SEAMLESS TRAVELLER JOURNEY
EMERGING MODELS OVERVIEW & FINDINGS REPORT

NOVEMBER 2019
Travel & Tourism growth continues to outpace that of the world economy, resulting in more people travelling than ever before. As one of the world’s largest economic sectors, Travel & Tourism supports one in ten jobs on the planet (319 million) and generates 10.4% of global GDP ($8.8 trillion). By 2029, 100 million more jobs will depend on the sector, representing one in nine jobs around the world. At the same time, according to IATA, the number of air travellers is expected to double from 4.2 billion in 2018 to 8.2 billion by 2037.

As a result, WTTC Members have identified Security & Travel Facilitation as a top priority.

The need to increase capacity to fulfil future demand and the economic opportunities it will bring, coupled with the absolute requirement for security processes to be as robust as possible means that a global, cross-industry solution which allows more people to travel more securely is urgently required. WTTC is addressing this challenge through our Seamless Traveller Journey Programme which is an ambitious initiative that brings together public and private sector stakeholders with technology providers to agree on models that will ultimately facilitate a seamless travel experience. The aim is to identify models which are globally interoperable, technology agnostic and cover the end-to-end journey from booking, through air travel and incorporating cruise, hotel, car rental and other non-air products where necessary.

Over the past year, we have consulted with over 200 stakeholders in order to map existing initiatives and have begun to develop a roadmap to take this initiative forward. This report shares in detail the potential future models which may deliver an end-to-end traveller journey. It also lists the findings of the initial assessment phase, in which we have identified over 80 existing initiatives within the Travel & Tourism sector that employ biometrics.

What has become clear from our work so far is that there is no “one-size-fits-all” solution, and even more crucially, that a solution will only be achieved by working collaboratively across national boundaries and based on strong partnerships between both private companies and government entities.
1.1. INTRODUCTION

1.1. INITIATIVE CONTEXT

THE CHALLENGE

Travel & Tourism is set to grow considerably over the coming years, with the number of air travellers projected to double from 4.2 billion in 2018 to 8.2 billion by 2037, according to the International Air Transport Association (IATA). Yet, we are already witnessing the strain on infrastructure, processes and systems, all of which are insufficient to meet this forecast demand, even with the implementation of current improvement plans and solutions. These pressures are expected to mount in coming years, making action to continue enabling the secure and seamless movement of legitimate travellers across international borders imperative.

Given that Security and Travel Facilitation are top priorities for the global Travel & Tourism private sector, it is essential to consider how to improve the traveller experience while maintaining or even increasing security.

THE OPPORTUNITY

Transformations of the travel experience through technological advances, notably biometrics and the use of digital identity, show strong opportunities to enable a seamless and secure end-to-end traveller journey, while promoting sector-wide growth. Such a solution aligns with the World Travel & Tourism Council’s (WTTC) consumer research undertaken in five European countries and in the United States, suggesting that, on average, 4 in 5 international and domestic travellers would be willing to share their photographs in advance of travel to speed up their journey. By capturing and uploading biometric and biographic data prior to travel, border and security agencies will be able to authenticate and pre-clear travellers in advance of arrival, thus reducing cumbersome checks and queues at ports and airports. This will in turn enhance security across the whole system, relieve pressure on infrastructure and capacity constraints, improve the traveller experience and ensure that the economic potential of Travel & Tourism to create jobs and drive economic growth can be fully realised.

From a traveller’s perspective, this vision is exemplified by a journey during which the traveller no longer needs to present travel documents and boarding passes multiple times to a variety of stakeholders at different stages of their journey. Rather, 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, and access myriad destination services, simply by confirming their identity and booking data.
WTTC APPROACH

Security and Travel Facilitation is a priority for WTTC not only to enable the sustainable growth of the Travel & Tourism sector and enhance security but also to offer an unparalleled experience to the traveller. WTTC is addressing this challenge and opportunity through its Seamless Traveller Journey (STJ) Programme, an ambitious initiative which brings together the public and private sectors alongside technology providers to agree on models that are globally interoperable, technology agnostic, and provide coverage across an end-to-end journey, incorporating both air and non-air. WTTC has taken a collaborative approach, building on the efforts underway with organisations including IATA, International Border Management and Technologies Association (IBMATA), International Civil Aviation Organization (ICAO), Airports Council International (ACI), Cruise Lines International Association (CLIA) and the World Economic Forum as well as independent efforts by airlines, airports and governments.

Building on consultations with over 200 stakeholders, WTTC has developed a clear vision for a seamless and secure end-to-end journey and has defined a roadmap to drive this initiative forward. Such an initiative requires the public and private sectors to join forces to pilot the changes WTTC envisions, build momentum, and encourage adherence to global standards that sustain a supportive policy framework.

In this context, the development of pilots that facilitate a round trip including both air and non-air is critical as it will provide the sector with a strong case, with quantified benefits, to scale this important work.

WTTC and IATA have agreed to work together on enhancing the travel experience. In effect, IATA, on behalf of its member airlines, is promoting the One ID initiative. IATA’s vision is an “end-to-end passenger experience that is secure, seamless, and efficient” which aims at offering passengers a frictionless airport process, allowing the possibility to walk through the airport without breaking stride. WTTC, on its end, is expanding the concept to the entire traveller journey i.e. air and non-air. Both organisations are facilitating progress by bringing together industry stakeholders, developing strong relationships with technology partners, and strengthening government ties to advocate for policy shifts and the development of standards required for interoperability.

These efforts have been supported by ICAO, which has expanded its mandate to ensure a more holistic and coordinated approach to traveller identification across the entire document and border control management system. To realise this strategy, ICAO has continued to advance the ePassport – which contains an added layer of security by embedding an electronic chip that stores biometric information in the passport – as a key means to facilitate a higher level of traveller identification and verification. ICAO is also developing policies and standards for a “Digital Travel Credential” (DTC), a form of digital identity that can be derived from existing government credentials, such as the ePassport. A DTC would benefit all parties participating in the STJ by improving security, reducing travel related costs for all stakeholders, and creating a more efficient travel experience.

THE BENEFITS

A seamless end-to-end travel experience enabled by technologies including biometrics, has five overarching benefits, notably:

- Releasing pressure on infrastructure and enabling travel growth
- Improving safety and security through better authentication and reduction of fraud
- Reducing and avoiding costs by ensuring it serves legitimate travellers
- Enhancing customer satisfaction by eliminating friction and bottlenecks across the journey
- Integrating all touchpoints of the journey enabled by technologies

More specifically, governments, the sector and the traveller would benefit in the following ways:

**GOVERNMENTS**

- Ensuring data accuracy and guaranteeing complete data for risk assessment purposes, in turn enabling better decision-making and more secure border control,
- Reducing staffing and training costs as passengers can be checked more efficiently,
- Enabling government agency staff to devote more time to focus on higher risk profile passengers,
- Driving job creation beyond borders through increased international arrivals into country.

**INDUSTRY**

- Maximising capacity and the ability to process more passengers with more efficiency, potentially representing the opportunity to defer infrastructure expansion,
- Ensuring increased accuracy of information, reduced distribution of customs forms, faster connections and potentially lowering of landing costs through the reallocation of spaces at airports to retailers,
- Achieving efficiency gains through higher productivity at check-in, bag drop and boarding,
- Streamlining of processes through information sharing between relevant providers across the sector.

**TRAVELLER**

- Improving overall experience through more efficient processes, the elimination of redundant document checks, the reduction of waiting times and the implementation of a harmonised approach throughout the journey,
- Ensuring travel security and traveller safety,
- Facilitating travel through accelerated decision-making from governments regarding entry.
1.2. EMERGING MODELS

To better understand the “biometrics” landscape, WTTC undertook a mapping of existing biometric initiatives around the world, resulting in the identification of over 80 (see Figure 9 in the Appendix). This exercise revealed numerous findings; for instance, one biometrics initiative reduced the boarding time of a 400-person capacity plan from 45 to 13-15 minutes on average thanks to improved efficiency. On this basis and realising that there is no “one size fits all”, WTTC has developed an updated perspective on potential end-to-end models and processes to support its vision of an end-to-end Seamless Traveller Journey. WTTC’s latest research, undertaken in collaboration with Oliver Wyman, characterises three models: the “Government” model, the “Per Trip” model and the “Per Life” Model. Each of these models have demonstrated applicability and implementation success, bringing together the insights and experience of existing pilots within the air-ecosystem, and offer opportunities to scale across non-air segments of the traveller journey.

