

System Initiative on Shaping the Future of Mobility

The Known Traveller

Unlocking the potential of digital identity for secure and seamless travel

In collaboration with Accenture

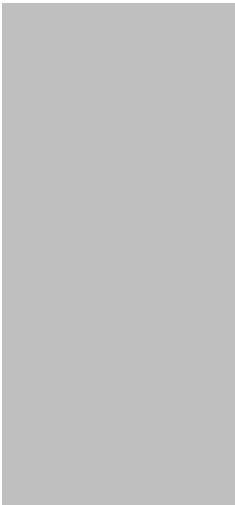
January 2018



Contents

| | |
|----|---|
| 3 | Preface |
| 4 | Foreword |
| 5 | Executive summary |
| 7 | 1. Increasing pressures on security in travel |
| 12 | 2. Methodology |
| 14 | 3. The Known Traveller Digital Identity concept |
| 21 | 4. Paradigm shift to a digital identity |
| 23 | 5. Principles and core technologies |
| 31 | 6. Building a prototype |
| 36 | 7. Next steps: Test and scale |
| 38 | Recommendations |
| 40 | Acknowledgements |
| 41 | Appendix A |
| 42 | Endnotes |

Preface



In today's fractured world, governments, travel and tourism industry leaders and the public are increasingly concerned by security threats. Rather than promoting isolationism and responding reactively to security shocks, stakeholders must collaborate to protect public safety while facilitating the movement of legitimate travellers. Although governments use private companies to help optimize travel security processes, they must deepen their engagement and increase collaborative relationships with diverse stakeholders to maximize transformation of the travel security system. In turn, international organizations that influence travel regulations, as well as airlines, hotels, financial services and technology providers selling services to travellers, must go beyond the typical industry alliances and work with governments and each other.

Emerging technologies – from biometrics to distributed ledger to machine learning – offer tremendous potential to transform and enhance the global travel security system. However, individuals with malicious intent can also manipulate technology, and technology alone will not solve the current security challenges. As the international organization for public-private cooperation, the World Economic Forum provides a platform for open dialogue and acts as an impartial moderator.

Throughout 2017, the Shaping the Future of Security in Travel project convened stakeholders in multiple day-long workshops and working calls on the topic of digital identity to continue to shift security in travel forward. This report details the Known Traveller Digital Identity concept as a catalytic prototype capable of transforming the travel and tourism sector as well as medical services, education and beyond. We look forward to implementation of this concept by stakeholders in 2018.

Foreword

Cross-border travel is fundamental to global prosperity and trade, the exploration of new cultures and the exchange of ideas. Travel broadens our horizons and drives economies. With the number of international arrivals expected to grow by 50% by 2030, we must accommodate the vast flow of travellers despite increasing security threats, limited infrastructure and numerous layers of screening. Currently, a secure and seamless traveller journey is not guaranteed and, if not managed well, the travel experience and the global travel industry might suffer.

Together with its partners, the World Economic Forum explored solutions to seamless and secure travel challenges and developed the Known Digital Traveller Identity concept as part of its project, Shaping the Future of Security in Travel. By applying design-thinking strategies and adopting a traveller-centric approach, constituents mapped the traveller journey and identified key pain points for the traveller, government agencies and businesses as they interact throughout the travel process. Fourth Industrial Revolution technologies such as biometrics, blockchain, cryptography and mobile devices enable efforts to overcome challenges faced by stakeholders to achieve a more secure and seamless traveller journey.

This Known Traveller Digital Identity concept is founded on the principle that an individual traveller has control over the use of their own identity and its components. Due to this decentralization of control over the components of their identity, a traveller can push proof of their identity information – secured by distributed ledger technology and cryptography – to governmental and private-sector entities throughout their journey. Access to verified personal biometric, biographic and historical travel data will enable entities along the way to undertake advanced risk assessment, verify travellers' identities and provide seamless access through biometric recognition technology. All of this can be achieved without the need to have personal data stored in one central database, which would pose too great a risk for stakeholders responsible for securely handling personal identity information.

A working prototype of the concept demonstrating specific use cases will be showcased at the World Economic Forum Annual Meeting 2018 to policy-makers, technology innovators and business executives. Moving forward, the project will seek to implement a scalable pilot of the Known Traveller Digital Identity with partner governments.

The World Economic Forum acknowledges and is inspired by the leadership of our partners whose commitment to this project shows that this future is possible. In particular, we wish to thank Marc Garneau, Minister of Transport of Canada, and the entire team from the Government of Canada for having contributed to ensuring the research and prototype development has been grounded in pragmatic public-sector experience. Together, the World Economic Forum and Accenture, collaborating on Shaping the Future of Security in Travel, hope that this report and the prototype will gain momentum, encouraging public and private parties to pilot and scale this concept in the coming year.

Executive Summary

World Economic Forum focus on secure and seamless travel

Forecasts indicate that cross-border travel will grow by 50% over the next decade and reach 1.8 billion international arrivals by 2030.¹ This increase presents an opportunity for the aviation, travel and tourism industry to further harness the economic benefits it contributes to GDP and job creation globally. To take full advantage of the economic opportunities this increase in demand generates, stakeholders must confront pressures on the traveller journey, particularly the increased risk and related security requirements, as well as the limited growth capacity of travel- and border-related infrastructure. Experts suggest that the monetary and economic costs of the current aviation security system will reach unsustainable levels in the coming decades. Digital innovations in travel security coupled with multistakeholder collaboration will unlock solutions to the challenges of today.

Traditionally, people have considered passenger facilitation and ensuring border security to be mutually exclusive. As presented in the 2017 report on *Digital Borders: Enabling a secure, seamless and personalized journey*, incorporating new technologies into the process will dramatically reshape how the industry and governments manage the secure cross-border movement of people. To do this, a cohesive vision for the future of security in travel must include user-centricity, digitization and trustful cooperation.

Prior research

Research undertaken with the International Criminal Police Organization (INTERPOL) and interviews with leaders of the 12 most advanced trusted-traveller and registered-traveller programmes revealed the impediments to achieving this future vision through such programmes alone. Challenges include the expensive and human resource-intensive nature of implementation, the lack of trust between participating countries – which results in the duplication of vetting processes – and the low rates of adoption due to the cost and onerous nature of the application process. As such, governments have a limited ability to reduce bottlenecks in screening and border management. Where registered traveller programmes have been adopted to improve uptake and implementation, determination of initial assessments remain dependent on the legacy system of risk-levels based on country of origin.

Digital Identity as a lever for change

A paradigm shift towards a Known Traveller Digital Identity concept will radically transform the way in which legitimate travellers are securely and seamlessly facilitated across borders and bring to life the ideas discussed in *Digital Borders*. The concept focuses on the use of traveller-managed digital identities, which will enable governments, in partnership with industry leaders and passengers, to conduct pre-vetting risk assessment and security procedures to enhance the seamless flow of travellers through borders. Security officials will redirect attention and resources to identifying threats, thus contributing to improved geopolitical security worldwide. The Known Traveller Digital Identity concept provides multiple applications for government and industry, across and beyond the travel and tourism sector, to provide more personalized and value-added services to travellers.

Emerging technologies for achieving the paradigm shift

To support the development of this concept, Fourth Industrial Revolution technologies will shift the Known Traveller Digital Identity from a concept to a reality:

1. Distributed ledger enables trust in the network without the control of one central authority
2. Cryptography allows an appropriate level of security in authorization and sharing of information
3. Biometrics connect the physical and digital world and ensure the legitimate use of identity information
4. Mobile interfaces and devices allow travellers to carry their digital identity with them and to choose to share it accordingly

In addition, the growing adoption and use by state and non-state entities of electronic passports (ePassports) could provide the means to unlock new ways to facilitate the low-risk traveller's journey, while still ensuring high levels of security. As expected with emerging technologies, sufficient evidence to identify the one “best” solution does not yet exist. Every technological decision taken in designing such an innovative concept must be considered in terms of its anticipated advantages and disadvantages. Pilot tests of a prototype developed to try out these technologies will take place in 2018 in both a lab and real-life environment.

Institutional relationships for driving change

The drive to achieve change must observe three key values. First, governments must commit to adopting individualized risk-based assessments of travellers. In doing so, they will more efficiently identify and process the large majority of travellers who are low risk. Such pre-vetting saves time, which can be better spent concentrating on the detection of risks and threats. Second, pursuit of global interoperability cannot take precedence over governmental sovereignty in decisions about their citizens' security. The Known Traveller Digital Identity concept preserves the right of governments to make their own immigration and security decisions while upholding the principle of proportionality. Finally, the traveller must be given the opportunity to move from playing a passive role to one of active partnership in the security process. By self-selecting the sharing of their digital identity, travellers will be integral to the security process and experience the reward of a more personalized and seamless journey.

Recommendations

The Known Traveller Digital Identity concept is the first step towards achieving this systemic shift in travel security. It serves as the catalyst for the necessary, subsequent multistakeholder actions that will help us achieve our shared

vision for the future of travel. Proposals for moving this from concept to prototype to impact include:

- A. **Act now:** Stakeholders must pilot the prototype policies, processes and technologies, adapt them iteratively and work to balance the inclusion of technological breakthroughs with ongoing progress and convergence based on what is currently available. To expand, pilots should be rolled out in additional locations that are geographically and economically varied in context.
- B. **Build momentum:** Service providers and authorities must design systems taking into account the traveller's intrinsic values and preferences to encourage behavioural change and adoption. Stakeholders should articulate sustainable and trusted business models for delivering Known Traveller Digital Identity capabilities and infrastructure.
- C. **Sustain a supportive policy framework:** There is a need to map, socialize and encourage adherence to global standards and recommended practices. Stakeholders must contribute to defining the guiding principles for the use of new technological choices and the use of advanced data analytics for risk assessment. At all times, cybersecurity and personal privacy must be preserved with the highest integrity.



1. Increasing pressures on security in travel

“Innovation is key to enhancing global competitiveness, mobility and productivity. Technological advancements provide opportunities to make security for air travel more efficient while improving the traveller experience.”

Marc Garneau, Minister of Transport of Canada

The aviation, travel and tourism sector is under pressure because of the growing number of travellers, increasing risk and security requirements and infrastructure capacity limits. These pressures hinder a secure and seamless cross-border traveller journey and cause various pain points for governments, businesses and travellers. Experts predict that the combination of these pressures on the international travel experience will reach a tipping point, putting at risk the future growth of the industry. Particularly with air travel, commentators expect the monetary and economic costs of the current aviation security system to reach unsustainable levels over the next 15–20 years² as the number of air travellers and the scale of air cargo continue to grow. However, digital innovations in travel security will unlock significant change and value, and the industry needs to act now.

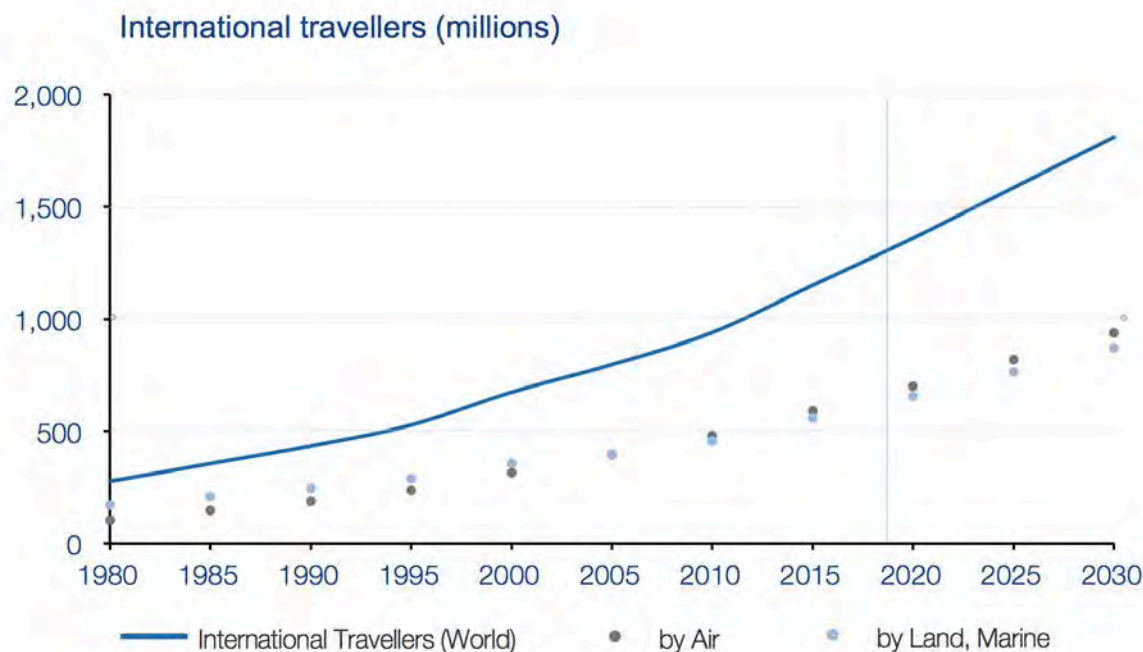
“Public-private partnerships have recognized value in the continued effort to improve efficiency of border processing. These collaborative efforts provide for government to benefit from research and innovation of the private sector to further expand both the pool of trusted traveller passengers and the travel experience at large.”

Matt Hayden, Deputy Assistant Secretary (acting), Private Sector Office, US Department of Homeland Security

Beyond the immediate efficiency gains of digitization of the travel journey, emerging technologies can be used to unlock changes in policy design and the mechanisms government agencies use to ensure the secure movement of people across borders. The concept presented in this report proposes using available Fourth Industrial Revolution technologies to demonstrate the ability to re-engineer the border-crossing experience. This redesign advances pre-travel and risk-based passenger screening by enlisting industry partners and travellers in the process, which will facilitate a more secure and seamless travel journey.



Figure 1: Growth in international arrivals⁶



Travel and the global economy

The aviation, travel and tourism sector provides global economic development and job creation and is a major contributor to prosperity throughout the world. In 2016, it directly contributed \$2.3 trillion in GDP and sustained 109 million jobs worldwide. When the scope is expanded to include the wider effects on industry and society at large, the sector contributed \$7.6 trillion in GDP and supported 292 million jobs in 2016 in the global economy. This is equal to 10.2% of the world's GDP and approximately 1 in 10 of all jobs.⁷

Increasing growth in international travel

The inexorable rise in the global movement of people shows no sign of abating.³ The *World Tourism Barometer*⁴ records that international traveller arrivals totalled 1.2 billion in 2016 and are expected to reach 1.8 billion by 2030, resulting in an expected compound average growth rate (CAGR) of approximately 3% (Figure 1). The aviation, travel and tourism sector, which saw 46 million more international travellers in 2016 than in 2015, has experienced a period of sustained uninterrupted growth for the past seven years, highlighting the industries' resilience.⁵

Increasing risk and security requirements

The challenge for border management agencies has always been to facilitate international trade and travel for the majority of people crossing borders for legitimate reasons while preventing illegal movement.⁸ In little more than a century, international travel has changed from a journey that did not require a passport and involved minimal security screening to a process with a progressively greater number of security measures.⁹ Security is increasingly the focus for international travellers and border agencies as a result of growing turmoil and uncertainty due to geopolitical tensions, complex international security policies, the threat of terrorism and the rise of global pandemics.



