHealth Pass can help countries and local authorities better prepare for future disease occurrence.
Other use cases include:

• vaccines,
• medical records,
• medical devices,
• kits.

Main technology used: CERTUS™ Digital Seal Technology sets a new standard in securing value documents, credentials and qualifications. It combines breakthrough digital seal technology, protected by the blockchain, with a secure QR-code applied to documents. The result is a QR code marking which is impossible to tamper with or forge and secures both paper-based and digital certificates. CERTUS™ enables independent and universal verification, safeguarding the value of holders' documents and the reputation of issuing authorities. Advantages of CERTUS™: it offers several distinct advantages over alternatives on the market:

• One-click universal and independent verification;
• Works for paper and digital certificates;
• Privacy-preserving, does not store sensitive data;
• Authenticates the issuer and the protected data;
• Lifelong validity of issued certificates;
• Immediate access to a simple and cost-effective online service for managing secure certificates, no infrastructure required;
• Enables offline verification;
• Versatile solution, protects any type of data structure.

Support secured / Implementation cases: SICPA's system has thus far been successfully piloted by groups including seafarers—a particularly hard-hit profession by the world's patchwork of testing and quarantine rules—and ice hockey players in the Kontinental Hockey League[7,8].

7. Ink World. (14 September 2020). SICPA Guarantees KHL COVID-19 Test Results with CERTUS myHealth Pass. Retrieved from https://www.inkworldmagazine.com/contents/view_breaking-news/2020-09-14/sicpa-guarantees-khl-covid-19-test-results-with-certus-myhealth-pass

8. European Scientist. (3 March 2021). Ready-made digital solutions offer the EU an olive branch on vaccine passports. Retrieved from https://www.europeanscientist.com/en/public-health/ready-made-digital-solutions-offer-the-eu-an-olive-branch-on-vaccine-passports/

ShareRing

Name: ShareRingID
Solution founded in: N/A
Founder(s): ShareRing
Country: Australia
Website: sharering.network
Contact: N/A

ShareRing has created the world's most secure and flexible digital identity solution.

Imagine a world where you are able to store all of your sensitive documents in one secure, encrypted lock-box, giving you the power to simplify everything from website registration, secure building/venue access, and booking international travel. No more worrying about where you have stored and saved all of your key documents, from passports, driving licenses, vaccination certificates through to educational certificates.

Added value: One login: One set of credentials for all your travel needs. There is no longer the need for multiple logins for multiple travel apps!

ShareRing ID: Your ID is yours to control. Choose where it goes and how it is stored. Your personal identification information is never stored in the ShareRing Ecosystem.

One app: All your travel needs in one place. ShareRing offers "the Amazon" of the travel marketplace; where you can book all your travel needs much quicker and more secure than ever before.
One payment: Payments are made in one step for all your travel needs. We take care of everything within the app. Without the need to submit your payment to many providers; security is greatly increased and the payment process is extremely quick.

Main technology used: ShareRing is built on distributed ledger technology, also known as a blockchain. This technology provides a system where transactions are super secure, fast and immutable. This is because data is managed by a network of publicly controlled "nodes" that confirm the data is true and correct. There is no central authority. This becomes 'decentralized' as opposed to traditional 'centralized' data access and storage.

Support secured: N/A

Implementation cases: N/A

sherpa°

Name: sherpa°*
Solution founded in: 2018
Founder(s): sherpa°
Country: Canada
Website: joinsherpa.com
Contact: Jake Kotzer, Director of Growth and Partnerships, jake@joinsherpa.com

We help travellers move freely around the world and shift the way the world's leading travel providers think about travel identification. sherpa° processes millions of data points to identify changes in travel rules and processes, and enables travel companies to build travel documentation into their digital products.

Added value: We make it easy for people to cross borders.

Main technology used: Big Data and Machine Learning.

Support secured: We work with OneWorld, Alliance, Star Alliance, American Airlines, Expedia Group, Amadeus, and True Ventures.

Implementation cases: Our most prominent integration is a co-branded page with American Airlines[9]. We also have integrations with 50+ travel companies (Airlines, OTAs, TMCs, Tour Operators, etc.).

Compliance of WHO Recommendations: Yes, we are approaching return to travel in a thoughtful and collaborative way.

Compliance of ICAO CART requirements: Yes, we are approaching return to travel in a thoughtful and collaborative way.