Through this report, we aim to:

1. Present and detail emerging models for data and traveller facilitation within the airline/airport ecosystem based on in depth research and extensive interviews with dozens of WTTC STJ Programme stakeholders.
2. Categorise and assess the captured emerging models to provide the STJ’s initial perspective on ways to extrapolate existing model types and methods of data facilitation across all segments of the traveller journey.

Following the insights gathered, WTTC’s Seamless Traveller Programme is undertaking five steps to advance the programme through 2019 and beyond:

- **Assess** and understand the current initiatives using biometrics worldwide
- **Align** the industry by working with IATA on air, T&T sector on non-air, and engaging with governments
- **Drive** the execution of global end to end round trip pilots
- **Lead** the drive for the adoption and deployment of biometrics
- **Document** and quantify the benefits of the Seamless Traveller Journey

This report is built on work completed during the STJ’s Phase 1 (“Assessment Phase”) in partnership with Oliver Wyman. This report summarises key learnings that build on the airport/airline ecosystem of the traveller journey and presents an initial perspective on extensions for end-to-end travel and data facilitation across all segments (air, car, hotel and cruise) of the traveller journey. This assessment resulted in the identification of three core categories of models: 1) “Government” Model, 2) “Per Trip” Model, 3) “Per Life” Model.

Through discussions with STJ stakeholders, WTTC and Oliver Wyman identified tangible next steps to refine model categorisation and assessment, whilst investigating opportunities to integrate non-air segments to create interoperable, cross-border end-to-end models.

**GOVERNMENT**
- Centralised model
- Government collects and verifies biometric data; stored in central databases (no traveller enrolment)
- Biometrics stored indefinitely
- Only facial and fingerprint biometrics used
- Government acts as identity management service provider (provides Identity as A Service (IDaaS) platform for travel providers)

**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 key biographic and biometric (facial) information
- Orchestration platform houses and maintains token

**PER LIFE**
- Federated model
- Traveller enrols once to create a digital identity in mobile digital wallet
- Lives indefinitely for the lifespan of travel document (e.g. passport)
- Digital wallet contains any data a traveller chooses; data verified using mobile enrolment or by person
- Traveller pushes data to a given stakeholder in advance of travel (e.g. through distributed ledger)
1.3. FRAMEWORK INTRODUCTION

The models use the following framework that traces the linear, end-to-end biometric lifecycle of data and digital identities - from enrolment through use and authentication across journey touchpoints.

![End-to-End Biometric Lifecycle Framework](image)

In addition, the three core models are assessed using the following framework that indicates the strengths and weaknesses for each model.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Low</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrolment / Digital Identity Creation</td>
<td>Pre-Journey Enrolment</td>
<td>Ability of traveller to expedite journey by enrolling &quot;off premise&quot;</td>
<td>No / low opportunity</td>
</tr>
<tr>
<td></td>
<td>Traveller Accessibility</td>
<td>Applicability &amp; ease of enrolment for a wide array of travellers</td>
<td>Limited / arduous</td>
</tr>
<tr>
<td></td>
<td>Integration of Data &amp; Booking Information</td>
<td>Potential to integrate digital identity with travel provider booking</td>
<td>Low (too challenging)</td>
</tr>
<tr>
<td></td>
<td>Data Retention</td>
<td>Potential use of digital identity beyond a single journey</td>
<td>Low (per trip)</td>
</tr>
<tr>
<td></td>
<td>Application of DTC</td>
<td>Easy integration with DTC concept (est. 2020)</td>
<td>Low</td>
</tr>
<tr>
<td>Verification</td>
<td>Level of Acceptance</td>
<td>Likelyhood of travel provider acceptance of verified identity</td>
<td>Unlikely (e.g. illegal)</td>
</tr>
<tr>
<td></td>
<td>Confluence of Verifiers</td>
<td>Number of stakeholders allowed to verify pieces of D.I.</td>
<td>Single Verifier (gov)</td>
</tr>
<tr>
<td></td>
<td>Potential for Preclearance</td>
<td>Potential for traveller to pre-clear destination border pre-journey</td>
<td>No opportunity</td>
</tr>
<tr>
<td></td>
<td>Government Acceptance</td>
<td>Likelyhood of government official acceptance of verified identity</td>
<td>Unlikely (e.g. illegal)</td>
</tr>
<tr>
<td>Data Facilitation</td>
<td>Platform Security / Data Privacy</td>
<td>Level of security of platform and adherence to privacy considerations</td>
<td>Low / no ops improve</td>
</tr>
<tr>
<td></td>
<td>Traveller Ownership Of D.I.</td>
<td>Level of traveller ownership of digital identity</td>
<td>Low / no ownership</td>
</tr>
<tr>
<td></td>
<td>Integration Required With Stakeholders</td>
<td>Impact of integrating stakeholder systems / processes w/ model</td>
<td>High impact</td>
</tr>
<tr>
<td>Authentication</td>
<td>Operational Efficiencies</td>
<td>Number of &amp; impact opportunities to improve operations</td>
<td>Low / no Ops improve</td>
</tr>
<tr>
<td></td>
<td>CX Improvements</td>
<td>Number &amp; impact of opportunities to improve CX</td>
<td>Low / no CX improve</td>
</tr>
<tr>
<td></td>
<td>Application Outside Airport Ecosystem</td>
<td>Level and ease of deployment outside airport environment</td>
<td>Numerous challenges</td>
</tr>
</tbody>
</table>
1.4. GLOBAL PROGRESS

Since 2015, the pace of development and deployment of digital identity and biometrics solutions has accelerated, with initiatives ranging from pilots and trials to full deployments. As discussed in the Emerging Models section, WTTC has researched more than 80 initiatives that use biometrics, and new initiatives are launched frequently using the latest technologies. Overwhelmingly, these initiatives focus on the airport, airline, and border environment, with few exceptions extending beyond the airport ecosystem. Progress towards an integrated end-to-end journey has been slow, as have efforts to involve multiple countries beyond those within common political and economic systems.

Although the range of work across the sector is encouraging, WTTC recognises that there is a global patchwork that results in complexity and fragmentation. The lack of standards and of initiative coordination means that solutions may not be able to work together. As a result, travellers are unable to move seamlessly from one part of their journey to another using biometric technology (e.g., to non-airline and non-border segments, as these needs are often not factored into ongoing work). This approach presents challenges – to interoperability, to seamless travel across the entire journey, and to achieving a global approach that maximises adoption and utilisation – that WTTC would like to address.

Lack of interoperability and standards across initiatives and countries: Travel implies multiple touchpoints — multiple airports, geographies, travel providers — and transitions between segments of the journey are often challenging. The emergence of fragmented initiatives with a localised focus exacerbates the challenge of interoperability, which implies that different systems and devices can connect, exchange, and use data among disparate stakeholders. A set of standards to enable interoperability and global deployment and adoption is necessary.

Risk of consumer adoption: Many biometric initiatives implemented are siloed, functioning only with a specific airport or airline. These efforts present challenges to the consumer. Typically, silos require a user to register and maintain information with individual travel providers, which is cumbersome and presents additional exposure for traveller personal data. This may drive travellers to opt out of biometrics programs or to not fully participate.

Confined to airport ecosystem: Most initiatives are focused on the airport ecosystem and on border control and management. The complexities, data and identification needs, and risk tolerance beyond the airport envelope differs, and in some ways could be simpler and less stringent. The lack of involvement of non-air travel providers in current initiative development and deployment could present challenges in the future, thereby risking travel provider and consumer adoption.

Data privacy concerns: Data privacy — particularly across borders and without individual consent — has become a significant concern. New privacy regulations are developing, and requisite controls are not yet in place globally. Given the patchwork, the onus is on technology and travel providers to address nation-state data privacy regulations. In some cases, travellers do not control information or its flow, causing concern about the protection of their personal data. Efforts to address data privacy and guidelines and safeguards for the development of biometrics initiatives are necessary.

Based on these challenges, WTTC believes an integrated, attribute-based approach that aligns with standards will help increase interoperability, maximise adoption, and alleviate data privacy concerns, and it will continue to develop details on the models. It will also leverage the detailed process document to advance discussions on standards, minimum requirements, data privacy, border management, etc.

2. GOVERNMENT-DRIVEN MODEL

2.1. OVERVIEW

The “Government-Driven” model is a centralised approach to passenger and data facilitation. The government establishes and verifies the traveller’s identity and serves as the identity management service provider to other stakeholders within the airport ecosystem.

This model does not depend on formal traveller enrollment or adoption, as the government uses centralised databases of pre-verified “own nationals” and foreigner biometrics (facial) to authenticate a traveller. No other data is collected, and no booking information is integrated to create a digital identity.