As a consequence, investment in aviation security and border management services continues to rise. For example, European airport investment has more than doubled in less than 10 years, reaching \$7.6 billion in 2011. Equally, United States government funding of the Transportation Security Administration (TSA) has increased significantly since its inception and grew from \$2.2 billion in 2002 to almost \$8 billion in 2013.¹⁰ In the meantime, countries have been advised to “tighten their belts” and “to do things differently” – even drive costs down. Human resource expenses represent a major overhead for security and border management agencies, and it is here that better distribution of resources is sought.¹¹ Unless significant changes are made, the cost of running and maintaining the current aviation security system is likely to become completely unsustainable in the next two decades as the number of travellers and the scale of air cargo continue to grow.¹²

Limited growth potential of physical capacity

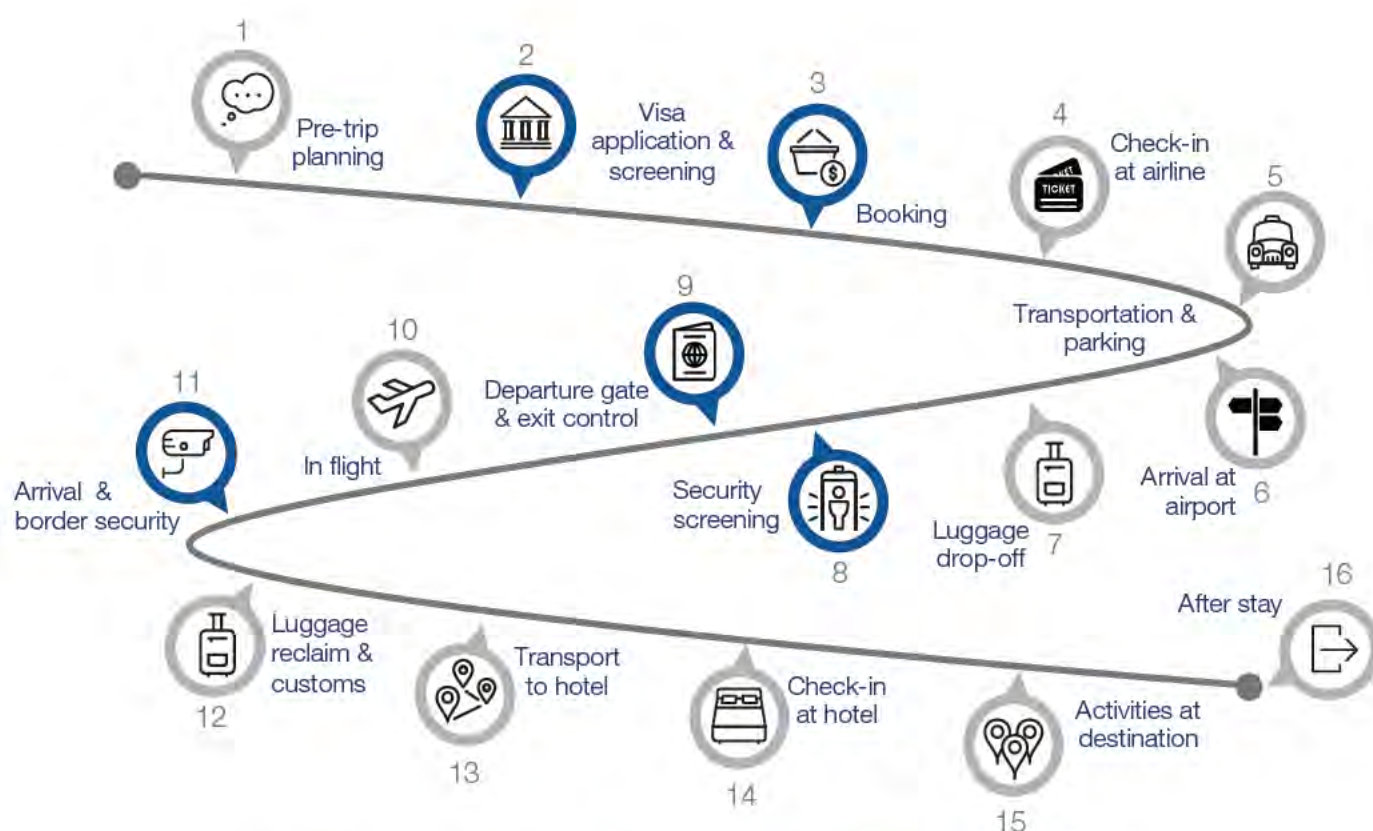
Due to the continuous rise of international travel, airports are reaching capacity. While some countries have space to increase the number of airports in operation – India plans to increase its tally from 95 in 2016 to 250 by 2020¹³

– most airports in Asia are operating at maximum or above capacity, with an estimated 100 million passengers arriving in the Asia-Pacific region each year.¹⁴ At some European airports, new terminals are being built to expand the technical capacity and maximum throughput. But there is often a long lead-time before these new terminals become operational, risking bottlenecks and long queues during screening or passport control at existing terminals. Governments and airports can also expect resistance from nearby residents to further expansion in built-up areas. With only limited physical space available for expansion, airports need to look for alternative ways to cope with the expected growth in international travel.

Pain points in the traveller journey

The rapid rise in international travel, increasing security requirements and limited growth potential all affect the traveller journey and cause pain points for governments, businesses and travellers. Figure 2 provides an overview of the 16 main steps in the traveller journey¹⁵ – from pre-trip planning to after-stay activities – with five identified as presenting the most aggravation (Table 1). The precise order of these steps, and the level to which they inconvenience governments, businesses and travellers, varies with individual airports and the processes in each country.

Figure 2: Traveller journey



Points marked in blue are identified as highest pain points, as explained in Table 1

Table 1: Pain points in the traveller journey

| Traveller journey | Pain points |
|---------------------------------|---|
| Visa application* and screening | <ul style="list-style-type: none">– Uncertainty about visa process requirements– Uncertainty about border guard interaction at immigration– Too many documents to be shared with embassies– Lack of integration between physical and digital identity |
| Booking | <ul style="list-style-type: none">– Previously provided information is not reused– Inconsistent management of identity information– Data entry errors may go undetected |
| Security screening | <ul style="list-style-type: none">– Differences in screening procedures create anxiety for passengers– Capacity constraints at security checkpoints– Lack of knowledge about travellers results in resource-intensive approach to passenger screening and congestion |
| Departure gate and exit control | <ul style="list-style-type: none">– Issues over the right to be forgotten**– Compliance for departure: border authorities know who exited and who overstayed their visa– Some countries do not have a clear exit strategy |
| Arrival and border security | <ul style="list-style-type: none">– Admissibility determination process results in long queues at immigration– Current positioning of airport screening process spoils the traveller experience and the overall optimization of the security process– Lack of government personnel and technological resources to meet demand for services– Policy constraints on operations |

* This instance refers to the traditional visa process, which involves in-person proofing and consular/foreign office interaction. Today there are many examples of more seamless visa waiver processes with eVisas (e.g. ETA and ESTA).

** In the EU’s new General Data Protection Regulation (GDPR) regulation, as of 2018, an individual is enabled to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

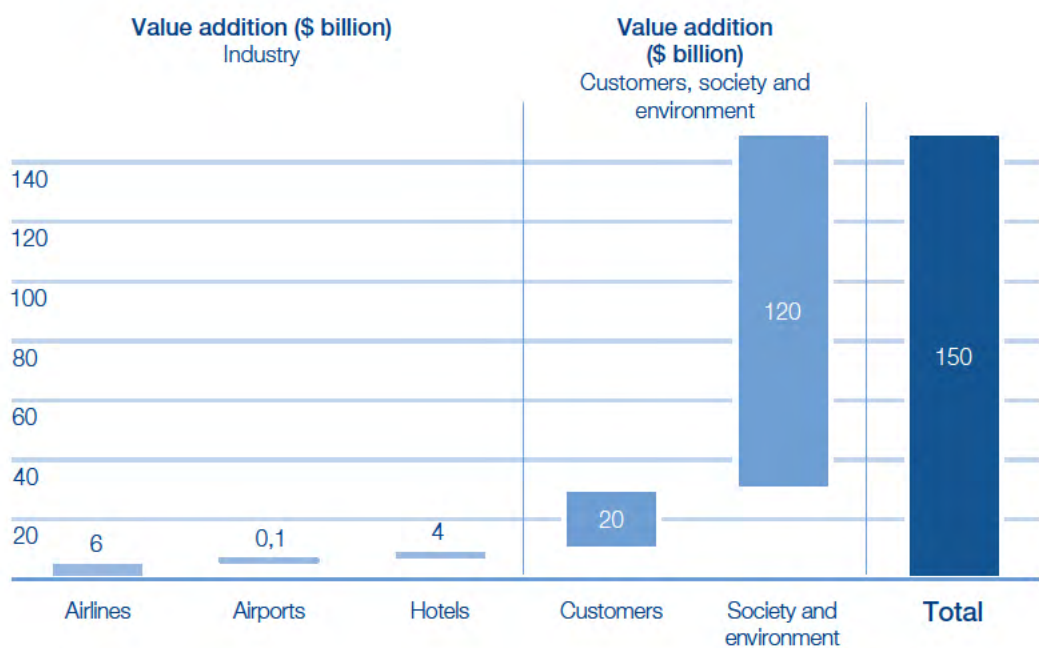
Digital opportunities in travel security offer significant value potential

While a seamless traveller journey is under increasing pressure, security remains a central concern across the aviation, travel and tourism ecosystem.¹⁶ The Fourth Industrial Revolution fuses the physical and digital worlds while revolutionizing the way global leaders think about security and global connectivity.¹⁷ This has prompted a rise in border automation technology, enabling the more efficient processing of travellers at points of exit and entry. Beyond automation, the capabilities of advanced technologies such as biometrics and predictive analytics make possible a complete redesign of traveller-screening processes, increasing the ability to screen passengers in advance and clear low-risk travellers at a rate faster than ever before.

As illustrated in Figure 3, between 2016 and 2025 the value at stake of utilizing Fourth Industrial Revolution digital technologies to improve safety and security in travel is estimated to be \$10 billion across airlines, airports and hotels (\$7 billion for efficiency gains and \$3 billion from increased air traffic).¹⁸ For the same period, it is estimated that the value to society would equal \$20 billion in time and cost savings, and a rough estimate of \$120 billion savings due to the avoidance of the economic costs of a major attack.

“The shift to a digitalized society presents a major opportunity to give travellers an optimal and safe experience, balanced against ongoing security demands and infrastructure pressures. As an industry we must grasp it.”

Figure 3: Value at stake from safety and security¹⁹





2. Methodology

To address the increasing pressures and to investigate how technology can be used as a lever to improve secure and seamless travel, the project followed a two-stage process. The first stage focused on articulating a technological intervention concept that would produce improvements to airport and border-security operations. The second phase was dedicated to developing a demonstrable prototype to bring the concept to life and prove that the enabling technologies can work effectively to deliver the desired process and cooperation outcomes. The prototype was developed through rapid ideation – a design methodology chosen to allow a wide variety of constituents to identify and address the complex policy and institutional barriers to achieving the potential presented by the concept.

Defining the concept

A cohesive multistakeholder vision for the Future of Security in Travel was defined in 2016, which focused on three elements: redesigning the process to be customer-centric; releasing the power of digital information and emerging technologies; and establishing the trustful agreements needed to support cooperation. Based on this vision, stakeholders collaborated to outline a set of core design principles to shape the intervention concept (Table 2).²⁰

Table 2: Design principles²¹

| Vision | PROCESS Customer-centric experience  | TECHNOLOGY Digital information  | COOPERATION Trustful agreements  |
|-----------------------|---|--|--|
| Key design principles | <ul style="list-style-type: none">• Flexible by design• Simple and easy to use• Real-time communication• Optimizes economic benefits• Effectively improves safety of travellers and nations | <ul style="list-style-type: none">• Biometric-based• Technology-agnostic• Modular and scalable• Internationally interoperable• Machine learning and AI to improve accuracy | <ul style="list-style-type: none">• Transparent• Government-supported• Minimum of two (global) stakeholders• Complies with international security standards• Inclusive by design (culture and traveller persona) |



With these design principles as guidelines, three distinct intervention concepts were proposed that focus respectively on access, data-sharing and establishing a Known Traveller Digital Identity (Table 3). The Known Traveller Digital Identity was selected as the most promising and ambitious intervention as it adheres most closely to the principles and offers the best hope of radically transforming the global approach to security in travel.

Developing the prototype

To move from intent to impact, demonstration of the concept through a prototype will prove that the enabling technologies can work effectively to deliver the desired process and cooperation outcomes. To demonstrate the capabilities that have the most potential, the prototype of the Known Traveller Digital Identity concept focuses on five components of the traveller journey: enrolment, pre-trip planning, departure, arrival and building Known Traveller profile credibility.

Table 3: Intervention concepts proposed and selected intervention²²

| | 1. Seamless access and verification | 2. Data-sharing platform | 3. Known Traveller Digital Identity (selected intervention) |
|-------------------------------------|---|---|---|
| | | | |
| Description | Identity verification and access granting with a single-digital token for proof of identity, based on biometrics, for private companies in the travel ecosystem. Once verified, the traveller can use a single token to identify themselves across the ecosystem of partners without a physical ID. | Integrated traveller data-sharing platform that enables better risk assessment by governments through the sharing of vetting outcomes (e.g. red or green light). Existing means of identity-proofing (a physical passport) remain unchanged to improve trust. | A digital identity that includes biometric, biographic and travel history data enables the traveller to authorize entities in the traveller journey to access selected information about them to allow for risk-rating, verification and access. |
| Pros | <ul style="list-style-type: none"> + Valuable to pilot with private companies + Required changes to current ecosystem are limited + No tracking of traveller personal data, thereby limiting potential privacy constraints | <ul style="list-style-type: none"> + Enables governments to improve risk assessment and personalization + Does not require governments to trust a "digital identity" + Ability to focus on potential high-risk travellers | <ul style="list-style-type: none"> + Enables traveller to be a partner in the security process + Respects sovereignty of countries + Incorporates ability to undertake verification and risk assessment + Enables extensive, upfront structured information sharing with entities + Risks identified through enhanced opportunity for data exploitation and analysis against other databases |
| Cons | <ul style="list-style-type: none"> - Technology is not used for risk assessment - Needs to harmonize with existing initiatives - Requires agreement between numerous private-sector companies | <ul style="list-style-type: none"> - Needs to overcome data protection/ privacy issues - Requires trust in the system, between governments - Risks related to the existence of centralized databases | <ul style="list-style-type: none"> - Requires trust between entities - Privacy risks must be addressed - Government support is critical for success |
| Scoring on design principles | Process ● ● Technology ● ● ● ● Cooperation ● ● | Process ● ● Technology Cooperation ● ● | Process ● ● ● ● Technology ● ● ● ● Cooperation ● ● ● ● |

3. The Known Traveller Digital Identity Concept

The Known Traveller Digital Identity concept will be central to enabling a more secure and seamless traveller journey. It provides the opportunity for law enforcement, immigration and aviation security officials to request and receive verified information from travellers far sooner in their journey. Receiving this earlier allows for a process redesign that shifts authorities towards increased advanced passenger screening and the clearance of low-risk travellers. In turn, officials will have more time to focus their efforts on vetting passengers who are less well known or who raise more concerns.

The concept is based on the idea that an individual is in control of providing specific identity information (e.g. biometric, biographic and travel history) to governmental and private-sector players along the journey, such as border control agencies, car rentals, hotels and airlines, for risk-profiling, verification and access (Figure 4). The traveller can select which information is shared for a specific time according to the authority or private entity's requirements to access the services. The identity of the traveller is authenticated through biometric verification and protected by distributed ledger technology and cryptography. The concept is not tied to a particular product, is modular, scalable and based on internationally accepted standards to ensure trust in the technology.

“Getting actionable police information, including biometrics, into the right hands at the right time is INTERPOL’s priority. Initiatives such as I-Checkit, that build bridges between the public and private sectors to develop a stronger global security architecture, have proved that we don’t need to reinvent the wheel, we just need to make it fit for purpose.”

Furthermore, the technology connects with the identity providers’ own legacy systems, as well as with national systems connected to the International Civil Aviation Organization Public Key Directory (ICAO PKD), which is the trusted global source of identity providers’ digital signature information, to ensure traceability to the trusted source.

Exploiting the benefits of ePassports

The rapid adoption of the electronic passport (ePassport) by states presents opportunities to enhance the security of border management, while facilitating travel for document holders. The passport’s contactless chip contains biographical data of the passport holder and a digital security feature in the form of a digital signature that seals this data and ensures its integrity and authenticity. Indeed, one of the core benefits of issuing ePassports is to provide border officials with the ability to electronically validate the integrity and authenticity of that document, whether it has been altered and whether or not it has been issued by the right authority.