---

9. Sherpa and American Airlines. (s.f.). Sherpa and American Airlines portal. Retrieved from https://apply.joinsherpa.com/travel-restrictions?affiliateId=americanairlines

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**No**	**No**
COMPLIANCE EXPLANATION	Yes, we have a detailed Privacy and Information Security Policy, and are preparing for SOC2 compliance.	Yes, our users are in control of their data, and we are GDPR-ready.	No, our products are based on REST APIs.	No, our commercial model is B2B2C, and we deliver document application services to travellers with the highest-possible transparency.

SimplyGo 🇩🇪

Name: SimplyGo
Solution founded in: 2020
Founder(s): ION Access & Health GmbH
Country: Germany
Website: ion-ah.com
Contact: Peter Bauer, Managing Director, info@ion-ah.com

Pitch: The SimplyGo app enables us to travel to any place in the world while never compromising on safety and reliability. It offers a unique experience to navigate through times of uncertainty.

Added value: Travel with peace of mind: plan your trip and view the most important entry test requirements for your destination. Get informed about latest corona related behavior rules and news which could impact your trip.

Find a lab and get tested: quickly find medical providers in your surrounding area who offer required tests. Book an appointment, conduct a test and receive the results directly via app.
View and share test results: access your test results in your health record, share them with airlines and immigrations to receive permission to enter your destination.

Main technology used: The backbone of SimplyGo is a platform that enables international information exchange.

Secure, standardized and multi-language compatible, it allows all relevant parties to be integrated to deliver and connect most recent information in order to allow users to meet their individual entry regulations. Through a convenient communication layer, users always have access to their personal data and are enabled to effortlessly pursue their plans while never compromise on safety and security.

Users grant third party providers access to their profile to deliver or read personal data. The platform honors local rules and regulations and acts in accordance with valid security requirements.

Support secured / Implementation cases: Travel app SimplyGo and SITA complete successful trial of COVID-19-focused health data platform with air travelers flying from Germany and Estonia to the United Arab Emirates[10].

---

10. SimplyGo. (3 February 2021). Travel app SimplyGo and SITA complete successful trial of COVID-19-focused health data platform. Retrieved from
   https://uploads-ssl.webflow.com/5f5f45ba968dd38be82f0851/601af4d361da053fef740fc0_210203_SimplyGo%20EN.pdf

VERIFLY

Name: VeriFLY
Solution founded in: N/A
Founder(s): Daon
Country: United States of America
Website: daon.com/products/verifly
Contact: N/A

VeriFLY is the smarter digital health passport that allows real-time verification of COVID-related credentials, such as health questionnaires and diagnostic lab test results, right on your smartphone.

Getting started is simple:

1. Choose your identity standards (registered mobile device, verified biometric, etc.).
2. Choose your credentials (health questionnaire, diagnostic test result, reservation, etc.).
3. Choose your access points (airport checkpoint, office entrance, facility gate, etc.).

Added value: VeriFLY compiles real-time wellness information from self-certified health questionnaires and/or diagnostic COVID-19 test results from over 20,000 performing labs and provides digital badging, proof of test status for both antibody or viral testing, and (in the future) proof of vaccine. Our HIPAA-compliant solution removes the burden from organizations to structure agreements for lab results in multiple locations.

Main technology used: VeriFLY compiles real-time wellness information from self-certified health questionnaires and/or diagnostic COVID-19 test results from over 20,000 performing labs and provides digital badging, proof of test status for both antibody or viral testing, and (in the future) proof of vaccine. Our HIPAA-compliant solution removes the burden from organizations to structure agreements for lab results in multiple locations.

Users enjoy countless ways to acquire, verify, and assert their credentials—proof of health status, age, enrollment, citizenship, membership, reservations, and more.
lid security requirements.

Support secured / Implementation cases: American Airlines: American Airlines Expands its Acceptance of VeriFLY App at All Airports[11].

Iberia has teamed up with VeriFLY for trips to the US[12].

---

11. American Airlines Newsroom. (3 February 2021). More Access, More Ease: American Airlines Expands its Acceptance of VeriFLY App at All Airports. Retrieved from http://news.aa.com/news/news-details/2021/More-Access-More-Ease-American-Airlines-Expands-its-Acceptance-of-VeriFLY-App-at-All-Airports-OPS-DIS-02/default.aspx

12. Iberia. (s.f.). Discover VeriFly™ for your trips to the US. Retrieved from https://www.iberia.com/es/es/covid-19/verifly/

Name: V-Health Passport*
Solution founded in: 2012
Founder(s): V-Health Passport/VST Enterprises
Country: United Kingdom
Website: v-healthpassport.co.uk
Contact: Louis-James Davis, CEO and Founder, louis@vstenterprises.com

V-Health Passport is a global, test & vaccine diagnostic, end to end secure solution. Using VCode allows the pass to become multipurpose e.g A Health Pass & Boarding Pass... Health Pass & Event Ticket all from the same code. This uses permissions such as geolocation, time, date, user id, device type and number of times scanned.