The core platform is a cloud-based biometric matching service. The government can extend this to private sector providers as an Identity as a Service (IDaaS), which provides a scalable, secure and seamless solution that easily integrates with providers’ systems through web-based API connections.

Upon arrival at any journey touchpoint, a traveller’s image is captured by facial recognition technology (e.g., eGate, stand-alone facial recognition camera) and sent to the government verification system for authentication, returning a match result to the travel provider.

The “Government-Driven” model demonstrates applicability and implementation success at touchpoints across the airport ecosystem. Any traveller providing consent to participate experiences a streamlined journey without having to enrol in advance. The core challenge with this model is legislative restrictions that prevent the extension of IDaaS beyond its current mandated realm. As a result, there may be limitations when attempting to integrate car rental services and hotels into a model that was developed and approved for use only in the airport/governmental ecosystem.
2.2. POTENTIAL END-TO-END INTEGRATION OPPORTUNITIES

Regulatory constraints pose the largest challenge in implementing an end-to-end version of the “Government-Driven” model across the traveller journey. In effect, lawmakers are likely to be hesitant for border protection agencies, which focus on the border-crossing and immigration component of the travel experience, to allow private sector stakeholders access to their databases.

Still, STJ stakeholders have indicated that the extension of this model beyond mandated touchpoints is possible in the near to medium term, with biometric technology platforms increasingly creating end-to-end solutions that are scalable beyond the border. From an integration perspective, non-airport environment stakeholders (e.g., car rental services and hotels) would need to define their workflows, invest in the required technology for biometric capture, and follow the same procedures for integrating their physical infrastructure and systems into the governmental systems. Authentication using these integrated systems would remain the same – a traveller would approach a car rental area or hotel counter, have his or her image captured by facial recognition technology, and be authenticated using the government’s data system.

While this would provide a useful means to authenticate the traveller identity, the government model poses limitations in providing car rental services and hotels with traveller data in advance or in a more integrated manner. This could mean that after identity authentication, the traveller and travel provider are likely to have to complete the check in process in a manner that is similar to the current state. The diagram below shows how a “Government-Driven” model would function.

Figure 4. Simplified Process Flow “Government-Driven” Model

2.3. APPLICATIONS OF THE GOVERNMENT-DRIVEN MODEL

A number of initiatives, outlined below, have been implemented using the “Government-Driven” model.

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>INITIATIVE NAME</th>
<th>KEY POINTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIA</td>
<td>Seamless Travel Australia</td>
<td>• Provides a means to combine identification documents into a single token, enabling a more efficient traveller experience</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All stakeholders participating in the traveller’s journey trust the token created by the preceding stakeholder</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Able to create different tokens in the traveller’s digital wallet, allowing the traveller to choose which information is shared</td>
</tr>
<tr>
<td>UNITED ARAB EMIRATES</td>
<td>eGates and Biometric Immigration Tunnel</td>
<td>• Collects/stores citizen, resident and eligible guest biometrics for authentication at “government” touchpoints using eGates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Seamless, automatic biometric immigration tunnel available for travellers who have undergone iris enrolment</td>
</tr>
<tr>
<td>UNITED STATES OF AMERICA</td>
<td>Traveller Verification Service (TVS)</td>
<td>• Obtains facial biometrics from legally mandated government databases (traveller does not enrol to participate)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Partner airlines and airports capture live photos of travellers approaching biometric capture interfaces for authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A multitude of airlines and airports have undertaken pilots with TVS – primarily for biometric boarding</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TVS creates a faster and more secure disembarkation process for cruise passengers with individuals disembarking using facial recognition-matching services provided by TVS</td>
</tr>
</tbody>
</table>

In addition, to the examples presented above, the case studies below provide a more comprehensive look at how stakeholder groups interact with the “Government-Driven” model.

2.3.1 UNITED ARAB EMIRATES

UAE has deployed biometrics-based immigration control programmes allowing UAE nationals, residents and visitors from 32 nationalities to utilise Smart Gates when arriving at or departing from terminals at Dubai International Airport, Abu Dhabi International Airport and Al Maktoum International Airport. In 2018, nearly 11 million passengers used Smart Gates, accounting for more than 22% of travellers.

Data Capture & Digital Identity Creation/Verification

Iris data is collected when the traveller arrives at or departs from the country at airport immigration checkpoints. There are special facilities within UAE international airports that capture and process biometric – and Iris – enrolment. Iris enrolment supplements fingerprint biometric data already collected when citizens or permanent residents obtain the national ID card. UAE citizens, permanent residents, and foreign nationals from 32 countries can opt-in to this enrolment process at immigration checkpoints.

1 Information collected as of July 2019
2.3.2. UNITED STATES OF AMERICA

The United States Customs and Border Protection (U.S. CBP) has leveraged its Traveler Verification Service (TVS) to provide secure, efficient, automated biometric identification verification for those entering and exiting the USA. TVS is a cloud-based biometric matching service, which CBP has extended to its private sector partners within the airport ecosystem (e.g., global airlines, US airports, and Transportation Security Administration (TSA)).

Enrolment/Digital Identity Creation & Identity Verification

Under this model, the traveller does not formally enrol to participate in any TVS supported initiatives. CBP builds a gallery of photographs based upon the flight manifest that is collected from Department of Homeland Security (DHS) holdings. These include the Department of State’s passport and visa databases and the U.S. Office of Biometric Identity Management (OBIM) that collectively contain facial biometrics of travellers who have previously entered or departed the United States, including US citizens, permanent residents, and foreign nationals. TVS does not collect any new biographic traveller data, in addition to the booking data that has historically been collected, nor does TVS integrate any booking data provided by travel providers. Photos of US citizens are purged from CBP systems within 12 hours. Photos of non-US citizens are retained for 75 years (this is consistent with existing CBP system of records notices).2

Verification of facial biometric data occurs at the point of collection; namely, during the passport application process (for US citizens), during the application for a US visa, or upon entry into the United States, and exit at select locations. This process allows the government to establish the identity of the traveller, which can be trusted by any other government official or private sector stakeholder.

Prior to a scheduled flight, CBP uses Advance Passenger Information System (APIS) data to build a temporary gallery of photograph templates and unique identifiers from DHS holdings (using defined targeting rules) for all expected passengers on flights departing from or arriving into the US. This gallery is updated in close to real time as updates are made to traveller APIS. These galleries result in a “one to small N” solution and facilitate biometric traveller identification from a subset of verified identities. Subsequently, CBP securely pushes these galleries and identifiers into TVS.

Data Facilitation

The CBP model relies entirely on TVS to manage traveller and data facilitation across the airport environment. This is a secure platform that has carefully defined business rules around how traveller facial biometric data can be used. Per the existing CBP business rules, stakeholders may not use data collected for TVS matching for any other business purpose, and the data cannot be retained.

CBP provides its partners with an array of tools to ensure easy and efficient connectivity between TVS and a partner’s interfaces and systems. TVS is technology-agnostic, which allows for flexibility in connecting with a partner’s facial biometric capture technology at any given airport touchpoint. TVS ensures the integrity of traveller data by irreversibly encrypting traveller photos before uploading to TVS’s secure cloud-based environment. Furthermore, beyond the unique ID (UID), no other traveller information is stored in the cloud.

Overall, CBP has a standardised, clear process for sharing TVS data with partner systems.

Traveller Verification

To identify and verify travellers at a respective touchpoint, partner airlines and airports can take a live photo of the traveller as the traveller approaches a biometric device. TVS

2 See www.cbp.gov/biometrics for more information
3 A biometric template is a digital representation of a biometric trait of an individual generated from a biometric image and processed by an algorithm. The template is usually represented as a sequence of characters and numbers. For CBP’s TVS templates cannot be reverse engineered to recreate a biometric image. The templates generated for the TVS are proprietary to a specific vendor’s algorithm and cannot be used with other vendor’s algorithms.
2.4. OPPORTUNITIES

compares the traveller’s photo against its photo galleries in real-time and responds with the identity verification match results, using the unique identifiers associated with the traveller. This removes the need for manual checks or for travellers to produce their travel documents to proceed through an airport touchpoint. The accuracy rate of the facial biometric process is as high as 99 percent, and the process takes less than two seconds. Once traveller verification is complete, the temporary gallery is deleted.

Currently, most efforts have focused predominately on biometric exit at the boarding gate; currently, CBP has partnered with airlines and airports at 21 exit locations. However, some airlines, including Delta Air Lines, are expanding biometrically enabled touchpoints using TVS to include check-in, bag drop, Transportation Security Administration (TSA) security, and boarding. Travellers have the option to use these biometric-enabled touchpoints or proceed with standard, manual processing.

