GLOBAL GUIDELINES FOR SAFE & SEAMLESS TRAVELLER JOURNEY

A global effort: The adoption of innovative digital technologies to enable seamless travel

WORLD
TRAVEL &
TOURISM
COUNCIL

OLIVER WYMAN

CONTENTS

FOREWORD

WTTC Members have identified security and travel facilitation as a top priority.

According to WTTC's 2019 data, the Travel & Tourism sector accounted for 10.3% of global GDP and supported the livelihoods of 330 million people in 2019, outpacing the growth of the global economy for nine consecutive years[1]. As one of the fastest-growing industries in 2019, responsible for one in four new jobs created worldwide over the last five years, the slowdown of Travel & Tourism has had devastating ripple effects beyond the sector itself.

The benefits of Travel & Tourism spread far beyond its direct impacts on GDP and employment. Indirect benefits apply throughout the supply chain and interlinkages to other industries, such as agriculture, retail, arts, and construction. Additionally, the Travel & Tourism sector is highly inclusive, employing and offering opportunities to people from all walks of life, including minorities, youth, and women.

In 2017 WTTC identified the need to increase capacity to fulfil the demand and the absolute requirement for security processes to be as robust as possible. This provides a global, cross-industry solution, allowing more people to travel more securely and enabling economic opportunity. WTTC addressed this challenge through our Safe & Seamless Traveller Journey Programme launched in 2018, which aims to enable a seamless, safe, and secure end-to-end traveller journey. Encompassing both air and non-air travel, the SSTJ vision promotes the use of biometrically verified identities and electronically verified traveller information at each stage of the journey. These replace manual verifications and create a more secure and safe environment for travellers and employees using advanced touchless technology.

As a result, WTTC brought together, through its representation of the Travel & Tourism private sector, more than 350 travel industry, technology, and government leaders in a series of workshops and interviews to drive forward this initiative. Efforts were focused on understanding, documenting, and identifying solutions across the sector to implement biometrics, processes, and technologies to facilitate seamless travel.

With the COVID-19 crisis the Travel & Tourism sector is in uncharted territory. At the global level, WTTC's latest projections (from October 2020) reveal that 143 million jobs have been impacted this year. If effective strategies are not developed to balance the public health needs with an effective economic restart, 174 million jobs could be lost by the end of 2020, more than half of those employed by the industry in 2019[1]. These new figures come from WTTC's latest economic data, which looks at the impact of COVID-19, as well as local and global travel restrictions on the Travel & Tourism sector. To support the recovery, WTTC is advocating for swift action to enable strong policies through the undertaking of several activities. In the wake of COVID-19, the SSTJ initiative aligns with the seamless travel concepts identified as a pillar within the tourism agenda for the G20 in 2020, under the Presidency of Saudi Arabia. ▶

▶ Over the last decade, the Travel & Tourism sector has made enormous gains in driving solutions that enhance security while improving the traveller experience. In particular, the aviation sector has embraced the use of biometrics to make travel safer, offer a better experience, reduce friction points in the traveller journey, and cut costs.

The SSTJ initiative encourages governments, travel stakeholders, and technology providers to agree on models, data facilitation methods, and global best practices to complement existing global and industry standards. While estimates vary on when domestic and international travel will return, government and industry should be poised to meet that demand and maximize efficiencies. Future planning to support and allow the adoption of biometrics, enabling features such as dynamic passenger screening and biometric boarding.

Significant technological advances in digital identities continue to enter the marketplace and can help overcome the COVID-19 crisis.

Several facial recognition solutions across aviation, including airport check-in and biometric baggage drop require no human contact. In sectors outside of aviation, these same biometric solutions can be leveraged to create touchless and contract-free experiences such as hotel check-in, cruise embarkation, and car rental retrieval. Furthermore, solutions can allow for additional health screening and increase the speed at which travellers are processed at checkpoints, enabling physical distancing where required.

WTTC identified significant quantitative benefits, in addition to those qualitative benefits. Key findings in 2019, show that over a period from 2020-2050, the net impact of global benefits across aviation including airports, airlines and users – passengers/cargo, car, cruise, and hospitality associated with the SSTJ end to end approach has a present value of $967 billion ($618 billion for aviation and $349 billion[2,3] for the other sectors).

The best practices defined herein aim to assist in the establishment of globally interoperable, technology-agnostic, biometric-enabled solutions, which cover the end-to-end traveller journey from booking to trip completion.

For this report, seamless travel is defined as a journey during which the traveller no longer needs to present travel-related documents (e.g. boarding passes) or identification documents (e.g. passport) multiple times to a variety of stakeholders at different checkpoints in their journey. Travellers will be able to book transportation, check-in, proceed through security, cross borders, board their aircraft, collect luggage, rent a car, check-in and out of their hotel and other non-air services, simply by confirming their identity and booking data in a contactless way.

Gloria

Gloria Guevara Manzo
President & CEO
WTTC

Scot W. Hornick

Scot Hornick
Partner, Transportation & Travel
Oliver Wyman

Note: This report has integrated the implications of COVID-19 into its consideration of seamless travel and looks specifically at the implementation of biometrics and digital identities to enhance security, facilitate travel, and drive a contactless experience.

[1] https://wttc.org/Research/Economic-Impact

[2] NEXTT Preliminary Cost Benefit Analysis: Technical Report, November 14, 2018

[3] Seamless Traveller Journey Cost Benefit Analysis: Cost Benefit Model & Technical Report 1st Quarter 2020

SUMMARY

Opportunities

Technological advances enable verified digital identities that use biometrics to confirm with high certainty the identity of a user. Applying these solutions to the Travel & Tourism sector offers significant benefits. Verified identities enable the secure, seamless movement and management of travellers across the air and non-air journeys. Utilizing traveller biographic, biometric, loyalty, credit card, travel history, proof of immunity or vaccine and other personal information, will allow governments and travel providers to move the traveller more efficiently and safely through journey touchpoints. Travellers will no longer be required to present and verify their identity, relevant travel (e.g. recently visited countries) and medical history (e.g. vaccine) at multiple touchpoints. The result reduces fraud and allows for the movement of more travellers securely and efficiently through existing infrastructure and easing resource requirements.

SSTJ aims to leverage standards and existing best-in-class solutions to achieve interoperability and a faster go-to-market solution.

WTTC's approach

WTTC is in a unique position to establish a unified voice to engage with governments around the world.

Security and travel facilitation are priorities for WTTC, enabling the sustainable growth of the Travel & Tourism sector and enhancing security while offering an unparalleled experience to the traveller. WTTC has taken a collaborative approach, building on efforts of organizations such as the International Air Transport Association (IATA), the International Border Management and Technologies Association (IBMATA), the International Civil Aviation Organization (ICAO), Airport Council International (ACI), the Cruise Lines International Association (CLIA) and the World Economic Forum (WEF), as well as independent efforts by airlines, airports, hotels, car rentals and governments.

Capturing and uploading biometric and biographic data before travel allows border and security agencies to authenticate and pre-clear travellers in advance of arrival. This enhances security across the entire system while relieving pressure on infrastructure & capacity constraints. In exchange, travellers experience reduced cumbersome checks and queues at ports and airports.

SSTJ solutions align with WTTC's consumer research undertaken in five European countries and the United States. The data states that on average, 4 in 5 international & domestic travellers would be willing to share their photographs in advance of travel to speed up their journey.

Five principles of success

The Travel & Tourism sector is at a critical point where biometric digital identity solutions are being designed and developed to serve travellers across air and non-air touchpoints.

The best practices contained herein are built on a foundation of five core principles:

1. Public/private sector collaboration

Governments need to work together and create bilateral and multilateral agreements, based on the foundation that all data is authenticated and verifiable. Collaboration between the public and private sector will be critical to drive innovation and adoption. The private sector needs to work together to advocate for regulations and global standards, which are needed to assist in making their businesses thrive using biometric-enabled digital identities.

2. Data collection and sharing

Data is owned, managed, and provided to stakeholders by the traveller. The foundation of a traveller's digital identity is the collection of authenticated and verifiable data. From an identity perspective, this must be based on a government-issued identification (e.g. passport, national ID, driver license). Any additional data the traveller chooses to include in their digital identity is authenticated and verifiable by stakeholders. When travellers are asked to share their data, it is done in a fully transparent manner, through simple and clear consent requests. Traveller data should only be shared when operationally required and zero-knowledge messages should be used when possible.

3. Data privacy

Solutions must adhere to the highest level of data privacy standards, using Data Privacy by Design principles. With the growing threat of cybersecurity, it is critical to protect the travellers' data as it is often the reason a person does not adopt a certain technology.

4. Interoperability

To connect the end-to-end traveller journey, it is operationally imperative that solutions are interoperable. This applies across governments and between the different sectors within Travel & Tourism. The critical element to interoperability is for a traveller's data to be stored based on global standards, allowing stakeholders (both public and private) to ingest the data.

5. Customer-first by design

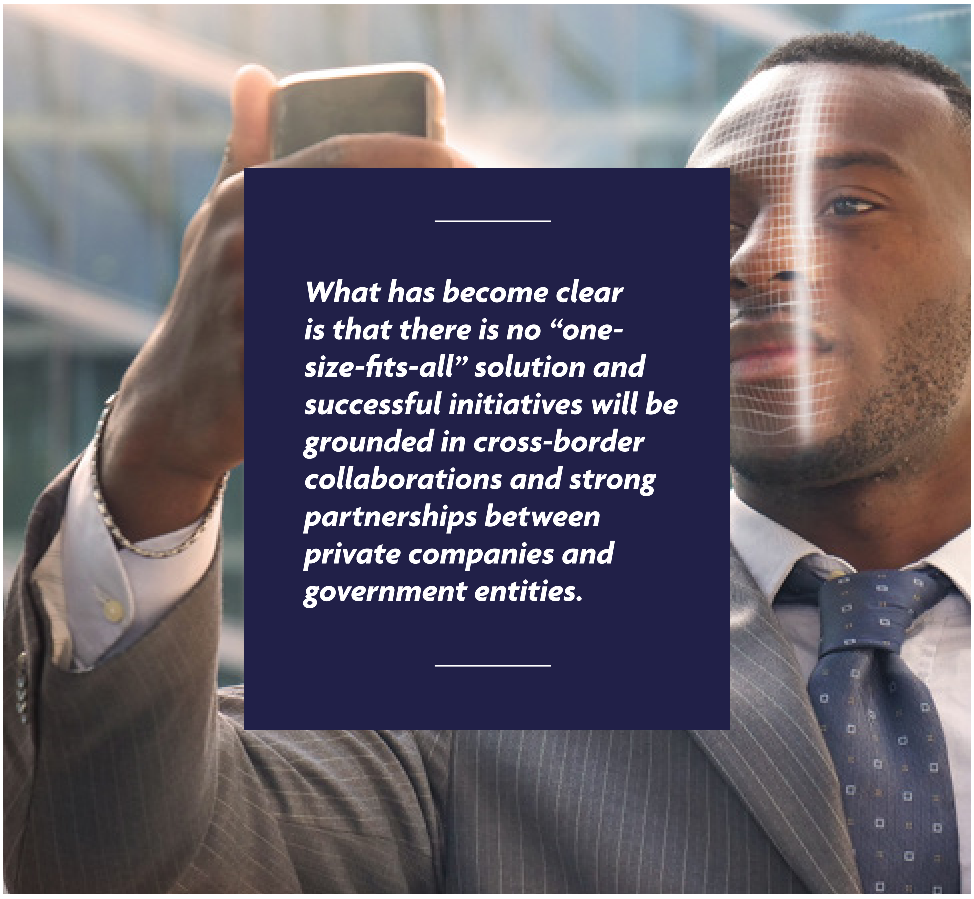
Enable technology companies and stakeholders to build simple solutions and operational processes to create a seamless, intuitive, and non-cumbersome customer experience.

Overview of best practice & recommendations

This paper lays out several best practice recommendations for biometric-enabled digital identities and their use across the end-to-end traveller journey. While WTTC recognizes the long path that leads to the end goal, a long-term vision and supporting best practices are the guide poles for each stakeholder.

A summary of the best practices for a successful global SSTJ programme, discussed herein, are:

- **Travellers create a single digital identity** containing their biographic data and any additional information required for identity establishment and verification. This is used across all stakeholders, public and private, in the traveller's journey
- Allow travellers to **enrol early in the traveller journey**, so they can use their digital identity across the end-to-end journey
- Digital identity management is done in a **decentralized manner**, where the traveller maintains and controls access to their data
- Traveller's digital identity **data is governed by a globally agreed-upon set of standards**, allowing for interoperability across governments and all sectors of the Travel & Tourism sector
- **Privacy standards are continually developed and enhanced** with guidelines to ensure they are of the highest quality



> ***What has become clear is that there is no "one-size-fits-all" solution and successful initiatives will be grounded in cross-border collaborations and strong partnerships between private companies and government entities.***

[4] Safe and seamless travel and improved traveller experience - OECD Report to G20 Tourism Working Group

Government landscape

The Organisation for Economic Co-operation and Development (OECD)[4] and WTTC have emphasised how traveller identity and security are critical areas which will support the recovery of the sector. Biometric digital identities enable contactless technologies, biometrics, faster clearance for both inbound and outbound passengers, and offsite processing are a few examples of WTTC's seamless travel concept.

The OECD and WTTC call on governments, in collaboration with the industry individually and collectively, to promote the use of digital traveller identity and biometrics while respecting data privacy based on agreed international standards and principles. For example, the OECD advocates for interoperability between systems which can be enabled by global cooperation between governments and international bodies.

Governments' current state of biometrics and digital identities

In recent years, governments worldwide have been actively deploying biometric technologies to enhance security and to allow for a more seamless travel facilitation process at their borders. Many countries have implemented programmes that leverage risk-based segmentation to allocate resources to higher threats while allowing lower risk travellers expedited passage such as, Global Entry in the US and EasyPass in Germany.

Advances in facial recognition technology have enabled border agencies to match live passenger images to those held in their passport and government databases with high accuracy and a low level of traveller intrusion. Biometric recognition technology has led to an increase in the adoption of eGates and kiosks at border control points around the world. Typically, eGates are used for specified traveller segments including "own nationals", "low-risk nationals", and "registered travellers" depending upon the policy of the country concerned. By clearing low-risk travellers in this way, Border Agencies can divert officer resources to intelligence-led targeting operations, focussed upon higher-risk individuals. Further, airport eGates and kiosks require a significant footprint and cost. Advances in technology may allow border agencies to screen travellers further away from the airport, requiring only a camera to confirm the identity of the traveller.

The introduction of the "electronic travel authority", the "e-visa" and the "digital travel credential" present border agencies with significant opportunities. Enhancing seamless travel on entry and exit for more traveller segments, without compromising security. All provided that there is compliance with the applicable legislation and data protection rules.

Security threats continue to evolve, particularly in the commercial aviation sector, requiring constant investment in personnel, infrastructure, and technology. Governments are challenged by the need to balance supporting an important economic driver with its primary mission to ensure the safety and security of its people. Given the limited resources of physical space and costs of hiring additional personnel, governments have increasingly turned to technology and innovation as a force multiplier to meeting the growing demand for the Travel & Tourism sector.

In November 2020, the ICAO released the Digital Travel Credential (DTC) standard, which presents an opportunity to accelerate digital travel identity using a global standard.

Opportunities for governments

Despite the current crisis, many countries continue to invest in biometric Entry/Exit Systems (EES). While significant progress is being made in many countries, key challenges exist within the technology landscape. Integration of biometrics used in visa and border systems with broader applications, including the police and immigration enforcement rely heavily on fingerprints rather than facial recognition to identify high-risk individuals. This means that although facial or iris recognition systems can continue to proliferate as a useful tool for automated passage across borders, we cannot ignore the need to capture fingerprints for law enforcement risk assessment in many cases. Associating fingerprints with a verified facial biometric can allow future use of facial biometrics for subsequent arrivals.

Public-private engagement is critical to driving forward biometric enabled digital traveller identity. The public sector has a major role in regulation and implementation, especially relating to aspects of security and government-issued identity credentials which is the foundation for the traveller's digital identity. The private sector plays a key role as a user of systems and a provider of technology and knowledge.

Public/private partnerships ensure biometric and digital identities do not have a detrimental impact on the private sector, governments maintain the level of security required, the technology is useful and affordable, and maximizes the traveller experience and efficiencies. Stakeholders have attested that using biometrics lead to faster boarding times, enhanced customer service, better use of resources, and faster flight clearance times on arrival[5].

International agreements are needed to develop "end-to-end" processes working at both ends of the international journey. These agreements should cover how to best obtain traveller data, integration within a traveller's digital identity (supported by biometrics), agreed standards and processes, protection of the traveller's data and privacy and components of a digital identity. For example, components of the digital identity may include digital health certificates, generated by government authorized agencies and based on standards set by international agencies such as the World Health Organization (WHO).

Government Imperatives

1. Increase acceptance and adoption of biometrics at government-regulated checkpoints, including advance capture and verification of identity that feed into risk assessment, screening, and checkpoint clearance processes.

2. Pave the way through legislation and regulations to allow for biometrics and digital identity usage by the Travel & Tourism sector. Also address key questions about roles and responsibilities and legislative challenges over the capture, transmission, and retention of data.

3. Work across borders with the private sector and standard-setting organizations to establish global standards for biometrics and digital identities, specifically around what information is included in a traveller identity and data privacy.

4. Set high levels of security and compliance that private sector initiatives must meet, as the government is ultimately responsible for safe, secure borders and the protection of its people.

[5] WTTC Emerging Model Overview Findings Report Security & Travel Facilitation | WTTC Initiatives | World Travel & Tourism Council (WTTC)

Key benefits

Traveller digital identity solutions will alleviate the strain on travel infrastructure as demand recovers from the COVID-19 pandemic. More immediately, SSTJ solutions will help the Travel & Tourism sector stimulate demand in the recovery from COVID-19 with the health and safety components native to biometric-enabled solutions. There are significant universal benefits to the entire sector including the promotion of a healthier journey, for both travellers and employees, through biometric-enabled touchless interactions.

To ensure there is a strong business case for investment, quantitative benefits must exist. In 2019, WTTC worked to define the quantitative benefits to the cruise, hotel and car rental sectors, to complement the work already done by IATA and ACI to measure the benefits to the aviation sector. The outcomes of the cost-benefit analysis (CBA) report[6,7] is significant and provide the baseline for a strong business case for investment.

Measuring benefit to cost ratios (i.e. dollar benefit per dollar investment), the CBA concludes that the cruise sector would benefit the most, but all sectors benefit greatly. The benefit to cost ratios for the Travel & Tourism sector by sector is shown below.

2019 cost to benefit ratios:

Subsector	North America	South America	Europe	Asia Pacific	Middle East & Africa	Global
Cruise[6]	$28.20	$28.10	$26.20	$29.00	$26.80	$27.70
Hotels[6]	$3.90	$3.90	$3.80	$4.00	$3.90	$3.90
Car Renta[6]	$4.70	$4.50	$4.60	$4.70	$4.50	$4.60
Aviation[7]						$18.00

The detailed benefits outlined below, can be quantified, and assist in developing a strong business case for the investment and adoption of biometric-enabled digital identities. These benefits reach across the public sector, private sector, and the traveller.

Public sector

- Increased efficiency at current checkpoints (e.g. streamline operations, maximize capacity)
- Increased health control mechanisms
- Increased border control and security
- Increased visibility on higher risk profile passengers
- Reduced resource requirements (e.g. border crossing personnel)
- Reduced strain on infrastructure
- Supports increased economic growth by encouraging innovation with advent of biometric technologies

Private sector

- Increased efficiency at current checkpoints (e.g. reduce resource requirements)
- Increased healthy facilitation of travellers
- Increased security for ongoing operations (e.g. check-in, boarding)
- Increased accuracy of information sharing between travellers and travel providers (e.g. API and PNR)
- Increased personalized customer interactions (e.g. up-sell, cross sell) leading to greater revenue potential
- Increased asset utilization (e.g. airplanes, hotel rooms, car rentals)
- Reduced recurring fees related to operations (e.g. credit card holding fees, card-not-present fraud, and hotel key cards)
- Reduced data liability (e.g. reduced need to store no/limited value-add data (e.g. credit card) while not impacting customer experience)

Traveller

- Enhanced travel experience by removing friction at checkpoints
- Increased customer satisfaction due to enhanced personalized service
- Increased personal safety (e.g. touchless capabilities, health controls) and security
- Increased control and transparency of personal data sent to stakeholders
- Supports permission to travel application
- Reduced data liability (e.g. traveller's data footprint decreased)
- Reduced fraudulent activity (e.g. incidences of stolen identity, stolen credit cards)

[6] Seamless Traveller Journey Cost Benefit Analysis: Cost Benefit Model & Technical Report 1st Quarter 2020 Security & Travel Facilitation | WTTC Initiatives | World Travel & Tourism Council (WTTC)
[7] NEXTT Preliminary Cost Benefit Analysis: Technical Report, November 14, 2018

Call to action: Private & Public Sectors

As of October 2020, more than 143 million jobs[8] and livelihoods in the Travel & Tourism sector have been impacted globally creating the worst economic and social crisis.