Passes are catered for people of all technical ability and can be both digital and physical (print).

Added value: Global reach of health clinics. A trusted global framework. Scan outside of the 2m safe distancing and up to 10 seconds faster.

Main technology used: VCode, VPlatform.

Support secured: ID2020, Good Health Pass Collaborative. Major events international.

In final discussions with governments such as: Sri Lanka, Malaysia, United Kingdom, Norway, Peru, Mexico, Ghana, Nigeria, Zimbabwe, South Africa.

Implementation cases: We have been live with the Health Passport across the world since June 2020. We are active in the Maritime Industry via companies such as: Fab-Medical (www.fab-medical.com), Airline Travel with the likes of Collinson Group and Salutaris People (www.salutarispeople.com) and Workplaces with the likes of Tutum (https://tutumtech.com).

Compliance of WHO Recommendations: Yes, we encourage all covid safe measures and regular testing. Our technology offers country specific notifications, so the correct message is ensured to be delivered to the user. We encourage safe distancing by default given the technology can be scanned further than 2m away, we also remind users when their tests are about to expire and encourage them to be tested again.

Compliance of ICAO CART requirements: Our system is built to the highest standard, we hold a host of patents for our in house created technology and hold certifications for the likes of GDPR. For data security, we offer in country sovereignty.

We also provide api or sdk access to ensure we're interoperable.

We operate an always on, load balanced geo redundant service.

Our labs meet all in country health standards such as UCAS and ICO.

KEY FACTS

|	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**Yes**	**No**
COMPLIANCE EXPLANATION	Yes, our data is stored encrypted offline and is only brought online to be displayed when a variety of security parameters are met (location, time, user ID etc.) We are GDPR Certified, our servers are ISO 27001 and Hipaa Compliant.	They have to display their own VCode to share data. Public views have no information such as name present. The user has to either display their VCode or email address to a medical professional to share more info.	Yes, it can. Data can be cashed locally. All scans are also stored locally regardless of if offline mode has been set up.	The solution has no cost to governments or institutions. The cost is included in the test kits who are associated with V-Health Passport.
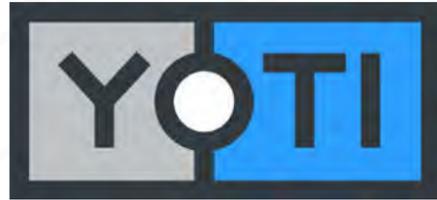
Name: Yoti Digital Identity*
Solution founded in: N/A
Founder(s): Yoti
Country: United Kingdom
Website: yoti.com
Contact: Gavin Watts, Commercial Director - Government & Transport, gavin.watts@yoti.com

Yoti provides a digital wallet, anchored against an individual's biometric and government issued document, which allows for the receipt and secure storage of verified credentials from trusted issuers. In this way, a test result or vaccination record can be bound to the individual's biometric, in a privacy centered way, and shared with relying parties in a variety of forms. It simplifies the process for the individual and relying party, can be easily integrated into digital systems and reduces the reliance on paper or email-based documents that are prone to fraudulent use.

Added value: Yoti launched in November 2017 and to date has approximately 10 million consumer installs of the app. Our focus is to provide the consumer with control of their identity, through the secure Yoti app, giving them the ability to choose what aspects of their identity they wish to share in a privacy forced way with relying parties. Yoti is a founding UK BCorporation.

To that end, Yoti provides individuals with cross industry utility for everyday interactions. It can be used to prove age on-line, to prove identity for financial transactions, to access government service, store employment credentials or indeed to provide information to airlines in order to travel. It is one app for your identity needs and thus has greater value than simply travelling to an individual.

With regard to travel:

- The Yoti app can securely hold biographic information that has been derived from a passport chip and matched to the individual using liveness and facial matching technology.

- Health information (and other credentials) can be consumed in the app in W3C format, allowing interoperability with other wallets.
- The app is future proofed to receive e-visas, or ETAs.
- In sum, the app is a wallet that can hold government identity document information, combined with information from trusted issuers in a secure way, all linked to a biometric.