Airlines and airports have invested in and implemented the required physical biometric technology infrastructure (e.g., eGates, stand-alone facial recognition cameras) at select airports, which varies depending upon the location. Some airports, like the Orlando International Airport, work independently to implement physical biometric technology infrastructure and lease biometrically enabled gates to airlines. Alternatively, airlines like Delta Air Lines, have led efforts to implement biometric infrastructure and technology at their major hubs since they own a sizeable amount of the airport.

A number of airlines and airports have undertaken pilots with TVS – primarily for biometric boarding, but more recently for other airport touchpoints as well. Pilot programs vary in approach, scope, and technology used; however, the majority share several commonalities, including no traveller requirement to pre-register to participate in the programme (CBP already has travellers’ biometrics, as mandated by US law), and no required additional traveller biographic information or documents (in person or online). CBP will continue to expand biometric partnerships with airlines and airports and has also partnered with four cruise lines to implement facial biometrics in the debarkation process of closed loop cruises.

2.4. OPPORTUNITIES FOR CONTINUED EXPLORATION

There are multiple opportunities for continued exploration and consideration, namely:

- Process of sharing biometric and biographic data with non-governmental entities
- Ability for private sector stakeholders to connect to government databases and the infrastructure associated with enabling such connections
- Limitations of travellers whose biometrics and identity are not already captured
- Ability to allow travellers to verify additional aspects of their identity and travel (e.g., Driver’s License, booking information, or payment information)

3. PER TRIP MODEL

3.1. OVERVIEW

The “Per Trip” model is a semi-federated approach to traveller and data facilitation throughout the traveller journey. Unlike the “Government-Driven” Model, the traveller has the choice to opt-in to participate in “Per Trip” travel experiences at the time of enrolment. Following enrolment, however, the traveller’s “Per Trip” digital identity is managed and facilitated by an identity management platform, which is responsible for safeguarding and supplying relevant parts of the traveller’s digital identity on a “need to know” and “authorised to know” basis.

The enrolment process for “Per Trip” travel experiences typically begins upon arrival at the airport, through the use of biometric check-in kiosks to verify travellers’ biographic information and facial image (biometric token), using approved verification capabilities embedded in the data orchestration platform. This creates a digital identity that lasts only for the duration of the journey.

In this model, data is stored, managed and facilitated by an orchestration platform, which all stakeholders trust to supply verified traveller data. Connections between the orchestration platform and travel provider or government agency systems normally only require API integrations. These platforms are built to adhere to “privacy by design” principles and securely store and transmit encrypted traveller data to stakeholders on a “need to know” and “authorised to know” basis.

A traveller is authenticated upon arrival at a touchpoint, with facial recognition technology capturing the traveller’s image and transmitting it to the orchestration platform, to then receive an authentication status as well as any data required for the touchpoint stakeholder to finish processing the traveller.

The “Per Trip” model has emerged as one of the most prevalent models tested and implemented worldwide. This model is widely accessible to a broad set of travellers, including infrequent travellers and non-nationals of that country. It is also relatively easy to implement from a technical perspective and easy to use from a customer experience perspective. A key challenge for designing an end-to-end model will be extrapolation beyond the airport environment as well as ensuring disparate parts of the journey (e.g., connecting flight at another airport) are included without needing to re-enrol.
3.2. POTENTIAL END-TO-END INTEGRATION OPPORTUNITIES

The “Per Trip” model leverages a public-private partnership model that serves as the foundation for stakeholder collaboration and trust; ensuring joint responsibility for managing a traveller’s digital identity and data over the course of the “Per Trip” duration. This model could enable travellers to enrol at the first point in their traveller journey – airport, hotel, car rental, or cruise - by stationing a check in or verification kiosk in these locations. Travelers would need to provide a valid biometrically embedded travel document to capture and verify biographic data and take a “selfie” to verify their facial biometrics. This process could integrate booking data with a digital identity, to ultimately create a “Single Journey Token” that lasts for the duration of the traveller’s journey.

Digital identity verification would also need to occur at enrolment, using biometric capabilities built into the orchestration platform and agreed upon by all partnering stakeholders. This end-to-end model relies on an orchestration platform integrated into stakeholder systems through API integrations, which securely store and manage the traveller’s data.

Given the public-private partnership nature of this model, it offers opportunities across many traveller journey touchpoints – including border control, security, airline, hotel, and car rental. Each touchpoint will require investment in technology to capture and authenticate travellers’ biometrics; however, stakeholders could define workflows that mirror current day processes while enabling integration with the orchestration platform. The diagram below shows how a “Per Trip” model would function.

Figure 5. Simplified Process Flow ‘Per-Trip’ Model

3.3. APPLICATIONS OF THE PER TRIP MODEL

The “Per Trip” model is being piloted or implemented in various countries. Below is an overview:

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>INITIATIVE NAME</th>
<th>KEY POINTS</th>
</tr>
</thead>
</table>
| ARUBA AND THE NETHERLANDS| Aruba Happy Flow, Seamless Flow Netherlands (Implemented) | • Traveller enrols pre-journey, allowing the government to store the data in a single biometric token that lasts 24 hours  
• Leverages existing stakeholder processes to authenticate and permit access at a given touchpoint |
| AUSTRALIA                | Sydney Airport - Facial Recognition Pilot (Piloted)  | • Travellers begin enrolment and create “Per Trip” token using biometric check-in kiosk upon airport arrival; the kiosk compares visitor’s facial data to biometric data  
• Sydney Airport strives for a “common-use goal” that allows any airline and vendor to integrate onto the platform |
| FRANCE                   | Air France - Biometric Boarding Pass (Piloted)      | • Encodes passenger’s biometric facial data in Biometric Boarding Pass barcode  
• At check in on Air France app or at airport kiosk, customers scan passport and issued biometric pass contains encrypted biometric facial data from passenger’s identification documents  
• At boarding or baggage drop, traveller scans boarding pass and a camera will identify and authenticate them, eliminating need for passenger to present identification |
| HONG KONG                | Smart Departure e-Channel (Fully operational)       | • Automated biometric arrival and departure process that speeds up air, land and sea immigration at control points  
• Frequent travellers can enrol in the e-Channel if they meet specific criteria and requirements  
• Departing visitors not enrolled can use e-Channel by scanning an ICAO compliant ePassport or electronic travel document from countries or regions designated by Immigration Department or Hong Kong Special Administrative Region (HKSAR) |
| UNITED KINGDOM           | London Heathrow (LHR) Passenger Identification Programme (Implemented) | • Utilises ‘Per Trip’ travel token that lasts 24-hours, leveraging infrared facial biometric cameras at touch points (e.g., bag drop, gates) to facilitate authentication of travellers  
• Heathrow testing use of off airport enrolment via mobile device and U.S. CBP’s IVPS |
| SINGAPORE                | Fast and Seamless Travel (FAST) (Implemented)       | • Passengers with fingerprints registered through Immigration & Checkpoints Authority eligible to use self-service facilities  
• Passengers will have photos taken at Auto Bag-Drop, Immigration Gate and Boarding Gate for identity verification  
• Registered travellers may use automated immigration gates by scanning their passport, boarding pass and fingerprints |

In addition to these examples, the case studies below provide a more comprehensive look at how stakeholder groups interact with the “Per Trip” model.

4 Information collected as of July 2019.
3.3.1. ARUBA HAPPY FLOW

Enrolment/Digital Identity Creation & Verification

Upon reaching the check-in touchpoint at Aruba International Airport, travellers begin the one-time enrolment process for Aruba Happy Flow by opting into the “Per Trip” experience at the biometric self-service check-in kiosk. The traveller presents an ePassport, the passport is authenticated, and the identity of the passenger is verified through biometric matching of the photo in the ePassport chip. This is done through 1:1 matching and the same standards set by the government for automated border control. Once the identity is established, the passenger finishes check in, and the traveller’s biographic information and captured facial image are consolidated to create a Passenger Data Envelope (Single Biometric Token) that is stored and managed for reuse throughout the traveller’s journey. Because of legal restrictions, the Passenger Data Envelope is only stored for 24-hours. The traveller uses only biometrics for identification at baggage drop, immigration, secure access points, and boarding zones.

Data Facilitation

Aruba Happy Flow’s data driven process is based on open standards and is vendor-agnostic, allowing flexible connectivity to any external platform, hardware, or software.

As a result, this platform provides seamless connectivity to existing workflows and high flexibility for workflow changes, minimising impact to stakeholder processes. The data platform stores and manages the Passenger Single Token throughout the life of the traveller journey, sharing required traveller biographic and biometric data with stakeholders on a “authorised to know” and “need to know” basis. The platform adheres to the internationally recognised “privacy by design” standard, and the architecture and design reflects GDPR privacy compliance standards and ensures that accountability and strong governance is built into the system. The platform generates real time information on the journey that stakeholders use for workflow management. This improves oversight, efficiency and timely delivery of operations.