This electronic validation is done by checking the digital signature contained in the contactless chip, which means verifying the digital certificate chain used by the state for sealing the biographical data. To perform the electronic validation of an ePassport, border authorities would need to collect other states’ digital certificate chain information, which, for security reasons, changes regularly. With more than 100 states now issuing ePassports, undertaking these types of exchanges bilaterally would be complex, inefficient and highly susceptible to mistakes. The ICAO PKD has been established to play the role of trusted global source to facilitate this exchange, providing an efficient and trusted means for states to upload their own digital certificate chain information and download that of other countries. ICAO PKD members using PKD validation at their borders are both demonstrating their commitment to border security and facilitating passage of low-risk ePassport holders.

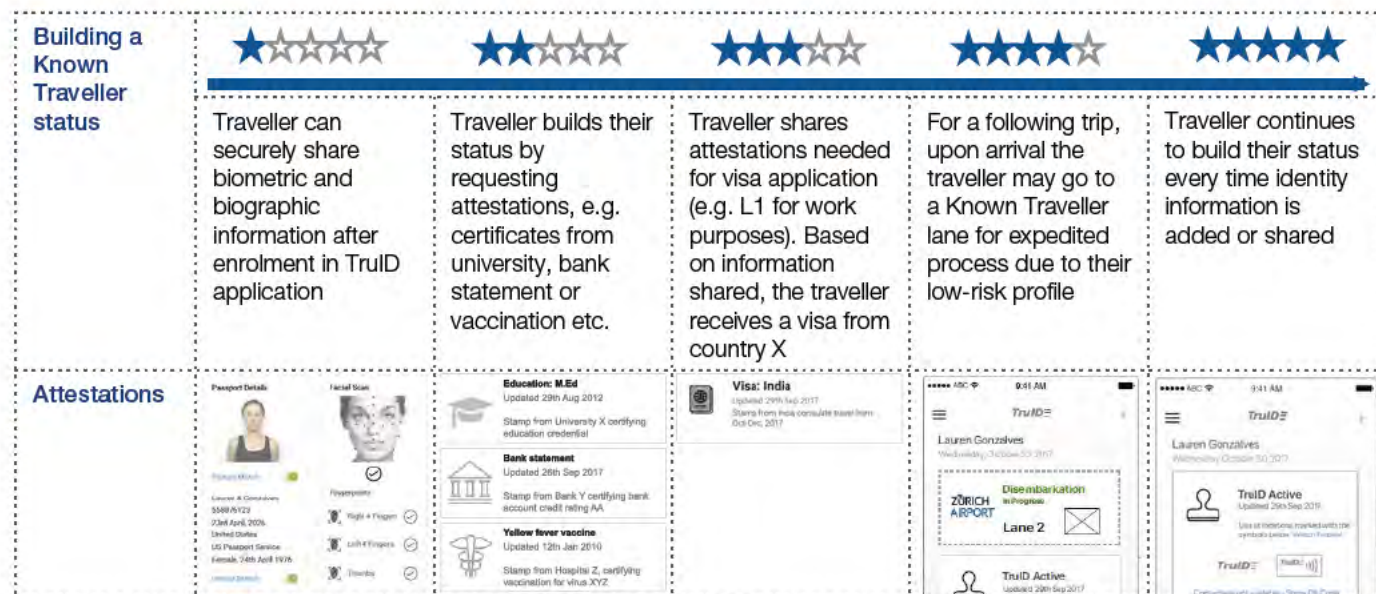
The Known Traveller Digital Identity concept is designed to enable the voluntary sharing of information whereby the individual builds up trust in their digital identity. To build a trusted “Known Traveller” status, travellers need attestations – authenticated claims as declared by a trusted entity – to be added to their Known Traveller Digital Identity each time a trusted entity – such as a post office or a governmental or educational institution – verifies a claim. In this concept, these attestations are the backbone of trust and the basis of reputation and, ultimately, how security decisions can be made.²³ Examples of attestations are proof of citizenship in country X, an educational degree from college Y and proof of vaccination for viral disease Z. In the future, country A might authorize a traveller to enter the nation based on a previous risk assessment and the resulting attestation by country B.

Use case for arrival and border security

Today, when a traveller arrives at a border, the border management authority must determine admissibility – permission to enter a country – rapidly and accurately. A border management agency then determines the class of admission – either citizen, permanent resident, third-country national with a visa or visa waiver – or the need for further scrutiny or the reason for a refusal of entry (or exit), such as criminal activity, the overstay of a visa, customs violations or deceit.



Figure 5: Building a Known Traveller status

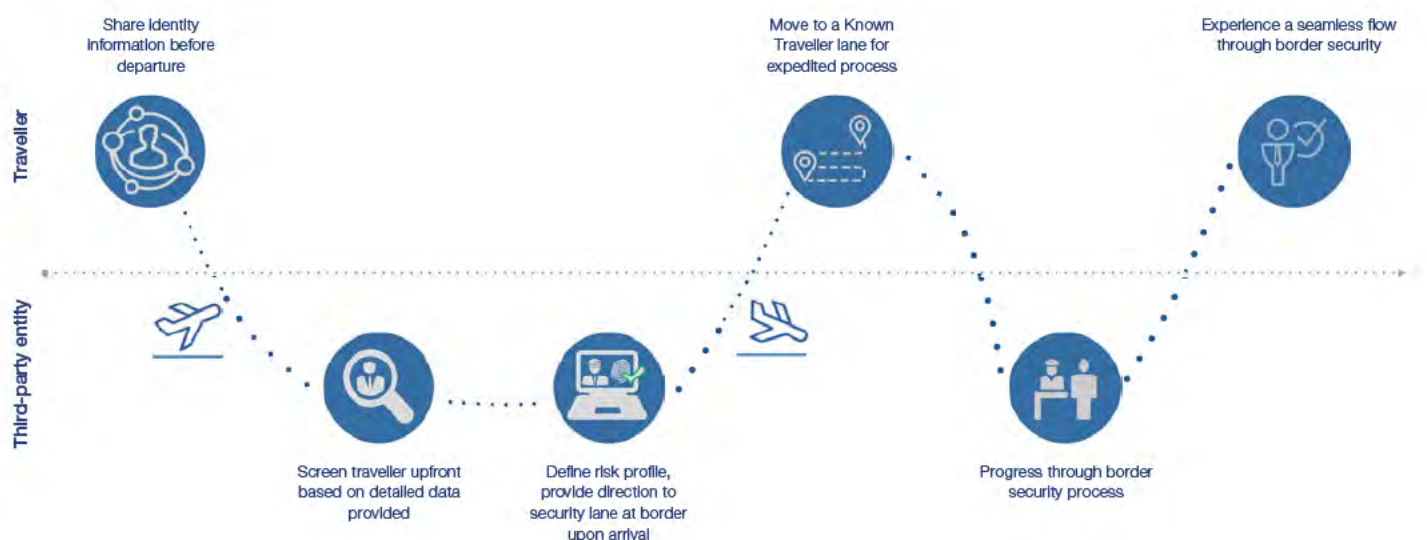




The Known Traveller Digital Identity concept enables individualized screening and risk assessment well before arrival. Increased pre-vetting allows for risk-based immigration lanes where, for example, one lane is for pre-screened travellers and a second is for those who have not provided their information upfront. Entities could receive advance answers to identity-related questions about travellers before their departure or arrival. Advanced assessment allows for better management of security-related risks at ports of entry (Figure 6), as border management agencies can assess the information in more detail before travel. In cases of serious doubt about an individual's reasons for travel, a border agent can pose more pertinent questions to confirm identity or to better understand more recent activities. Conversely, a traveller with a low-risk profile could benefit from a more seamless journey without compromising security.

“Technology has drastically changed most aspects of our daily lives yet international travel and the framework of policies that enable it largely look the same as they did 50 years ago. Collaboration with industry partners and customers is needed to construct a new framework to pre-vet legitimate, low-risk travelers. In turn, government agencies can devote more resources to true threats, improving secure and seamless travel, which will allow more people to see the world.”

Figure 6: Example use case at arrival and border security



Data parameters that support common border security screening processes

The Known Traveller Digital Identity concept provides the potential for law-enforcement agencies to request a structured packet of data from a traveller before travel. The table below shows the sections of data that, if integrated into a passenger's Known Traveller profile, could help facilitate border security screening. As in the Guidelines on Advance Passenger Information,²⁴ sections A–C represent the maximum data fields recommended that countries request from carriers through Advance Passenger Information systems. Section D represents additional information that a passenger could integrate into their Known Traveller profile to improve their profile credibility and provide authorities with more information than the maximum data collected currently through Advance Passenger Information systems.

| Section A | Section B | Section C | Section D |
|---|--|---|--|
| Core data elements found in the Machine Readable Zone of the Official Travel Document (OTD) | Additional data elements normally found in airline systems | Additional data not normally found in airline systems and which can be collected by, or on behalf of, an airline | Additional information that passenger could provide through the Known Traveller Digital Identity (as recommended by law-enforcement stakeholders) |
| <ul style="list-style-type: none"> – OTD number – Issuing state or organization of OTD – OTD type – Expiration date of OTD – Surname/given name(s) – Nationality – Date of birth – Gender | <ul style="list-style-type: none"> – Seating information – Baggage information – Traveller's status – Place/port of original embarkation – Place/port of clearance – Place/port of onward foreign destination – Passenger name record locator number (or unique identifier) | <ul style="list-style-type: none"> – Visa number – Issue date of the visa – Place of issuance of the visa – Other document number used for travel – Type of other document used for travel – Primary residence – Destination address – Place of birth | <ul style="list-style-type: none"> – Contact number – Contact email – Countries visited on this trip prior to arrival – Flight number – Travel itinerary – Purpose of trip – Duration of trip – Extended travel history – People with whom travelling – Currency being brought into the country – Recent interactions with agriculture or livestock – Health information (e.g. vaccinations) – Criminal history (positive declarations) – Driving licence number |



Measuring the value of secure and seamless travel

Stakeholders anticipate that the Known Traveller Digital Identity concept will unlock an estimated potential value of \$150 billion through digitally enhancing travel security.²⁵ Quantifying the value of the concept justifies the investment it requires and creates additional buy-in to expand its adoption and use.

The analysts can use the value tree as a basis for operationalizing the drivers and measuring value realization in a quantitative and qualitative way. The value tree consists of two main value drivers at level one: a seamless experience and secure travel. The seamless experience value driver is divided into speed, comfort, personalization and complexity. The secure travel value driver is divided into identity determination and authorization (Figure 7). The third level of the value tree provides a breakdown of the level two drivers, and the fourth level contains a list of non-exhaustive example drivers. The seamless value driver is primarily defined from a traveller and private-sector perspective. The secure value driver is particularly relevant for society in general, including governments and border agencies.

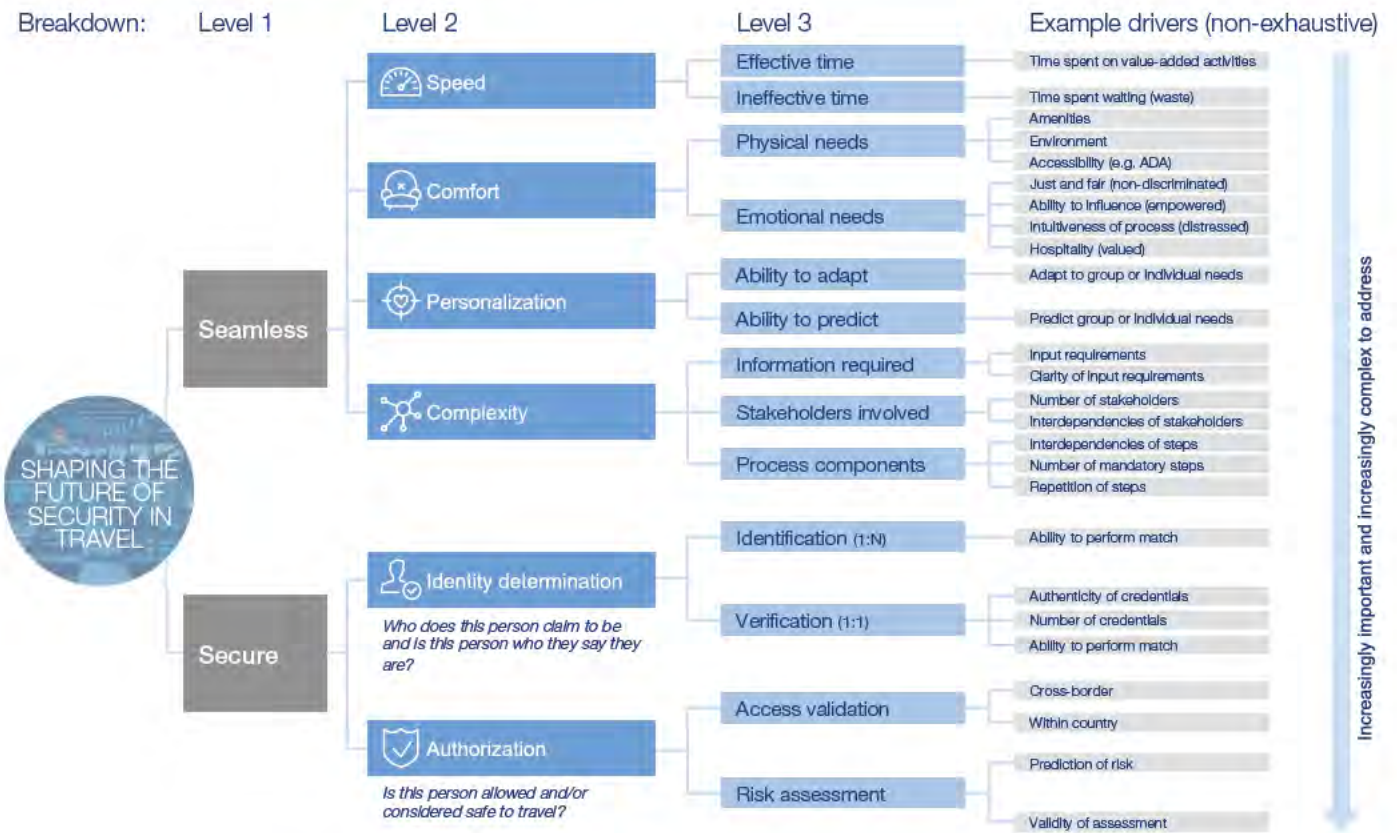
The Known Traveller Digital Identity concept addresses several pain points in the traveller journey and realizes value

across various value drivers, as illustrated on the value tree in Figure 7.

Table 4 indicates how the concept addresses each pain point and, consequently, which value drivers are relevant for each step in the travel journey. Pain points highlighted in grey are those that would be alleviated by creating a more seamless experience, but which do not promise great value for improving both security and seamlessness simultaneously at this time.

Table 5 shows how the level three value drivers can be operationalized and measured quantitatively or qualitatively. Governments could benefit from efficiency cost savings by moving from existing to new systems, and this value can be measured using Tables 4 and 5 to identify and measure against certain key performance indicators (i.e. better use of effective time, fewer stakeholders involved and a reduction in process components). For example, the value of using facial recognition to achieve secure travel in step 11 of the traveller journey (Table 4) can be measured through corresponding metrics in drivers 11, 12 and 13 (Table 5.) Similarly, the value of achieving seamless travel in this process step could result in cost savings demonstrated through measuring drivers 1, 7 and 9.