Elements of the above information can be shared with a relying party across the travel ecosystem, as an individual's digital passport. This can be in a fully integrated way, which drives some of the benefits we list below or can simply be presented as a visual card with a scannable QR code. In this way, we cater for a range of applications depending on technical maturity.

Benefits:
- Returning to the use of on-line check-in and self-service checkpoints, safe in the knowledge that travellers are 'fit' to travel and possess the correct documentation.
- Use of biometrics in terminals, hire car collection points or hotels to drive contactless processes using just your face to authenticate identity. This concept was proven with Heathrow airport in 2019. Link to a video is shown here: https://www.youtube.com/watch?v=4MxZiDWWRJk
- The passenger only needs to share their identity once. Provided the necessary IT infrastructure is in place, this can be used across the end-to-end journey.

In today's market travellers are less 'sticky' to airlines. They are more likely to select the flight that best matches their schedule and that offers the best value. To that end, an individual does not want to have multiple apps for each airline, particularly low-cost airlines, and this is where Yoti adds value. It can be used across any airline, hotel, hire car or cruise liner that wishes to use Yoti tech, in much the same way as the cross-industry utility I describe above.

Importantly, Yoti pledges to be interoperable and conform to the emerging standards when it comes to health credentials.

Finally, Yoti has also developed a Health Testing Application that businesses and organisations can use to manage their testing programs. It is compatible across the range of test types and works with the Yoti app.

The high-level features include:
- Linking of an individual to a test using either the Yoti app or a web form.
- Management of test through the process, in point of care use cases.
- Issuance of result in a W3C format to the Yoti app or a provided email.
- Managing and reporting of information.

Main technology used: A secure mobile wallet:

- Available on both Android's Play Store and Apple's App Store.
- Storage of private encryption keys in the smartphone secure element secured by a 5 digit PIN and user's facial biometric template. Sophisticated encryption mechanism AES-256 encryption and authenticated by RSA signatures and signed timestamps. Use of an encrypted 'partitioned key-value store', a form of directed graph-structure database Multi-layer 'wrapped key' encryption model Use of HSM Private RSA keys issued to the secure element of user's device.   Near Field Communication (NFC) Document Chip Reading
- Support for ICAO 9303 passport reading on both Android and IOS platforms
- Fast and highly accurate data extraction from Data group 1
- Fast and high assurance gained for document authenticity
- Enables best possible facial recognition using clean image from Data group 2

Facial Recognition:
- 1 to 1 matching between user onboarding image and image on a government issued document
- 1 to 1 matching between a live image and image held in the user's account, for authentication and access to data.   Liveness Detection
- iBeta level-2 / NIST Level 2 certified Active liveness detection
- Zoom Facetec (https://www.liveness.com/)
- Passive liveness detection (undergoing NIST certification). Optical Character Recognition (OCR). Use of OCR technology to capture visual text from ID documents from over 200 countries. Use of OCR to read barcodes and other machine-readable elements on documents. W3C Credential interoperability Support for W3C Verified Credential lifecycle, supporting relying party definition, automatic revocation, forced revocation and update. A recipient is able to transact this credential with another relying party, also passing the proof, allowing another party to verify that the credential and the issuer are genuine. Securely encrypted and stored according to Yoti's defined data handling and storage mechanism.

Open-Source SDKs:
- A suite of SDKs is available in 7 different languages, Java, NodeJS, .NET, PHP, Python, Golang, Ruby, supporting the server-side implementation.
- JavaScript library or REST API FOR client-side implementation.
- Native mobile SDKs in Android, IOS and React Native Third Party API suite

- Yoti integrates with multiple third parties to provide 'direct to source issuer verification' depending on the document type and issuing country.

- Yoti also utilises police fraud databases at point of document onboarding, checking for lost, stolen and fraudulently obtained genuine documents.
- Yoti offers additional integrations to supplementary data providers, such as address checking or AML services. Yoti is ISO 27001 accredited and holds a clean SOC2 type 2 report, which is audited annually.

Support secured: The Government of Jersey:
- Yoti is the official ID provider for the Government of Jersey.
- Citizens living in Jersey use Yoti to verify their identity to access Government services on-line.
Examples of this include:
- Registering to complete on-line tax returns.
- Applying for settled status for the right to remain in Jersey post the UKs exit from Europe. Yoti is used to provide necessary information, including nationality.