There is a unique window of opportunity for leaders from the public and private sector to work together to create the path forward to provide the economic recovery needed for the Travel & Tourism sector without compromising the necessary health measures and, bring back millions of jobs.

Under the leadership of Saudi Arabia and its Presidency of the G20, the global Travel & Tourism private sector was asked to put together a plan to support the recovery of the sector and bring back 100 million jobs . Biometrics and traveller identities were a critical component of that plan.

WTTC Members, other private sector leaders and international organisations have identified the following relevant private sector SSTJ actions:

- Develop and adopt innovative and digital technologies that enable seamless travel, better manage visitor flows, and improve the traveller experience, while also making it safer.
- Provide consistent and coordinated communication to travellers, offering information to have a better risk assessment, awareness and management, facilitate their journeys and enhance their experience.
- Continue to invest in crisis preparedness and resilience to better equip the sector to respond to future risks or shocks, while working closely with the public sector.
- Cooperate with governments in their efforts on COVID-19 testing before departure and contact tracing tools within an international testing protocol and framework.

However, the private sector cannot reduce the time frame of recovery and bring back 100 million jobs alone. Public-private collaboration is essential to the success of the plan.

We call upon governments to establish a task force in each country. The task force's responsibility is to define a specific strategy to achieve the vision for digital identity and biometrics at a Secretary/Minister level and to coordinate internationally.

While each country has a unique process for enacting statutes that authorize its executive branch agencies to issue and administer regulations. The processes governing legislative or executive action often depend on the individuals serving in those roles, priority, and efforts made to collaborate with colleagues, stakeholders and the public to drive forward. SSTJ, biometrics and digital traveller identity has a value from an economic and security standpoint and should be a priority for any government who is seeking to be globally competitive and be in the best position to anticipate future challenges and threats. Regardless of the legislative or regulatory context, governments and their "task force", should be deliberative in outlining the specific use cases, including stakeholder, and undertake an aggressive outreach to the public to thoughtfully explain the need for additional regulation or legislation.

The "Task Force" to set a vision for Traveller Identities that includes a guiding set of principles to ensure that efforts are tracked along that path.

Goals of a government-focused task force:

- Adopt the upcoming Digital Travel Credential, established by ICAO, building on the e-passport, as the basis for containing and conveying a traveller's digital identity.
- Establish, where applicable, of a multi-national 'trusted traveller' programme, based on agreed standards[9].
- Facilitate a harmonised and consistent adoption, nationally and internationally, of the use of digital traveller identity supported by biometrics.
- Invest in digital and physical infrastructure to facilitate the process.
- Ensure effective liaison between ministries responsible for tourism, national security, and transport in the development of related policies and initiatives.
- Ensure international coordination among governments for the implementation of standardized global protocols across all industries and geographies.
- Develop and adopt innovative and digital technologies that enable better management of visitor flows, and improvement of traveller experience while making it safer.
- Provide consistent, simple and coordinated communication to citizens and travellers to ensure better risk assessment and awareness via a communications campaign (PR and media).

[8] https://wttc.org/Research/Economic-Impact
[9] http://www.ibmata.org/wp-content/uploads/2019/10/IBMATA_Seamless_Secure_Travel.pdf

EUROPE
AMERICA
MIDDLE EAST
SOUTH AMERICA
30,000
25,000
20,000
15,000
10,000
5,000
0
Human Resources
Legal
Accounting
Finance
Marketing
Publicity
Promotion
Research
Business
Development
Engineering
Manufacturing
Planning
ASIA
EUROPE
MIDDLE EAST
AFRICA

THE IMPORTANCE OF SEAMLESS TRAVEL

Current state – Private Sector

The private sector has begun to implement several solutions which employ biometric enabled digital identities as part of the traveller journey. While the majority of these are within individual industries (e.g. aviation) within the Travel & Tourism sector, it is important to consider:

1. Solutions that facilitate an end-to-end biometrically enabled journey are becoming readily available in the marketplace.

2. Significant lessons learned can be understood from existing initiatives.

The key emerging themes:

- Technology/solution coverage and investment have been spearheaded independently or in partnerships between technology companies, airlines, and airports. These efforts have produced biometric solutions ranging from eGates to biometric bag drop.
- New initiatives showcase more integrated experiences within airport environments. They are impacting several steps within the airport experience, and in some cases are broadly deployed across an airport terminal.
- Other industries within the sector are progressing at a slower pace. Hotels and car rentals have deployed limited use cases for biometric solutions. Cruise lines depend on border agencies to deliver biometric initiatives. Rail has recently started to focus on biometrics through Eurostar piloting a project for seamless ticket check-in 2021. Other industries (e.g. travel companies, OTAs, retail) have yet to fully explore the potential of biometric solutions.

Current state – Public Sector

Several promising initiatives are occurring at the national level. While from an international standpoint, little coordination of these forward-looking traveller programmes has begun.

- Most initiatives have applicability unilaterally, or at a minimum bilaterally with neighbouring countries. International agreements are needed on what may be required to develop “end-to-end” processes that work at both ends of the international journey.
- Agreements on standards and processes should cover specific issues such as how data can best be obtained, stored, and integrated within a digital identity supported by biometrics while maintaining the highest data protection.
- Digital identity data should include digital health certificates, generated by government authorized agencies and based on standards set by international agencies such as the World Health Organization (WHO).

Several governments are taking a lead in using biometrics and digital identities to enhance their security and immigration processes.
Below are a few examples:

United States: In the United States, U.S. Customs and Border Protection (CBP) has recently enhanced their international arrival process with the new "Simplified Arrival Process" at selected airports, seaports, and land borders. The Simplified Arrival Process allows travellers to verify their identity through facial biometrics. Also, foreign travellers who have previously travelled to the U.S. will no longer need to have their fingerprints captured, as their identity will be confirmed through the facial biometric comparison process. Similarly, CBP is delivering its core biometric exit mission by enabling facial biometric comparison between live images and travellers' passport and/or visa photos held in a secure government database to allow for a passport-free boarding process upon departure from the country. Additionally, the Transportation Security Administration (TSA) has conducted pilot tests to assess the feasibility of using facial recognition technology (FRT) for security clearance, although this is still at the early stage for assessment of TSA's compliance with privacy protection principles.

UK: The government already makes extensive use of biometrics in their immigration and border processes. All travellers coming to the UK for more than 6 months must include the submission of biometrics (face and finger). This requirement will be extended to EU/EEA/Swiss nationals when the Brexit transition period ends on 1 January 2021. Under the new Immigration Points Based System (PBS) all non-British / Irish passport holders will need digital permission to enter the UK, which will include a new UK electronic travel authority (ETA) for non-visa visitors.

EU: The European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA) is driving new information architecture for internal security and border management for the EU. A new biometric Entry/Exit System (EES) is being developed by eu-LISA. The EES will register the time and place of entry and exit of all third-country nationals crossing external EU borders, facilitating control of authorised stay and the management of migration flows. The EES is expected to be operational in 2022 and EU Member States are already in the process of acquiring biometric border control solutions necessary for the implementation of the EES. Likewise, they will implement a new "European Travel Information and Authorization System (ETIAS) which will require all visa-exempt third-country visitors to obtain a prior authorisation to travel before entering the EU. The main aim of all these initiatives is to facilitate traveller flows in and out of the EU, while at the same time strengthening border control and internal security.

UAE: The Department of Civil Aviation - Ras Al Khaimah "RAK DCA" in the United Arab Emirates (UAE) is gearing up for touchless solutions through e-Services and mobile apps. Iris scan is already in-place for serious issues, and the scanning of biometrics through mobile apps is in progress. Given the need for touchless experiences, existing biometric programmes using fingerprints are planned to become touchless with the introduction of eGates via facial recognition.

Canada: Winnipeg Airports Authority has determined they will use biometric automated border crossing (ABC) eGates to check the facial biometrics of arriving travellers enrolled in the NEXUS Programme. The NEXUS programme is operated by the Canadian Border Services Agency (CBSA), expediting border crossings for pre-approved Canadian, American, and Mexican citizens with enrolled biometrics. Those travellers can pass through specially reserved lanes at airports when entering the country. CBSA has also planned a pilot implementation of their Chain of Trust seamless border clearance programme for low-risk travellers. The programme will include touchless arrival processes to address COVID-19 using the traveller's smartphone (identity verification, e-declaration), and the use of a biometric lane for border clearance.

Australia: The Department of Home Affairs (DHA) has announced a new enterprise biometric identification system (EBIS) to optimize passenger visa and border processing and detect criminals and national security threats. In 2019, Australia registered some 9.5 million visitors. In the next 10 years, the DHA predicts an increased number of applications whose identity verification and authentication processing will be ensured and sped up by the new system.

Uruguay: The focus has been on reducing the contact of the passengers with the immigration officials, using ABC eGates. The verification of the Digital Sanitary Declaration was integrated into the immigration control system at Carrasco International Airport. The intention is that if the initial implementation is satisfactory and the process proves to be efficient, it will be replicated at the other border control points in the country.

New Zealand: At Auckland, Wellington, Christchurch and Queenstown airports travellers will find eGates. Those traveller's over 12 years of age and has an ePassport from a list of specified low-risk countries can use eGates. eGates use facial recognition technology to match your live image to your ePassport, thus reducing the need for face to face examination by an officer.

Aruba: The first end-to-end journey initiative is the Aruba Happy Flow programme which aims to develop a touchless end-to-end solution that leverages biometrics. Phase one, which is currently operational, enables a touchless experience for outbound travellers for one airline, and a touchless immigration experience for most of the inbound and outbound travellers using ABC eGates. Phase two, currently in development, will expand the biometric-enabled trusted digital identity touchless journey to include car rental, hotel check-in, health declaration, and departure immigration processes.

Key benefits

WTTC's focus on the entire, end-to-end travel journey allows for several important benefits that impact stakeholders to varying degrees.

Improves safety and security:

Leveraging biometric enabled digital identities allows for more accurate confirmation of an individual's identity against their government-issued identity documents. Thus, reducing identity fraud - a priority for all border agencies. Outside of air travel, hotel and car rental stakeholders can use biometrically enabled check-in and in-journey experiences as a more secure method to ensure the identity and documentation of their travellers and create contactless interactions.

Improves healthy facilitation of travellers:

Touchless checkpoints among travellers and stakeholders reduces the likelihood of viral transmission. SSTJ solutions enable digital information sharing as opposed to the exchange of relevant paperwork as travellers move along their journey. Biometric enabled solutions to allow for a touchless experience, protecting both travellers and employees.

Achieves operational efficiencies:

Creates process efficiencies for the travel provider and transactional efficiencies for the traveller. This allows both the travel provider and the traveller to focus on the more meaningful aspects of their journey. As examples, airlines can board passengers much more quickly, in some cases recorded as up to 50% improvement[1]. Hotels can eliminate lengthy, transactional check-in experiences by implementing biometrically enabled check-in using pre-verified traveller data and focus on delivering a more personalized and elevated experience. Additional operational efficiencies can be realized from collaboration and data sharing between travel stakeholders.

Operational efficiencies also assist in infrastructure constraints. While COVID-19 has had a detrimental impact demand, all industry professionals anticipate a full recovery from COVID-19. Biometric solution deployment allows for more throughput, whether at a border crossing, security checkpoints, aircraft boarding, etc. At airports that have tested biometrics, data shows a near 35% improvement in travellers processed at critical touchpoints[2]. Similar benefits are expected for key cruise checkpoints, including faster and more secure border processing during embarkation and disembarkation.

Reduces and avoids costs:

Biometrics enables travel providers to perform their business at a lower risk and therefore lower cost. Airlines, cruises, and car rental companies avoid serving customers who do not have proper visas or present fraudulent documentation all of which are costly to stakeholders. Additionally, travel stakeholders can better manage their inventories and utilization of their assets by deploying them when needed, rather than securing assets that do not get utilised as expected. For example, a hotel can prioritize rooms to be cleaned based on the anticipated arrival of their guests based on the connected data.

Reduces data liability for both stakeholders and travellers:

When a digital wallet is decentralized, it allows the traveller to control the data elements contained within it. The traveller can decide what information to store and whom to share it with. This reduces the digital data footprint a traveller and travel stakeholder must maintain.

Creates commercial value:

An integrated travel experience enables a technology platform to send indicators to stakeholders in a traveller's journey as the traveller moves through their journey (with the traveller's consent). This allows travellers to have an improved experience while enabling travel stakeholders to enhance loyalty, customer satisfaction and operational effectiveness. Improved loyalty for a brand and improved customer satisfaction translates to a larger share of the traveller's wallet over time and lifetime value.

Improves customer satisfaction:

Leveraging the use of biometrics throughout the travel journey could lead to improved customer satisfaction in nearly all segments of the Travel & Tourism sector. Travellers value getting to their destination and enjoying the life experience that they are seeking.

Integrates digital identity platforms across the sector:

Perhaps the most significant benefit of the SSTJ programme is the integration of digital identities across all touchpoints in the traveller journey. Eliminating the need for siloed digital identity initiatives and burdening the traveller to create a digital identity with each stakeholder. A cross-industry integration of digital identities in an interoperable manner will allow a traveller to choose their preferred digital identity platform and use it across all their preferred travel partners and destination governments.

[1] NEXTT Preliminary Cost Benefit Analysis: Technical Report, November 14, 2018
[2] CBP

SSTJ response to Covid-19

The health and safety elements enabled by biometrics and digital identities are all critical in creating a foundation to control the future spread of disease. Identifying infected travellers and removing them from the travel ecosystem reduces the risk of spreading a virus and reduces the risk of future pandemics impact on the Travel & Tourism sector.

WTTC urges Governments around the world to adopt an internationally consistent, risk-based approach to COVID-19 testing that could replace traveller quarantine periods and disruptive travel bans. Lengthy 14-day quarantines and their often-sudden introduction are viewed by travellers as the primary disincentive to international travel and are having a devastating impact on the global travel industry.

WTTC encourages public/private partnerships to:

- Establish common criteria for determining the COVID-19 risk and epidemiological situation on a detailed global and regional level
- Implement common protocols for COVID-19 testing on departure, that when combined with already established health and safety standards implemented by the Travel & Tourism sector can eliminate the need for blanket travel restrictions and traveller quarantines
- Establish common standards and a digital framework for the collection and use of traveller information for contact tracing

COVID-19 testing should be at or ahead of departure, rather than at the point of arrival to protect the whole travel system and be affordable, reliable, scalable and produce rapid results.

WTTC also recommends a global framework to share electronic testing or vaccine certificates. These certificates should be internationally recognized. If a traveller has a test certificate from one country it should be recognized across borders and apply across industries and usages (e.g. events, return to work). Global requirements and standards for digital test and vaccine certificates need to be agreed upon without delay by governments and health authorities.

To support the return of demand to the Travel & Tourism sector, rapid, affordable, and reliable COVID-19 testing and tracing are important factors and should be led by government health authorities. Governments must therefore urgently take leadership in implementing rapid testing, with rapid results and robust COVID-19 testing solutions to support the safe return of international travel without the need for quarantines.

Note: WTTC supports the recommendations from ICAO Civil Aviation Recovery Taskforce (CART) and its 'Testing & Cross Border Risk Management Manual' for the globally consistent application of COVID-19 testing standards.

Testing

- Where required, WTTC recommends virologic COVID-19 tests
- WTTC does not recommend antibody testing at this time in accordance with WHO's recommendation
- In-line with ICAO's protocols published on May 27th, 2020, WTTC recommends that rapid tests should be used when they become reliable
- Tests used should be validated by a reputable agency, reliable, scalable to hundreds of tests per hour and allow for results within an hour
- If/when rapid testing is available, it is not advised for testing to take place at the time of departure due to operational viability unless real-time, rapid and reliable tests become available

Test/vaccine certificate

- Where required, test result certificates should be provided by the traveller directly to the government who provides travel clearance and in an electronic form using technologies which attach and authenticate a traveller's identity to their test result
- Due to the sensitivity of the data, Privacy by Design principles should be used and only information required by the government or travel stakeholder should be shared
- Self-declaration symptom questionnaires may be required until electronic forms are available. Questionnaires will include health-related questions for the shared with the departing and/or arriving government
- Self-declaration health forms may be used but are not recommended due to fraudulent concerns

Tracing

- Government and health authorities' collection of a traveller's contact information and with the checkpoints (e.g. a flight) encountered during their journey. Information should be collected in electronic form (e.g. Government App/ portal)
- In-line with ICAO's recent point of view, WTTC believes tracing information should be used to support public health authorities in contact tracing
- *Note: This should be in line with applicable data privacy protection rules per local regulations*

Conclusion

The use of biometric technology to verify a traveller's identity is essential in the sector's pandemic recovery and positioning the industry for success post-recovery.

The emergence of the COVID-19 pandemic in 2020 has raised awareness of the ways a digital traveller identity and biometrics can significantly benefit the Travel & Tourism sector in times of crisis. Biometrics and digital identities enable a seamless experience that enhances traveller safety and health.

Verifying a traveller's identity and sharing paper documents at various points in their journey creates bottlenecks, points of friction for the traveller, and exposes both employees and travellers to health risks. These can be detrimental to the traveller experience and serve as a significant deterrent for travel demand.

Biometrics and digital identities enable efficient and seamless identity verification, and traveller data sharing allow processes to become streamlined and improves the traveller experience while increasing traveller safety and security. An opportunity to address this situation lies in the application of existing and emerging digital solutions and new technology.

The health and safety components of SSTJ are paramount to the COVID-19 recovery assistance and rebuilding the trust and confidence of the traveller. The primary objective is to create the healthy facilitation of travellers across their end-to-end journey. A traveller's device, biometric scans, and technologically powered information sharing are additional tools to help stop the spread of a virus. The SSTJ enables core elements to facilitate a healthy journey, including:

- The enablement of touchless checkpoints
- Digital sharing of trusted health information including test results and vaccine health certifications
- Sharing of traveller information ahead of their journey

Furthermore, by integrating into stakeholder's ecosystems additional automation is possible. Stakeholders can use this opportunity to enhance the travel journey through personalization and customization of services. Such specialized services also add opportunities to upsell and cross-sell products and services.

2

BEST PRACTICES & RECOMMENDATIONS

Overview

The Safe & Seamless Traveller Journey initiative plays a critical role in developing foundational best practices, laying the groundwork for globally interoperable solutions. When including public and private sectors synergistic value, it has the potential for an unprecedented traveller experience. In today's COVID-19 environment, SSTJ solutions are a foundational element in the restoration of global traveller confidence, confronting notable challenges COVID-19 has presented (e.g. facilitating a safe and healthy journey).

It is important to note that depending on a country's regulations, the age of a traveller using biometric-enabled solutions may be limited. For this paper, we assume a traveller meets all age requirements for the country(ies) in which they travel, and we do not detail exception processing which will be a critical component to operationalising biometrics into the traveller journey.

PUBLIC AND PRIVATE SECTOR COLLABORATION

Engagement is required from both the public and private sector. There are a few key recommendations to be achieved in the collaboration through public-private partnerships:

- **Creation of global standards and frameworks:** The public and private sectors need to build global standards for data being the foundation for interoperability. Ensuring data elements can be ingested by each stakeholder (both public and private) is critical. In November 2020 ICAO released the Digital Travel Credential (DTC) standard, which presents an opportunity to accelerate digital travel identity using a global standard. It has the potential to be implemented electronically for existing e-passport holders as it is derived from the existing travel documents.
- **Development of partnerships for innovation:** The public and private sectors have different demands which all need to be accounted for in solutions. Working together with the technology industry will be critical for solutions to be designed with a customer-first by design philosophy
- **Public/private partnerships:** Partnerships will allow the public sector to leverage digital identity created by the private sector.

DATA COLLECTION AND SHARING

A core component of any biometric and digital identity solution is collecting and sharing traveller data. To facilitate the collection, storage and sharing of data, two emerging models became the backbone of the biometric traveller journey:

Per Trip allows a single journey token containing traveller data to be created in advance via mobile devices or in-person during their journey. Following the trip, the token containing the traveller data is purged.