Authentication

Aruba Happy Flow is a streamlined sequence of user-friendly, self-service touchpoints across the airport environment. At each touchpoint, the traveller uses interfaces that contain facial-recognition devices to authenticate his or her identity, with the facial image matched to the one stored in the Passenger Single Token. The systems at these touchpoints are linked through API connections to the Aruba Happy Flow platform. The match occurs in real-time (1:N matching), returning data required by the stakeholders to process a traveller. No passports or other documents are needed post-check in/enrolment; the traveller’s face serves as the single token required for access at all subsequent touchpoints.

The model offers the potential to extend beyond airports to include car rental and hotel touchpoints as well as mobile enrolment, the focus of “Aruba Happy Flow Phase 2”. Car rental services and hotels would be required to define existing workflows and connect their systems to the platform through API connections. They will then join the federated identity management system and accept the identity established by one of the stakeholders (government). Key challenges to expansion include ensuring hotel and car rental process requirements are met and regulatory requirements are addressed. Once operational requirements and workflows are defined, the Passenger Data Envelope can expand to hold any data fields required by car rental and hotel minimum requirements.

Aruba Happy Flow also wants to prepare for digital passports, allowing for home or mobile enrolment.
3.3.2. LHR PASSENGER IDENTIFICATION PROGRAMME

London's Heathrow Airport has operated a facial biometric system for 10 years. The current system is being utilised in Terminals 2 and 5 at security checkpoints and boarding gates, by domestic travellers.

Heathrow has collaborated with the airline community and the UK Government to enhance its current biometric system and create a seamless travel experience for all customers. One initiative revolves around a “Per Trip” digital identity that allows travellers access across various airport touchpoints. Other initiatives include collaboration with the U.S. CBP’s TVS system and testing an off-airport mobile solution. Although many initiatives are still in pilot mode, they focus on leveraging boarding passes and facial biometrics to authenticate travellers against their ePassport across the airport ecosystem. Heathrow is working with a global group of airports and airlines to create an end-to-end cross-border pilot and create a truly seamless journey. Once enrolled, this system will allow a customer to use his or her face as identification throughout the departure process. Additionally, Heathrow is working with the UK Government on extending the use of biometrics into arrivals.

Enrolment/Digital Identity Creation & Identity Verification

Heathrow has partnered with several suppliers to create digital identities for travellers and develop their passenger identification programme. All activities create a “Per Trip” travel token, to comply with regulatory requirements. This is stored using an identity management software that clears associated references after a 24-hour period. “Per Trip” token creation only requires travellers to supply passport-related biometric and biographic information using an ePassport; no additional information is collected by Heathrow nor is booking data integrated into the digital identity. The captured facial image serves as the key for travellers to access touchpoints across the traveller journey. The system interfaces with airline DCSs but does not hold the biographic information (i.e. APIS) that is required by the airline.

For mobile enrolment, a traveller uses an identity management platform on a mobile device. First, the traveller uses the app to read the Machine-Readable Zone (MRZ) of his or her passport to gain access to the chip and the biographic data from the passport. Next, the biographic data uploaded through the MRZ is verified and the traveller can take a “selfie” with liveliness to authenticate the image on the passport. Heathrow is continuing to explore when this capability would be integrated into its solution.

For in-person enrolment, a traveller undertakes a similar process by using a biometric check in kiosk, at Self Service Bag Drop or at a manual check in desk. All methods require the use of an ePassport.

Data Facilitation

The Heathrow model also depends on a form of boarding pass at each touchpoint. The boarding pass serves as a key with embedded standards that direct a touchpoint system towards the specific database containing the traveller’s digital identity. This is essential for model feasibility, given the number of databases used at Heathrow. Heathrow believes there will not be one method for verifying identity and does not wish to store unnecessary personal data on airport servers.

Heathrow is identifying and piloting how integration between systems will work and continues to consider data security and privacy questions. The next step is identifying key standards around biometrics (particularly format and content standards) to ensure model feasibility and interoperability.

Authentication

Heathrow leverages various biometrically enabled touchpoints to facilitate traveller authentication. Touchpoints include Self Bag Drop, entrance to security, and self-boarding gates. The use of gates through the departure and arrival journey provides a level of control from an operational perspective and gives passengers a degree of assurance that they are completing the digital process correctly. Upon arrival at a touchpoint, a traveller scans their boarding pass and captures their facial image. These two pieces of data allow for an authentication match against the appropriate database and return the authentication status for traveller admissibility.

3.3.3. SYDNEY AIRPORT FACIAL RECOGNITION PILOT

Since 2017, Sydney Airport has explored and implemented biometric initiatives to improve customer experience and terminal planning. Sydney Airport’s “Per Trip” model utilises active and passive traveller facilitation. Travellers create a travel token at airport check in, leveraged at check in, bag drop and boarding. Sydney has also installed additional biometric kiosks in security areas and at airline lounges to passively identify travellers, improve on-time performance, and enhance the traveller experience.

Sydney Airport has completed the pilot phase for this “Per Trip” experience and is continuing to identify opportunities to integrate in order to enable the government to process passengers earlier in the traveller journey. Sydney Airport also hopes to explore opportunities around “Per Life” Digital Identities.

Enrolment/Digital Identity Creation & Identity Verification

Travellers begin enrolment upon arrival at airport check in. In its pilot phase, Sydney Airport has had limited participation from a subset of Qantas passengers, who must explicitly consent to participate by accepting an electronic, on-screen privacy agreement valid for the duration of the trial.

Travellers create their “Per Trip” token by inserting their ePassport at a biometric check-in kiosk. The kiosk reads the traveller’s biometric and biographic information, which are verified against the traveller’s airline booking information and through a live image taken by the passenger. No additional traveller information is required to create the “Per Trip” travel token, which lasts for the life of the trial. Following enrolment, a traveller proceeds onto the airline’s application (at the same kiosk) to finish check in and obtain their boarding pass, through the integration of the check in application. The travel token is stored on the Identity Management Platform layer.

Data Facilitation

Sydney Airport strives for a “common use goal” that allows any airline and vendor to integrate onto the platform, which connects to relevant touchpoints (e.g., bag drop, boarding) and adheres to “privacy by design” principles. Sydney Airport has proactively undertaken privacy impact assessments and data breach plans to provide assurance and response in the case of an incident.

Authentication

Upon arrival at bag drop and boarding touchpoints, the traveller’s image is captured by facial recognition technology and compared against a gallery of images stored within the platform, which subsequently returns the authentication results. For the pilot, travellers are required to obtain a paper boarding pass for contingency arrangements should an issue arise in the journey. Due to regulations, passports must be presented at boarding after biometric authentication.

Sydney Airport has also installed “on the move” cameras that passively capture traveller movements at security and lounge entry. The platform is updated with location information via operational dashboards, which provide updates to relevant airport stakeholders and can be useful for assisting airline operations.
3.4. OPPORTUNITIES FOR CONTINUED EXPLORATION

There are opportunities for continued exploration of the “Per Trip” model including:

- Evaluating requirements for extending a “Per Trip” travel token beyond a single airport environment (connecting flight, hotel, car rental services, etc.)
- Ensuring that the “Per Trip” token lasts for the traveller’s entire journey
- Understanding how biometric and biographic data is shared with different stakeholders before the traveller reaches the touchpoint
- Aligning on types of verification required to ensure stakeholder trust (e.g., in-person verification versus eVerification)
- Deciding who invests in and pays for the infrastructure required to create this system

4. PER LIFE MODEL (MULTIPLE TRIP MODEL)

4.1. OVERVIEW

The “Per Life” model is a federated approach to traveller and data facilitation throughout the traveller journey. The traveller has full discretion over how much, to whom and at what point his or her data is shared. The traveller also retains data integrity by storing his or her digital identity on a mobile device.

The “Per Life” travel experience typically begins with the creation of a digital identity on a traveller’s mobile device using a digital identity management app. This initial enrolment allows the traveller to upload and verify core pieces of his or her identity (e.g., passport biographic information, facial image) using the app’s built in eVerification capabilities. Upon completion, the digital identity resides on the traveller’s mobile device “for life”. The traveller may add as much additional information as desired and can perform one-time verification of this information with relevant, trusted stakeholders (who may be but are not required to be government agencies). Finally, the traveller easily integrates bookings into digital identity to allow for seamless data management and sharing.