Figure 7: Value of secure and seamless travel²⁷



Value creation of visa policy

Research indicates the value of a more seamless travel experience. WTO has quantified that improvement of visa facilitation has historically increased international travellers to G20 countries by 5-25% following the implementation of policy changes.²⁶

Table 4: Value proposition of a Known Traveller Digital Identity

| | | Concept enables | Value for secure travel | Value for seamless travel |
|------------|---------------------------------|--|--|--|
| Pre-trip | | | | |
| 1 | Pre-trip planning | | | |
| 2 | Visa application and screening | <ul style="list-style-type: none"> Online visa/travel authorization application | <ul style="list-style-type: none"> Verification Access validation Risk assessment (real time, repeated <24 hrs prior to departure) | <ul style="list-style-type: none"> Effective time Emotional needs Ability to adapt Information required Stakeholders involved Process components |
| 3 | Booking | <ul style="list-style-type: none"> Auto-fill identity information | <ul style="list-style-type: none"> Verification Risk assessment (PNR, general risk score) | <ul style="list-style-type: none"> Effective time Information required |
| 4 | Airline check in | <ul style="list-style-type: none"> Self-check-in | <ul style="list-style-type: none"> Verification Risk assessment (based on Advance Passenger Information) | <ul style="list-style-type: none"> Effective time Information required |
| On trip | | | | |
| 5 | Transport and parking | | | |
| 6 | Arrival at airport | | | |
| 7 | Luggage drop-off | <ul style="list-style-type: none"> Self-drop-off | <ul style="list-style-type: none"> Verification | <ul style="list-style-type: none"> Effective time Emotional needs |
| 8 | Security screening | <ul style="list-style-type: none"> Individual security assessment | <ul style="list-style-type: none"> Verification Risk assessment (final before departure, includes behavioural detection and security enforcement) | <ul style="list-style-type: none"> Effective time Emotional needs Ability to adapt Ability to predict |
| 9 | Departure gate and exit control | <ul style="list-style-type: none"> Individual security assessment Self-exit Self-boarding | <ul style="list-style-type: none"> Verification Risk assessment (final before departure, includes behavioural detection and security enforcement) Access validation | <ul style="list-style-type: none"> Effective time Emotional needs Ability to adapt Ability to predict |
| 10 | In flight | | | |
| 11 | Arrival and border security | <ul style="list-style-type: none"> Individual risk assessment | <ul style="list-style-type: none"> Verification Access validation Risk assessment | <ul style="list-style-type: none"> Effective time Emotional needs Ability to adapt Ability to predict Information required Stakeholders involved Process components |
| 12 | Luggage reclaim and customs | <ul style="list-style-type: none"> Secure reclaim | <ul style="list-style-type: none"> Verification | <ul style="list-style-type: none"> Emotional needs |
| 13 | Transport to hotel | | | |
| 14 | Check-in at hotel | <ul style="list-style-type: none"> Self-check-in | <ul style="list-style-type: none"> Verification Risk assessment (for example, where industry partners can participate in programmes like I-Checkit – see call-out box) | <ul style="list-style-type: none"> Effective time |
| 15 | Activities at destination | | | |
| After trip | | | | |
| 16 | After stay | <ul style="list-style-type: none"> Individual risk rating | <ul style="list-style-type: none"> Risk assessment (risk of overstay and whether individual left the country and acted appropriately on visit) | <ul style="list-style-type: none"> Emotional needs Ability to predict |

INTERPOL I-Checkit

I-Checkit is a screening solution that complements and enhances national border security systems and is a valuable example of the cooperation potential between public and private sectors. It allows trusted partners in the private sector to collaborate with the law-enforcement community to conduct advanced passenger checks in real time against INTERPOL's database of stolen and lost travel documents. Given the ease with which terrorists, organized crime groups and travelling sex offenders are able to access regularized travel routes, there is a pressing need for further expansion of I-Checkit.

Table 5: Suggested key performance indicators (non-exhaustive)

| # | Driver | Description | Measurement | Example metric |
|----|-----------------------|---|--------------|--|
| 1 | Effective time | Time spent on value-added activities (customer or business value add) | Quantitative | – Process time for X number of travellers for each step |
| 2 | Ineffective time | Time spent waiting (non-value add) e.g. due to resource efficiencies | Quantitative | – Process time for X number of travellers for each step |
| 3 | Physical needs | Ability to adhere to physical needs regarding amenities, environment and accessibility | Qualitative | – Level of satisfaction (1–5) |
| 4 | Emotional needs | Ability to adhere to emotional needs regarding a just and fair process, ability to influence, intuitiveness of process and hospitality | Qualitative | – Level of satisfaction (1–5) |
| 5 | Ability to adapt | Ability to adapt to group or individual needs | Qualitative | – Number of complaints – Severity of complaints |
| 6 | Ability to predict | Ability to predict group or individual needs | Qualitative | – Number of complaints – Severity of complaints |
| 7 | Information required | Information required as determined by number of input requirements, difficulty of adhering to requirements and clarity of the input requirements | Quantitative | – Number of input requirements – Level of difficulty – Level of satisfaction |
| 8 | Stakeholders involved | Covers the number of stakeholders involved and the interdependencies between these stakeholders | Quantitative | – Number of stakeholders – Number of interdependencies – Number of officials per traveller per transaction or per unit of time |
| 9 | Process components | Components in a process as determined by the interdependencies of steps, number of mandatory steps and repetition of steps | Quantitative | – Number of links – Number of repetitive steps |
| 10 | Identification | Ability to perform match of an individual; the person themselves is token for one-to-many (1:N) in crowd identification | Quantitative | – % of correct match (TPIR, TNIR) – Time required to perform match – Cost per match |
| 11 | Verification | Credential provided is token for verification of that person; considering the authenticity of credential, number of credentials and ability to perform 1:1 match | Quantitative | – % of correct match (TMR, TNMR) – Time required to perform match – Cost per match |
| 12 | Access validation | Admissibility is determined by cognizant authority based on information that includes a form of risk assessment (e.g. traveller is authorized to access a country or a specific service/enter a venue | Quantitative | – % of correct match – Time required to perform validation – Cost per validation |
| 13 | Risk assessment | Contains prediction of risk and validity of the assessment. Risk assessment is based on: (1) internal holdings; (2) shared identity information; and (3) data sharing with external entities. | Quantitative | – % data available – % data error (false alarms, misses) – Time required to process – % decrease in fines and/or costs to airlines for incorrectly boarded passengers |

4. Paradigm shift to a digital identity

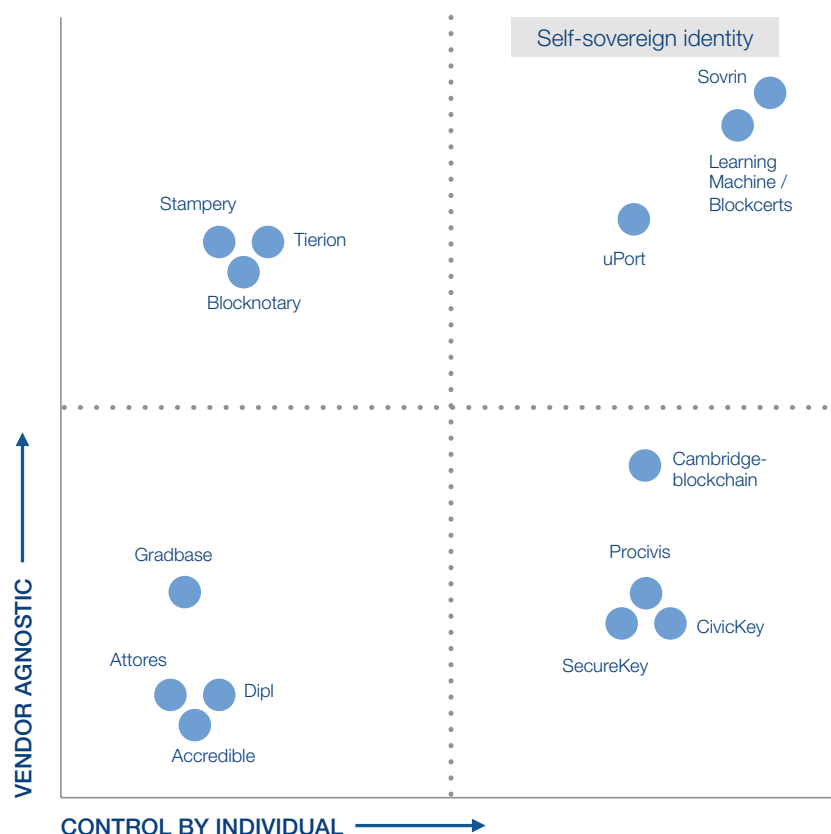
Several digital identity concepts exist today. Each exhibits varying degrees of user control and differs in the extent to which it is tied to a specific product (“vendor agnosticism”). Control by the user allows individuals to manage information compiled about themselves and make decisions on when and with whom they share it (as per the requirements of the relying party). The degree to which a digital identity concept is vendor-agnostic depicts the degree to which gaining access to the information and verification of the identity does not rely on any specific vendor or use of that vendor’s technologies.

Figure 8 shows the landscape of current digital identity initiatives.²⁸ Many do not allow for full independence or control by the user. The initiatives are predominantly point solutions – that is, fixes that address very specific use cases, such as identity verification for banking. The opportunities for re-use in a travel context initially seem limited but may need to be explored further. Nonetheless,

the framework demonstrates a shift towards self-control and vendor independence, two important design principles integrated into the Known Traveller Digital Identity concept.

When adopting the Known Traveller Digital Identity concept, authorization to travel to or enter a foreign country will be based on the individual traveller and their assessed level of risk rather than a blanket risk level primarily based on an individual’s country of origin. Enabling the individual, when requested and at their own discretion, to share their personal information with selected entities in the traveller journey is a key element in encouraging the shift to a traveller-centred secure and seamless travel experience. The pre-emptive sharing of identity information allows for the personalization of services for travellers, while importantly allowing entities that receive the information to use it in advance and to expedite administrative or security-screening processes for the traveller.

Figure 8: Non-exhaustive overview of Digital Identity initiatives²⁸



A self-sovereign identity

A self-sovereign identity is “owned” by the individual. As owner, the individual has access to, can refer to and share components of this identity at their discretion. While certain components of the identity are established by issuing authorities (i.e. passport number, bank details), the individual must consent to the sharing of their identities and any related data. This is achieved by individuals securely storing their own identity data on their own personal devices and providing it efficiently to those who need to validate it, without relying on a central repository of identity data.²⁹

Critical to this paradigm shift is the maintenance of a delicate balance between a more secure and seamless traveller journey and an individual's right to privacy. Many individuals today are sceptical of sharing vast amounts of personal data with authorities. We need to thoroughly consider the design of technologies that allow the sharing of identity information, or proof of identity claims, to ensure that governments request, receive and use data with sufficient proportionality. In line with the design principles formulated, the future of security in travel must include a system that individuals can understand. People must be aware that providing their identity and travel data in advance not only expedites security and leads to a more seamless journey, but also contributes to greater safety for the broader public.

International guidelines and standards exist for Advance Passenger Information and Passenger Name Record data and are developed and maintained jointly by the World Customs Organization (WCO), the International Air

Transport Association (IATA) and ICAO. As highlighted in the design principles, the Known Traveller Digital Identity concept should adhere to established best practices and requirements that allow travellers to act autonomously and to share similar Advance Passenger Information and Passenger Name Record data with authorities in addition to more granular – optional – information earlier in the journey.

“In the Netherlands we have seen the value of ‘digital borders’ and automated border control technologies. We believe the real security value could be realized through knowing more about passengers before they travel through programmes such as RTP-NL that enable travellers to be willingly ‘known’ and processed by authorities.”

Digital identity

Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known.³⁰ Currently, many nations uniquely identify their citizens and residents and provide them with a type of digital identity in the form of an ePassport. Travellers use ePassports to make identity claims at host countries, enabling other countries to access the traveller's personally identifiable information (PII). These are digitally signed by the issuing authority and include a mandatory facial biometric (finger and iris are optional).



Proportionality in relation to data protection³¹

Proportionality as a principle expects authorities to strike a balance in the exercise of their powers between the means used and the intended aim. Where rights to protection of personal data are concerned, proportionality requires that any limitation on this right must be justified, such that only the personal data adequate and relevant for the purposes (and intended advantage) of the processing is collected and processed.

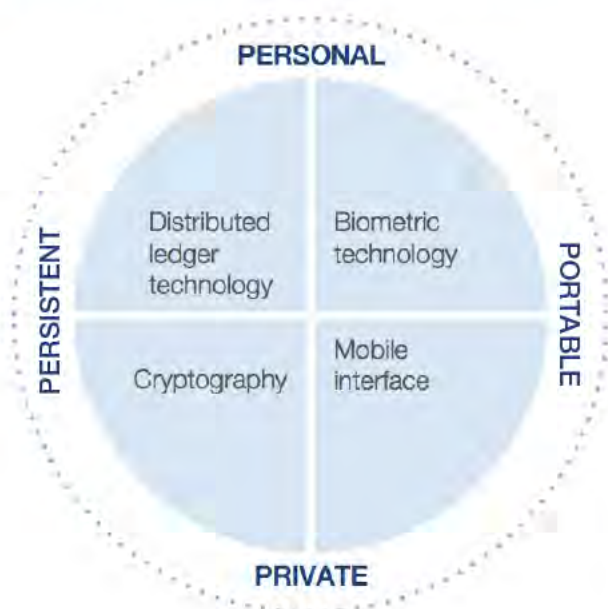
5. Principles and core technologies

The technological developments of the Fourth Industrial Revolution have enabled the conceptualization and construction of a Known Traveller Digital Identity concept. They allow “ownership” and management of the many components of an individual’s identity to be migrated from management by centralized services to management by individuals themselves. Through Known Traveller Digital Identity, individuals will have control over the use of their personal data and be empowered as active contributors to the security of broader society.³² This chapter describes the four key values – personal, portable, private and persistent – of a self-sovereign digital identity that allow this shift towards individual management of identity. Furthermore, it outlines the four core technologies that are currently considered the most advanced options for enabling the required policy and system redesign (Figure 9).

Technology architecture principles

The Known Traveller Digital Identity concept is designed to adhere to the values and principles of self-sovereignty. The four key values – that it is personal, portable, private and persistent – are each expanded into corresponding principles as detailed in Table 6. The table indicates how the Known Traveller Digital Identity concept adheres to these principles by relying on the most advanced technologies currently available – each of which will be built into the demonstration prototype.

Figure 9: Outline of values and core technologies



Core enabling technologies explained

Distributed ledger technology, public-private key cryptography, advanced biometrics and a mobile interface enable the achievement of the next step in the development of a globally acceptable Known Traveller Digital Identity infrastructure:

1. Distributed ledger enables trust in the network without the control of one central authority
2. Cryptography allows an appropriate level of security in authorization and sharing of information
3. Biometrics connects the physical with the digital world and ensures legitimate use of identity information
4. Mobile devices enable the traveller to carry their digital identity and autonomously choose to share it accordingly

As expected with emerging technologies, sufficient evidence to identify the one “best” solution does not yet exist. It is important to consider every technological decision taken in designing such an innovative concept in terms of its anticipated advantages and disadvantages. Several further considerations need to be taken into account that are not specifically linked to a single technology but which are equally important to bear in mind.

Distributed ledger technology, blockchain, pointers and hubs

Conventional identity management systems are based on centralized authorities whereas the absence of a centrally owned registry is fundamental to a self-sovereign digital identity system.³⁴ As identity management moves to digital, it is crucial to make a collaborative effort to boost cybersecurity and protect traveller data privacy to maintain customer trust, promote service adoption by users and improve public safety.³⁵ A distributed ledger is a consensus of replicated, shared and synchronized digital data geographically spread across multiple countries or institutions. No central administrator or centralized data storage exists and, therefore, the distributed ledger serves as a dedicated peer-to-peer network.

A non-blockchain distributed ledger

Distributed ledger technology shows great potential for a self-sovereign Known Traveller Digital Identity since inherently it is distributed and sustainable, indelible, transparent and auditable, orchestrated and flexible, consensus-based and transactional.³⁶ Alternative to the blockchain, a non-blockchain distributed ledger could also fit the principles. For example, R3's Corda has many of the necessary elements for self-sovereign digital identity systems – coordinated workflow, digital signatures and rules about data evolution.³⁷ Another example is X-Road, the data-exchange layer for information systems of the Estonian government. X-Road creates a technological and organizational environment that enables a secure internet-based data exchange between information systems.³⁸

For the Known Traveller Digital Identity concept, blockchain is used to implement the distributed ledger, although alternatives are available. Blockchain refers to the data structure comprising cryptographically linked data blocks.³⁹ It implies an ability to verify reliably the contents of the blocks but does not imply a distribution of any kind.⁴⁰ The combination of a blockchain, to cryptographically link data blocks, and distributed ledger technology securely transmits information without the control of one central authority.