The Improvement Service in Scotland:
- Is the 'go to' organisation for Local Government improvement in Scotland.
- They provide the 'MyAccount' service to the 32 Local Authorities across Scotland for accessing online services. Yoti provides the identity verification solution through the Yoti app to allow the delivery of online services where a highly level of user verification is required.
- They also administer the National Entitlement Card Scheme (NEC) and in July 2020 launched an online portal getyournec.scot to allow for online applications and updates. This requires the user to use the Yoti App or alternatively carry out a one-off transaction using Yoti Doc Scan (our business-to-business service) to access the portal.

The Post Office UK:
Yoti have entered into a strategic partnership with the Post Office to provide a consumer facing digital identity service in the UK, supplemented with in-branch verification services. The Service launches in April of this year.

The World Economic Forum (WEF):
We are members of the WEF Digital Identity Innovators initiative and are actively participating in the Future of Health and Future of Travel programmes.

In final discussions with governments such as: Sri Lanka, Malaysia, United Kingdom, Norway, Peru, Mexico, Ghana, Nigeria, Zimbabwe, South Africa.

Implementation cases: The solutions Yoti offers, including the consumer digital identity app, is in use by many clients across a range of countries. Specifically with regard to travel use cases:

-Virgin Atlantic:
Virgin Atlantic is using the Yoti app and the Health Testing Application for all of their staff, including flight crews, as part of their testing programme.

Flight crews use the Yoti app to share their information, linking themselves to a test and in return receive a result in the form of a W3C compliant credential directly to the app on their phone.

The team administering the testing process uses the Health Testing Platform that Yoti have developed to manage the end-to-end process.
A video run through can be seen here: https://www.youtube.com/watch?v=pXW4Q5TrWxU&feature=youtu.be

-Norway:
Nordic DX and Aker Solutions are using the solution to test Polish nationals working in the shipyards to ensure they have a negative Covid-19 status prior to them travelling home on leave. This is expected to be expanded to all employees working on the sites shortly.

-Heathrow Airport:
As previously described, through 2018 and into 2019 we demonstrated, with Heathrow Airport and Atkins, how the solution (Yoti app) can be used to provide accurate passenger information (API) and a unique biometric at the point of checking in for a flight. This information, when combined with a boarding pass, formed a single token against which the individual is authenticated against, with their face, at key airport checkpoints. This was successfully demonstrated at Passenger Terminal Expo, held in London, in 2019.

Compliance of WHO Recommendations: There is yet to be a definitive WHO recommendation on either test results or vaccine record credentials that could be stored in digital wallets.

Yoti is following the interoperable frameworks proposed by the World Economic Forum (WEF), World Health Organisation (WHO). Yoti is a member of the World Economic Forum Digital Identity Innovators, Future of Health and Future of Travel programmes, the Good Health Pass Collaborative and the COVID-19 Credentials Initiative.

Yoti is keen to interoperate with the WEF 'CommonPass', the 'SMART Health Cards Framework' laid out by the Smart Vaccination Certificate working group and the Vaccination Credential Initiative - also based on W3C Verifiable Credential, the Good Health Collaborative, HL7 FHIR standards and LOINC.

Compliance of ICAO CART requirements:
When we refer to 'digital passport standards' we must be clear what we mean when we refer to standards or requirements. There are many different aspects at play here, which mean different things, depending on your role:

Establishing identity: Standards around digital identity assurance are becoming better understood and are generally referred to as Levels of Assurance (LoAs), although they differ as frameworks between countries.

Yoti has contributed to the national Trust Framework development in the UK, Canada, Australia, New Zealand, eIDAS. Yoti is also involved in a range of vertical market trust frameworks including employment credentials (Velocity Network Foundation), property conveyancing (etive), financial services KYC (TISA).

Verified Credentials (VC): The general accepted standard for VCs is the W3C standard, that allows for interoperability between wallets and is followed by Yoti.

Health Credentials / Vaccine records: There is a lot of work on-going with regard to this topic across many groups, both with regard to the standard, such as HL7 FHIR and the exchange protocols by which they are to be shared.

Yoti is involved in these discussions wherever possible.