Per Life allows travellers to enrol once, creating an authenticated and verifiable digital identity which can be used across several journeys until the traveller decides to purge the digital identity. It is important to note, that while the digital identity of the traveller may exist until the traveller chooses to purge it, components of the digital identity will require renewal. Any component which has an expiration date (e.g. passport, driver license, and credit card) will need to be renewed and may require re-authentication of one's identity.

To enable the Per Trip and Per Life models, traveller data needs to be stored and shared across multiple stakeholders. There are three data facilitation methods which enable both the Per Trip and Per Life models, which ensure the safe and secure passage of a traveller's data.

Data facilitation method:

Centralized

- Traveller data is centrally stored and managed by a 3rd party
- Travel providers connect to the databases via secure API connections
- There are two centralized providers:
    - Private corporation: Traveller actively enrols their digital identity which is stored by a 3rd party
    - Government: Traveller biographic and biometric data collected and stored on government-controlled databases (passive and active enrolment by travellers)

Decentralized

- Digital identity data managed by the traveller (e.g. on their mobile device) and stored in a digital wallet
- Traveller manages which data is shared to chosen stakeholders during the traveller's journey after providing consent

Hybrid

- Utilises multiple technologies and/or facilitation options across stakeholder systems throughout the travel journey
- Processes for integration not yet designed, so many options may exist

Per Trip

- Semi-federated model
- Traveller creates a single journey token in advance via mobile device or in-person at check-in
- Token lasts for duration of journey
- Token contains only required key biographic & biometric (facial) information
- Orchestration platform houses and maintains token

Per Life

- Federated model
- Traveller enrols once to create a verified "digital" identity
- Lives indefinitely / for the life of a travel document (e.g. passport)
- As documents expire (e.g. passport), reauthentication and establishment of identity occurs
- A digital wallet may contain any data a traveller chooses
- Traveller pushes only required data to a given stakeholder in advance of travel (through e.g. distributed ledger)

In today's environment, centralized is the most prominent data storage and facilitation method used by the private sector. Centralized platforms align with traditional strategies where consumers provide large institutions with personal data and each company owns and manages that data in exchange for customers receiving benefits.

The fundamentals of the decentralized data storage and facilitation method allow a traveller to have ownership and transparency over how their data is used and shared. However, the reality is that certain institutions, such as governments, will always have some form of centralized data (for example, retaining personally identifiable information based on national security and immigration policies). A government stores the data of its citizens and visitors who are paramount to national security and will, therefore, maintain ownership and management of their data. Since government validation of identity will always be a critical component of a traveller's journey, the reality is that end-state solutions will need to support a hybrid of centralized and decentralized data storage.

Data management

It is important to understand how a traveller maintains his/her digital identity, which is central to the SSTJ vision. In decentralized solutions, travellers manage their authenticated and verifiable data on their mobile device in their digital identity wallet. A digital identity wallet can be a comprehensive storage facility for all of the traveller's pertinent information. Data stored can include, but is not limited to, biometric, biographic, health, travel history, payment, and miscellaneous (e.g. loyalty information).

Information stored in a traveller's digital identity wallet should originate from trusted sources and be verifiable by any stakeholder who receives the data elements. All data should be stored following global decentralized standards and designed to ensure interoperability, including the secure passage of traveller data.

It is important to note that a traveller's digital identity wallet may exist within a single mobile app or across several integrated apps all containing various portions of the digital identity. To make this possible it is critical for the data to be verifiable and based on standards. For example, payment information may be stored in Apple Pay, health data in Apple Health, and government-issued IDs (e.g. passport, driver license, national ID, etc.) in a separate Travel Identity mobile app.

During a traveller's journey, data and/or zero-knowledge messages that are shared with stakeholders are sent from the mobile device and housed in a data escrow account (managed by a technology provider). For each data transaction between a traveller and a stakeholder, a separate data escrow account is created and assigned to an individual stakeholder. Data is securely sent and stored in the data escrow account per details consented to by the traveller. Access to the data escrow account (for a stakeholder) is granted using state of the art security measures (e.g. unique access keys).

Today, travellers store personal data across all stakeholders in their journey to unlock a less friction prone experience. Utilizing a comprehensive digital identity wallet allows travellers to minimize their digital identity footprint by leveraging a single storage source of all personal and private data. They share only those data elements or zero-knowledge messages a stakeholder requires for a given trip.

A common example would be to allow a traveller to only store their credit card information in their digital identity wallet, versus with each stakeholder to be used during booking. If stakeholders integrate with a traveller's digital identity wallet platform, the traveller continues to have a frictionless experience during booking while not having to maintain their credit card information with each stakeholder.

DATA PRIVACY

The risk of one's data continues to grow with the expansion of cyber attacks on both the public and private sectors. Over the past couple of years, there have been several successful cyber attacks to government and private sector platforms. Therefore, upholding the most recent and thorough data privacy standards must be observed by all SSTJ solutions. SSTJ solutions provide all stakeholders with the opportunity to reduce their data footprint while maintaining operational processes.

Technology and data create opportunities for every organization, and this will remain true in the future. However, attention to legal, ethical, and social aspects has become indispensable for successful innovations. The growing attention in the media and among policymakers demonstrates this. As an organization, you want to remain in control.

Nations all around the globe have issued or improved privacy legislation as an answer to fast-moving digital innovations. The most prominent, comprehensive, and strict privacy rules are imposed by the EU Regulation 2016/679, better known as the General Data Protection Regulation (GDPR). WTTC, as part of the SSTJ initiative, worked with Considerati (a legal consultancy specializing in Privacy in the EU) to help identify privacy aspects critical for SSTJ. Their analysis focused on data sharing and, to a lesser extent, biometric technology, all from a GDPR perspective.

Principles and rationale of the GDPR

For an organization to legitimately process personal data it is important to first have a purpose for the processing activity. The processing activity should be necessary to achieve the intended purpose. Secondly, one of the six legal bases to process personal data should be applicable. These legal bases are:

1. Consent.

2. Necessary for the performance of a contract (e.g. certain information is necessary to book a flight or a hotel room).

3. Necessary for compliance with a legal obligation (e.g. tax obligations).

4. Necessary for a vital interest of the person in question (almost exclusively applicable in life or death situations).

5. Necessary for the performance of a task in the public interest (e.g. law enforcement or border control).

6. Necessary for a legitimate interest (e.g. security or some types of marketing).

After successfully identifying a purpose and legal basis, the processing activity is most likely to be legitimate. However, there are many other requirements to fulfil to process personal data responsibly. An exhaustive list of these requirements goes beyond the scope of this article, but think about transparency, data management and data security requirements.

Biometric data to uniquely identify a person

One of the pillars of SSTJ is the use of biometric technology, more specifically facial recognition. The GDPR prohibits the processing of biometric data to uniquely identify a person unless one of the exceptions applies.

The only relevant exceptions in the context of SSTJ are either:

- Explicit consent by the user; or
- Whenever the processing of biometric data is necessary for reasons of substantial public interest.

The former is the only possible exception for private organizations. The latter is a possible exception for public organizations, depending on the context. For instance, biometric technology could be necessary for substantial public interests relating to border control.

INTEROPERABILITY

A core component of creating a successful ecosystem of solutions that are interoperable across governments and private sector stakeholders is ensuring multilateral, consensus-driven standards create and maintain trust between countries. These standards ensure that countries can maintain their security while facilitating the movement of travellers. For the foreseeable future, additional health protocols will need to be included, but any updating of standards must ensure that travellers will enjoy a safe and seamless experience.

To enable biometrics, digital identities and the touchless capabilities it provides to travel globally, each component of the traveller digital identity will rely on standards and next-generation systems and solutions, such as not limited to, the ISO (International Organization for Standardization)[1], the NIST Information Technology Laboratory (ITL)[2], the ICAO's passport digitalization[3], the IATA One ID[4], the Open Travel Alliance (OTA) cross-industry technology standards[5] and the Hotel Technology Next Generation (HTNG) for the hotel industry[6].

These programmes should be leveraged to rapidly develop interoperability for new components of the traveller digital profile, such as a health certificate and travel history.

Components of the safe & seamless traveller journey

To assist in the definition of SSTJ best practices we developed nine components a traveller encounters along their journey where biometrics digital identities should be accepted. At each of these checkpoints, the traveller can choose and use elements of their digital identity wallets if desired. In this section, we define the application of the Safe & Seamless

1. Enrollment

User enrolls into a biometric program, either in a passive manner (e.g. government programs which collect traveller data from government issued documents) or actively through a digital identity management program using government issued IDs as the foundation of their identity

2. Booking

The act of a traveller making a purchase with a travel provider

3. Permission to travel

Traveller leverages their biometric digital identity components to apply for documents such as a visa or electronic visa

4. Check-in

Traveller actively engages the travel provider within a short time period (typically 24 hours) prior to the traveller's experience beginning

5. In-journey experiences

Traveller's interactions, with a travel provider, once their journey with the given travel provider has begun. For example: aircraft boarding, car rental facility exit, cruise embarkation, on-property purchases, in-flight purchases, etc.

6. Security checkpoint

Government mandated security checkpoint a traveller encounters during their journey

Note: these checkpoints can be operated by government agency or private contractors

7. Border crossing

Border crossings which are controlled by governments where individuals are required to identify themselves to officials

Note: Where open borders agreements exist (e.g. EU) allowing travellers to cross without showing identification are out of scope for STJ

8. Check-out

Traveller ends a portion of their journey with a particular travel provider

9. Traveller data management

Traveller controls their data being stored locally on their device, transfer to travel providers and/or governments, and storage by travel providers

[1] https://www.iso.org/home.html
[2] https://www.nist.gov/
[3] https://www.icao.int
[4] https://www.iata.org/
[5] https://opentravel.org/
[6] https://www.htng.org/

1. Enrolment

There are several ways and times within the traveller journey in which a traveller can enrol in a digital identity programme. Enrolment via mobile device ahead of departures is the preferred method. WTTC does acknowledge that there will always be travellers who either do not have access to a mobile device, are slow to adopt the mobile solutions or are travelling in a location where they choose not to use their mobile device. Therefore, kiosks and other in-person enrolment options will exist. These in-person enrolment options also support in-travel enrolment, which may be more prevalent in the early stages of traveller's adoption of digital identities.

To achieve the greatest benefits from SSTJ, we recommend travellers enrol ahead of their journey, allowing them to use their digital identity through the end-to-end traveller journey. Enrolment ahead of travel enables a traveller to use their digital identity pre-travel, including booking and Electronic Travel Authorisation (ETA) when required. Pre-travel enrolment also supports the airline and airport industry's long-time initiative to move as much pre-departure activities off-airport as possible. Lastly, the earlier in the journey a traveller enrols and establishes a digital identity, the more he/she will assist in creating a streamlined traveller experience, reducing points of friction, and easing the anticipated future strain on infrastructure.

There are several minimally required steps when a traveller enrols and establishes their digital identity.

1. Travellers must establish their identity using a government-issued ID (e.g. passport, driver license, national ID card)
   Note: When using government-issued IDs, technology platforms should leverage existing standards to ensure interoperability, global acceptance, etc. For example, the use of ICAO's DTC standards for uploading passport information via the e-Passport chip using mobile device NFC technology.

2. Biometric matching should be done using liveness detection capabilities

3. All customer information originates from an authenticated source and is trusted and verifiable by any receiving stakeholder in a traveller's journey

4. Traveller consent to the storage and use of their digital identity, including details on their "right to be forgotten"

Lastly, based on a traveller's itinerary (stakeholder and destination), there will be requirements for the data elements contained within their digital identity (detailed list in appendix):

Example of data component requirements based on stakeholder

Car rental:
General biographic information; driver license; a form of payment

Hotel:
Name; proof of age; proof of identity; a form of payment; passport (where applicable)

Cruise:
General biographic information; passport; visa (where applicable)

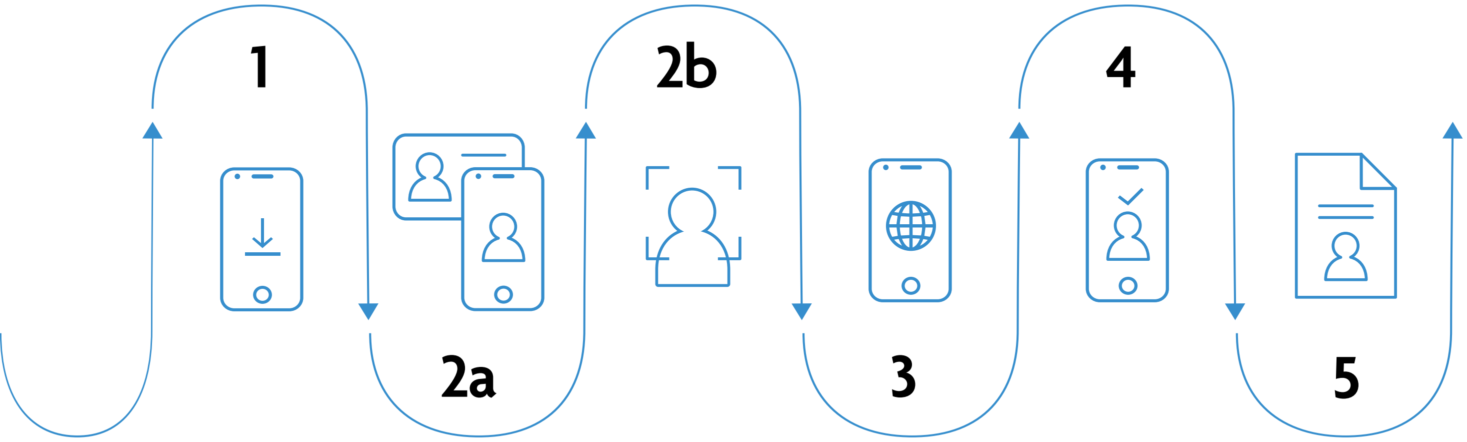
Airline:
General biographic information; booking reference; passport/driver license/national ID (location dependent)

Domestic itinerary:
Digital identity can be established using a National ID/driver license and/or a passport

International itinerary:
Traveller's digital identity contains an authenticated passport

Identity assurance level: Based on the touchpoint and stakeholder a traveller interacts with will require different levels of identity assurance. For example, a border-crossing will require the highest level of identity assurance, while checking into a hotel may require a lower level of required identity assurance

1. Enrolment



1 Traveller downloads digital identity application on their mobile device

2a Traveller uploads government issued identification (e.g. passport, national ID, drivers license, etc.)

2b Traveller captures a selfie

3 Digital identity provider authenticates traveller's enrollment (e.g. authenticates government issued ID and selfie based on ISO standards such as liveliness detection and matching technology to uploaded government issued IDs)

4 Traveller receives confirmation of digital identity enrollment

5 Traveller connects (e.g. Apple Pay) or enters additional personal information into their digital identity wallet such as payment, address, phone number, loyalty, etc.

2. Booking

Booking is the point of conversion in the sales process between the traveller and the stakeholders. WTTC recognises the immense amount of investment stakeholders undertake to refine their traveller's booking experience.

The recommended best practice is to continue using each brand's unique traveller booking experience and leverage technological solutions which incorporates a digital identity into existing technologies and processes.

Travellers begin by creating their digital identity wallet as described in the enrolment process. One of the core principles of the Safe & Seamless Traveller Journey initiative is for all solutions to be interoperable and use global standards. This allows data elements from a traveller's digital identity wallet to traverse stakeholders across the Travel & Tourism sector and the array of a stakeholder's booking solutions (e.g. online, call centre, travel agent, etc.). As traveller information is needed during the booking process, it is requested by the stakeholder via a transparent consent request.

A traveller can then consent to sharing the requested data with the stakeholder, providing the traveller full transparency over what information is being collected and its use. Once consent is provided, the data elements are securely transferred to the stakeholder allowing a booking to be confirmed.

Traveller use of a digital identity during the booking process allows a traveller to no longer need to store personal data with each stakeholder. Thus, reducing the traveller's digital data footprint and reducing time in the management of the same information across travel stakeholders. From a stakeholder perspective, it decreases their data liability by reducing the storage of personal information which provides limited business intelligence value, while maintaining a strong customer experience.

Booking (continued)

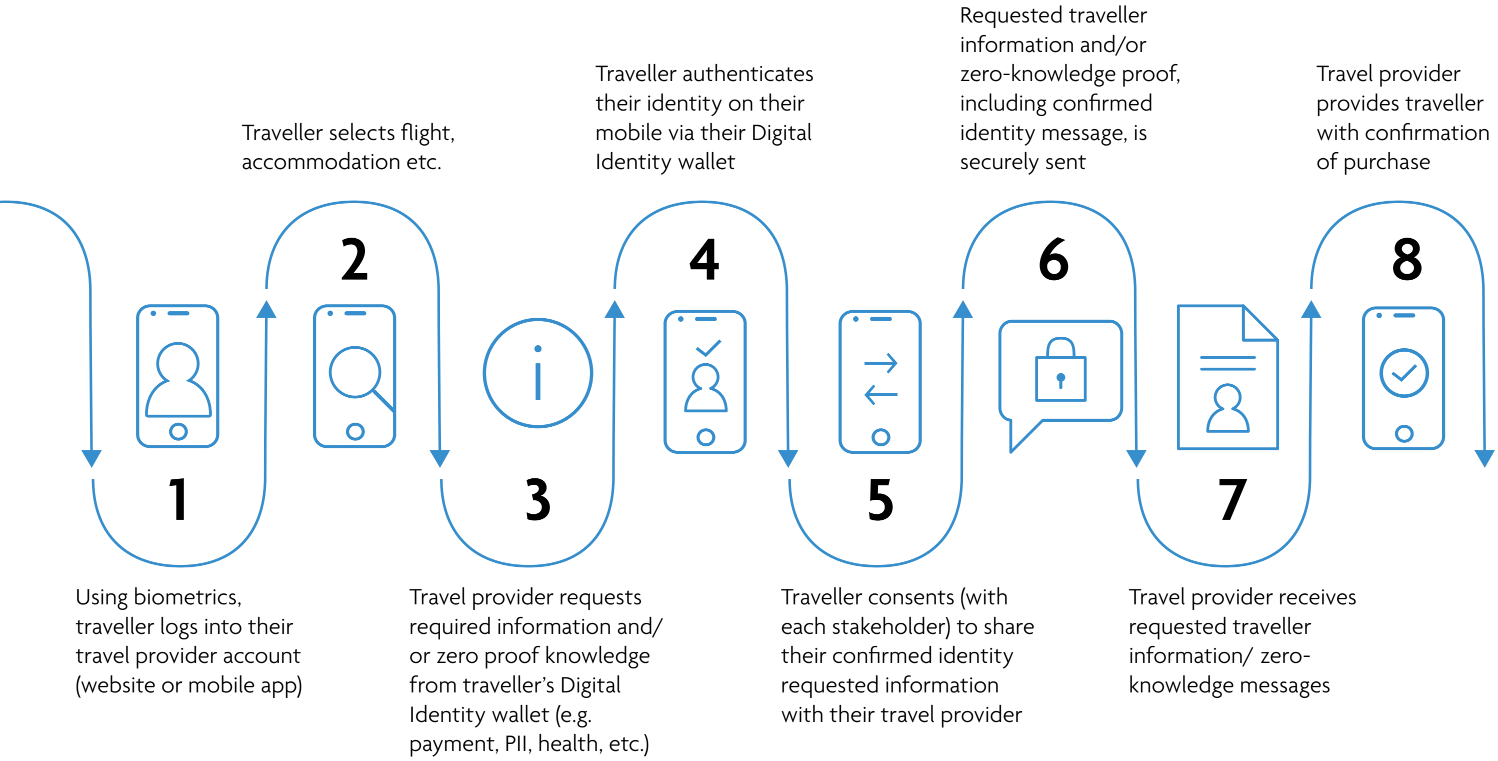
Examples of what a fully transparent traveller information consent request may include are:

- Data elements
- Duration of data element storage by a stakeholder
- The zero-knowledge message requested (e.g. a message confirming traveller's information based on business rules without sharing traveller's data)
- Criteria for accessing information if only needed in certain scenarios (e.g. a hotel can access an international traveller's passport data elements if a local authorities requests)

Illustrative example

Today: a traveller provides their drivers license information to their car rental company, providing proof of a valid drivers license and allow the car rental company to store that information in the event the traveller has a car accident

Future with trusted digital wallet: a traveller books a rental car and using the driver license data in their trusted digital wallet, a zero-knowledge message is provided that the traveller has a valid drivers license and the corresponding data exists to prove it. The traveller consents that during the rental and for a defined period thereafter, the required data from the traveller's driver license data is securely stored in an "escrow" account and only accessed by the rental car company if required (e.g. an accident occurs). Following the "escrow" period, the data in the "escrow" account is purged.