Essentially, it is a distributed database whereby a blockchain serves as a public ledger that can never be erased or rewritten. Entries can be altered but not deleted from a blockchain-based distributed ledger. Data can be changed only if consensus is gained among network participants that a proposed transaction is correct and valid. The chain is immutable because every new block in the data store also contains a hash of the previous block in the chain. The longer the chain, the more secure and harder it is to break.⁴¹

Table 6: Principles of a self-sovereign digital identity concept³³

| Key values | Concept adheres to principle | 0 indicates lowest value of the technology to adhere to principle, 4 is high | | | |
|---|--|--|--------------|-----------|---------------|
| | | Distributed ledger | Cryptography | Biometric | Mobile device |
| Personal (secure) <i>The identity information must be protected from unintentional disclosure</i> | Protection <i>The right of users must be protected when there is a conflict between the needs of the network and the right of individuals; the latter should be the priority</i> | ● ● | ● ● ● ● ● | ● | ● |
| | Minimization <i>Disclosure of claims must be minimized</i> | ● ● ● | ● | ● | ● ● |
| Portable <i>The identity owner must be able to use their identity data wherever they want and not be tied into a single technology provider</i> | Interoperability <i>Identities should be as widely usable as possible</i> | ● ● | ● | ● ● ● ● ● | ● ● |
| | Transparency <i>The system and its logic must be transparent in how they function, how they are managed and how they are kept up to date</i> | ● ● ● ● ● | ● | | ● ● |
| | Transportable <i>All information about identities must be transportable; the identity must be held by the user, and not by a third party</i> | ● ● ● | ● | ● ● ● | ● ● ● ● ● |
| | Access <i>Users should have direct access to their own identity and all related data; all data must be visible and accessible without gatekeepers</i> | ● ● ● | ● ● | ● ● ● | ● ● ● |
| Private (control) <i>The identity owner must be in control of who can see and access their data and for what purposes</i> | Existence <i>Users must have an independent existence; it can never only exist digitally</i> | | | ● ● ● ● ● | |
| | Control <i>Users are able to push selected data to selected entities</i> | ● ● | ● ● | | ● ● ● ● ● |
| | Consent <i>Users must provide consent to the use of their identities and the sharing of related data</i> | ● | ● ● | | ● ● ● ● ● |
| Persistent <i>The identity lives with the individual from life to death</i> | Persistence <i>Identities must be long-lived, at least for as long as the user desires, but it should not contradict a "right to be forgotten"</i> | ● ● ● | | | |

The call for distribution

Until now, the only option to store identity information has been in a centralized manner with a single point of control. The problem with a central database, such as the ones used to house social security numbers or credit reports, is that once compromised it poses a massive security risk to large numbers of people. Recent examples of compromised data include: the Equifax breach, which affected 140 million people; the Home Depot breach, which affected 50 million customers, and Yahoo, which reportedly suffered hacking of more than 3 billion customer accounts.⁴²

Instead of the actual identity data, the blockchain contains pointers to the data. These pointers are related to an identity and stored on the blockchain to allow participants to access the identity data upon authorization. Pointers lead to hubs, which enable secure data sharing, data storage and maintain data integrity. A hub is a datastore containing fragments of identity data at a well-known location (in this case, secured databases with identity information could be considered a hub). Each object in a hub is signed by an identity and is accessible via a globally recognized application programming interface format that explicitly maps to semantic data objects.⁴³ Identity data is not stored on the blockchain. The blockchain holds the pointer, which directs the entity to the right place on a hub that is associated with the identity. The blockchain can be viewed as a distributed certificate authority that maintains the mapping of identities to public keys. Additionally, smart contracts can add a sophisticated logic that helps with revocation and recovery, which lessens the management burden for the end user (Figure 10).⁴⁴

As distributed ledger and blockchain technology is still very much in its infancy and the current pace of development is rapid, new solutions regularly influence or even disrupt the landscape. An evaluation of various technological choices, as well as their potential drawbacks, provides detailed insight into the current understanding of the technologies. In general, three types of distributed ledger architectures are distinguished: public, consortium and private ledgers. These types vary according to who is allowed to participate in the network, who executes the consensus protocol and who maintains the shared ledger.

For the Known Traveller Digital Identity to be self-sovereign, a liberal approach is required to maximize autonomy for the individual. Therefore, a permission-based public ledger is seen as most applicable. Selected trusted nodes will have certain write permissions, but each individual and each entity is allowed to read the distributed ledger, allowing for full transparency.

A decision also needs to be made on whether storage of the identity-related data is held on or off the blockchain. Based on the most advanced thinking, storage of identity information off the blockchain is seen to be the most suitable to enable both the required privacy and scalability. Finally, it is necessary to consider the use of smart contracts to enable a granular permission structure. It is currently unclear which parties should have which permissions.

Figure 10: Visualization of technology

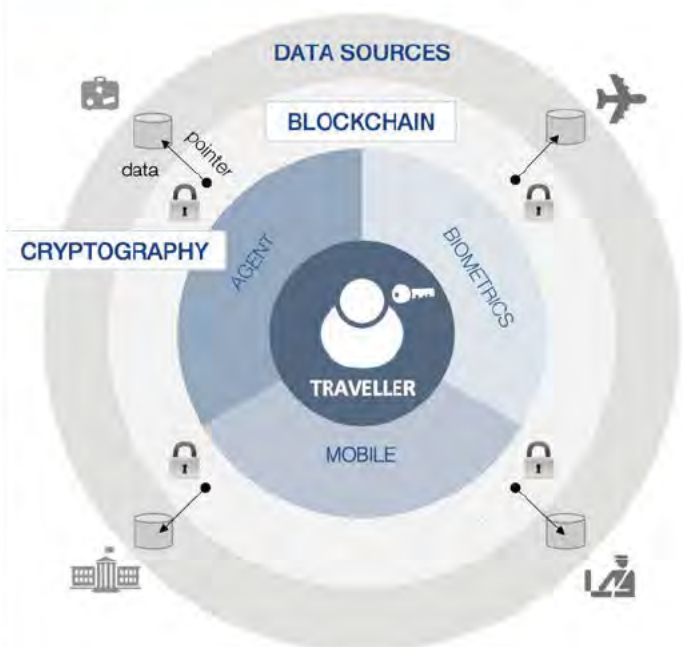


Table 7: Types of distributed ledger architectures⁴⁵

| | Permissionless public ledger | Permissioned public (consortium) ledger | Permissioned private ledger |
|-----------|---|---|---|
| Rationale | <p>Consensus-based</p> <p>Decentralized: cuts out the intermediary</p> <p>Peer-to-peer transactions</p> <p>Each transaction is verified and synced with every node affiliated</p> <p>Fully decentralized security and control</p> | <p>Permission-based</p> <p>Logical decentralization: a few selected nodes, known entities, are predetermined to control the system and ensure consensus</p> | <p>Permission based</p> <p>Centralized: includes an intermediary, where one node writes and verifies each transaction; the node can choose who has read access (read access can be public)</p> |
| Pros | <ul style="list-style-type: none"> + Completely open, everybody is allowed + Incentivizing mechanism to encourage more participants to join the network + High security, every transaction is public and users can maintain anonymity + Full transparency + Censorship-resistant + Tamper-proof | <ul style="list-style-type: none"> + Requires an invitation and must be validated by (a set of rules) put in place by the network starter + Permits greater scalability in terms of transactional throughput + Enables fast transactions due to greater efficiency + Transaction privacy possible | <ul style="list-style-type: none"> + Participants need to obtain an invitation or permission to join + Restrictions on who is allowed to participate in the network + Permits greater scalability in terms of transactional throughput + Enables fast transactions due to greater efficiency + Greater privacy due to restrictions on read permissions |
| Cons | <ul style="list-style-type: none"> - High computational power needed for Proof of Work due to lack of trust - Little to no privacy for transactions due to openness - Higher costs | <ul style="list-style-type: none"> - Lower decentralized security - Not fully resistant to censorship - Requires trust in known entities | <ul style="list-style-type: none"> - Lower decentralized security - Undesirable censorship possible - Limited risk of data tampering - Requires trust in one entity |
| Examples | Bitcoin, Ethereum | Hyperledger, Ripple | R3 CEV, DAH |

Automated teller machine (ATM) network

An ATM network is a “public permissioned” distributed ledger design. Essentially, anyone can use an ATM (it is public), but only those who have been given special permission can add a new ATM to the ATM network (permissioned).⁴⁶

Public-private key cryptography

A public key infrastructure (PKI) enables secure digital authentication and signing.⁴⁷ In public-key cryptography, information is secured with a “keypair”, consisting of a public key, which is visible to everyone, and a private key, which is visible to and controlled only by the identity owner.⁴⁸ With the private key, a public key is generated together with hashed additional meta-information, which creates the pointer address. This address is visible to the participants in the network; however, the private key cannot be generated from the public key, making authentication secure. Because the pointers are stored on a blockchain, each identity owner may serve as its own root authority – an architecture referred to as decentralized public key infrastructure (DPKI). These pointers achieve global uniqueness without the need for a central registration authority. This comes, unfortunately, at the cost of human memorability. The algorithms capable of generating globally unique identifiers automatically produce random strings of characters that have no human meaning.

This demonstrates the axiom about identifiers known as Zooko’s Triangle: “human-meaningful, decentralized, secure – pick any two”.⁴⁹ A combination of all three is, for now, considered impossible.

“The security and safety of all travellers is the top priority for all stakeholders. Knowing who your customer is at all times is a critical component to ensuring the attainment of that goal. But it must be done within the constraints of existing laws and regulations governing personal data and privacy. These critically important objectives can be achieved by utilizing advanced technologies to achieve privacy and security by design.”

Several mechanisms for encrypting and securing identity information exist. The use of zero-knowledge proof (ZKP) capabilities is considered to be a viable option for identity verification technology. ZKP is a cryptographic algorithm that allows users to verify information without actually disclosing the information – verifying only that the information is indeed correct with a very high probability.

Essentially, ZKP allows one user to receive proof of an identity credential without ever having any knowledge of the actual information being proved. In low-criticality processes, where, for example, governments are not involved, alternative mechanisms such as Fast Identity Online (FIDO) Universal Authentication Framework (UAF) can be explored.

ZKP can solve the privacy of personal data challenge with blockchains

ZKP is a protocol used in cryptographic systems to allow a party to prove that it knows something – for example, an identity credential – without having to expose this credential to anyone else. ZKP should not be confused with encryption. The result that is returned from a ZKP is binary and reveals only that the entity either knows the piece of information, or it does not. Nothing regarding the information itself is ever revealed. This is especially important if the information is sensitive or subject to controls.

There are two significant challenges concerning the use of identity data in or with blockchains, which ZKP technology can address. A key feature of a blockchain is **decentralization**, which means that no central administrator or application logic is required to run it. Decentralization is important since it guarantees that there is no single point of failure. However, decentralization comes at the cost of **privacy**. Every node on the chain must verify every transaction independently and this in turn means that it sees what everyone else is doing.

Second, privacy legislation, particularly the European Union General Data Protection Regulation (GDPR), requires the “right to be forgotten”, which means that personal data must be deleted and purged in a system on request by an EU citizen. If this right were applied to a blockchain containing personal data, the deletion of any data in the blockchain would break the chain, causing a “hard fork” or worse, which would destroy the chain altogether. Hence, there is a need to have the means to use blockchains to manage personal data, without having any personal data on the blockchain itself. ZKP can address and solve these privacy challenges.



FIDO UAF architecture can help authentication without sharing biometrics with an authentication server

The FIDO UAF framework allows local biometric authentication using the native security features of an end-user device. Biometric data is securely stored locally by the FIDO-certified application while only a user's public key is shared with the FIDO-certified server. This technology would, for example, enable face and voice recognition, as well as iris or fingerprint recognition for authentication of the traveller, or a combination of the above, without the need for an external device. The traveller would have to carry their own FIDO-certified device. This architecture is best suited to low-criticality processes where government authorities are not involved, such as in exchanges between hotels and travellers.

Biometrics

Today, validating identity claims is the cornerstone of effective aviation security and border management. Many security and border management agencies rely on text-based information derived from the document the traveller presents to validate passenger manifests, conduct watchlist checks and determine those who have overstayed their visa. However, there is no certainty that the individual presenting the documents is the legitimate holder.

There are three primary methods of digital authentication: something you **know**, a password such as a PIN code; something you **have**, a smartcard like a hardware token generator; and something you **are**, a biometric such as fingerprints. Other authentication methods include: **where** you are, geo-location; and **how** you are interacting, behavioural biometrics, for instance, keystroke dynamics.

Biometrics are used to connect the digital identity with the physical world. The authentication of identity claims is the foundation of trust-based relationships. Modern security systems are contingent on successfully validating identities to grant or deny access rights and privileges based on assurance levels associated with an established identity. The introduction of biometric systems for authentication offers the opportunity for travellers to connect their physical identity with their digital identity⁵⁰ and verify that an individual who provides a claim to an identity can in fact provide proof of that claim. One ID, an initiative led by IATA, investigates the transformative use of biometrics to enable an airport-specific, friction-free process, providing a more seamless and personalized airport experience.

When using biometrics, it is crucial to safeguard privacy and security since, unlike a password, a biometric cannot be changed when compromised.⁵¹ Biometric recognition has proved to be more effective than humans in its ability to rapidly and accurately determine individual admissibility.⁵²

IATA's One ID Initiative

IATA's One ID initiative seeks to introduce a streamlined, friction-free and passenger-centric process that allows an individual to assert their identity, online or in person, to the required level at every process step in the end-to-end passenger journey, while maintaining the privacy of personal data. The concept relies on a single capture and controlled distribution of passenger data among the various stakeholders on an authorized-to-know basis. If a passenger's identity can be confirmed at every touchpoint, it will become easier to deliver a more personalized customer experience, while enabling significant improvements in operational efficiency and security. To achieve this, true collaboration between stakeholders will be paramount.

Currently, the use of a facial biometric is the common means of verification. With technological advancements, the biometric used throughout the traveller journey might change in the future. The characteristics listed in Table 8 provide guidance for assessing the fitness of a biometric trait. In the future, other biometrics from emerging modalities, including 3D face, DNA, gait and electrocardiogram, show potential as a means of connecting the digital and physical world and enabling a secure and seamless traveller journey. The acceptance of the use of these biometrics may change depending upon the user's ability to control when their identity is authenticated and what information is linked to their identity.

“Biometric authentication technologies are the key to digital transformation in air travel, enhancing the security process and enabling a personalized, seamless flow. They have the possibility to transform our daily lives beyond travel.”



Biometrics at borders

Border management agencies can benefit from using biometrics-enabled digital identities to improve the passenger experience while maintaining safety and security:⁵³

- 73% of citizens believe using biometrics to verify the identity of everyone crossing borders would increase security
- 62% of citizens would share biometric data to improve border security
- 58% of citizens say they would share biometric information to make border processing faster and more efficient.

Table 8: Comparison biometrics (0 is low, 4 is high)⁶⁴

| Biometric | | Finger-print | Face | Iris | Voice | Vascular | Signature |
|--|----------------|------------------------------------|----------------------------------|---|--|--|--|
| Identification of individual through | | Distinctive features on fingertips | Distinctive features of the face | Distinctive features in the pigmented portion of the eye separating the pupil from the white sclera | Physiological & behavioural aspects of the voice | Vein patterns, usually in the back of the hand, the palm or the finger | Behavioural modality, typically only used for verification |
| Accuracy: False acceptance or rejection rate in various situations | Identification | ● ● ● ● | ● ● | ● ● ● ● | | ● ● | |
| | Verification | ● ● ● ● | ● ● ● ● | ● ● ● ● | ● ● | ● ● ● | ● ● |
| Universality: presence of the trait in all members of the relevant population | | ● ● ● | ● ● ● ● | ● ● ● | ● ● ● | ● ● ● ● | ● ● ● |
| Stability: permanence of the trait over ageing, disease, injury | | ● ● ● | ● ● ● | ● ● ● ● | ● ● ● | ● ● ● ● | ● ● ● |
| Collectability: ease by which good quality samples can be acquired | | ● ● ● | ● ● ● ● | ● ● ● | ● ● | ● ● ● | ● ● |
| Resistance to circumvention: vulnerability of the modality towards fraud | | ● ● | ● ● | ● ● ● | ● ● | ● ● ● | ● ● |
| Acceptability: user reservations around the use of a specific modality | | ● ● | ● ● ● | ● ● | ● ● ● | ● ● | ● ● ● |
| Usability: ease of user interfaces with a system | | ● ● ● | ● ● ● ● | ● ● ● | ● ● ● ● | ● ● ● ● | ● ● ● |
| Cost: hardware/software cost of collecting a sample, then deduplication | | ● ● ● | ● ● ● ● | ● ● | ● ● ● ● | ● ● ● | ● ● ● |
| Overall score | | ● ● ● | ● ● ● | ● ● ● | ● ● | ● ● ● | ● ● |

Mobile interface

In the short term, a mobile interface is seen as the most convenient way to generate private keys, to send public keys to issuers and to hold digital records with the corresponding private key or decentralized identifier.⁶⁵ The mobile identity application should give users holistic visibility of their digital identity components and supply an interface through which they can provide them to government and private entities. Users will benefit from having control over multiple components of their digital identity as it allows for these components to be packaged, transmitted and handled through a variety of channels and mechanisms, depending on the requirements of the service they wish to access. The identity information shared with a border management agency will be very different from the identities required at other points in their trip – for example, when accessing transport services.