Pre-journey, a traveller “pushes” minimum required data to relevant travel providers or government officials from a mobile device. Data facilitation is managed by distributed ledger technology and cryptography, ensuring the secure transfer of data. Upon receiving traveller data, stakeholders can perform a host of activities: government officials can perform risk-based assessments to streamline security processes and travel providers can leverage shared data to enhance the traveller experience. Upon touchpoint arrival, a traveller is authenticated via facial recognition technology, which captures the traveller’s image, authenticates it against received data, and receives an authentication status.

The “Per Life” model offers numerous opportunities for secure, seamless travel experiences across a multitude of use cases. The key challenge for end-to-end model consideration will be ensuring stakeholder acceptance and trust in this level of federated digital identity.
4.2. POTENTIAL END-TO-END INTEGRATION OPPORTUNITIES

The “Per Life - multiple trip” model allows the traveller to seamlessly share desired data when and with whom they want. The traveller creates and manages his or digital identity on a mobile device, creating a federated model for identity management and verification.

Enrolment/Digital Identity Creation & Verification

The “Per Life” travel token would be created before a journey when the traveller opts in by downloading a digital identity management app on his or her mobile device. In a one-time enrolment process, the traveller uses the app to scan his or her passport MRZ to gain access rights to the chip and read the biographic data. The traveller could then add additional biographic, biometric and other data (e.g., payment or frequent traveller information) as well as upload supporting documents (e.g., passport or driver's license) through the app’s interface, creating the complete “Per Life” digital identity.

One-time digital identity verification would also need to occur at enrolment. Upon successful verification of the data uploaded to the virtual wallet against supporting documentation with the relevant stakeholder, the verifying authority digitally signs off on the traveller’s “Per Life” digital identity by securely adding the verification results to the public blockchain using one-way hashes.

Data Facilitation

The supporting infrastructure consists of four enabling components: biometrics, mobile technology, distributed ledger and cryptography. Mobile technology and cryptography ensure that the digital identity can live on the traveller’s mobile device indefinitely and that the traveller retains full ownership over his or her digital identity. Distributed ledger technology and cryptographs manage the secure facilitation of the traveller’s data between the traveller’s mobile device and travel provider/government agency systems. From a technical perspective, the data exchange between a traveller’s phone and a stakeholder’s systems occurs through a secure envelope that is digitally signed and encrypted.

Blockchain serves as the primary validation point for traveller data. Each time a new record is added, it is encrypted and signed with the private key of the writing party, creating an authenticated audit trail of certifications. This serves as a safeguard against hackers, who cannot access original traveller data.

Traveller Data Sharing

Prior to travel, a traveller would receive minimum data requirements to share with stakeholders, based on regulatory or operational requirements. Data should only be shared on a “need to know” and “authorised to know” basis, although the traveller may provide more or less information. The traveller pushes this data from a mobile device and allows the distributed ledger infrastructure with cryptography safeguards to facilitate the data transfer to the intended government agencies or travel providers.

Traveller Authentication

Stakeholders may access shared data prior to traveller arrival at a touchpoint, enabling government officials to pursue more rigorous information verification, stronger risk assessments, and earlier decisioning. Travel providers can also streamline customer experience using advanced traveller data.

An industry stakeholder installs facial recognition technology at a given touchpoint and connects it to the internal back-end system. This system is further integrated with the blockchain infrastructure to access and verify shared traveller information and flag exceptions for manual processing.

The touchpoint’s facial recognition technology captures and sends the traveller’s image through the travel providers/government agency’s system to authenticate against the embedded, shared traveller biometric in the blockchain. After authentication, blockchain will provide the travel provider/government official any data shared previously by the traveller that is needed to finalise a decision.

The diagram below shows how a “Per Life” model would function.

Figure 6. Simplified Process Flow – “Per Life” Model
4.3. APPLICATIONS OF THE PER LIFE (MULTIPLE TRIP MODEL)

Several initiatives leveraging various technologies have been implemented using the “Per Life” model.

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>INITIATIVE NAME</th>
<th>KEY POINTS</th>
</tr>
</thead>
</table>
| CANADA          | Chain of Trust Project (In Development) | - Used to identify low-risk individuals to facilitate processing and improve the traveller experience  
|                 |                  | - Traveller uploads/verifies core biographic data and facial image to enrol, creating a traveller token that lasts for the life of a passport  
|                 |                  | - Traveller data is sent to the cloud for identity verification  |
| INDIA           | Dig Yatra (Pilot implementation, expected in December 2019) | - Passengers enrol in a Government-Airport shared platform by providing name and identity details  
|                 |                  | - Airport registration kiosk used for one-time validation (online for Aadhaar digital identity or manually for Central Industrial Security Force (CISF) verification)  
|                 |                  | - Passengers scan boarding pass or e-ticket and identity verified using facial recognition technology  
|                 |                  | - A single token is created for the journey, facial recognition is enabled at security, baggage, immigration, and boarding  |
| MALAYSIA        | AirAsia – Fast Airport Clearance Experience System (FACES) (Implemented) | - AirAsia’s Fast Airport Clearance Experience System (FACES) emphasises facial recognition for boarding  
|                 |                  | - Traveller’s facial image compared against gallery associated with the flight, allowing approved travellers to proceed seamlessly and others to undergo checks  |
| NOT APPLICABLE  | Forum – Known Traveller Digital Identity (KTDI) (In Development) | - Interoperable system being piloted between the Netherlands and Canada that connects security systems of stakeholders and enables them to access a traveller’s identity data  
|                 |                  | - To build trusted “Known Traveller” status, travellers need authenticated claims added to their KTDI profile  |
| SOUTH KOREA     | SmartPass (In Development – Initial phase to be tested in 2020 with initiative to be accomplished in 2023) | - Travellers pre-register facial recognition and biometric data with SmartPass service prior to the journey  
|                 |                  | - Incheon Airport plans to implement the following technology-enabled services, using the pre-registered data:  
|                 |                  | - Facial recognition technology enabled SmartPass check-in and boarding  
|                 |                  | - Home luggage drop-off courier service enabling passengers to have luggage delivered to airport and loaded onto aircraft  
|                 |                  | - Walkthrough tunnel security screening  
|                 |                  | - Intelligent CCTV security surveillance system  |
| UNITED STATES OF AMERICA | CLEAR (Implemented) | - Collects traveller biographic, biometric, and payment data at time of enrolment pre-journey and stores it in secure cloud-based platform  
|                 |                  | - Expanded model to multiple journey touchpoints, including TSA security, boarding, lounge access, and car rental  |

In addition to the highlighted examples, the below case studies provide a more comprehensive look at how stakeholder groups interact with the “Per Life” model.

4.3.1 AIRASIA - FAST AIRPORT CLEARANCE EXPERIENCE SYSTEM (FACES)

AirAsia’s Fast Airport Clearance Experience System (FACES) is a “Per Life” passenger and data facilitation model, with an emphasis on facial recognition for boarding. Unlike the “Per Life” model in which the traveller’s digital identity is stored on a mobile device, FACES stores the traveller’s digital identity in a cloud solution for multiple trips, until a traveller has to renew the passport. As a result, FACES lends itself to effective scalability as AirAsia expands biometric capabilities at other airports and across other journey touchpoints, pending any regulatory restrictions and approvals.

Enrolment/Digital Identity Creation

The traveller opts-in to perform one-time enrolment for FACES either off-premise via a mobile device or in person at the airport before or after check-in. For in-person enrolment, a traveller uses a kiosk to scan the ePassport and/or MyKad [for domestic flights in Malaysia]. The kiosk extracts the traveller’s biographic data using the MRZ and verifies this information against the biographic data stored in the ePassport chip. The traveller then uses the kiosk to capture his or her live image, which is verified against the face image stored in the ePassport chip. This process takes approximately 30 seconds.

Mobile enrolment (for iOS and Android) follows a similar process: a traveller downloads the AirAsia app and creates a myFACES account. The traveller takes a video of his or her face and scans passport information, creating a pre-verified digital identity stored in the FACES cloud and a QR code stored on the traveller’s app for accessing the digital identity. Afterwards, the traveller must perform a one-time in-person verification with a ground agent, who accesses the uploaded biographic and biometric information using the QR code. The ground agent scans the QR code, which locates the digital identity stored in the cloud and verifies the identity against the traveller’s physical documentation. The ground agent makes a final verification decision and uses their system to sign-off on the digital identity, allowing travellers to skip verification on subsequent trips. This digital identity is stored “Per Life” in the FACES’ cloud-based solution. No other traveller information is required and no booking information is stored in the digital identity.

Data Facilitation

The traveller’s digital identity is stored securely until document renewal in the FACES cloud platform, which is provided by Google (AirAsia’s technology partner) but owned and managed by AirAsia. AirAsia seamlessly connects the cloud platform to security and boarding touchpoints using APIs, which will transfer the required information to a stakeholder agent at the appropriate time in the journey.