Traveller selects flight, accommodation etc.
Traveller authenticates their identity on their mobile via their Digital Identity wallet
Requested traveller information and/or zero-knowledge proof, including confirmed identity message, is securely sent
Travel provider provides traveller with confirmation of purchase
2
4
6
8
1
3
5
7
Using biometrics, traveller logs into their travel provider account (website or mobile app)
Travel provider requests required information and/ or zero proof knowledge from traveller's Digital Identity wallet (e.g. payment, PII, health, etc.)
Traveller consents (with each stakeholder) to share their confirmed identity requested information with their travel provider
Travel provider receives requested traveller information/ zero-knowledge messages

Note: Traveller's can make booking on a computer and use their established identity and digital identity wallet through technologies existing technology (e.g. identity is established and consent is provided on a phone, using a QR code on a website that information can be transferred securely)

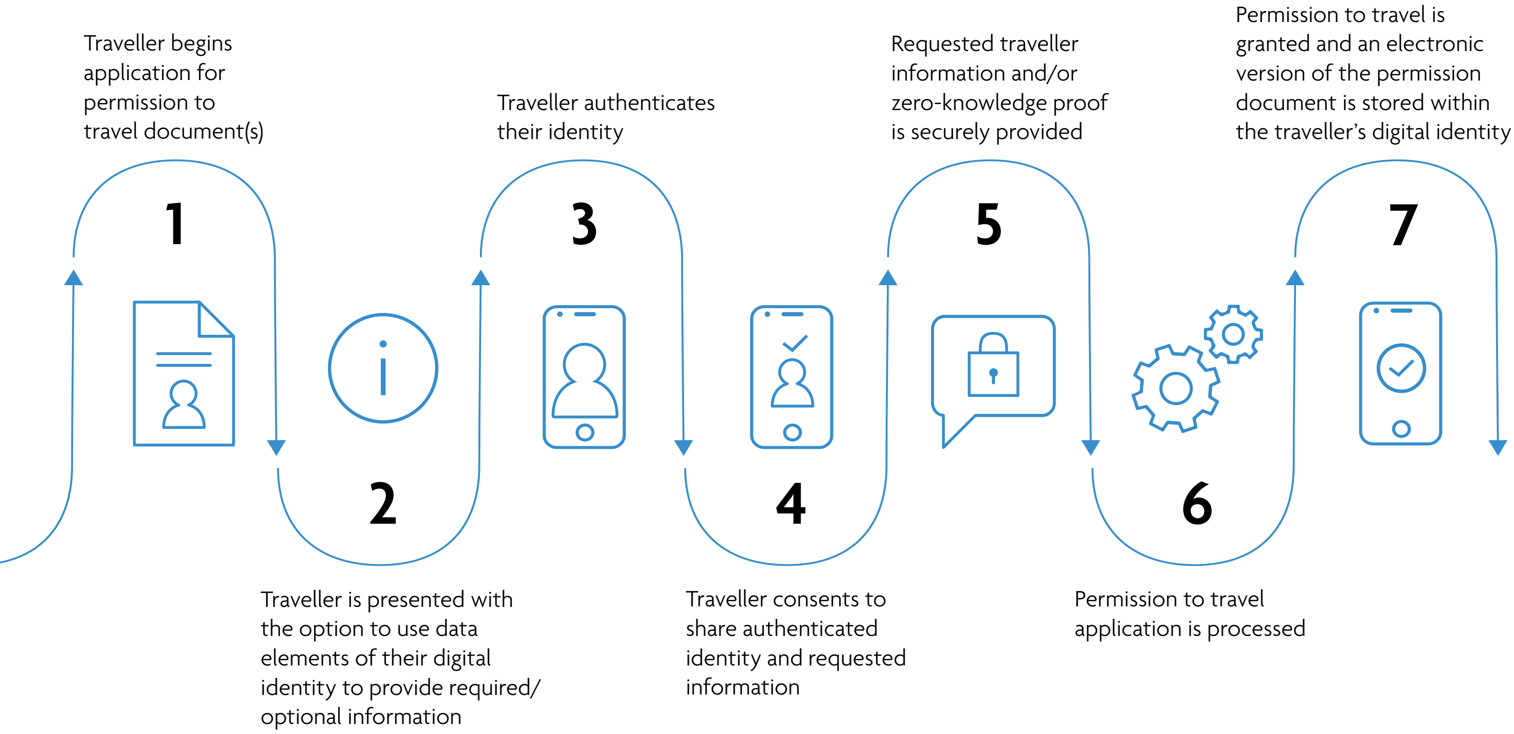
3. Permission to travel

Travellers who undertake cross-border trips may require permission to travel. WTTC advocates for governments to allow travellers to use trusted and verifiable data elements from their digital identity wallet in the application for permission to travel. For example, a traveller can use their biometric-enabled digital identity when completing their application for an Electronic Travel Authorisation in Australia using the new Mobile ETA app.

In the above example, a traveller using their digital identity wallet in their permission to travel application allows the application processes to be done without the physical exchange of identification paperwork. Leveraging a trusted and verifiable data element in a traveller's digital identity wallet can also reduce the processing time currently required.

Digital identities also provide government agencies processing permission to travel requests a high-level of identity authentication without the need for a traveller to appear in person in front of an agent. This reduces friction for the traveller and frees up agent resources for other critical activities. Furthermore, upon confirmation of successful permission to travel document, the associated document(s) can be electronically stored as part of the traveller's digital identity wallet.

Note: there are several occasions where for certain permission to travel applications to occur, in-person application may be required. For example, Visas requiring fingerprints.



1 Traveller begins application for permission to travel document(s)

2 Traveller is presented with the option to use data elements of their digital identity to provide required/optional information

3 Traveller authenticates their identity

4 Traveller consents to share authenticated identity and requested information

5 Requested traveller information and/or zero-knowledge proof is securely provided

6 Permission to travel application is processed

7 Permission to travel is granted and an electronic version of the permission document is stored within the traveller's digital identity

4. Check-in

Travellers can check-in using their digital identities in one of two avenues – mobile and on-site (e.g. airport kiosks, installed cameras, etc.). Considering the rising standards for health-conscious operations, WTTC's recommended best practice for check-in is leveraging a biometric infrastructure (mobile or on-site) enabling a touchless experience. When a traveller checks-in using their digital identity, regardless of method, stakeholders receive required traveller data, with the consent of the traveller, through a secure data transfer. Upon authentication of the traveller's identity and secure receipt of the required information, the stakeholder inputs the received data into their existing check-in processes. Ultimately leading to a touchless and frictionless check-in experience for the traveller.

Note: if consent is provided at the time of booking to share required information at check-in, and the traveller does not rescind their consent, additional consent is not required at time of check-in.

It is important to note that certain checkpoints may not provide the traveller with an option to use their mobile device to authenticate their identity. This is due to the need for a higher level of assurance than the mobile device can provide. To accommodate these checkpoints, one option is to have dedicated lanes with special cameras to capture a traveller's image at a high-resolution, resulting in a higher assurance of a 1:1 match to the traveller's image contained in their digital identity.

Multiple benefits are unlocked for both the travel provider and traveller. Travel providers can ease traffic flow at natural bottlenecks like check-in lines, allowing for redistribution of staff. The process is also less error-prone (e.g. inaccurate traveller information) as the identity of each traveller and his or her travel itinerary is authenticated and verified electronically by the stakeholder. Moreover, leveraging zero-knowledge messages allows travellers to maintain the highest level of privacy while travel providers de-risk their vulnerability to data breaches of sensitive traveller information.

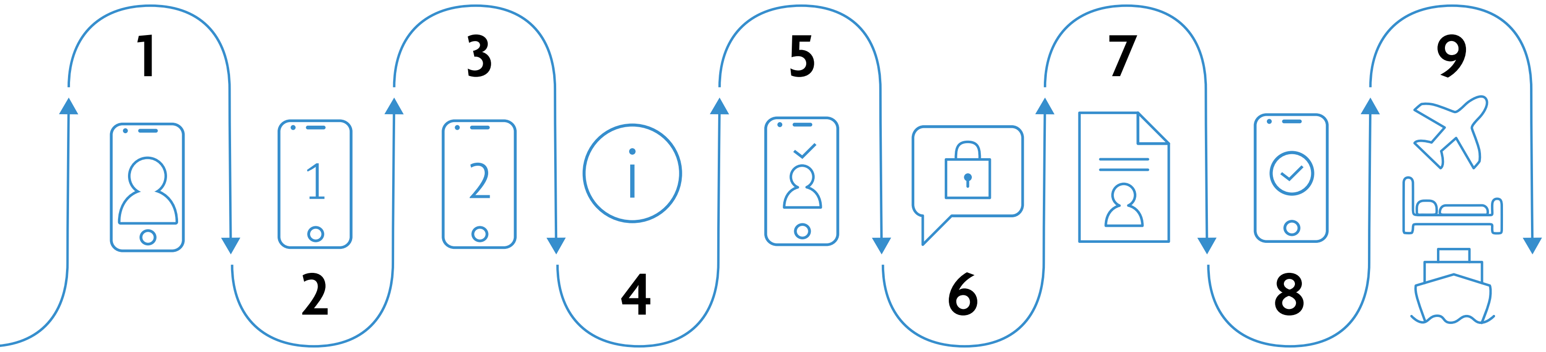
For travellers, the ease of check-in stems from using their digital identity wallet (possibly integrated into existing stakeholder mobile apps). Traveller's sharing their authenticated identity and required check-in information with their respective travel provider creates a frictionless experience (e.g. identity confirmation for an airline, proof of age for a retailor, proof of valid driver license for a car rental company, etc.). It also provides the ability for the traveller to take control of their in-person interactions with the stakeholders. Making those interactions more meaningful and value-added versus transactional. Moreover, as the sector moves to contactless processes, this advocated approach mitigates the risk of viral transmission (e.g. COVID-19), keeping travellers and travel providers' staff healthier.

Illustrative Examples

Airline: Traveller presented with boarding pass

Hotel: Traveller receives mobile room key

Cruise: Confirmation to present at port terminal



1 Using biometrics, traveller logs into their travel provider account (website or mobile app)

2 Traveller begins check-in process

3 Travel provider confirms check-in status and identifies any additional information required from traveller

4 Traveller presented with required information for check-in, and asked to authenticate their identity on their mobile via Digital Identity wallet

5 Traveller consents to share their trusted and verifiable information with their travel provider

6 Requested traveller information and/or zero-knowledge proof, including confirmed identity message, is securely sent

7 Requested traveller information and/or zero-knowledge proof, including confirmed identity message, is securely sent

8 Traveller successfully completes the check-in process

9

5. In-journey experiences

Today travellers are required to present several pieces of information throughout their in-journey experience with stakeholders. Most commonly these include payment, identification, and proof of age. These common points of friction occur at checkpoints such at the airport, in-air travel, hotel, and throughout the cruise experience. A prime example is a traveller who desires to purchase alcohol at duty-free and gets an alcoholic drink at an airport bar will have to present proof of age and payment twice in a single visit.

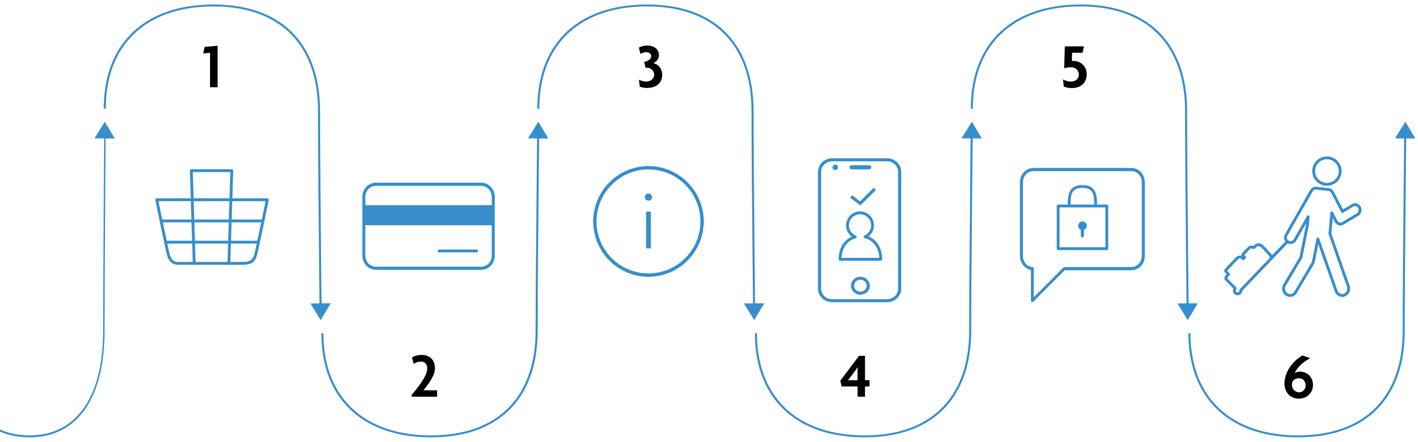
The SSTJ aims to eliminate these points of friction and remove the need for physical interaction between travellers and Travel & Tourism professionals. Leveraging one's digital identity, on their mobile device, a traveller can make purchases on the retailers' app, provide proof of age zero-knowledge messages, confirm identity, and share payment details in a secure and touchless fashion. Retailers retrieve the traveller's information in a seamless fashion given the digital identity's interoperability, thus facilitating a frictionless and touchless sales process. All while increasing customer satisfaction and being able to operate a more streamlined operation.

One additional benefit, which can be achieved when stakeholders across the traveller's journey participate in SSTJ solutions, is the ability to receive intelligence regarding traveller movement. Like beacons previously used in airports, as travellers pass through checkpoints in their journey subsequent stakeholders can receive notification of their progress. For example, if a traveller purchases a coffee on a retailors app at an airport airside, when the traveller passes through the security checkpoint, the retailer receives a notification and fulfils the traveller's order. This notification not only increases the likelihood of a traveller's coffee being fresh when they arrive, increasing customer satisfaction but also allows for operational efficiencies.

Illustrative example

Today: a traveller desires to purchase a sandwich and drink from an airport retailer, located airside. Traveller makes the touchless purchase using the retailers app and picks it up from the retailer

Future with trusted digital wallet: a traveller makes their desired food and beverage purchase prior to airport arrival with an airport retailer located airside between airport security checkpoint and their departure gate. The traveller provides a general estimated time of arrival to the retailer at time of purchase, along with payment information from their trusted digital wallet. As the traveller passes through the airport security check-point, a notification is sent to the retailer of the traveller's location and an accurate estimated arrival time. The traveller picks up their purchase in a touchless manner, which is freshly prepared due to the retailer knowing an accurate estimated arrival time of the traveller



1 Traveller identifies a desired in-journey purchase from a stakeholder

2 Traveller makes desired purchase for current or future consumption

3 Traveller presented with required information for purchase

4 Traveller authenticates their identity and consent to share required information (e.g. payment, proof of age, etc.)

5 Requested traveller information is securely provided

6 *Optional for future consumption purchase:* As traveller interacts with a touchpoint in their journey ahead of the retailer, a notification is sent to retailer with an accurate ETA of the traveller's arrival

6. Airport security screening

Security checkpoints promote the safe facilitation of travellers in their journey. The scope of safe facilitation has broadened beyond the promotion of physical safety. In the wake of the COVID-19 pandemic, facilitating travellers' health is critical. Traditionally, security checkpoints are a point of friction for the traveller, bottlenecks in airport operations, and strategic locations to ensure the safety and security. Considering COVID-19, these checkpoints are also prime locations for high physical touchpoints and extensive interaction between people.

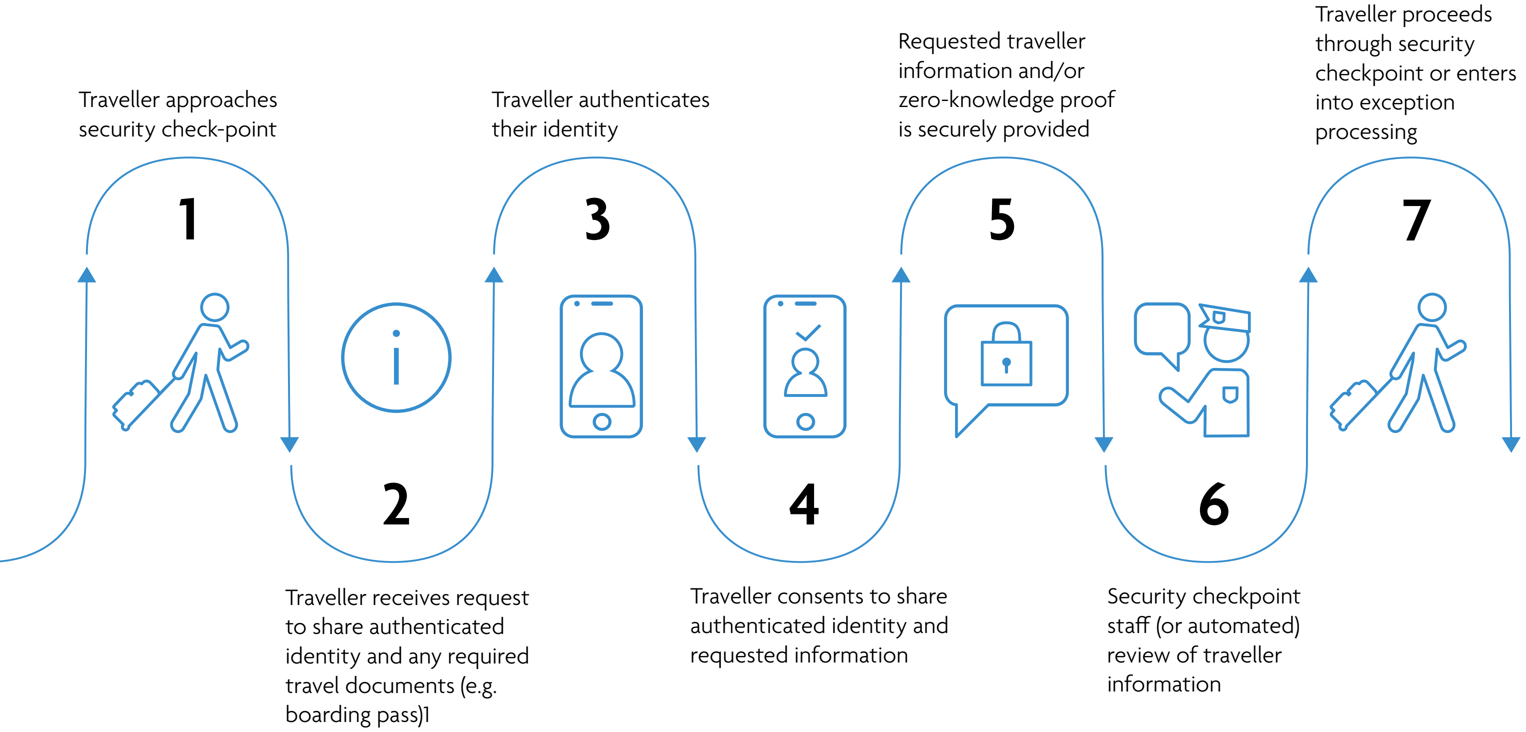
Biometric enabled digital identity promotes the elimination of physical interaction, currently required at security checkpoints, to authenticate a traveller's identity and travel documents.

Note 1: Travellers consent to share their authenticated and verifiable identity and other required data elements from their digital identity (e.g. related travel document information) with agents via automated eGates.

Note 2: If consent is provided at the time of booking to share required information at the security checkpoint, re-consent is not required unless the traveller revoked consent before arrival at the checkpoint.

Introducing automation to this segment of the journey greatly benefits the security checkpoint personnel in three critical ways.

1. The integrity of the traveller information originates from an authenticated tamper-proof government-issued identification documents reducing elements of identity fraud.
2. Technology-enabled identity verification provides higher levels of accuracy when verifying one's identity.
3. Automation increases the efficiency of traffic flow, reducing overall wait time, and creates bandwidth for existing security agents to focus on high-risk profile travellers. Reduced physical contact between travellers and agents helps to mitigate the risk of viral transmission.


Traveller approaches security check-point
1
Traveller receives request to share authenticated identity and any required travel documents (e.g. boarding pass)1
2
Traveller authenticates their identity
3
Traveller consents to share authenticated identity and requested information
4
Requested traveller information and/or zero-knowledge proof is securely provided
5
Security checkpoint staff (or automated) review of traveller information
6
Traveller proceeds through security checkpoint or enters into exception processing
7

7. Border crossing

Border crossings promote the sovereign security and safety of its citizens and travellers. As travellers approach a border crossing, they use their digital identity to share the required authenticated and verifiable information from their digital identity wallet. This allows the use of automated border control processes versus manual traveller identification and processing.