It also gives individuals the opportunity to actively, autonomously and conveniently manage the usage of their digital identity. This management should include the ability to review interactions with services and help users

understand the wider implications of identity-sharing for their privacy and personal security.

The mobile interface may receive push messages with requests for consent to share personal information with receivers for any given time. In this respect, the mobile device acts as a user interface to interact with the network. A mobile interface can be anything ranging from a mobile phone to a smart watch to augmented reality glasses. Ultimately, there may be other ways to receive these requests – for example, through screens conveniently positioned at airports prior to departure, which show a personal message when someone walks by.

Not every traveller is expected to have a mobile device. Therefore, alternatives should be provided to enable individuals to consent to sharing their information. In addition, there is much variety in the types of mobile interfaces, requiring broad compatibility of the technology behind the concept. Widely used technology standards are most promising if a critical mass of adopters is to be reached.

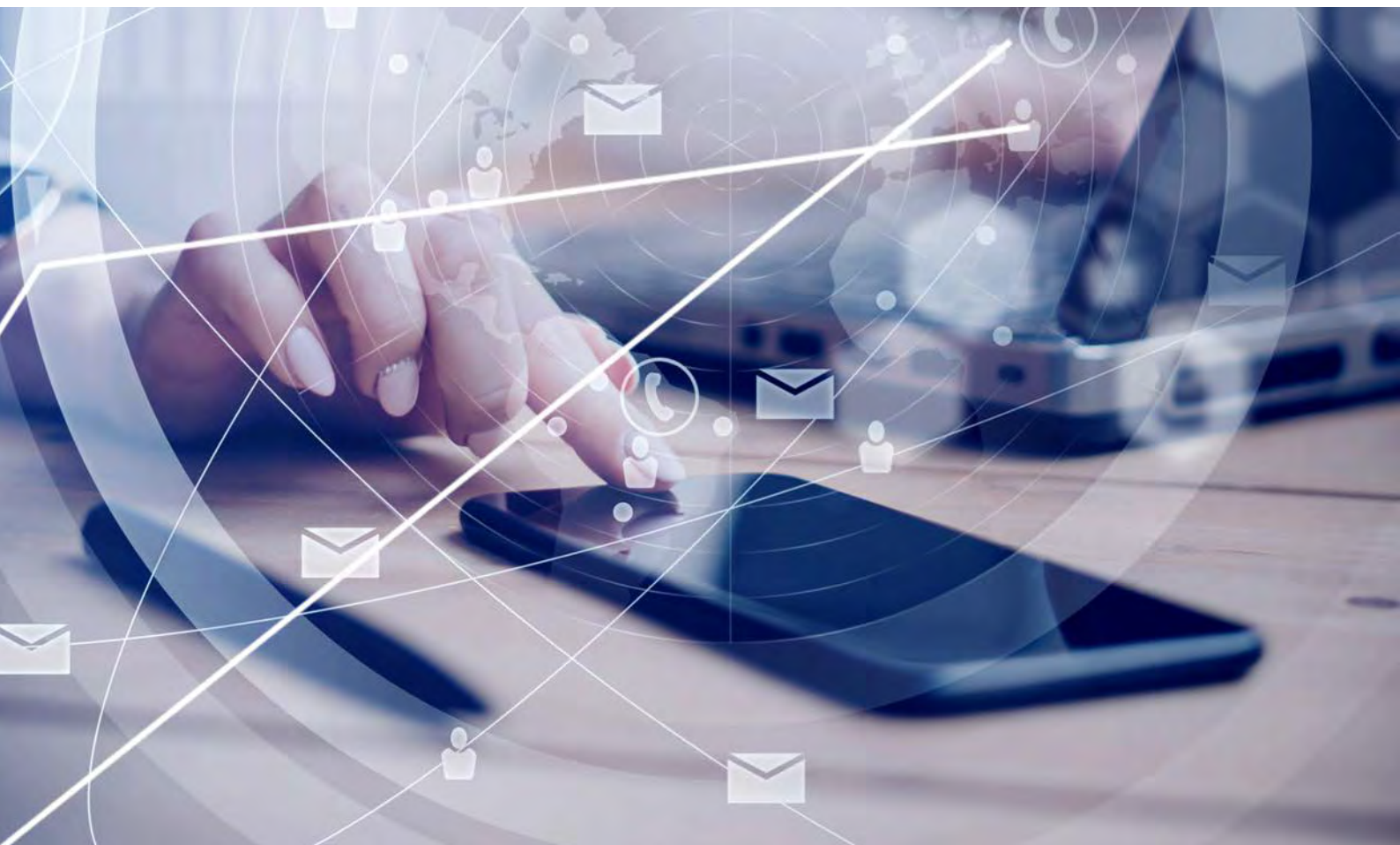
General considerations

A number of issues still need to be addressed regarding privacy, security, governance, technology and protocols, policies and standards. Stakeholders will need to continue to work together to address questions such as:

1. As technologies continuously evolve, how can we ensure that we take these developments into account and make the right choices regarding which technologies are incorporated?
2. Interoperability relies on interchange protocols, data schemas and governance. How might we engage the relevant stakeholders in the ecosystem and come to agreed standards?
3. How do we ensure General Data Protection Regulation (GDPR) compliance? Are current cryptographic expression mechanisms up to the task?
4. What does the financial structure for a Known Traveller Digital Identity system look like? Are the right incentives in place to maintain, exploit and adapt the infrastructure for all actors?
5. What specifications, protocols and implementations of applications, services, packages and libraries that ensure interoperability across systems and providers already exist, and what new aspects may need to be developed?
6. How do we define the contractual arrangements (smart contracts) between parties that are used to add attestations to the digital identity and enable more granular decision-making about access control?

Use case of smart contracts in uPort concept

The purpose of having a proxy contract as the core identifier is that it allows the user to replace their private key while maintaining a persistent identifier. If the user's identifier was the public key corresponding to their private key, they would lose control over their identifier if they were to lose the device where the private key is held. In the case of device loss, the controller contract maintains a list of recovery delegates who can help the user recover their identity. These delegates can be individuals, such as chosen friends and family members, or institutions, such as banks and credit unions. A quorum of delegates is required to let the user recover their identity and connect it to a new device.⁵⁶



Rising privacy concerns

In April 2016, the European Parliament approved GDPR, which is designed to improve the security and privacy of personal data in the EU and which requires control of personal data to rest with the individual.

6. Building a prototype

Creating a prototype brings the concept to life. The value of a working prototype is the opportunity it affords stakeholders to robustly question assumptions made in the concept design and identify the challenges that need to be addressed for the system to change. The prototype includes the five intervention steps in the traveller journey that demonstrate the greatest potential value-add of the Known Traveller Digital Identity concept.

This chapter lays out the following elements:

1. An overview of five key selected intervention steps in the user journey
2. A detailed description of each intervention step
3. A conceptual technology architecture blueprint.

Overview of the selected intervention steps

Figure 11 shows the key process steps selected for demonstration and illustrates the concept's potential in different scenarios. For example, the capabilities demonstrated in the travel-planning phase illustrate the ability of passengers to seamlessly initiate a travel authorization application through the Known Traveller Digital Identity profile elements captured in travel booking activities. It also demonstrates the critical action whereby a passenger provides their Known Traveller profile to border agencies at both immigration exit and entry long before the date of travel, triggering an advanced risk assessment, pre-clearance and expedited processing on site at border control.

Table 9 shows the key intervention steps of the traveller journey linked to the core technology capabilities that redesign the process.

Figure 11: Overview of selected intervention steps

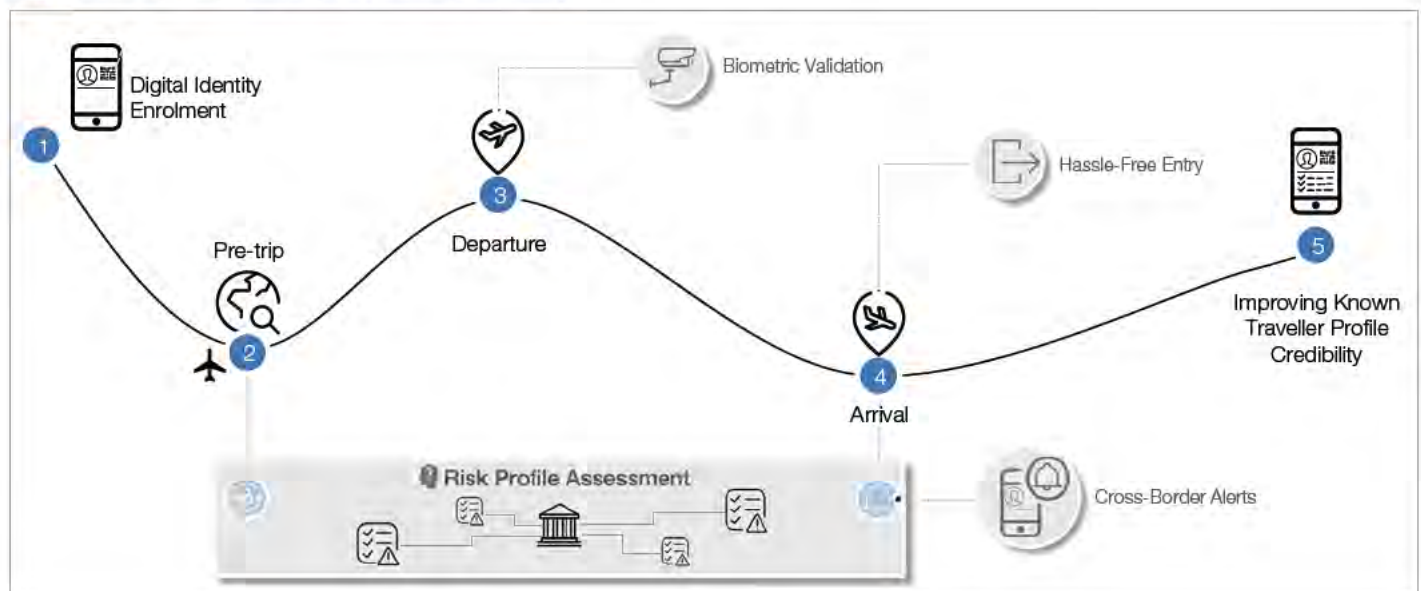


Table 9: Overview of intervention steps considered for the prototype

| Enrolment | Pre-trip | Departure | Arrival |
|---|---|--|--|
| <p>Overview: Traveller downloads the application and creates a digital identity profile in the application; this requires biographic and biometric information.</p> <p>Technology capability: Enrol and verify identity and create a digital identity owned by the traveller.</p> | <p>Overview: Traveller books flight with the airline. During identity information entry at booking, the traveller is prompted to share information with departure and destination countries to speed up border processing. Should travel authorization be required, traveller will be directed to an ETA/visa application site.</p> <p>Technology capability: Sharing accurate and verified identity information – including additional information such as hotel reservations and complete travel history – in advance so government authorities can process risk assessment and travel authorization prior to travel.</p> | <p>Overview: Traveller navigates through check-in and security, immigration exit control and boards using seamless identification technology.</p> <p>Technology capability: Sharing trusted biometric identity information with the airport eliminates the need to show a passport and boarding pass and allows access to expedited lanes.</p> | <p>Overview: Traveller proceeds through an expedited immigration lane due to pre-screening. Expedited lanes exploit seamless identification technology.</p> <p>Technology capability: Sharing trusted biometric identity information with an airport eliminates the need to show a passport on arrival to validate identity. Pre-screening of previously shared data enables authorities to focus on high-risk travellers.</p> |