Authentication

Currently, FACES only works at boarding checkpoints, with additional touchpoints being explored pending regulatory constraints. These additional touchpoints may require different system and data requirements and will present additional challenges when identifying financiers for new infrastructure.

Initially at Senai Airport, AirAsia installed eGates for traveller authentication, and has recently leveraged “rovers” at airport gates it does not own. Rovers provide an efficient, scalable solution that runs on Wi-Fi with encrypted servers. At boarding gates, gate agents can easily set-up the rovers one to two hours before boarding; they can start a rover at a gate and use the administrative interface to select the flight, which pulls the digital identities for that flight from the iCloud based on the flight itinerary. This...
4.3.2. CANADA - CHAIN OF TRUST CANADIAN SAFETY AND SECURITY PROGRAMME CSSP

Localised approach allows for faster authentication since it narrows the match results the system must explore. Upon arrival at a touchpoint, a traveller’s facial image is captured by the rover and compared against the gallery associated with the flight. The rover will instantaneously return authentication results, allowing approved travellers to proceed and others to undergo additional checks. In the background, the relevant traveller information is also pushed through the API call-back to the Navitaire DCS, to record that the passenger has boarded. Once boarding is complete, the rovers are shut down and the locally stored digital identities are immediately deleted.

4.4. OPPORTUNITIES FOR CONTINUED EXPLORATION

There are opportunities for continued exploration and consideration for the “Per Life” model, including:

- Deciding what data should be integrated into a “Per Life” digital identity
- Deciding who establishes the traveller’s identity and at what point in the traveller lifecycle it should be established
- What verification will be required to ensure that all stakeholders trust the digital identity
- How legislation will need to change to allow government officials to accept digital identities as a form of identity authentication

Authentication

Upon arrival at the Canadian border, pre-verified travellers use an immigration biometric corridor for seamless authentication without breaking stride via “on the move” technology. Border control agents provide guidance as travellers progress across the border, but due to the advanced risk-based assessment, their focus is redirected towards higher threats, only intervening in the authentication process for travellers who require additional screening or questions.

Enrolment/Digital Identity Creation & Verification

Traveller enrolment leverages a mobile-enabled “automated digital enrolment and claimed identity verification service” designed for immigration and border management. To enrol, a traveller opts-in by downloading the supporting app on a smartphone and creating an account. The traveller uploads and verifies core biographic data by taking a picture of the data page on the passport. The traveller then places the passport near the smartphone to extract the data and signed certificates from the chip that allow for data verification. Finally, the traveller captures a “selfie” to verify the facial biometric against that of the passport chip. In the demonstration project, university and CBSA partners researched and tested the ability to recreate a biometrically derived token without storing biometric data directly.

Throughout enrolment, the automated back-end system “verifies the claimed identity, checks the validity of documentation, feeds into the prototyped processes to determine eligibility, checks for watchlist alerts, and facilitates risk analytics to process the final decision”. The solution is built using best practice standards based on ICAO-compliant eMRTD and trusted International Organization for Standardization (ISO) quality images for biometric matching. This verification process results in enhanced facilitation for lower risk travellers at border control, increased security, and better targeting of higher risk threats.

Data Facilitation

This data management platform seamlessly integrates with application processing and identity management solutions used at borders. The solution leverages stakeholder workflows to readily identify required configurations, integrations and monitoring capabilities to connect to stakeholder systems. The solution is designed to inherently adhere to “privacy by design” and GDPR mandates to provide the highest level of security for a traveller’s data. After verification, the data is passed to the government systems and no longer retained by the front-end verification application or server components.
5. MODELS COMPARISON & ASSESSMENT

As the previous sections illustrated, the three core categories of emerging models contain rich and multifaceted examples of how these models have been or are planning to be deployed. There is no “one-size-fits-all” approach to create a seamless travel experience. As such, these model types form a strong foundation upon which WTTC’s vision for a Seamless Traveller Journey can be built.

As work continues to build the STJ initiative, it is important to assess the strengths and weaknesses of each model type. Figure 7 below presents a comparison of the model types using the Comparison Framework presented in the Introduction section of this paper and employed throughout the Emerging Models section. To supplement this comparison, Figure 8 provides an initial analysis of key strengths and limitations through the lens of the Assessment Framework also presented in the Introduction.

Figure 7: Models Comparison (Completed Based on Captured Insights)

<table>
<thead>
<tr>
<th>ENROLLMENT / DIGITAL IDENTITY CREATION</th>
<th>GOVERNMENT</th>
<th>PER TRIP</th>
<th>PER LIFE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMING IN TRAVELLER JOURNEY</td>
<td>N/A</td>
<td>Check-in</td>
<td>Pre-journey</td>
</tr>
<tr>
<td>TRAVELLER ADOPTION</td>
<td>Biometric collection mandated by law; traveller participation in experience through opt-in</td>
<td>Opt-in</td>
<td>Opt-in (downloading identity mgmt. app on mobile device)</td>
</tr>
<tr>
<td>DATA REQUIREMENTS</td>
<td>Facial biometric, iris, fingerprint</td>
<td>Biometric (APIS); biometric (facial)</td>
<td>Any biographic, biometric, other data</td>
</tr>
<tr>
<td>SYSTEM / TECHNOLOGY REQUIRED</td>
<td>Government-driven (Daas)</td>
<td>Biometric self service check-in (Kiosk)</td>
<td>Mobile device; identity mgmt. app</td>
</tr>
<tr>
<td>PROCESS FOR ENROLLING / CREATING D.I.</td>
<td>N/A</td>
<td>Use passport and selfie at check-in kiosk or counter to create identity</td>
<td>Download app; upload desired data into app (creates digital wallet)</td>
</tr>
<tr>
<td>TOKEN RETENTION</td>
<td>Biometric ‘galleries’ last 10 years</td>
<td>Per trip (24 hours)</td>
<td>Per life</td>
</tr>
<tr>
<td>INTEGRATION OF BOOKING DATA</td>
<td>N/A</td>
<td>Airline reservation information (at check-in)</td>
<td>After given booking (Add to digital identity)</td>
</tr>
<tr>
<td>VERIFICATION</td>
<td>N/A</td>
<td>Check-in</td>
<td>Initial enrolment &amp; ongoing (for additional pieces of information added to D.I.)</td>
</tr>
<tr>
<td>VERIFYER OF DATA</td>
<td>Government</td>
<td>Orchestration system’s built-in verification capabilities</td>
<td>eVerification capabilities of identity management app (initial enrolment); stakeholders of sufficient authority (e.g. credit card issuer for payment info)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ENROLLMENT / DIGITAL IDENTITY CREATION</th>
<th>GOVERNMENT</th>
<th>PER TRIP</th>
<th>PER LIFE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA VERIFIED</td>
<td>Facial biometrics</td>
<td>Biographic (APIS); biometric (facial) - against passport and booking data</td>
<td>Any data added to D.I. (biographic, biometric, other data)</td>
</tr>
<tr>
<td>SYSTEMS / TECHNOLOGY REQUIRED</td>
<td>N/A</td>
<td>Biometric self-service check-in kiosk; orchestration system’s built-in verification capabilities</td>
<td>eVerification capabilities of identity management app (initial enrolment); manual document inspection against digital identity (ongoing)</td>
</tr>
<tr>
<td>VERIFICATION PROCESS</td>
<td>N/A</td>
<td>Verification capabilities in orchestration platform; eVerification (on app)</td>
<td>Use eVerification or manual check against supporting docs; results added to traveller’s blockchain</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUTHENTICATION</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>TIMING WITHIN TRAVELLER JOURNEY</td>
<td>Each journey touchpoint (post-check-in) in airport environment</td>
<td>Each journey touchpoint (post-check-in) in airport environment</td>
<td>Each end-to-end touchpoint</td>
</tr>
<tr>
<td>AUTHENTICATOR</td>
<td>Touchpoint stakeholder</td>
<td>Touchpoint stakeholder</td>
<td>Touchpoint stakeholder</td>
</tr>
<tr>
<td>DATA REQUIRED</td>
<td>Input: Captured traveller facial image</td>
<td>Input: Captured traveller facial image</td>
<td>Input: Captured traveller facial image</td>
</tr>
<tr>
<td>SYSTEMS / TECHNOLOGY</td>
<td>Facial recognition technology at touchpoint (eGate, stand-alone facial recognition camera)</td>
<td>Facial recognition technology at touchpoint (eGate, stand-alone facial recognition camera)</td>
<td>Facial recognition technology at touchpoint (eGate, stand-alone facial recognition camera)</td>
</tr>
<tr>
<td>PROCESS FOR AUTHENTICATION</td>
<td>Captured facial image compared against encrypted image in orchestration platform; result &amp; min data required returned to stakeholder</td>
<td>Captured facial image compared against encrypted image shared from traveller; result &amp; min data required returned to stakeholder</td>
<td>Captured facial image compared against encrypted image shared from traveller; result &amp; min data required returned to stakeholder</td>
</tr>
</tbody>
</table>
6. ADDITIONAL CONSIDERATIONS FOR DESIGNING PROPOSED STJ RECOMMENDATIONS

Through the examination of the three core model types, several key constraints have emerged that must be addressed in designing the Seamless Traveller Journey end-to-end recommendations.