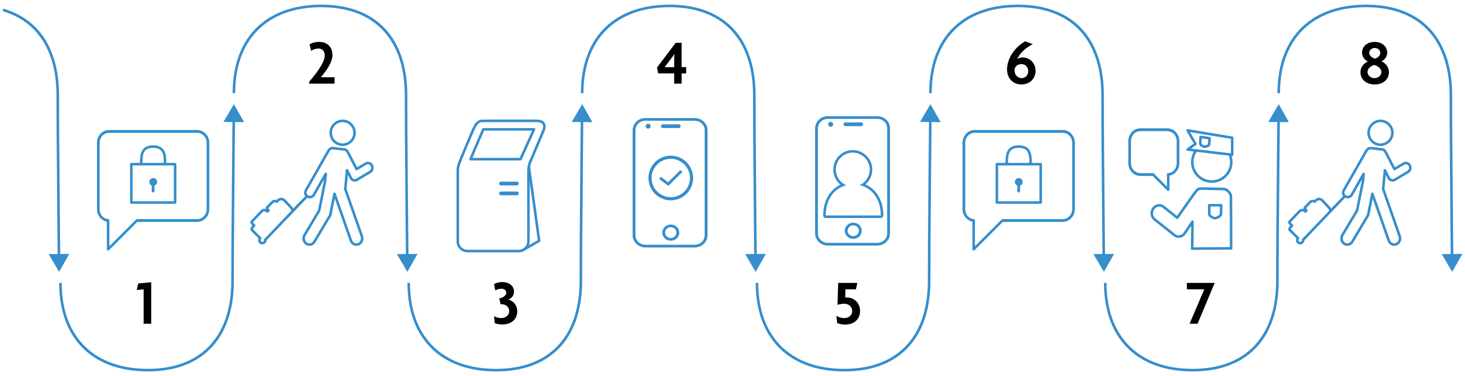
There are several components of SSTJ which increase border safety.

1. Before the traveller's arrival, the local authority can receive the traveller's information.

2. Increased efficiency in the movement of travellers at checkpoints, promotes improvement in travellers' satisfaction.

3. Increased automation allows existing resources (agents) to dedicate time to high-risk profile travellers.

4. Increased accuracy of biometrics to confirm one's identity reduces identity fraud.



1 *Optional*: pre-arrival, traveller information is shared with the arriving government[7]

2 Traveller approaches border crossing

3 Traveller chooses to use Automated Border Control process

4 Traveller consents to share required information by border agency

5 Traveller authenticates their identity using the government's ABC method (e.g. mobile, kiosk, eGate, etc.) and shares required information

6 Government receives authenticated identity and other required information and or zero-knowledge messages

7 Border agent (or automated) review of traveller information

8 Traveller proceeds through border control or enters exception processing

[7] Image "gallery" of arriving traveller's can be created using pre-arrival shared digital identity images, allowing faster and more accurate 1:1 matching

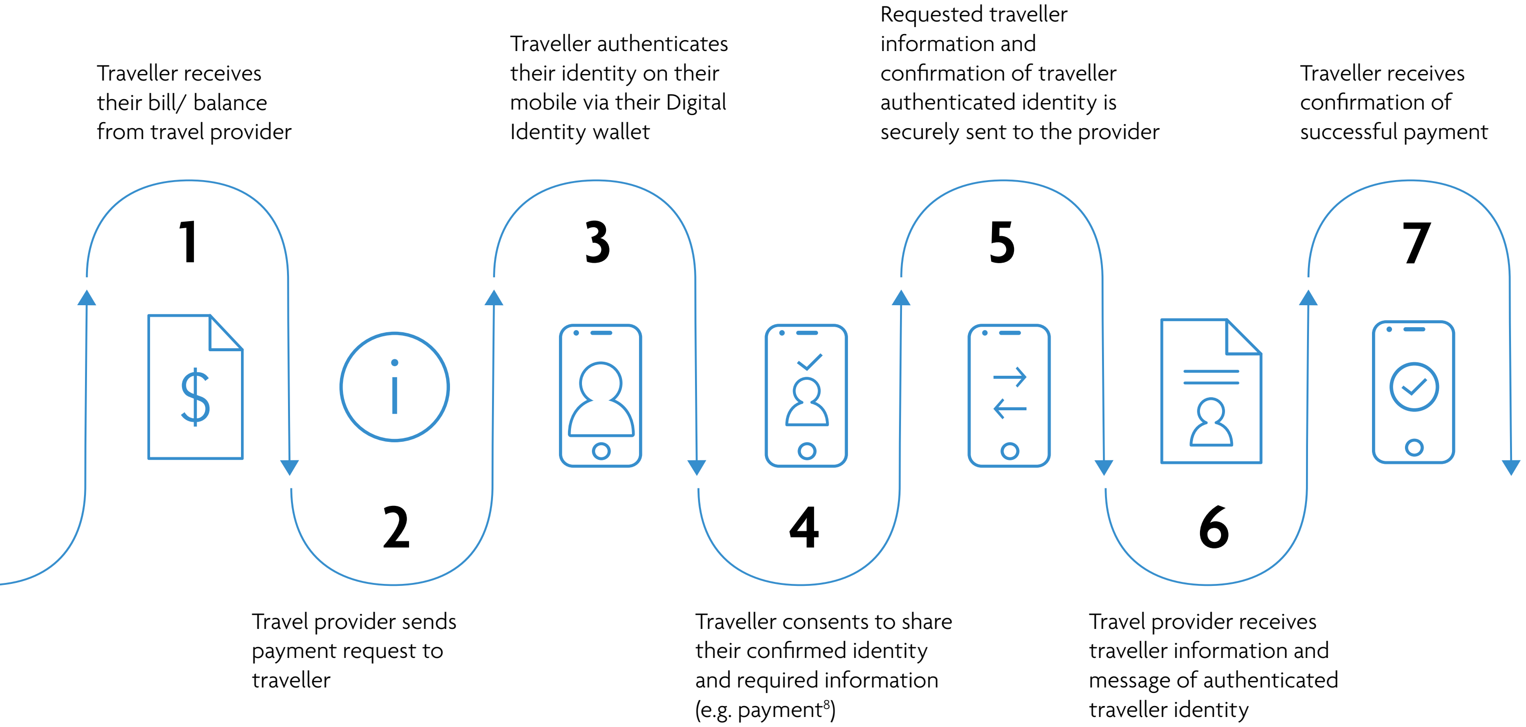
8. Check-out

At check-out, a traveller is completing a portion of their journey with a given stakeholder. Typically, travellers are presented with final confirmation of departure and, if applicable, a final payment.

WTTC advocates for travellers and stakeholders to leverage their digital identity wallet to facilitate the check-out process (e.g. payment).

Doing so allows for a seamless transaction, reducing the friction of check-out processes and is done in a touchless manner. Using a digital identity to facilitate personal data in a one-time transaction at check-out, versus storing locally for the duration of a traveller's journey (starting at check-in), can assist in reducing a stakeholder's data liability.

Following a successful check-out, any Per Trip identity tokens created for use during the traveller's specific journey with the stakeholder is purged. Ensuring the purging of Per Trip tokens is critical in maintaining the highest levels of privacy and traveller trust.


Traveller receives their bill/ balance from travel provider
1
$
Travel provider sends payment request to traveller
2
Traveller authenticates their identity on their mobile via their Digital Identity wallet
3
Traveller consents to share their confirmed identity and required information (e.g. payment[8])
4
Requested traveller information and confirmation of traveller authenticated identity is securely sent to the provider
5
Travel provider receives traveller information and message of authenticated traveller identity
6
Traveller receives confirmation of successful payment
7

[8] If as part of the travel provider check-in process, the travel providers requests final bill settlement payment information, and if consent is provided by the traveller, the payment information can be automatically provided at check-out without traveller interaction

CUSTOMER-FIRST BY DESIGN

The final, and possibly most critical principle of success is ensuring the customer is at the centre of any biometric and digital identity solution design. It is important to understand that there are two critical users, the stakeholder and the traveller. In this paper, we focus on the traveller, but the stakeholder user should be kept in mind during design.

To inform the design process, it is important to illustrate how a traveller may use their biometric-enabled digital identity across the several components listed herein. Two personas and corresponding use cases were developed to demonstrate the interactions throughout a journey. WTTC recognizes there are an array of adoption scenarios when it comes to the enablement of SSTJ solutions across the Travel & Tourism sector. The two personas and corresponding use cases are available in section IV of this report to illustrate the wide spectrum in a traveller usage of a digital identity during their journey.

PATH FORWARD

There are several steps governments, industry associations, standard-setting bodies, technology companies and travel providers will need to take to achieve the SSTJ vision. Requirements (technical, privacy, data, etc.) for each of the components of a digital traveller profile, such as health certificate and travel history, must be defined in partnership with industry experts outside of travel.

Two critical stakeholders are governments and travel providers:

- **Travel providers** need to execute two critical pieces of work:
    1. Provide input into the development of standards, to ensure that they are workable for the industry
    2. Develop their biometric digital identity strategies, fully endorsed by their organizations. These strategies must be customer-centric while considering shifting post-COVID-19 government requirements
- **Governments** need to focus on key regulations required for biometric-enabled solutions to be widely accepted as they may differ per country and region. The adoption of biometrics systems begins with a national strategy that enables discussions between countries about bilateral or multilateral agreements.

To clearly define the building blocks required to achieve the long-term vision, we broke down the required high-level activities in three phases each with their key objectives.

SSTJ Vision in a phased approach:

Near-term
0-2 years

- Create private sector coalitions and champions to advocate for solution investment
- Development of solutions applicable to air and non-air stakeholders
- Identify and launch end-to-end pilots of biometric digital identities across the private sector and with willing government participants
- Engage governments in Digital Travel Credential education & border pilots
- Include early health/vaccination e-certificates where possible and available
- Educate travellers on biometrics and its use in travel – e.g. myth busting, benefits, etc.

Mid-term
2-5 years

- Integration of government and private sector solutions (e.g. border crossing within digital identity wallet and Digital Travel Credential)
- Global agreements and standards on Health certificates and future protocols
- Pilots move into full scale production use starting with major travel centres

Long-term
6+ years

- Acceptance of decentralized digital identity solutions across all Travel and Tourism sectors and governments
- Adoption by a significant portion of the travelling public
- Adoption of decentralized digital identity wallets as sources which contain authenticated and verifiable data across the public and private sector stakeholders

Within each phase, we identify those high-level activities which pertain to each core stakeholder in the SSTJ ecosystem. The four stakeholder groups are, governments, travel stakeholders, technology stakeholders, and travellers. While we outline key high-level activities for each stakeholder group, collaboration across stakeholders will be critical to SSTJ's success.

Government path forward activities:

Near-term
0-2 years

- Governments to identify key "owners" and advocates to own seamless travel related legislation changes and pilots
- Include strategic components in design now for new systems (eg ETA, EES), even if implementation is later
- Support industry onboarding by allowing government ID verification electronically (e.g. PKD verification structure)
- Implement touchless interaction for borders, immigration & security screening
- Accept industry derived DTC Virtual Component to encourage adoption by traveler and use in One ID programs
- Innovation taskforce(s) for funding
- Global governance framework definition

Mid-term
2-5 years

- Complete legislative changes as needed to facilitate seamless travel models fit to the country
- Pilots moving to full implementation for permission to travel applications to use electronic IDs/DTCs (Digital Travel Credential)
- Health certificates have a global standard electronic format and verification process
- 50% of low-risk travelers submit pre-arrival border declarations electronically and can be cleared for accelerated border processes
- Security clearance checkpoints have opt-in biometric processing lanes for travelers participating in seamless travel pilots and programs

Long-term
6+ years

- Travel permissions in electronic format that generates a verifiable credential
- 90% of low-risk travelers interact with border agencies in advance of arrival and receive confirmations for biometric based border clearance
- Updated data sharing agreements between countries allow for limited use exchange of data to support biometrics and digital identities

Technology stakeholder path forward activities:

Near-term
0-2 years

- Development of solutions designs applicable to air and non-air stakeholders
- Pilots identified, started and expanded
- Travel sector can derive Digital Travel Credential as part of traveler onboarding and store in digital wallet
- Traveler gives permission to share required information to individual travel providers for a trip
- Educate private sector on SSTJ strategic roadmaps and included in designs now for next phases

Mid-term
2-5 years

- Drive the increase of zero-knowledge messaging adoption
- Increase traveller centric solutions which allow traveller to adopt a "single digital identity app"
- Integration into existing travel provider technology solutions (e.g. booking solutions via web and app)
- Integration into non-travel provider stakeholders (e.g. third-party)
- Traveler gives permission to share required information to a list of travel providers for a trip or multiple trips

Long-term
6+ years

- Shift from centralized to decentralized storage, as the main form of traveller data storage
- Full end-to-end journey stakeholder connections
- Integration of advanced analytics and notifications across stakeholders in a journey

Travel provider path forward activities:

Near-term
0-2 years

- Create sector coalitions and champions to advocate for digital identities within each sector of the Travel and Tourism industry
- Identify and advocate for investment in digital identities
- Identify and begin end-to-end pilots of biometric digital identities
- Integrate governments (e.g. border crossing) as possible

Mid-term
2-5 years

- Cross sector connections with stakeholders to unlock technology benefits across the SSTJ ecosystem
- Lobby governments to connect to existing and future planned digital identities
- Advocate with key customers to drive adoption of Seamless Traveller journey solutions
- Incorporate decentralized digital identity platform into existing technology platforms (e.g. website and mobile app)

Long-term
6+ years

- Incorporate opportunities for Seamless Traveller Journey solutions to inform operating plans (e.g. through data analytics and traveller movement notifications, etc.)
- Expanded use of zero-knowledge messages versus the secure transfer and storage of traveller personal data

Traveller path forward activities:

Near-term
0-2 years

- Educate travellers on
  - Outline how Seamless Traveller Journey solutions allows for the safe and healthy facilitation of travel (COVID recovery)
  - Biometric use in the seamless traveller journey
  - Debunk myths with biometrics
  - Benefits
  - Privacy

Mid-term
2-5 years

- Drive adoption of decentralized digital identity wallet solutions through technology providers and travel stakeholders
- Consolidation of a traveller's personal data footprint from multiple stakeholders
- Consistent enrollment in Seamless Traveller Journey solutions across multiple journeys
  - Single-trip
  - Per life

Long-term
6+ years

- Enrollment in a "single" interoperable digital identity wallet
- Use of a "single" digital identity wallet across multiple travel stakeholders, across all sectors of the Travel and Tourism industry

APPENDICES

APPENDIX A:

Principle Data Privacy page 20 –
Analysis of the Biometric Digital Identity Facilitation Models

Data sharing

Another important aspect of SSTJ is data sharing. It would be detrimental for a 'seamless' travel journey if travellers must share their data repeatedly with the next partner whenever they enter the next step in their journey. It is important to note that both the data receiving party and the data sharing party need to have a purpose and a legal basis for the data transfer. In the context of SSTJ that legal basis would most likely be the consent of the user.

In the case of cross-border data sharing, it is important to be aware of different legal regimes in both countries. Within the EU there is, for the most part, harmonization of privacy legislation through the GDPR. However, outside of EU/EEA borders other – less strict - standards may apply. Some countries have received an adequacy decision from the European Commission, meaning they are considered to have a similarly high standard of data protection, such as Canada, Argentina, Japan, the United States of America (only for organizations within the Privacy Shield framework) and Israel. For cross-border data transfers (from within EU/EEA to the outside of those borders) to be legitimate, and adequacy decision or additional contractual safeguards (standard contractual clauses, provided by the European Commission) should be in place, among other more complex options.

Analysis of the models

The biometric digital identity solutions presented by the WTTC have three facilitation options: centralized, decentralized and hybrid. With each facilitation, option come different legal challenges and privacy risks, which should be mitigated in different ways. In this chapter, the most important challenges and risks shall be set out for each facilitation option. Please note that this is not an exhaustive list, but merely an overview of the most important or notable challenges and risks.

Centralized: The idea behind the centralized facilitation model is that traveller data shall be centrally stored and managed by one party. This party could be part of the SSTJ partnership or a third party. In many cases, this party shall be a government body. Because of the multitude of parties involved in SSTJ (air carriers, airports, border authorities, hotels, car rentals, cruise lines and more) that all process personal data for different purposes, legal bases and exceptions, it can be a challenge to determine which party is best suited to collect or store the personal data. Another challenge is determining the best moment and means of requiring and managing consent. Upon requiring consent, (a subset of) the personal data shall be distributed between the relevant involved parties.

Generally, consent is acquired during an enrolment procedure, either on-site on an enrolment kiosk, or remotely through an app or browser. Consent should always be freely given, informed, specific and unambiguous. Considering the plurality of partners a traveller encounters on a traveller journey, and the complexity of the data processing activities, it can be challenging to provide the traveller with complete yet comprehensible information on which the traveller can base their consent. Moreover, travellers always have the right to revoke their consent. SSTJ partners not only should inform travellers of this right to revoke consent, but the process of revoking consent should be just as easy for the traveller as to grant consent. For instance, if consent can be provided by a mere click of a button, revoking consent cannot require a traveller to log-in to a website, fill in a form, substantiate the reason for revoking consent, and subsequently take days to process before the data are ultimately deleted.

It is important to determine, either jointly or separately, where the controllership, duties and liabilities of one-party end and those of another party begin. Arrangements regarding governance, data security and handling data breaches are key, especially regarding centrally storing the data and data in transit.

Lastly, dealing with a multitude of (global) parties can be complex, even for lawyers. Transparency requirements demand travellers to be informed about the data processing activity and the parties involved, in a comprehensible way, and if the data processing activity is not based on user consent. Considering the complexity of SSTJ, this might prove to be a challenge, especially in a global travel and tourism context where travellers come from different places and speak different languages. Therefore, utilizing universally used icons is advised, as well as the use of clear and plain language.

Decentralized: In the decentralized facilitation option, the biometric digital identity of the traveller is stored on their mobile device. In this model, travellers can choose by themselves which mobile device and provider they like and trust. Effectively providing them with more control over their data. However, considering the complexity of SSTJ, providing more choices for the traveller can be overwhelming. Can it be expected of the traveller to fully understand the consequences of their choices and actions? This is not so much a legal as it is an ethical point. However, organizations do have an obligation to inform their users adequately and intelligibly, for them to be able to make an informed decision on whether to share their data.

Providing travellers with more choices might also mean that data controllers have fewer choices, for instance picking the mobile devices on which the (very sensitive) biometric data is stored. Each SSTJ partner that processes personal data of travellers, whether as a data controller data processor, should still ensure security for their own data processing activities, which might be problematic considering some mobile devices are more trustworthy than others.

Hybrid: In the hybrid model, multiple technologies or facilitation options are used throughout the travel value chain. As processes for integration are not yet fully developed, the specific challenges paired with the hybrid facilitation option are yet to be determined as well. However, it shall probably be a combination of the aforementioned two facilitation options.

Considerations: Safe & Seamless Travel Journey might hugely impact the way the Travel & Tourism sector develop itself soon. The benefits for both travellers and organizations in the travel sector are evident, but so are the privacy risks and challenges involved. There is a great variety of organizations with varying backgrounds and applicable legal regimes, that may deploy the technology for differing purposes and uses. Therefore, a case-by-case assessment of the specific challenges and risks is in order. The best way to assess the legality and identify the risks and recommended risk-mitigating measures of a specific data processing activity is to perform a Data Protection Impact Assessment or DPIA in short. In the context of SSTJ and the facilitation options, it is always obligatory to perform a DPIA, under EU law.

Besides performing a DPIA, key points to take into consideration are:

- Processing personal data should be lawful, fair, and transparent. Adequately inform travellers about the identity of the involved parties, their purposes, the way they handle and protect the personal data and the travellers' rights.
- Whenever the data processing activity is based on consent, ensuring the consent is freely given, informed, specific and unambiguous. Furthermore, consent should be logged, and revoking consent should be just as easy as providing consent.
- Data security. Both organizational and technical measures should be implemented to safeguard confidentiality, integrity, and availability of personal data.
- Personal data should be processed only for specified, explicit and legitimate purposes. No more data than necessary should be processed to achieve the intended purpose and the personal data are must be deleted upon achieving those purposes.