Detailed description of intervention steps

Figure 12: Known Traveller Digital Identity enrolment

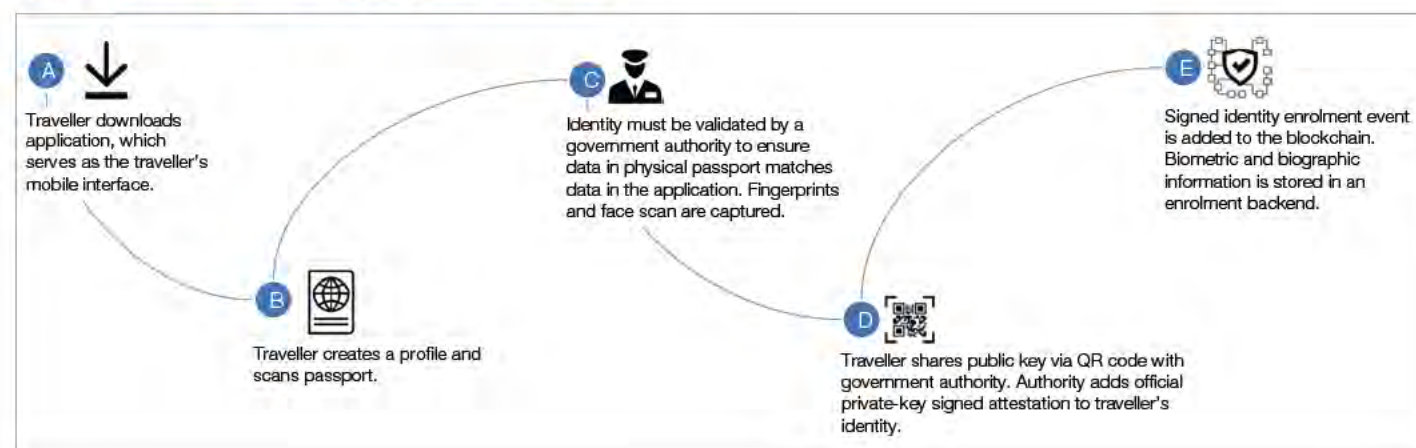


Figure 13: Pre-trip: Booking, travel authorization and pre-screening

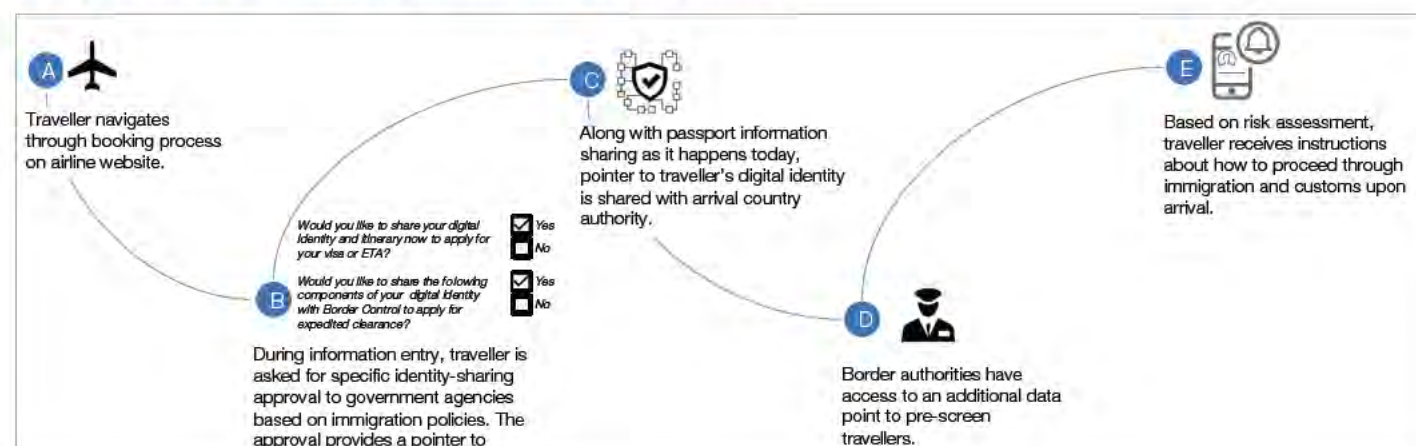


Figure 14: Departure

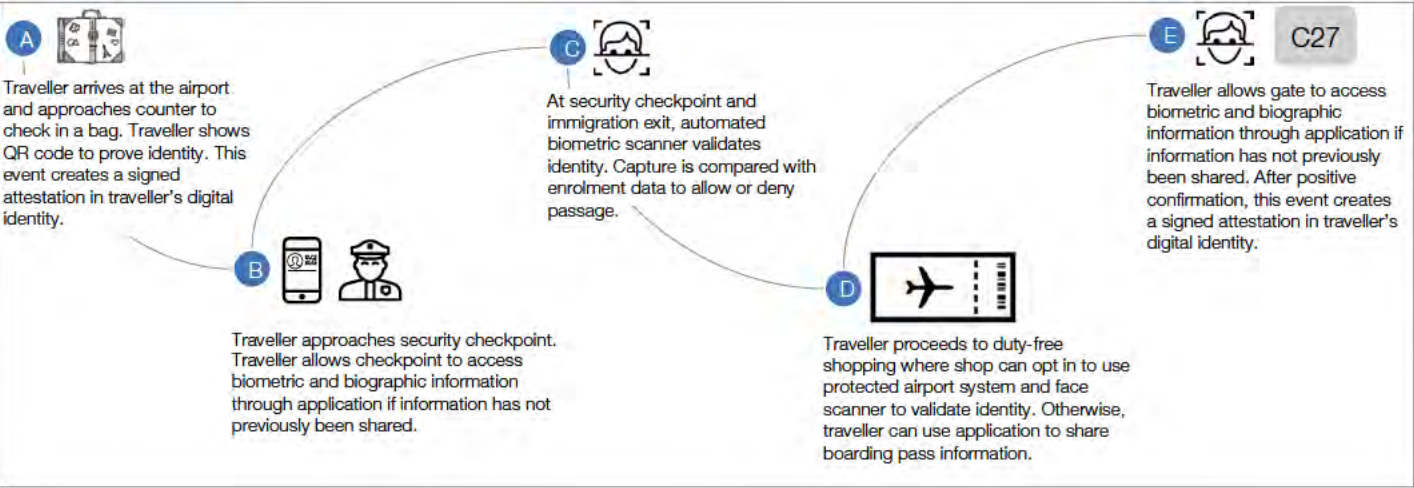


Figure 15: Arrival

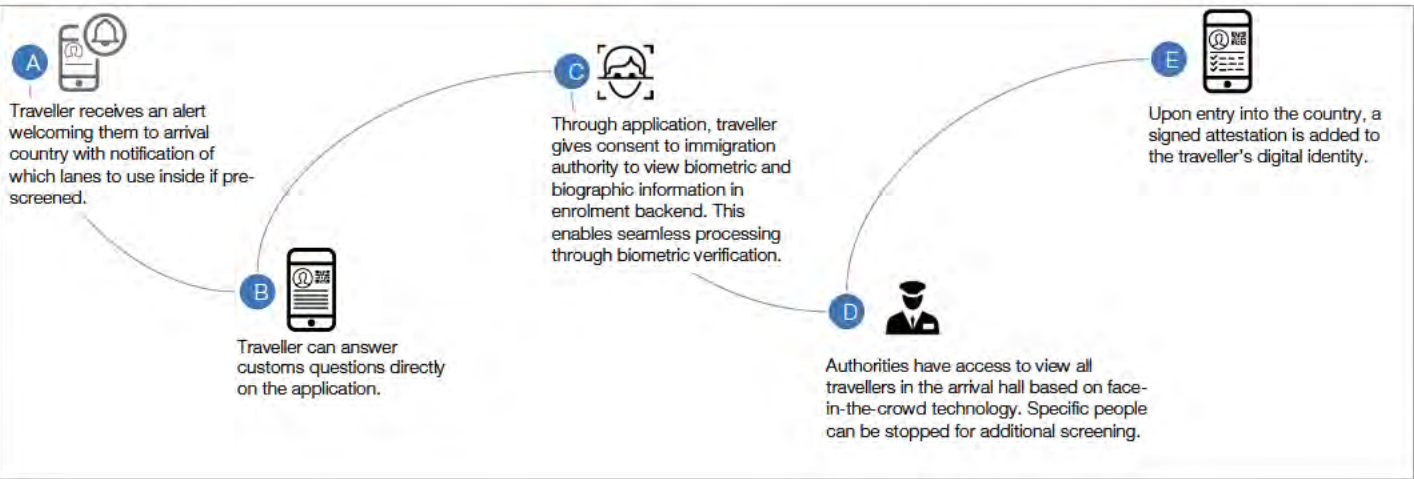
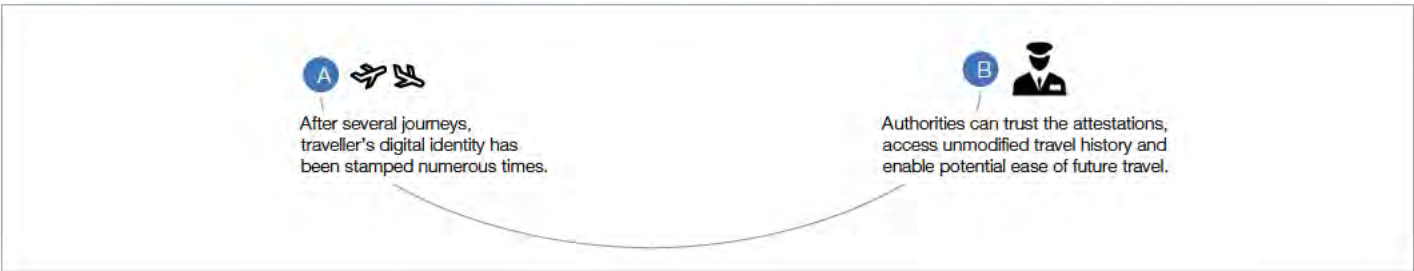


Figure 16: Improving Known Traveller Digital Identity profile credibility



An illustrative mobile application interface provides a conceptual journey of the enrolment process. Figure 17 represents the traveller's viewpoint, while Figure 18 represents a border authority's viewpoint. Further details and wireframes are provided in Appendix A.

Figure 17: Mobile interface traveller perspective

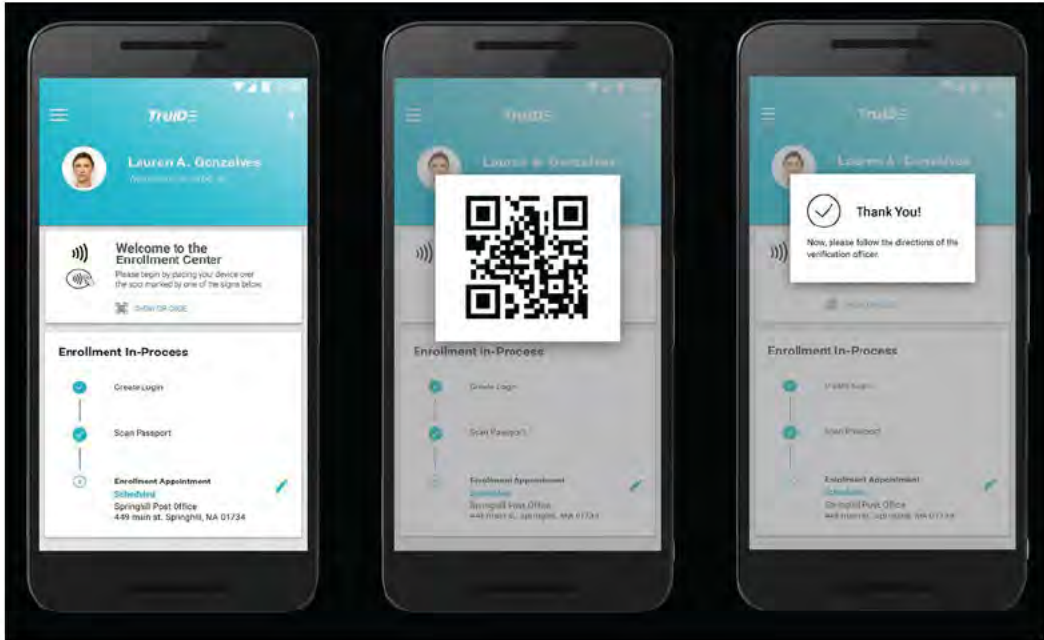
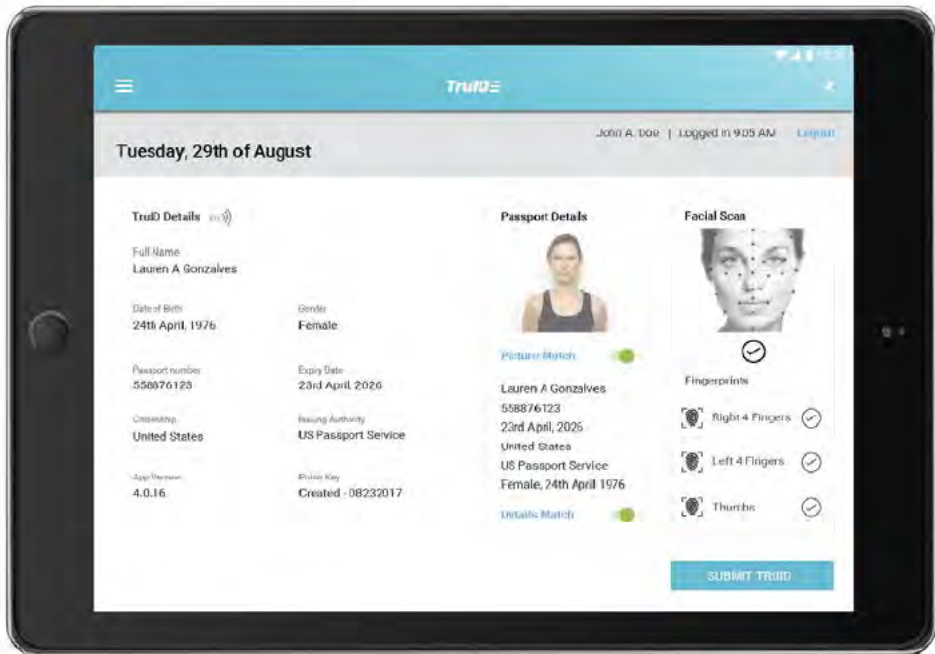


Figure 18: Mobile interface authority perspective

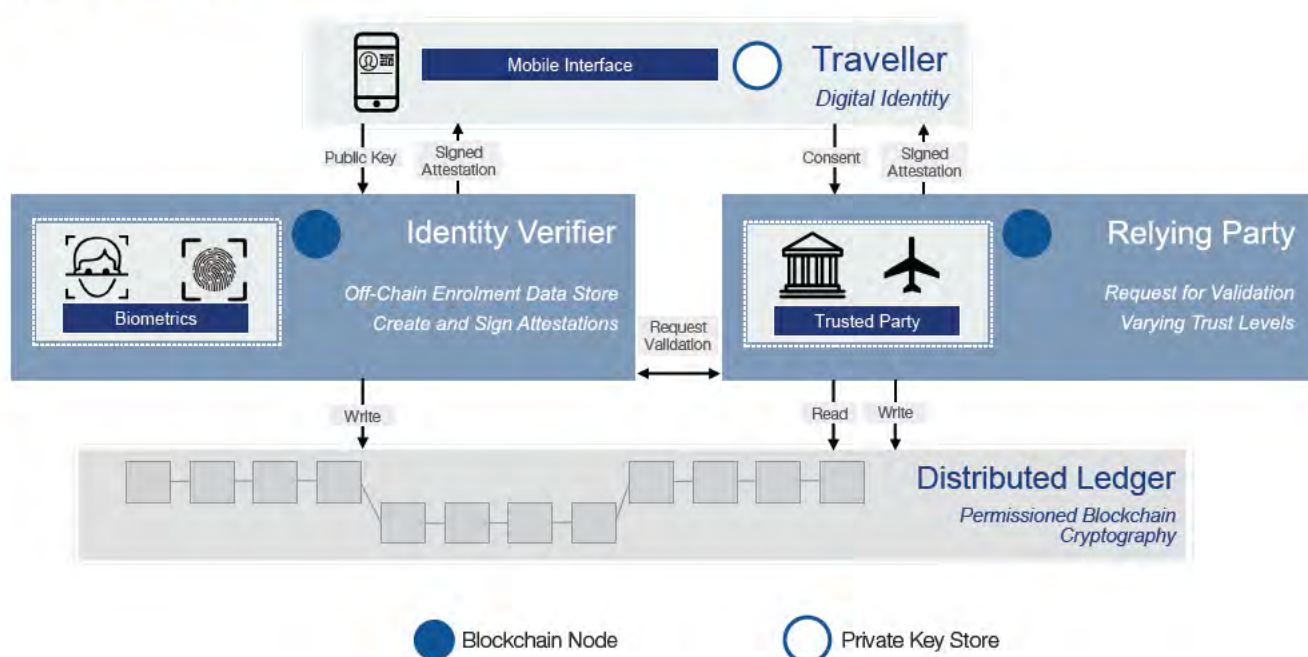


Conceptual technology architecture blueprint

The prototype makes use of all four core technologies – distributed ledger, cryptography, biometrics and mobile interface. Figure 19 shows the high-level blueprint of the prototype. At first, the prototype is not able to integrate with live production systems from stakeholders in the travel ecosystem (e.g. governments, border agencies etc.). Therefore, it is designed to connect with mock data sources to demonstrate the end-to-end process utilizing the four core technologies. The model can be extended to other entities in the future (e.g. hotels, universities etc.), beyond the steps outlined in this prototype.

The mobile interface is the traveller's private key store and holds all attestations. The traveller's identity must first be verified by their citizenship government (the identity verifier). Following verification, the traveller's digital identity is created in an enrolment backend, a proof of identity is added to the distributed ledger and an attestation is added to the traveller's digital identity. Subsequently, the traveller can give consent to a relying party to view and validate their attestations. To do so, the relying party can check the distributed ledger using the traveller's shared public key and subsequently request identity information from the identity verifier. The relying party can then add attestations to the traveller's identity. The prototype demonstrates important technology barriers to stakeholders and invites experimentation to seek solutions and improve the concept from a technology perspective. Additionally, re-evaluation assesses the prototype feasibility to expand to the wider public- and private-sector ecosystem.

Figure 19: High-level prototype blueprint



7. Next steps: Test and scale

To bring the concept and prototype closer to full-scale implementation, a roadmap details the milestones required for stakeholders to start small and grow quickly (Figure 20).