KEY FACTS

	Data privacy	User's control of data	Off-line mode available?	Does it imply cost for governments?
	Yes	**Yes**	**No**	**Depends**
COMPLIANCE EXPLANATION	Our solution is designed with privacy, security and data minimisation in mind. We have no access to user data once their account is set up and only users can access and manage their own data, access to which is through a private key stored in the secure module of the users' phone. All data is encrypted at rest and in transit. The aim of the app is to only provide the information required for a given scenario rather than, say, an entire ID document to prove an age or an address. Thus, conforming to data minimisation requirements. Credentials such as proof of vaccination can be added from trusted sources and stored securely in the same manner. Relying parties can integrate the technology to get yes / no responses rather than actual data. We are ISO 27001 accredited and hold a clean SOC2 type 2 report, which is audited annually.	As stated above, the user is in full control of their data and only they have access to it. A user must choose if they wish to share information with a relying party and complete 2 steps when doing so: 1. Review the information that the relying party is asking them to share, such as name and address. This is clearly displayed to the individual in the app consent to share page. 2. Consent to share the information by pressing the 'consent' button in the app. This may also be supplemented by a biometric challenge, as an extra security measure, which can be selected by the relying party.	Our solution does not currently operate in an off-line mode.	The SDKs to implement the solution are readily available for the client and server-side implementation. Yoti supports both web and native client-side applications and there is no charge to integrate these. These open-source SDKs, along with our documentation are publicly available on our public GitHub repositories and documentation site at: https://developers.yoti.com They have been designed to be easily integrable from the outset and will take from a few hours to a few days to integrate, depending on the complexity of the platform and experience of the developer. We provide a dedicated integration support team, at no cost, who will work closely with your development, QA and infrastructure teams to ensure the implementation is sound and follows Yoti's best practices, ensuring optimal use of the system.

RESOURCES

Introduction:

Covid-19 Credentials Initiative (CCI). (s.f.). Retrieved from https://www.covidcreds.org

Good Health Pass Collaborative. (2021). Good Health Pass. A safe path to global reopening. Retrieved from https://www.goodhealthpass.org/wp-content/uploads/2021/02/Good-Health-Pass-Collaborative-Principles-Paper.pdf

IBM. (s.f.). What is blockchain technology? Retrieved from https://www.ibm.com/blockchain/what-is-blockchain

International Civil Aviation Organization's Council Aviation (ICAO). (s.f.). ICAO Council Aviation Recovery Taskforce (CART). Retrieved from https://www.icao.int/covid/cart/Pages/default.aspx

ID 2020. (s.f.). ID 2020. Retrieved from https://id2020.org

Vaccination Credential Initiative (VCI). (s.f.). Vaccination Credential Initiative (VCI). Retrieved from https://vaccinationcredential.org

World Health Organization (WHO). (5 February 2021). Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers. Retrieved https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers

RESOURCES

Digital Health Passes:

Airside Mobile ID + Health Passport.
UNWTO Digital Health Passes Collection Form.

CommonPass.
UNWTO Digital Health Passes Collection Form.

CoronaPass.
CoronaPass. (s.f.). CoronaPass powered by Bizagi. Retrieved from https://www.coronapass.org

hi + Card.
UNWTO Digital Health Passes Collection Form.

IATA Travel Pass.
UNWTO Digital Health Passes Collection Form.

IBM Digital Health Pass
IBM. (s.f.). Digital Health Pass. Retrieved from https://www.ibm.com/products/digital-health-pass

ICC AOKpass.
UNWTO Digital Health Passes Collection Form.

iLife. UNWTO Safe Travel Solutions Form.
UNWTO Digital Health Passes Collection Form.

IMMUVID.
UNWTO Digital Health Passes Collection Form.

myHealth Pass
SICPA. (s.f.). myHealth Pass. Retrieved from https://www.sicpa.com/MyHealthPass
SICPA. (s.f.): CERTUS Digital Seal Technology. Retrieved from https://www.sicpa.com/solutions/certus-verifying-certificates

ShareRing ID.
ShareRing. (s.f.). ShareRing ID. Retrieved from https://sharering.network/app.html

SimplyGo.
ION Access & Health GmbH. (s.f.). SimplyGo. Retrieved from https://ion-ah.com

Sherpa.
UNWTO Digital Health Passes Collection Form.

VeriFLY.
Daon. (s.f.). VeriFLY. Retrieved from https://www.daon.com/products/verifly
VeriFLY. (s.f.). VeriFLY. Retrieved from https://www.myverifly.com/#/

V-Health Passport/VST Enterprises.
UNWTO Digital Health Passes Collection Form.

Yoti Digital Identity.
UNWTO Digital Health Passes Collection Form.