APPENDIX B:

Principal Interoperability page 21 –
Details for the components of a Safe & Seamless Traveller Journey

Enrolment:

Step		Description	Sample Benefits
1	Mobile download of digital identity application	Traveller chooses their desired digital identity management program and downloads the App	Provides travellers the ability for them to choose their preferred vendor
2a	Traveller identity establishment	Traveller uploads government issued identification (e.g. passport, national ID, drivers license, etc.) and consents for their document to be authenticated	Reduces the need to continually show identification along the travel journey
2b	Traveller captures a selfie	Traveller takes a selfie with their mobile for the purpose of establishing their identity	Reduces the likelihood of identity fraud
3	Traveller document and identity authentication	Digital identity provider authenticates traveller's enrollment and identity by • authenticating the government issued ID • selfie matching based on ISO standards (e.g. liveliness detection and matching technology to uploaded government issued IDs)	Creates a level of identity assurance allowing a traveller to utilize their established identity as touchpoints in their journey bypassing ID checks Note: touchpoints requiring high levels of identity assurance (e.g. border crossing) will require biometric matching using specialized cameras
4	Enrolment complete	Traveller receives confirmation of enrollment	N/A
5	Traveller provides/ links additional data	Traveller adds authenticated and verifiable personal data (e.g. payment, address, phone number, loyalty, health, travel history, etc.) or links existing trusted data sources (e.g. Apple Health, Google Pay, etc.) to digital wallet Note: adding information is a continuous process	Traveller can leverage existing components of their digital wallet in a single pace, without creating multiple instances of the same information

Booking:

Step		Description	Sample Benefits
1	Traveller logs into travel provider account	Traveller logs into their travel provider account (if applicable), using their biometrics as login credentials	Reduces username and password management; increases cyber security
2	Traveller identity establishment	Traveller makes their desired selection using the existing travel provider customer experience	Maintains existing/future CX investment and competitive advantage
3	Travel provider requests required information	Travel provider will request required information and/or verification of existing information to complete booking and consent for use, handling, duration of data storage, etc.	Data received originates from authenticated and verifiable sources
4	Traveller identity authentication	Traveller authenticates their identity, giving the travel provider high assurance of the traveller's identity	Eliminates current opportunity areas such as card-not-present fraud
5	Traveller consent	Traveller consents, with each stakeholder, to share their data in accordance with the travel provider intentions	Reduces stakeholder receipt of inaccurate traveller information
6	Secure messaging to travel provider	Traveller data and/or zero-knowledge messages are securely transferred to the travel provider and/or a data 'escrow' facility	Receives and stores only operationally required data while maintaining CX
7	Travel provider receives required information	Travel provider receives requested information and/or access keys if data in 'escrow' is required	Reduces data liability by only receiving required information on the traveler
8	Traveller booking confirmation	Travel provider provides traveller with confirmation of purchase and related travel information	N/A

Permission to travel:

Step		Description	Sample Benefits
1	Application process begins	Traveller begins application for permission to travel document(s)	N/A
2	Traveller presented with information required	Traveller is presented with the option to use data elements of their digital identity to provide required/optional information	Traveller retains control of what information, if any, is shared and with whom
3	Traveller identity authentication	Traveller authenticates their identity, giving the government or 3rd party a high assurance of the traveller's identity	Reduces the likelihood of identity fraud and promotes more robust security infrastructure
4	Traveller consent	Traveller consents to share authenticated identity and requested information	Reduces stakeholder receipt of inaccurate traveller information
5	Secure messaging of traveller information	Traveller data and/or zero-knowledge messages are securely transferred to the government agency or 3rd party	Reduces data liability by only receiving required information on the traveler
6	Application processing	Permission to travel application is processed	N/A
7	Permission to travel granted and stored in traveller's digital identity	Permission to travel is granted by government agency; the electronic version of permission document is stored within the traveller's digital identity	N/A

Check-In:

Step		Description	Sample Benefits
1	Traveller account log-in	Traveller logs into their travel provider account (if applicable), using their biometrics as login credentials	Reduces username and password management; increases cyber security
2	Traveller initiates check-in process	Traveller enters the stakeholder's standard check-in process	Promotes contactless process, mitigating risk of viral transmissions
3	Check-in status confirmation	Stakeholder confirms traveller's check-in status and identifies additional information required to complete check-in	Reduces information requirements by leveraging digital identity wallet thereby easing traffic flow
4	Traveller information and consent request	Traveller presented information request, consent message, and asked to authenticate their identity Note: step is only required if required information and consent was not provided during booking	Traveller retains control of what information, if any, is shared and with whom
5	Traveller consent	Traveller consents to share their data in accordance with the stakeholder intentions	Reduces stakeholder receipt of inaccurate traveller information
6	Secure messaging to stakeholder	Traveller data and/or zero-knowledge messages are securely transferred to the travel provider and/or a data 'escrow' facility	Receives and stores only operationally required data while maintaining CX
7	Travel provider receives required information	Stakeholder receives requested information and/or access keys if data in 'escrow' is required	Reduces stakeholder data liabilities by receiving zero-knowledge message of required information
8	Check-in complete	Traveller and stakeholder successfully completes the check-in process and applicable stakeholder process occurs (e.g. hotel guest receives mobile key)	N/A

In-Journey experience:

Step		Description	Sample Benefits
1	In-journey purchase identified	Traveller identifies a desired in-journey purchase from a stakeholder (e.g. hotel F&B and/or spa, airport retailer, cruise retailer and/or F&B, etc.	Digital identity is linked to retailors allowing for seamless customer experience
2	Traveller executes purchase	Traveller makes desired purchase for current or future consumption	Purchases can be made in retailer App to keep existing CX experience
3	Required traveller information for purchase	Traveller presented with required information for purchase	Reduces fraud as all traveller data is authenticated and derived from trusted and verifiable sources
4	Traveller consent	Traveller authenticates their identity and consents to share required data such as payment, proof of age, etc. in accordance with the stakeholder intentions	Increases traveller transparency of information being captured and its purpose
5	Secure messaging to travel provider	Traveller data and/or zero-knowledge messages are securely transferred to the travel provider and/or a data 'escrow' facility	Reduces stakeholder data liabilities by receiving knowledge of only required information and existence of authenticated and verifiable data
6	Traveller movement notification to stakeholder	Optional for future consumption purchase As traveller interacts with a touchpoint in their journey ahead of the retailer, a notification is sent to retailer with an accurate ETA of the traveller's arrival	Increases retailer efficiency in fulfilling digital orders Increases traveller satisfaction with freshness due to more accurate consumer ETA

Security checkpoint – airport:

Step		Description	Sample Benefits
1	Traveller enters security checkpoint	Traveller approaches security check-point	N/A
2	Traveller identity authentication and information request	Traveller receives request to share authenticated identity, any required travel documents (e.g. boarding pass, including any consent required	Reduces touchpoints for staff and travellers Improved traveller movement efficiencies
3	Identity authentication	Traveller authenticates their identity	Increases level of identity verification as compared to human ID authentication
4	Traveller consent	Traveller consents to share authenticated identity and requested information	Increases traveller transparency of information being captured and its purpose
5	Secure messaging to stakeholder	Requested traveller information and/or zero-knowledge proof is securely provided to checkpoint staff or automated process (e.g. automated security gate)	Reduces stakeholder receipt of inaccurate traveler's information
6	Security review of traveller	Security checkpoint staff (or automated) review of traveller information	Allows for automated decision making with exception processing as required (similar to todays ABC, automated border control, eGates used during immigration process)
7	Traveller proceeds through security	Traveller proceeds through security checkpoint or enters into exception processing	N/A

Border crossing:

Step		Description	Sample Benefits
1	Pre-arrival information	Optional: pre-arrival, traveller information is shared with the arriving government	Government awareness of incoming travellers increases efficiency and security
2	Traveller enters border crossing	Traveller approaches border crossing	N/A
3	Traveller enters automated process	Traveller chooses to use Automated Border Control process	Automation creates bandwidth for border crossing personnel to focus on exception handling and high-risk travellers
4	Traveller consent	Traveller consents to share required information by border agency	Increases traveller transparency of information being captured and its purpose
5	Identity authentication	Traveller authenticates their identity using the government's ABC method (e.g. mobile, kiosk, eGate, etc.) and shares required personal information and/or zero- knowledge message	Reduces fraud as all traveller data is authenticated and derived from trusted and verifiable sources
6	Secure messaging to stakeholder	Government receives authenticated identity and other required information and or zero-knowledge messages	Reduces stakeholder data liabilities by receiving knowledge of only required information and existence of authenticated and verifiable data
7	Traveller information review	Border agent (or automated) review of traveller information	Authenticated and verifiable data Contactless interaction with traveller
8	Traveller decision (enter or exception processing)	Traveller receives notification to proceed through border control or enters exception processing	N/A

Check-out:

Step		Description	Sample Benefits
1	Traveller receives bill/ balance for payment	Traveller receives their final bill/ balance from travel provider	N/A
2	Traveller receives notice payment	Travel provider sends payment request to traveller	Reduces likelihood of erroneous payment requests
3	Identity authentication	Traveller authenticates their identity	Increases level of identity verification as compared to human ID authentication
4	Traveller consent	Traveller consents to share their confirmed identity and required information (e.g. payment information)	Increases traveller transparency of information being captured and its purpose
5	Secure messaging to stakeholder	Requested traveller information and confirmation of traveller authenticated identity is securely sent to the provider	Traveller reduces their personal data footprint by having a single storage mechanism for payment information Reduces liability of card-not-present fraud Reduces liability of storing traveller payment details while maintaining CX
6	Stakeholder receipt of payment	Stakeholder receives traveller payment information and message of authenticated traveller identity	Reduces data liability by only receiving required information on the traveler
7	Payment confirmation	Traveller receives confirmation of successful payment	N/A

APPENDIX C:

Principle Interoperability page 21 – Standards from key organizations

ICAO Digital Travel Credential (DTC)

Replacing a conventional passport with digital travel credentials

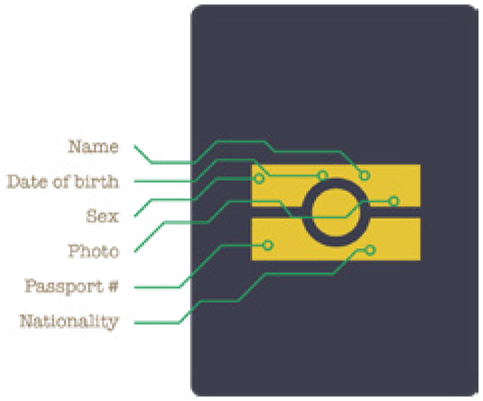
By ICAO's Traveller Identification Programme in collaboration with New Technologies Working Group, Digital Travel Credential Sub-Group

In response to this fast-moving landscape, the ICAO's New Technologies Working Group (NTWG)[1] established a subgroup to standardise the issuance of travel credentials in a digital format. In developing these technical specifications and policies, the ePassport is used as the benchmark given that it offers a secure, portable and verifiable token.

A digital travel credential (DTC) is intended to temporarily or permanently substitute a conventional passport with a digital representation of the traveller's identity, which can, in turn, be validated using the travel document issuing authority's public key infrastructure

The current security of the ePassport results from the ability to verify: the authenticity of data; and the consistency of the physical and electronic information. The digitized data stored on the chip is identical to the printed information (the exception being the optional secondary biometrics and some special data groups) and ties the data on the chip to the holder of the document through a process of matching the primary biometric to the presenter of the Passport. Comparison of digitized data stored on the chip to the printed information on the data page provides the binding with the secure physical document.

To ensure integrity and authenticity can be validated to the same level of security as an ePassport, the DTC approach is based on a 'hybrid' concept, in which the DTC will consist of a Virtual Component (DTC-VC) containing the digital representation of the holder's identity and one Physical Component (DTC-PC) that is securely linked to the Virtual Component. The DTC-VC does not have any copy protection or access control protection as it is a simple file structure.



The DTC can be implemented in three types:

1. **Type 1 - eMRTD bound DTC** – consist of a DTC-VC only, with the eMRTD as a physical authenticator. Which means Data is extracted from the physical ePassport and stored in a digital container (Mobile, smartphone); holder must carry the physical travel document as a back-up.
2. **Type 2 - eMRTD- PC bound** – consists of DTC-VC and a DTC-PC in addition to the eMRTD : Data is extracted from the issuer database and digitally signed by the issuing authority; the DTC digital container (mobile) is the primary back-up, a physical book is an alternate back-up.
3. **Type 3 - PC bound** – consists of a DTC-VC and a DTC-PC but NO eMRTD: The issuing authority would only issue the traveller with a DTC and no physical book. The DTC can be stored.

The specifications for Type 1 DTC have been endorsed by the ICAO Technical Advisory Group for the Traveller Identification Programme (TAG/TRIP)[2] and will be published on the ICAO website[3] along with the Guiding Core Principles for the Development of Digital Travel Credential (DTC).

[1] https://www.icao.int/Security/FAL/TRIP/Pages/terms-of-reference.aspx
[2] https://www.icao.int/Security/FAL/TRIP/Pages/terms-of-reference.aspx
[3] https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx

IATA One ID

The One ID Vision aims to provide a passenger-centric experience within aviation, using their trusted digital identity and biometric technologies to enjoy contactless and seamless processing through required checkpoints in the air travel journey[4].

Through the definition of 'Interoperability in the One ID Ecosystem, IATA aims to guide the establishment of a One ID solution that allows robust identity management at the early stage of the journey, and preferably off-airport, to ensure a seamless flow for the passenger, from making their booking to arriving at their destination.

The guidance includes functional requirements, as well as outlines some of the technical requirements and interface solutions that will support stakeholders in their discussion with providers, manufacturers and integrators. One ID is technology agnostic, wherever possible, and seeks an interoperable solution that will enable multiple implementations and approaches.

In an One ID process, the passenger is always in control of their data, by providing explicit consent to stakeholders, while being informed about all the purposes for which the data is being processed.

By placing the passengers' privacy at its core, One ID is designed as a system of agreed controls that govern the interactions between all participants, where every stakeholder knows their role, rights and obligations. This approach supports the processes and configurations that best achieve the required performance levels, makes options available to support integration with external systems, and supports data exchanges securely and in respect of privacy best practices.

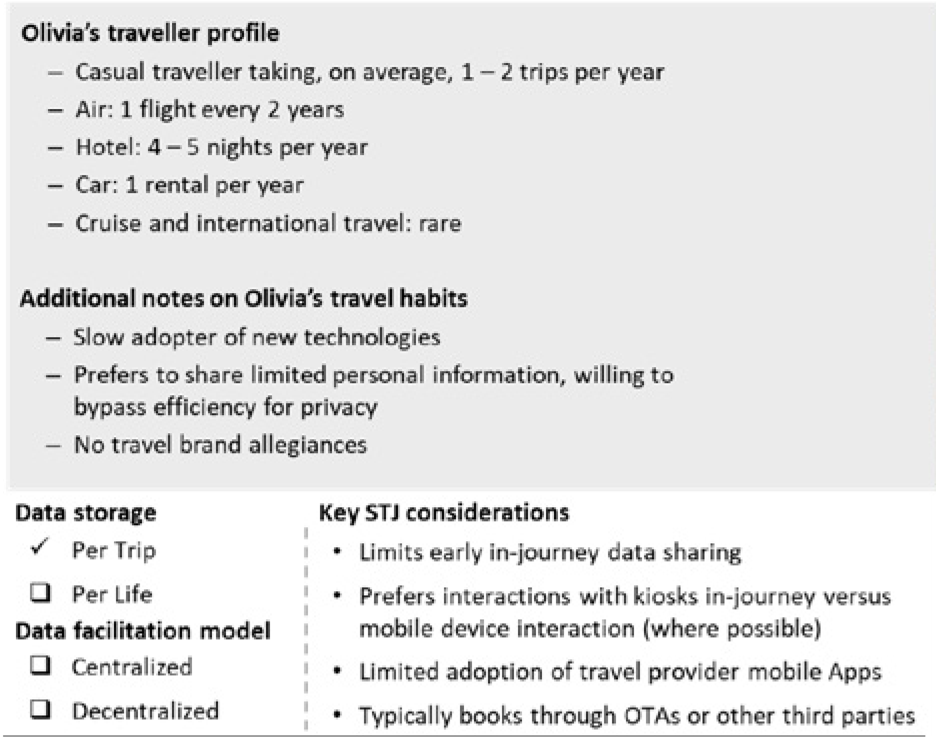
The One ID project defined a One ID Ecosystem. The ecosystem details such an approach and describes the various functions, roles and actors, and the underlying principles and standards at an industry level. This allows global interoperability and compatibility of various and different implementations and approaches.

[4] https://www.iata.org/en/programs/passenger/one-id/

APPENDIX D:

PRINCIPAL CUSTOMER-FIRST BY DESIGN page 32 – Use case details

Olivia, the casual traveller: 1-2 trips per year



Olivia's traveller profile

– Casual traveller taking, on average, 1 – 2 trips per year
– Air: 1 flight every 2 years
– Hotel: 4 – 5 nights per year
– Car: 1 rental per year
– Cruise and international travel: rare

Additional notes on Olivia's travel habits

– Slow adopter of new technologies
– Prefers to share limited personal information, willing to bypass efficiency for privacy
– No travel brand allegiances

Data storage

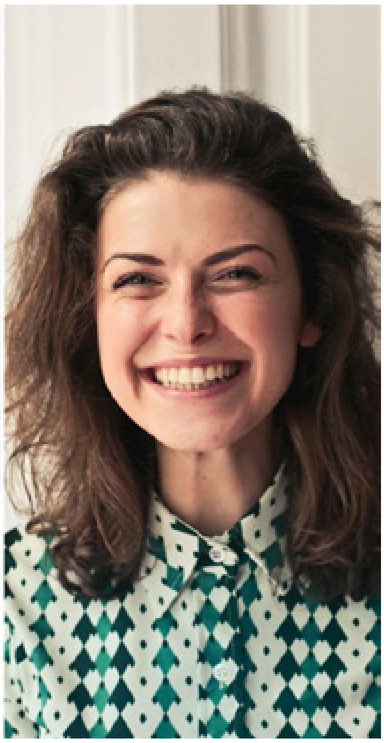
✓ Per Trip
□ Per Life

Data facilitation model

□ Centralized
□ Decentralized

Key STJ considerations

- Limits early in-journey data sharing
- Prefers interactions with kiosks in-journey versus mobile device interaction (where possible)
- Limited adoption of travel provider mobile Apps
- Typically books through OTAs or other third parties



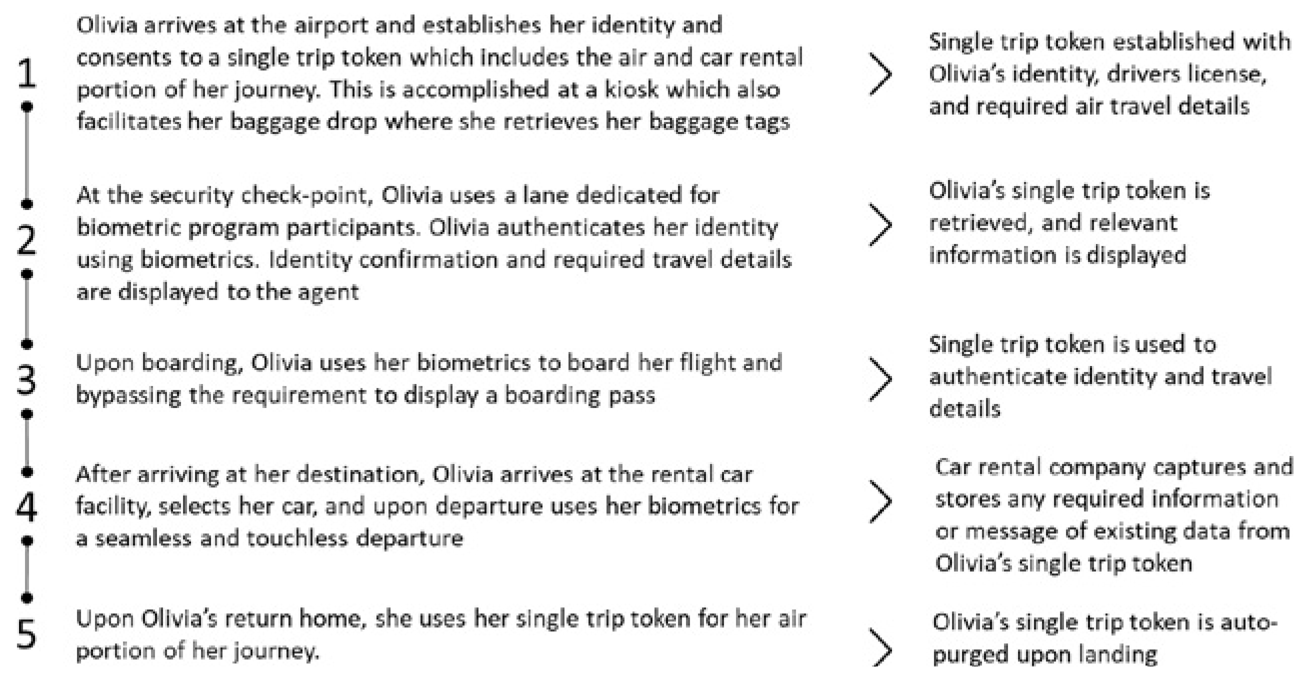
Olivia is a casual traveller who embarks on one to two trips per year. She rarely flies when travelling but does stay in hotels several nights a year.