- Feasibility of technology
  - Certain solutions still in conceptual phase/shown limited proof of concept in market
  - Potential high-level of customisations required to ensure integration with existing systems/technologies and interoperability across providers

- Privacy consideration and data security
  - Growing data privacy regulations (e.g., GDPR) & increased/more proactive compliance
  - Outdated legislation that does not consider current technologies/solutions in market

- Exchange of personal data between stakeholders (responsibility risk & liability)

- Willingness and ability to store personal data on stakeholders’ own systems
- Disparate stakeholder business requirements and siloed industry initiatives

- Cross-geography differences in legislation and requirements (e.g., challenges of a roundtrip international journey)

7. NEXT STEPS

Following the insights and assessments presented in this report, WTTC’s Seamless Traveller Journey Programme will undertake the following next steps to progress the programme.

- **ASSESS**
  Evaluate the privacy and data sharing implications of the models and further analyse the attributes of the STJ.

- **ALIGN**
  Build alignment across stakeholders while driving the execution and evaluation of global end-to-end round-trip air and non-air pilots. Provide progress reports with next steps around data privacy, standards, and minimum data requirements.

- **DRIVE**
  Drive the development of a STJ business case, and the creation of a roadmap for STJ implementation. Document: Document and quantify the benefits of an end-to-end Seamless Traveller Journey.

- **LEAD**
  Maintain and enhance advocacy efforts with border agencies and governments to promote the adoption and deployment of biometrics across travel providers in the end-to-end journey.

Join the effort by contacting Helena Bononi, WTTC’s VP Industry Affairs at helena.bononi@wttc.org
## 8. APPENDIX

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. This information was compiled and analysed in order to ultimately develop the three core emerging model types delineated in this report. 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 INITIATIVE NAME

<table>
<thead>
<tr>
<th>COUNTRY</th>
<th>SECTOR</th>
<th>INITIATIVE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARUBA</td>
<td>AVIATION</td>
<td>Aruba Happy Flow</td>
</tr>
</tbody>
</table>
| AUSTRALIA      | AVIATION     | • Seamless Traveller Initiative  
                             • SmartGate  
                             • SmartPath  
                             • Pilots testing facial recognition at various airports (ex. Sydney, Brisbane, -  
                             Canberra)  
                             • Universal ETA |
| BARBADOS       | AVIATION     | Entry/Exit                                                                      |
| CANADA         | AVIATION     | Chain of Trust                                                                  |
| CANADA + USA   | LAND CROSSING| Nexus                                                                           |
| CHINA          | AVIATION     | Biometric Initiatives at various airports (ex. Beijing, Guangzhou, Landzhou, YanCheng  
                             Nanyang, Yinchuan)                                                               |
| CHINA          | HOSPITALITY  | Marriott + Alibaba                                                              |
| EU             | BORDER CROSSING| • Government Initiatives  
                             • Entry Exit System (EES)  
                             • eu LISA Biometrics Matching System (BMS)  
                             • European Travel Information and Authorization System (ETIAS)             |
| FINLAND        | AVIATION     | Finnair + Helsinki Airport Biometric Initiative                                 |
| FRANCE         | AVIATION     | Biometric Boarding Pass (Air France)                                            |
| FRANCE + UK    | TRAIN        | Eurotunnel                                                                      |
| GERMANY        | TRUSTED TRAVELLER | EasyPASS                                                                        |
| HONG KONG      | TRUSTED TRAVELLER | Smart Departure eChannel                                                        |
| INDIA          | AVIATION     | Digi Yatra                                                                       |
| JAPAN          | AVIATION     | • eGates using facial recognition for international arrivals at Tokyo Airports (Japanese Citizens)  
                             • Narita Airport Biometric Initiative |
| JAPAN          | FACILITATION | Tokyo 2020 athletes, staff, media to be screened with facial recognition         |
| MALAYSIA       | AVIATION     | Fast Airport Clearance Experience System (FACES) - AirAsia                       |
| MEXICO         | TRUSTED TRAVELLER | Viagens Confiable                                                                 |
| MEXICO + USA   | LAND CROSSING| Secure Electronic Network for Travelers Rapid Inspection (SENTRI)               |
| NETHERLANDS    | AVIATION     | • Schiphol Airport Biometric Initiative  
                             • Seamless Flow Netherlands                                                     |
| NETHERLANDS    | TRUSTED TRAVELLER | Privium / Flux                                                                   |
| QATAR          | AVIATION     | Hamad Airport Biometric Initiative                                               |
| SAUDI ARABIA   | AVIATION     | Airport Modernization Project (26 airports)                                     |
| SINGAPORE      | AVIATION     | Fast and Seamless Travel (FAST)                                                  |
| SINGAPORE + US | TRUSTED TRAVELLER | Singapore - US Trusted Traveller Programme                                       |
| SOUTH KOREA    | AVIATION     | SmartPass                                                                        |
| UAE            | AVIATION     | eGates and Biometric Immigration Tunnel                                          |
| UAE + UK       | AVIATION     | Dubai International Airport & London Gatwick Joint Biometric Initiative         |
| UK             | AVIATION     | • London Gatwick Airport Biometric Initiative  
                             • London Heathrow Passenger Identification Programme                           |
| UK             | TRUSTED TRAVELLER | Registered Traveller Service                                                      |
| URUGUAY        | AVIATION     | Easy Airport Programme at Carrasco International Airport                         |
| USA            | TRUSTED TRAVELLER | Global Entry - Customs and Border Protection (CBP)                              |
| USA            | TRAVELLER EXPERIENCE | • CLEAR  
                             • MyDisney Experience                                                            |
### SOURCES REFERENCED

![Image of travel information](https://example.com/travel_info)

**SOURCES REFERENCES**

Information and references collected between January 2019 and June 2019:

- "S3, United States CIP Interview." 2019.
ACKNOWLEDGEMENTS


GLORIA GUEVARA, PRESIDENT AND CHIEF EXECUTIVE OFFICER, WORLD TRAVEL & TOURISM COUNCIL
MIKE MATHEIS, GLOBAL INDUSTRY ASSOCIATION LEAD, OLIVER WYMAN
SCOT HORNICK, SENIOR PARTNER, OLIVER WYMAN

CONTRIBUTORS

ANNET STEENBERGEN, ARUBA HAPPY FLOW
CHUA CHING HOCK, CHANGI AIRPORT [SIN]
GORDON WILSON, WORLDREACH SOFTWARE
GILLIAN ORMISTON, IDEMIA
HEIDRUN HOLIN, LUFTHANSA
MELESA JONES, LISA AIRTH, ANNA FANTONI, SYDNEY AIRPORT [SYD]
MICHAEL HARDIN, KIMBERLI WEISSMAN, US CUSTOMS AND BORDER PROTECTION
PETER SUTCLIFFE, SITA
RICHARD CAMMAN, VISION-BOX
ROB BROERE, EMIRATES
SHASHA RIDZAM, AIRASIA
SIMON WILCOX, LONDON HEATHROW AIRPORT [LHR]
TONY SMITH, THE INTERNATIONAL BORDER MANAGEMENT AND TECHNOLOGIES ASSOCIATION [IBMATA]

WTTC is the body which represents the Travel & Tourism private sector globally. Members consist of CEOs of the world’s Travel & Tourism companies, destinations, and industry organisations engaging with Travel & Tourism. WTTC has a history of 25 years of research to quantify the economic impact of the sector in 185 countries. Travel & Tourism is a key driver for investment and economic growth globally. The sector contributes US$8.3 trillion or 10.4% of global GDP, and accounts for 313 million jobs or one in ten of all jobs on the planet.

For over 25 years, WTTC has been the voice of this industry globally. Members are the Chairs, Presidents and Chief Executives of the world’s leading, private sector Travel & Tourism businesses, who bring specialist knowledge to guide government policy and decision-making and raise awareness of the importance of the sector.

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].