Olivia also represents those who are slow to adopt new technologies. She would rather use on-premises facilities like kiosks or front desks to check-in. She is very conscious of her digital identity footprint, sharing only limited personal information to the point that she is willing to forgo convenience to keep her data private.

Traveller perspective: Upon arrival at the airport, Olivia approaches a kiosk and chooses to enrol her digital identity in a single trip token, using her driver's license and form of payment. This single trip token includes links to the air and car rental portions of her journey. Upon retrieving her baggage tags, she uses her enrolled digital identity in a dedicated lane security checkpoint lane for biometric programme participants. At boarding, Olivia utilises her biometric identity to board the plane removing the need for her to present a boarding pass. Upon arrival at her destination, Olivia arrives at the car rental facility, selects her car, and departs the facility by using her biometrics, thus removing the need to present a form of payment or driver's license. Upon completion of Olivia's trip, her single trip token is purged.

Technical/operational perspective: Technology providers create a single trip token with Olivia's trusted and verifiable identity (e.g. driver's license) and required air travel details. That single trip token is stored centrally by the identity provider and is relevant information to each stakeholder. It is shared with stakeholders like security checkpoint personnel and the car rental company during her journey. Once the trip is complete, the technology provider auto-purges the single trip token of all relevant personal information and details.

Casual Traveller:



	Use case step and description	Technical/operation details
1	Olivia arrives at the airport and establishes her identity and consents to a single trip token which includes the air and car rental portion of her journey. This is accomplished at a kiosk which also facilitates her baggage drop where she retrieves her baggage tags	Single trip token established with Olivia's identity, drivers license, and required air travel details
2	At the security check-point, Olivia uses a lane dedicated for biometric program participants. Olivia authenticates her identity using biometrics. Identity confirmation and required travel details are displayed to the agent	Olivia's single trip token is retrieved, and relevant information is displayed
3	Upon boarding, Olivia uses her biometrics to board her flight and bypassing the requirement to display a boarding pass	Single trip token is used to authenticate identity and travel details
4	After arriving at her destination, Olivia arrives at the rental car facility, selects her car, and upon departure uses her biometrics for a seamless and touchless departure	Car rental company captures and stores any required information or message of existing data from Olivia's single trip token
5	Upon Olivia's return home, she uses her single trip token for her air portion of her journey.	Olivia's single trip token is auto-purged upon landing

Ross, the frequent traveller: 20+ trips per year

Ross's traveller profile

- Frequent business and leisure traveller taking, on average, 20+ trips per year
- Average trip includes the following modes transportation:
  - Air, hotel, car rental/ride-sharing, airport retail
- International travel encompasses about 4 trips per year
- Current member of a trusted traveller program

Today: trusted traveller program membership is country-by-country
Future: How to facilitate trusted traveller program membership across multiple countries?

Additional notes on Ross's habits

- Early technology adopter
- Willing to share personal data for a better experience and efficiencies in travel experience
- High-value member of several travel brands

Data storage and facilitation model

❑ Per Trip
✓ Per Life

❑ Centralized
❑ Decentralized
✓ Hybrid

Key STJ considerations

- Prefers to setup and maintain a single digital identity wallet for all travel purposes
- Books reservations through company travel agent and/or travel provider mobile App

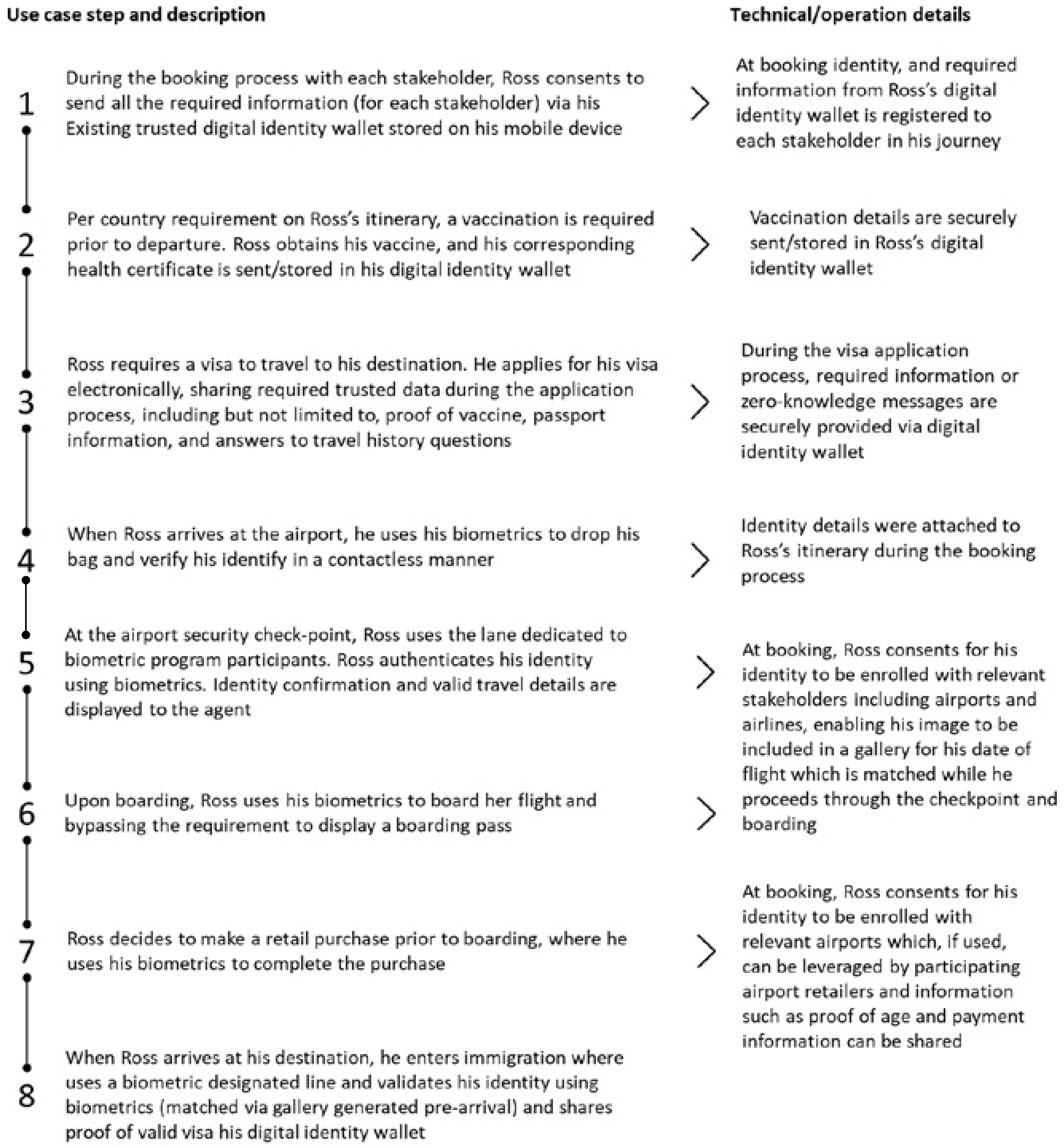
Ross is a frequent traveller, who travels both for business and personal purposes. Completing more than twenty trips per year, Ross's typical trip includes air, hotel, car rental/ridesharing, airport retail. He also takes international trips and is, therefore, an existing member of a trusted traveller programme.

Due to Ross's extensive travel and the fact that he is typically an early technology adopter, he is willing to create a decentralized digital identity on his mobile device. He sees the incredible value in a more seamless travel experience and efficiencies he will recognise.

Frequent Traveller:

Traveller perspective: During the booking process, Ross consents to send all the required information (one consent per stakeholder) via his digital identity wallet stored on his mobile device. For this trip, he needs proof of vaccination and a visa, which he provides using data elements contained within his digital identity wallet. Whether arriving at the airport, passing through security, crossing borders, embarking on cruises, making in-journey purchases, Ross leverages his digital identity to provide the necessary documentation to each stakeholder along the travel journey.

Technical/operational perspective: Technology providers leverage the data elements shared by Ross from his digital identity to complete their respective transactions. Each stakeholder accesses the required information from their assigned data escrow account containing the consented data elements and zero-knowledge messages. These data transactions, for each stakeholder, may occur before, during, and/or after Ross's interaction during his journey.



Use case step and description

Technical/operation details

1 During the booking process with each stakeholder, Ross consents to send all the required information (for each stakeholder) via his Existing trusted digital identity wallet stored on his mobile device

At booking identity, and required information from Ross's digital identity wallet is registered to each stakeholder in his journey

2 Per country requirement on Ross's itinerary, a vaccination is required prior to departure. Ross obtains his vaccine, and his corresponding health certificate is sent/stored in his digital identity wallet

Vaccination details are securely sent/stored in Ross's digital identity wallet

3 Ross requires a visa to travel to his destination. He applies for his visa electronically, sharing required trusted data during the application process, including but not limited to, proof of vaccine, passport information, and answers to travel history questions

During the visa application process, required information or zero-knowledge messages are securely provided via digital identity wallet

4 When Ross arrives at the airport, he uses his biometrics to drop his bag and verify his identify in a contactless manner

Identity details were attached to Ross's itinerary during the booking process

5 At the airport security check-point, Ross uses the lane dedicated to biometric program participants. Ross authenticates his identity using biometrics. Identity confirmation and valid travel details are displayed to the agent

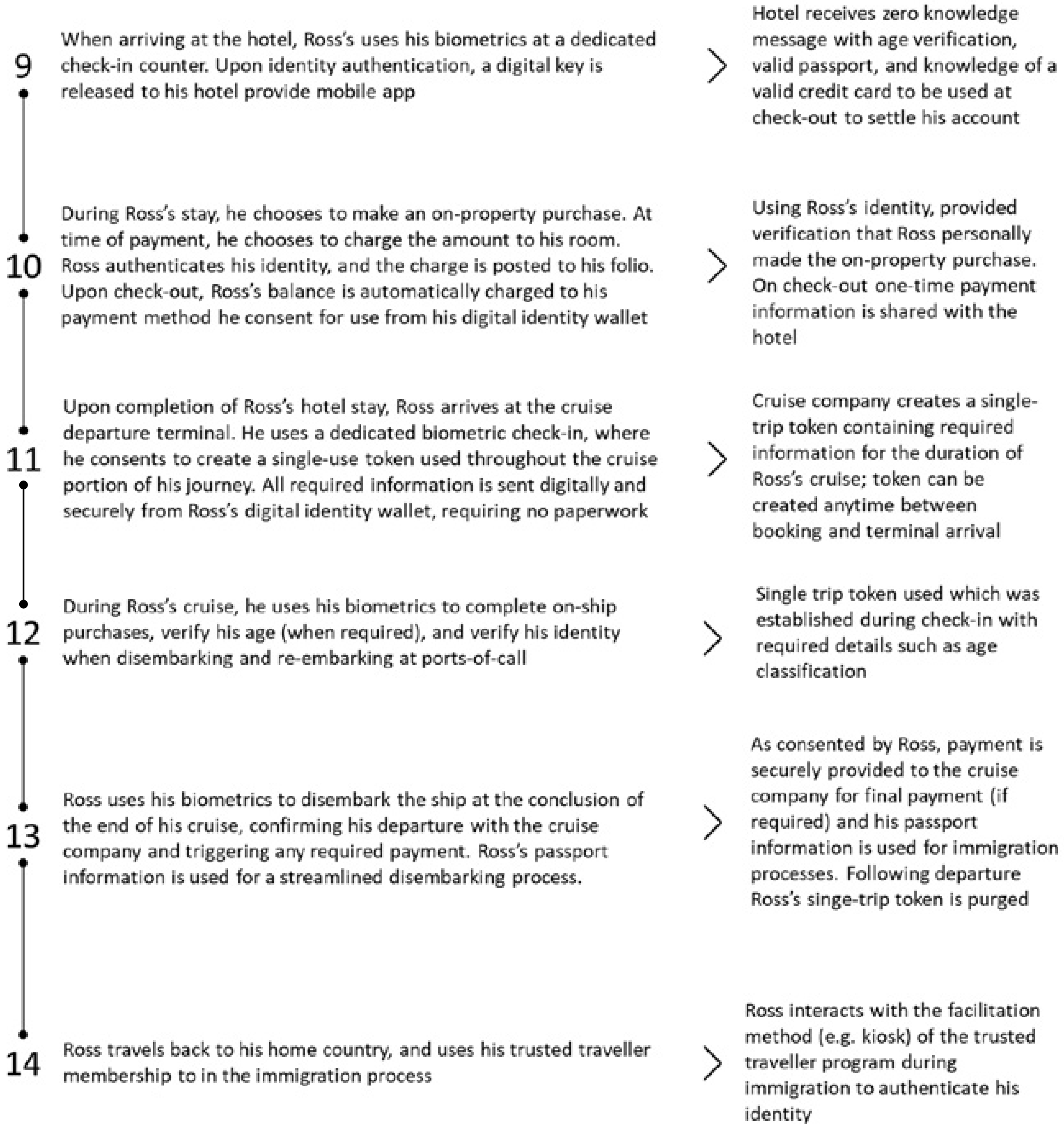
6 Upon boarding, Ross uses his biometrics to board her flight and bypassing the requirement to display a boarding pass

At booking, Ross consents for his identity to be enrolled with relevant stakeholders including airports and airlines, enabling his image to be included in a gallery for his date of flight which is matched while he proceeds through the checkpoint and boarding

7 Ross decides to make a retail purchase prior to boarding, where he uses his biometrics to complete the purchase

At booking, Ross consents for his identity to be enrolled with relevant airports which, if used, can be leveraged by participating airport retailers and information such as proof of age and payment information can be shared

8 When Ross arrives at his destination, he enters immigration where uses a biometric designated line and validates his identity using biometrics (matched via gallery generated pre-arrival) and shares proof of valid visa his digital identity wallet



9 When arriving at the hotel, Ross's uses his biometrics at a dedicated check-in counter. Upon identity authentication, a digital key is released to his hotel provide mobile app

Hotel receives zero knowledge message with age verification, valid passport, and knowledge of a valid credit card to be used at check-out to settle his account

10 During Ross's stay, he chooses to make an on-property purchase. At time of payment, he chooses to charge the amount to his room. Ross authenticates his identity, and the charge is posted to his folio. Upon check-out, Ross's balance is automatically charged to his payment method he consent for use from his digital identity wallet

Using Ross's identity, provided verification that Ross personally made the on-property purchase. On check-out one-time payment information is shared with the hotel

11 Upon completion of Ross's hotel stay, Ross arrives at the cruise departure terminal. He uses a dedicated biometric check-in, where he consents to create a single-use token used throughout the cruise portion of his journey. All required information is sent digitally and securely from Ross's digital identity wallet, requiring no paperwork

Cruise company creates a single-trip token containing required information for the duration of Ross's cruise; token can be created anytime between booking and terminal arrival

12 During Ross's cruise, he uses his biometrics to complete on-ship purchases, verify his age (when required), and verify his identity when disembarking and re-embarking at ports-of-call

Single trip token used which was established during check-in with required details such as age classification

13 Ross uses his biometrics to disembark the ship at the conclusion of the end of his cruise, confirming his departure with the cruise company and triggering any required payment. Ross's passport information is used for a streamlined disembarking process.

As consented by Ross, payment is securely provided to the cruise company for final payment (if required) and his passport information is used for immigration processes. Following departure Ross's singe-trip token is purged

14 Ross travels back to his home country, and uses his trusted traveller membership to in the immigration process

Ross interacts with the facilitation method (e.g. kiosk) of the trusted traveller program during immigration to authenticate his identity

APPENDIX E:

Technology self-assessment

Technology vendors and capabilities: Through discussions with members and affiliates, WTTC collected a set of technology providers who can support the implementation of the concepts discussed in this paper.

WTTC provides a set of technology providers for consideration of the government and private entities, but inclusion does not represent an endorsement. It is recommended that any party interested conduct further due diligence to understand which vendor is best suited to the needs of that party.

Additional vendors may be available and not included at this time. We asked the following technology companies to self-assess against the technology requirements outlined. Below are their responses.

Founded: 1989
Headquarters: Dublin, Ireland

Web: accenture.com
Contact: Christine.c.leong@accenture.com

Platform(s):

Accenture World ID Travel (previously Digital Identity for Travel)

Target users:

Governments, Airlines, Airports and Travel Providers

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile & on-site)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized & decentralized)	Enable touchless	Yes (aviation)
Health certificate and self-declarations	Yes	Auditing capabilities	Yes

Initiative example:

Accenture was WEF's partner in defining KTDI, decentralized identity proof of concept. Accenture, using open-source Hyperledger Indy, built a decentralized identity solution that enables holders (travellers) to receive standards-based verifiable credentials from multiple issuers (governments, airlines, etc.) and selectively disclose identity information to verifiers (governments, airlines, etc.) that request specific information for a specified purpose.

Airside

Founded: 2010
Headquarters: Arlington, VA

Web: airsidemobile.com
Contact: Jessica.patel@airsidemobile.com

Platform(s):

Airside App, AirsideX, Mobile Passport

Target users:

Travellers looking for a privacy-based digital identity; Travel Companies that need biometric solutions or to confirm COVID test results

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile)	Speed & usability	Yes
Data management and operational flexibility	Yes (decentralized)	Enable touchless	Yes
Health certificate and self-declarations	Yes	Auditing capabilities	Yes

Initiative example:

With American Airlines, Airside is piloting airport check-in and luggage drop at DFW and DCA. Using Airside's app, passengers upload their passport or driving licence, adding a photo of themselves and giving consent for their mobile ID to be shared and used on the day of travel.
www.nfcw.com/2020/11/02/368994/american-airlines-pilots-mobile-digital-identity-system

CLEAR

Founded: 2010
Headquarters: New York

Web: clearme.com
Contact: Mitch.nadler@clearme.com

Platform(s):

CLEAR, CLEAR for Sports, Health Pass by CLEAR, CLEAR Pass Mobile Passport Control, Home-to-Gate

Target users:

Travellers, Airlines, Airport Operators and Employees, Travel- and Hospitality-related Businesses, Sports Business and Venue Operators

Requirements:

Platform readiness	Yes - Available and in-use today by Airlines (Delta, United), Airports (36 U.S. Airports), Sports Venue Operators (25+ stadiums and arenas, the NHL, MLB, NBA), Hotels (MGM Resorts), Restaurants (Union Square Hospitality, others)	Data privacy & security	Yes
		Speed & usability	Yes
Establish & authenticate identity	Yes (mobile and onsite)	Enable touchless	Yes - airlines, airports, sports, hotels / hospitalty
Data management and operational flexibility	Yes (centralized)		
Health certificate and self-declarations	Yes (health certificate only)	Auditing capabilities	Yes

Initiative example:

Health Pass partnerships with NHL for Stanley Cup Playoffs, NFL Teams (**www.seahawks.com/news/seattle-seahawks-and-clear-announce-partnership-to-create-safer-return-to-football**), MGM Resorts (**www.prnewswire.com/news-releases/mgm-resorts-international-announces-comprehensive-health-and-safety-plan-for-meetings-and-conventions-301140240.htm**l),

Critical Insights – Consultancy provides NEC Corporation strategic alliance and business development services.

Founded: 1899
Headquarters: Tokyo, Japan

Web: nec.com/aviation
nec.com/en/global/solutions/safety/aviation
Contact: Mick.oc@critical-insights.co.uk

Platform(s):

NEC I:Delight Platform

Target users:

Airlines, airports and relevant governments (+ enterprise customers such as hotels, car rental agencies, theme parks, gaming establishments, cruise lines, etc.)

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized and decentralized)	Enable touchless	Yes (aviation)
Health certificate and self-declarations	Yes	Auditing capabilities	Yes

Initiative example:

Led by Star Alliance with NEC I:Delight, with Lufthansa Group as the initial airline, created a one-time consent-based enrolment via the airline app, using the face as a seamless identity from airport to airport, airline to airline, for enhanced hygiene, security operational efficiency and passenger experience.

Hawaii 'Alohapass'; Delta + TVS; Japan – Narita airport immigration services and the 2021 Olympics; Singapore – with their ICA for face, iris and fingerprint automated contactless immigration services; Argentina – with their DNM immigration agency.

Founded: 1945
Headquarters: Montreal, Canada

Web: iata.org/en/publications/travel-pass
Contact: IATATavelPass@iata.org

Platform(s):

IATA Contactless Travel App, IATA Contactless Travel Solution, IATA Travel Pass

Target users:

International travellers, Airlines, Airports, Border Control Authorities

Requirements:

Platform readiness	Yes (in-pilot)	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile)	Speed & usability	Yes
Data management and operational flexibility	Yes (decentralized)	Enable touchless	Yes (aviation)
Health certificate and self-declarations	Yes (health certificate)	Auditing capabilities	n/a

Founded: 1911
Headquarters: Armonk, NY

Web: ibm.com
Contact: Greg.land@us.ibm.com

Platform(s):

Cloud, Cognitive, Blockchain, Enterprise Mobile, IBM Travel Platform, IBM Travel Retail, IBM Travel Operations, IBM Travel Maintenance, Cyber Security, Watson Health

Target users:

Airlines, Hospitality, Travel Distribution, Cruise, Car Rental, Immigration, CBP, Security Screening

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile and onsite)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized and decentralized)	Enable touchless	Yes (multi-sector)
Health certificate and self-declarations	Yes (health certificate only)	Auditing capabilities	Yes

Initiative example:

IBM Digital Identity for Blockchain: **www.ibm.com/blockchain/solutions/identity**

IBM Digital Health Pass: **www.ibm.com/products/digital-health-pass**

Video Demo for Travel IBM Digital Health Pass: **vimeo.com/448967890/e15dabc1db**

Founded: 1949
Headquarters: Geneva, Switzerland

Web: sita.aero
Contact: Andy.smith@sita.aero

Platform(s):

Travel Authorisation, API/PNR Gateway, Advance Passenger Processing (APP / iAPI for Denial of Boarding), Aviation Contact Tracing Solutions

Target users:

Immigration, Tourism, Health, Airports, Carriers

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (kiosk & mobile)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized & decentralised)	Enable touchless	Yes
Health certificate and self-declarations	Yes (self-declaration)	Auditing capabilities	Yes

Initiative example:

Beijing Capital International Airport – SITA Smart Path deployment comprising over 600 biometric devices across multiple checkpoints, including manual check-in, self-service check-in, bag drop, restricted access, security, duty free and boarding. Dallas Fort Worth International – trial of SITA's self-service bag-drop in a pilot program, the first in the US to employ the Traveler Verification System, the US Customs & Border Patrol's biometric entry-exit system. Biometric Boarding and Exit Check at Orlando and Miami.

Founded: 2001
Headquarters: Lisbon, Portugal

Web: vision-box.com
Contact: sales@vision-box.com

Platform(s):

vb Orchestra™– Identity Management Platform and Traveller Flow Management ecosystem and its Software Suite (on-prem, cloud and mobile); Traveller hardware touchpoints – eGates, Kiosks, Totems, IoT Cameras; Biometrics Enrollment and Matching algorithms; Professional Services & Consulting; Life Cycle Managed Services

Target users:

Governments, Airports, Airlines, Hospitality, Major Events, Retail

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile and kiosk)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized and decentralized)	Enable touchless	Yes
Health certificate and self-declarations	Yes	Auditing capabilities	Yes

Initiative example:

Aruba, Aruba International Airport; The Netherlands, Schiphol Airport; India, Bengaluru Airport; Malaysia, AirAsia; Uruguay, Carrasco Airport; UAE, Emirates at Dubai Airport T3 ; Finland, The Finnish Border Guards and Helsinki Airport; USA New York, John F. Kennedy Airport / T1.
www.vision-box.com/pressroom/press-releases/aruba-international-airport-inaugurates-extension-of-aruba-happy-flow
www.vision-box.com/pressroom/press-releases/schiphol-airport-facial-recognition-boarding-vision-box-platform
www.vision-box.com/pressroom/press-releases/digi-yatra-seamless-flow-goes-live-at-blr-airport
www.vision-box.com/pressroom/press-releases/vision-box-airasia-touchless-travel-experience
www.easyairport.biz/
www.vision-box.com/pressroom/press-releases/contactless-emirates-dubai-international-airport
www.raja.fi/guidelines/automated_border_control
www.vision-box.com/pressroom/press-releases/new-york-jfk-launch-facial-recognition-boarding-vision-box

Founded: 1998
Headquarters: Ottawa, Canada

Web: worldreach.com
Contact: Gordon.wilson@worldreach.com

Platform(s):

IdentityReach based on the Know Your Traveller (KYT) Platform

Target users:

Government agencies & commercial service providers in travel, tourism, borders, and immigration

Requirements:

Platform readiness	Yes	Data privacy & security	Yes
Establish & authenticate identity	Yes (mobile)	Speed & usability	Yes
Data management and operational flexibility	Yes (centralized)	Enable touchless	Yes
Health certificate and self-declarations	Yes	Auditing capabilities	Yes

Initiative example:

Canada – Chain of Trust (Air) with Canada Border Services Agency: pilot program to facilitate low risk travellers through immigration and border clearance using biometrics. Eurostar Pilot – Seamless Biometric Check-in and Departure: Rail passengers using Eurostar services will be able to take advantage of a facial biometric corridor to enable contactless journeys. United Kingdom – EU Settlement Scheme and Immigration Programs: The Home Office allowed applicants to choose a digital onboarding route to submit an application for Settled Status in the UK following Brexit.

APPENDIX F:

Comparison of initiatives

Throughout the "Assessment" phase for the development of the STJ programme, WTTC conducted extensive research to understand the existing initiatives that utilise biometrics across the Travel & Tourism sector. Below is a comprehensive listing of the global biometrics initiatives that WTTC has explored to date, as of July 2019. WTTC will continue to research additional and new initiatives as they are identified or established.

COUNTRY	SECTOR	INITIATIVES	2020 UPDATE
ARUBA	AVIATION	Aruba Happy Flow	Aruba Happy Flow v2 - Pilot plan for 2021 with air and non-air. Aruba aims to be ready for tourists who will use a digital wallet and or airline apps to share their digital travel credential and trusted Covid-19 test results or vaccination certificate.
AUSTRALIA	AVIATION	• Seamless Traveller Initiative • SmartGate • Smart Path • Pilots testing facial recognition at various airports (ex. Sydney, Brisbane, - Canberra) • Universal ETA	The Department of Home Affairs (DHA) launched a new "Enterprise Biometric Identification System" (EBIS) to optimize passenger visa and border processing and detect criminals and national security threats.
BARBADOS	AVIATION	Entry/Exit	No additional updates or information at time of publishing
CANADA	AVIATION	Chain of Trust	Chain of Trust will begin test operations in early 2021 starting with returning Canadians.
CANADA + USA	LAND CROSSING	NEXUS	• Land & Air Border Crossing - ABC Gates at Winnipeg International Airport in Canada to check the facial biometrics of arriving travellers enrolled in the NEXUS Program • "Expanded use of facial biometrics to pedestrian processing for entry into Detroit, MI and Champlain, NY + Five other Land Crossings: 1. El Paso, Texas 2. Laredo, Texas 3. Nogales, Arizona 4. Progreso, Texas 5. San Luis, Arizona"
CHINA	AVIATION	Biometric Initiatives at various airports (ex. Beijing, Guangzhou, Lanzhou, Yancheng Nanyang, Yinchuan)	As of December 2019, 27% of Chinese airports have self-boarding gates using biometrics with travel documents but in just three years this will jump to 66%. And more than half of the airports have plans for secure single biometric tokens for all touch points by 2022.
CHINA	HOSPITALITY	Marriott + Alibaba	No additional updates or information at time of publishing
EU	BORDER CROSSING (LAND, AIR, SEA)	Government Initiatives • Entry Exit System (EES) • eu-LISA Biometrics Matching System (BMS) • European Travel Information and Authorization System (ETIAS)	• "Biometrics on the Move" • Project Protect - to build an advanced biometric-based person identification system that works robustly across a range of border crossing types and that has strong user-centric features.
FINLAND	AVIATION	Finavia + Helsinki Airport Biometric Initiative	Automated Border Control
FRANCE	AVIATION	Biometric Boarding Pass (Air France)	No additional updates or information at time of publishing

COUNTRY	SECTOR	INITIATIVES	2020 UPDATE
FRANCE + UK	TRAIN	Eurotunnel	Eurostar pilot project for seamless ticket check through departure with remote ID verification with facial Biometrics to start trial in 2021.
GERMANY	TRUSTED TRAVELLER	EasyPASS	No additional updates or information at time of publishing
HONG KONG SAR, CHINA	TRUSTED TRAVELLER	Smart Departure eChannel	Addition of “Single Token Experience” announced
INDIA	AVIATION	Digi Yatra	Now available for AirAsia India / Planning expansion to airlines Vistara and IndiGo at Varanasi Airport
JAPAN	AVIATION	• eGates using facial recognition for international arrivals at Tokyo Airports (Japanese Citizens) • Narita Airport Biometric Initiative	The Immigration Services Agency announced that facial recognition will be used to scan short-term international visitors who are leaving the country. Six major airports set to adopt facial recognition technology. (New Chitose Airport, Narita International Airport, Haneda Airport, Chubu International Airport, Kansai International Airport and Fukuoka Airport.)
JAPAN	FACILITATION	Tokyo 2020 athletes, staff, media to be screened with facial recognition	No additional updates or information at time of publishing
MALAYSIA	AVIATION	Fast Airport Clearance Experience System (FACES) - AirAsia	Malaysia plans single token biometrics launch for Kuala Lumpur International Airport
MEXICO	TRUSTED TRAVELLER	Viajero Confiable	No additional updates or information at time of publishing
MEXICO + USA	LAND CROSSING	Secure Electronic Network for Travelers Rapid Inspection (SENTRI)	No additional updates or information at time of publishing
NETHERLANDS	AVIATION	• Schiphol Airport Biometric Initiative • Seamless Flow Netherlands	No additional updates or information at time of publishing
NETHERLANDS	TRUSTED TRAVELLER	Privium / Flux	No additional updates or information at time of publishing
QATAR	AVIATION	Hamad Airport Biometric Initiative	No additional updates or information at time of publishing
SAUDI ARABIA	AVIATION	Airport Modernization Project (26 airports)	The Saudi Ministry of Interior unveiled plans to introduce an iris recognition biometric system in all its land, sea and airports in efforts to use highly advanced technology to identify passengers and ensure the nation’s safety.
SINGAPORE	AVIATION	Fast and Seamless Travel (FAST)	Update to integrate Facial & Iris + Contactless Check-in & bag drop Kiosks
SINGAPORE + US	TRUSTED TRAVELLER	Singapore - US Trusted Traveller Programme	No additional updates or information at time of publishing
SOUTH KOREA	AVIATION	SmartPass	No additional updates or information at time of publishing
UAE	AVIATION	eGates and Biometric Immigration Tunnel	• Smart Gates (Dubai), Smart Travel (Abu Dhabi), Smart Path (Sharjah) / Identity documents using biometrics for own nationals, eGates • Emirates expand programme - Integrated Biometric Path

COUNTRY	SECTOR	INITIATIVES	2020 UPDATE
UAE + UK	AVIATION	Dubai International Airport & London Gatwick Joint Biometric Initiative	No additional updates or information at time of publishing
UK	AVIATION	• London Gatwick Airport Biometric Initiative • London Heathrow Passenger Identification Programme	The UK government already makes extensive use of biometrics in their immigration and border processes. All travellers coming to the UK for more than 6 months must include the submission of biometrics (face and finger).
UK	TRUSTED TRAVELLER	Registered Traveller Service	No additional updates or information at time of publishing
UK	BORDER CROSSING	–	Launched a Public Consultation to develop "2025 UK Border Strategy"
URUGUAY	AVIATION	Easy Airport Programme at Carrasco International Airport	2020 Update - ABCs located at the arrivals area currently accept 37 different nationalities and 45% of arriving passengers use them, while those in Departures accept 4 nationalities and 30% of departing passengers use them.
USA	TRUSTED TRAVELLER	Global Entry - Customs and Border Protection (CBP)	Airports Where U.S. CBP Deployed Facial Recognition Technology for the Global Entry Program, as of May 2020: 1. Aruba–Queen Beatrix International Airport (AUA) 2. Dallas/Fort Worth International Airport (DFW) 3. Detroit Metropolitan Airport (DTW) 4. Dublin Airport, Ireland (DUB) 5. Fort Lauderdale/Hollywood International Airport (FLL) 6. George Bush Intercontinental Airport, Houston (IAH) 7. Hartsfield-Jackson Atlanta International Airport (ATL) 8. John F. Kennedy International Airport, New York (JFK) 9. Miami International Airport (MIA) 10. Newark Liberty International Airport (EWR 11. Orlando International Airport (MCO) 12. Philadelphia International Airport (PHL) 13. Phoenix Sky Harbor International Airport (PHX) 14. Salt Lake City International Airport (SLC) 15. San Diego International Airport (SAN) 16. Shannon Airport, Ireland (SNN) 17. William P. Hobby Airport (HOU)"
USA	TRAVELLER EXPERIENCE	MyDisney Experience	• Traveller Apps integrating a "Health Pass" with Covid-19 testing information • Verifly at Denver Intl Airport
USA	AVIATION (SECURITY CHECK POINTS)	Transportation Security Administration (TSA) Initiatives • Phoenix Sky Harbor International Airport (PHX) • Los Angeles International Airport (LAX) • John F. Kennedy International Airport (JFK)	• Hartsfield-Jackson Atlanta International Airport (ATL) / Las Vegas McCarran International Airport (LAS) / Detroit Metropolitan Wayne County Airport (DTW) * Plan
USA	SEAPORTS	Customs and Border Protection (CBP) - Traveller Verification Service (TVS) with pilots at Seaports with Royal Caribbean and Carnival Cruise Lines	"Six Sea Ports: 1. Cape Liberty Cruise Terminal, Bayonne, New Jersey 2. Pier 66, Seattle, Washington 3. Pier 88, New York City, New York 4. Port Canaveral, Florida 5. Port Everglades, Fort Lauderdale, Florida 6. Port Miami, Miami, Florida "

COUNTRY	SECTOR	INITIATIVES	2020 UPDATE
USA	AVIATION	Customs and Border Protection (CBP) - Traveller Verification Service (TVS) with pilots at several airports with numerous airlines including: • U.S. Airports – Detroit Metropolitan – Wayne County Airport (DTW) – Dallas Fort Worth International Airport (DFW) – Fort Lauderdale–Hollywood International Airport (FLL) – General Edward Lawrence Logan International Airport (BOS) – George Bush Intercontinental Airport (IAH) – Hartsfield Jackson Atlanta International Airport (ATL) – John F. Kennedy International Airport (JFK) – Los Angeles International Airport (LAX) – McCarran International Airport (LAS) – Miami International Airport (MIA) – Minneapolis-St. Paul International Airport (MSP) – Newark Liberty International Airport (EWR) – O'Hare International Airport (ORD) – Orlando International Airport (MCO) – Ronald Reagan Washington National Airport (DCA) – Salt Lake City International Airport (SLC) – San Diego International Airport (SAN) – San Francisco International Airport (SFO) – San Jose International Airport (SJC) – Seattle–Tacoma International Airport (SEA) – Tampa International Airport (TPA) – Washington Dulles International Airport (IAD) – William P. Hobby Airport (HOU) • Non-U.S. Airports – Abu Dhabi International Airport (AUH) – Dublin Airport (DUB) – Queen Beatrix International Airport (AUA) – Shannon Airport (SNN) • Airlines: American Airlines, ANA, British Airways, Delta Airlines, Japan Airlines, JetBlue, KLM - Air France, Lufthansa, Norwegian	• CBP has deployed Facial Recognition Technology as of May 2020 at: – 27 Air Exit Locations in the US – 18 Air Entry Locations – 6 Sea Ports / 5 Land Ports – 17 Airports for the Global Entry Programme + more than 20 Airline Partners • Passenger experience using Biometrics at Denver Airport
REGIONAL	TRUSTED TRAVELLER	APEC Business Travel Card	No additional updates or information at time of publishing
GLOBAL	AVIATION	• IATA – OneID • New Experience Travel Technologies (NEXTT) by ACI + IATA	IATA Contactless Travel
		ICAO - Digital Travel Credential (DTC)	The new ICAO Digital Travel Credential (DTC) standard is expected to be approved in late 2020/early 2021
		Star Alliance	Lufthansa group airlines will be the first to use the Star Alliance biometric system on selected flights in November 2020 at Frankfurt/Main Airport (FRA) and Munich Airport (MUC).
COUNTRY	BEYOND TRAVEL & TOURISM	National ID Documents	No additional updates or information at time of publishing
GLOBAL	TRAVEL & TOURISM	World Economic Forum – Known Traveller Digital Identity (KTDI)	• Currently piloting components of the KTDI concept in a real-life, cross-border context • CommonPass framework (By the Commons Project together with The World Economic Forum)

Acknowledgements

This report was prepared by the **World Travel & Tourism Council** (WTTC) in collaboration with its **Knowledge Partner Oliver Wyman.**

The authors of the report would like to thank the representatives from the following companies and associations, who participated in the related Interviews and discussion groups, in alphabetical order:

Advisors:

CONSIDERATI

IATA

IBMATA

PANGIAM

Contributors:

- Accenture
- Amadeus IT Group
- Airside Mobile
- Apple Leisure Group
- Aruba Government
- Carnival Corporation
- Chicago Department of Aviation
- Clear
- Critical Insights
- Coporación América Uruguay – Easy Airport Division
- Dallas Fort Worth International Airport
- Denver International Airport
- Emirates Group
- El Cid Resorts
- Greater Toronto Airports Authority
- Grupo Iberostar
- Grupo Posadas
- Hilton
- Hospitality Technology Next Generation
- IBM
- Japan Airlines
- KLM
- Libertador Hotels, Resorts & Spa
- Linksrez
- Lufthansa
- MSC Cruises
- Peninsula
- SITA
- Uber
- Vision-Box
- Worldreach Software

WORLD TRAVEL & TOURISM COUNCIL

The World Travel & Tourism Council is the global authority on the economic and social contribution of Travel & Tourism.

WTTC promotes sustainable growth for the Travel & Tourism sector, working with governments and international institutions to create jobs, to drive exports and to generate prosperity. Council Members are the Chairs, Presidents and Chief Executives of the world's leading private sector Travel & Tourism businesses.

Together with Oxford Economics, WTTC produces annual research that shows Travel & Tourism to be one of the world's largest sectors, supporting 330 million jobs and generating 10.3% of global GDP in 2019. Comprehensive reports quantify, compare and forecast the economic impact of Travel & Tourism on 185 economies around the world. In addition to individual country fact sheets, and fuller country reports, WTTC produces a world report highlighting global trends and 25 further reports that focus on regions, sub-regions and economic and geographic groups.

To download reports or data, please visit **www.wttc.org**

OLIVER WYMAN

Oliver Wyman works with the world's leading travel and leisure companies, including hotels, airlines, passenger rail and bus operators, theme parks, cruise operators, gaming and lottery companies, tour operators and travel agencies, travel technology companies, airports, rail stations, and concessionaires, as well as private equity firms. The firm has more than 4,700 professionals around the world and draws on deep industry expertise and specialized capabilities to develop growth strategies and operational excellence initiatives with its clients to transform their business. Oliver Wyman is a trusted advisor to the World Travel and Tourism Council advising on its growth strategy, and has been directly supporting the development of the Seamless Traveller Journey programme. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC].

Gloria Guevara
President & CEO
World Travel & Tourism Council

Scot Hornick
Partner, Transportation & Travel
Oliver Wyman

Mike Matheis
Global Industry Association, Civic
& Economic Organization Lead
Oliver Wyman

Editors:

Helena Bononi
VP Membership & Commercial
World Travel & Tourism Council

Lawrence Burka
Associate
Oliver Wyman

Scott Boland-Krouse
Principal
Oliver Wyman

Design:
World Travel & Tourism Council

WORLD TRAVEL & TOURISM COUNCIL

STRATEGIC PARTNERS

AMERICAN EXPRESS

Hilton

Ministry of Tourism
Saudi Arabia