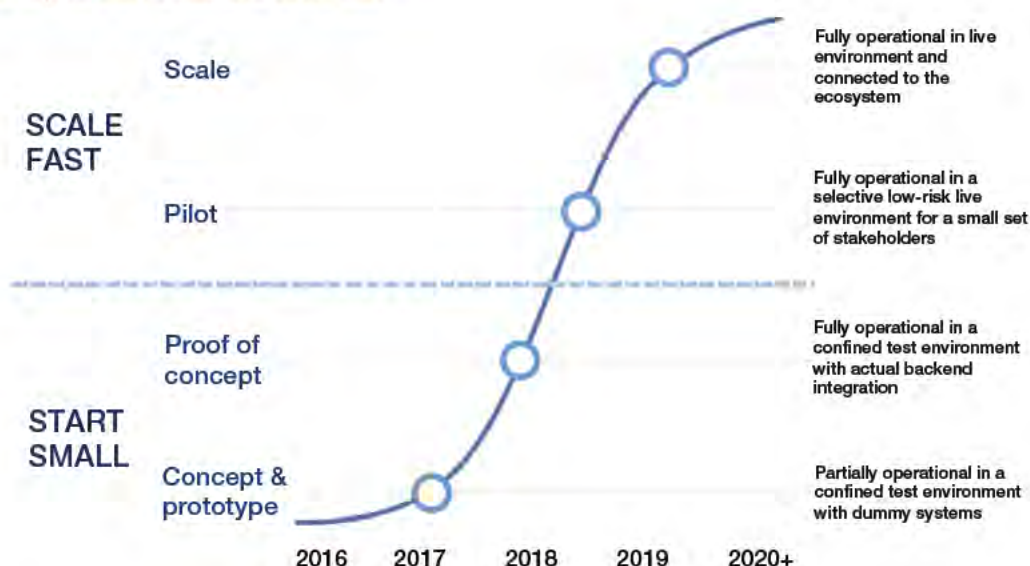
The aviation, travel and tourism sector is complex, with each region, country and agency characterized by its own nuanced contextual and political implications. While the concept assumes that a global interoperable system for passenger-controlled digital identities will have a positive effect on security in cross-border travel, it will remain a vision unless it is designed and developed to be adopted at scale. As a first step in testing its suitability for adoption and growth, the necessary institutional relationships are now being established to test a proof of concept in a secure “lab environment” and then in a live pilot.

The first goal is to connect the prototype to actual third-party systems in the ecosystem – not live systems, only test environments. In the launch phase, the ecosystem is extended to a number of private-sector stakeholders such as technology vendors, hotels and other service providers, as well as governmental agencies. Once the Known Traveller Digital Identity concept is shown to work within the lab environment, a live pilot study will allow travellers and other stakeholders to test the concept. The pilot study should be trialled in a low-risk zone such as one specific area of an airport for a specific flight with pre-screened passengers. If the pilot study is to succeed, it will require the wilful collaboration of diverse public- and private-sector partners.

“Technology companies have made major strides in data mining, machine learning and artificial intelligence enabling enhanced predictive analytics. In combination with passenger-provided information, these technologies can be used by governments to provide a more seamless, passenger-centric experience at borders and to analyse complex patterns in big data with the goal of predicting border security risks.”

It is essential that private-sector leaders in advanced data analytics, risk prediction, data privacy and fraud prevention share their expertise and innovation with the public sector to demonstrate the technologies’ potential. Simultaneously, the pilot study must be adequately measured for success while barriers to success are identified and adapted for future iterations. In 2018–2019, the World Economic Forum will facilitate the implementation of a geographically confined pilot in collaboration with various stakeholders (e.g. governments, airports, airlines). The Government of Canada has been actively exploring the testing of the concept with the Forum.

Figure 20: Roadmap to start small and scale fast



To enable a scaling up, it is critical to exploit network effects and broaden applications of the concept to entice not only travellers but also the public and private sectors to opt in. Leaders at an official and political level in different ministries need to collaborate in support of the concept intergovernmentally and with international organizations such as INTERPOL, ICAO, WCO, the UN High Commissioner for Refugees and the International Organization for Migration. There needs to be robust engagement with the travel industry – including airlines, shipping companies, port operators, hospitality and other travel and tourism service providers. There also needs to be trusted private-sector engagement to ensure the most effective use of new and emerging digital technologies and support for the transformation that would be required.

A Known Traveller Digital Identity shows great potential for use beyond travel, such as in healthcare, education, banking, humanitarian aid and voting. To raise the concept beyond occasional cross-border travel, the pilot must exploit the network effects associated with the platform economy and highlight to users the potential broad range of **everyday** applications. By 2020, the Known Traveller Digital Identity concept should be ready to expand beyond the traveller journey and made available to a wide audience, noting that broad adoption is crucial for the success of the concept.

Digital identity at the World Economic Forum

The Forum has recently embarked on an initiative in partnership with Accenture to develop a framework for digital identity for use beyond travel and takes into consideration the digital identities of people as well as inanimate objects and entities. The Known Traveller Digital Identity concept will fit in the broader digital identity standards and protocols defined in that Forum project.

Decentralized Identity Foundation

Decentralized Identity Foundation (DIF) is an open-source decentralized identity ecosystem that equips the decentralized identity community with the protocols, tools and implementations necessary to create and validate identity attestation. DIF furthers the ability of people, organizations and machines to have a single identifier akin to today's DNS entries for computers. Part of DIF's work is to solve the "last mile" problem of associating the identifier with the human (or similar characteristics of a thing). With these capabilities, users of blockchain-based systems will interact as a single, consistent identity to which all their activity (value and information) will be linked and indexed. Users will have control over who gets to access their information through granular access control for each piece of information. Counterparties to the user will be able to verify that the data has not been tampered with and evaluate the attestations and the provenance of their origins.⁵⁷



Recommendations

A. Act now

Pilot and develop iteratively

To demonstrate the feasibility of the Known Traveller Digital Identity concept in a real-life environment, private- and public-sector stakeholders must pilot the prototype, apply iterative development methodologies to demonstrate its value, seek continuous feedback from stakeholders and adapt accordingly. An iterative approach will encourage the necessary paradigm shift among stakeholders and establish an environment for large-scale adoption.

Implementing partners should use the framework provided to assess value-potential for all stakeholders and agree on the measurements for success. Reviewing progress against these measurements will help to identify which components of the concept need further attention if related value drivers are underperforming. Furthermore, the objective demonstration of the value of the Known Traveller Digital Identity concept for multiple stakeholders will reinforce the rationale for adoption.

Ensure inclusivity to drive scalability

Vast differences in infrastructure and resourcing for border and travel security exist between nations. To accelerate global scalability, it is imperative to pilot the intervention across varying contexts with different groups of travellers. Industry and government leaders should initiate pilot studies in more locations to ensure tests include a reasonable range of countries, geographies and economic levels. To support this, public- and private-sector partners should collaborate to develop a toolkit to empower decision-makers as they launch additional pilots.

Continuously monitor new developments

It is essential for all public- and private-sector stakeholders to continuously monitor new technological breakthroughs and policy considerations and indicate their ability to advance adherence to the design principles. A constant tension between what has already been built and the “fit” with new technological solutions is expected. Policy-makers especially are advised to retain agility in their policy-making to build upon regular learning without jeopardizing progress and convergence.



B. Build momentum

Focus on traveller-centric design to accelerate adoption

Travellers are at the centre of the success of the Known Traveller Digital Identity concept. Stakeholders must understand the traveller's intrinsic values and preferences for a fit-for-purpose concept and show travellers the benefits of adoption. With every technological or policy development, stakeholders must consider a traveller-centric design approach, which will ultimately make the Known Traveller Digital Identity concept more appealing to the broader aviation, travel and tourism industry. This, coupled with targeted behaviour-change strategies, will provide the incentive for travellers to become active partners in ensuring security in travel.

Explore new business models

The determination of viable, sustainable and trusted business models for delivering Known Traveller Digital Identity capabilities and infrastructure upgrades can entice the private and public sectors to participate in promoting secure and seamless travel. There is increased opportunity to use digital identity data, not only to improve security but also to enhance service offerings. Additionally, new models for managing and authenticating online identities have developed organically. Innovation can be driven by convenience for the customer, cost efficiencies for service providers and greater return on investment via new income streams for those public- and private-sector organizations that choose to, or have already, invested in identity management.

C. Sustain a supportive policy framework

Uphold standards and recommended practices

To maximize the exponential value and reach a critical mass of users, the Known Traveller Digital Identity prototype requires interoperability across geographies, policy environments and industries. Industry leaders and public-sector partners must maintain a technology-agnostic approach as well as promote a recognized framework of open standards and protocols. To map existing frameworks, stakeholders should collate all existing standards that govern the use of personal identity data and relevant technologies, across the full travel-security environment. Where gaps exist, stakeholders must continue to take the lead in new thinking and work collaboratively with agencies mandated to develop and maintain standards to ensure appropriate evolution.

Develop advanced risk profiling to expedite the security process

As the traveller is inclined to share more information as part of their digital identity, data for analysis will become available at a more granular level and allow for advanced data analytics for security vetting and personalization. By recognizing patterns, identifying correlations and using advanced algorithms, agencies can create detailed insights about the traveller. For example, a detailed risk profile of one individual allows authorities to direct this traveller to a specific security lane for intensified screening. This may expedite the security process for most travellers by pre-

emptively removing the perceived threat from the pre-vetted, low-risk traveller lane. The emergence of artificial intelligence and machine learning extends the opportunities to benefit from individual identity information. Stakeholders across the financial services, insurance and technology industries are well positioned to develop data analysis and risk-modelling best practices on identities that could be shared with government agencies for adaptation into their sovereign risk-assessment processes.

Prioritize privacy and cybersecurity

Privacy and cybersecurity considerations remain at the forefront of all stakeholder interests. Private- and public-sector stakeholders must ensure the high integrity of proposed security frameworks and technological concepts. Consideration must be given to how the system will adhere to or address statutory requirements for identity management across countries and meet the approval of privacy oversight bodies. Additionally, it is critical that security features are properly communicated to those who take it up – especially the travellers who entrust the systems with their private, personal data.

Acknowledgements

The World Economic Forum would like to acknowledge the many valuable contributions to this work through expert knowledge, interviews and research. In particular, the Forum recognizes the valuable participation of members of the Future of Security in Travel Working Group.

Future of Security in Travel Working Group

[Redacted text block containing names and affiliations of the Future of Security in Travel Working Group members]

[Redacted text block containing names and affiliations of other individuals and organizations acknowledged]

For further information on this report or the work undertaken by the World Economic Forum on the Future of Security in Travel, contact:

[Redacted contact information]
World Economic Forum LLC
@weforum.org
Tel: [Redacted]

Appendix A

Mobile application designs for enrolment process step (front-end)

Traveller arrives at an enrolment station and scans QR code.



Via QR code, traveller shares passport information, which is displayed on the official's screen.



Enrolment official scans traveller's passport on document scanner.

Passport chip is read; the data and photo are sent to the screen.

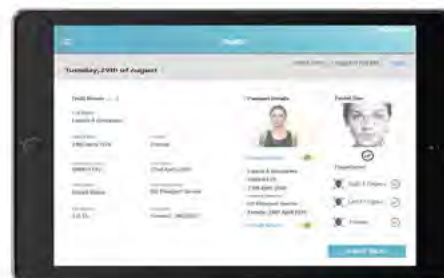


Enrolment official scans traveller's biometrics (e.g. face).

Biometric matching compares scanned face with the photo from the passport chip.

The traveller's passport data is also compared with the enrolled identity.

Enrolment official scans traveller's fingerprints.



The traveller can set up recovery contacts who could be asked to verify their identity when the traveller gets a new phone (or if their phone is stolen).



The traveller is now fully enrolled and can give access to their identity to third parties, enabling a more secure and seamless experience.



Endnotes

- ¹ **UNWTO.** UNWTO World Tourism Barometer – Advance Release January 2017. *UNWTO*. [Online] January 2017. [Cited: 18 October 2017.] http://cf.cdn.unwto.org/sites/all/files/pdf/unwto_barom17_01_january_excerpt_.pdf. Air travel on a whole is expected to double from the 3.8 billion air travellers recorded in 2016 to 7.2 billion air travellers in 2035. **IATA** <http://www.iata.org/pressroom/pr/Pages/2016-10-18-02.aspx>
- ² **Gillen, David and Morrison, William.** *Aviation Security: Costing, Pricing, Finance and Performance*. s.l. Elsevier, 2015.
- ³ In general, global movement of people for travel is disaggregated by local or cross-border (national or international), mode (land, marine and air) and purpose (business or leisure). This report focuses on international travel by air, for all purposes.
- ⁴ **UNWTO.** UNWTO World Tourism Barometer - January 2017. *UNWTO*. [Online] January 2017. [Cited: 18 October 2017.]
- ⁵ Ibid.
- ⁶ Ibid.
- ⁷ **WTTC.** *Global Economic Impact & Issues 2017*. s.l. World Travel & Tourism Council, 2017.
- ⁸ **Accenture.** *Border Management Global Trends Report*. s.l. Accenture, 2016.
- ⁹ **Gillen and Morrison.** *Aviation Security*.
- ¹⁰ Ibid.
- ¹¹ **Accenture.** *Border Management Global Trends Report*.
- ¹² **Gillen and Morrison.** *Aviation Security*.
- ¹³ **World Economic Forum,** *Incredible India 2.0*, October 2017.
- ¹⁴ **TTG Asia.** Airport Capacity Limits Asia Arrivals Growth. *TTGnordic.com*. [Online] TTG, March 2016. <http://ttgnordic.com/airport-capacity-limits-asia-arrivals-growth/>
- ¹⁵ The traveller journey is understood to differ from the land or sea border-crossing experience.
- ¹⁶ **World Economic Forum.** *Digital Transformation Initiative: Aviation, Travel and Tourism Industry*. Geneva: World Economic Forum, 2017. REF 060117.
- ¹⁷ **World Economic Forum.** *The Fourth Industrial Revolution, What It Means and How to Respond*. s.l. World Economic Forum, 2016.
- ¹⁸ Value at stake for airports is considered limited as a large part of security measures take place at the airport but are under the responsibility of other entities such as airlines and governments.
- ¹⁹ **World Economic Forum.** *Digital Transformation Initiative*.
- ²⁰ **World Economic Forum.** *Digital Borders*. s.l. World Economic Forum, 2016.
- ²¹ *Future of Security in Travel Workshop*. Amsterdam: Accenture, 2017. Debrief from the working group meeting on 9 June in San Francisco.
- ²² **World Economic Forum, Accenture Strategy.** *Shaping the Future of Security in Travel: Selection of Technological Intervention for Prototype*. Amsterdam: Accenture, August 2017. Draft discussion document prepared for the World Economic Forum.
- ²³ **DIF.** *Identity Foundation*. [Online] Decentralized Identity Foundation , 2017. <http://identity.foundation/>
- ²⁴ **WCO/IATA/ICAO** *Guidelines on Advance Passenger Information (API)*, WCO/IATA/ICAO, 2013.
- ²⁵ **World Economic Forum.** *Digital Transformation Initiative*.
- ²⁶ **UNWTO, WTTC.** *The Impact of Visa Facilitation on Job Creation in the G20 Economies*. s.l. World Tourism Organization and World Travel & Tourism Council, 2012. Report prepared for the 4th T20 Ministers' meeting Mexico, 15–16 May 2012.
- ²⁷ **World Economic Forum, Accenture Strategy.** *Shaping the Future of Security in Travel: Value Tree*. July 2017. Draft discussion document prepared for the World Economic Forum.
- ²⁸ **Jagers, Chris.** Digital Identity and the Blockchain: Self-Sovereignty Isn't Automatic; It Must Be Explicitly Architected into Any Blockchain-Based Social Infrastructure. *medium.com*. [Online] learningmachine.com, 16 July 2017. <https://medium.com/learning-machine-blog/digital-identity-and-the-blockchain-10de0e7d7734>
- ²⁹ **Lewis, Antony.** A Gentle Introduction to Self-Sovereign Identity. *Bits on Blocks*. [Online] 17 May 2017. [Cited: 18 October 2017.] <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/>
- ³⁰ **Grassi, Paul, Garcia, Michael and Fenton, James.** Digital Identity Guidelines. *pages.nist.gov*. [Online] June 2017. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>
- ³¹ **European Data Protection Supervisor.** Necessity and Proportionality. *European Data Protection Supervisor*. [Online] 29 March 2017. [Cited: 1 November 2017.] https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en
- ³² **Lundkvist, Christian, et al.** *Uport: A Platform for Self-Sovereign Identity*. s.l. UPORT, 2017.

- 33 **Tobin, Andrew and Reed, Drummond.** *The Inevitable Rise of Self-Sovereign*. s.l. The Sovrin Foundation, sovrin.org, 2016., and **ID2020.** *Why Digital Identity?* *ID2020.org*. [Online] ID2020, 2017. <http://id2020.org/digital-identity-1>
- 34 **DIF.** *Identity Foundation*. [Online] Decentralized Identity Foundation , 2017. <http://identity.foundation/>
- 35 **World Economic Forum.** *Digital Transformation Initiative*.
- 36 **IBM.** *Fast Forward: Rethinking Enterprises, Ecosystems and Economies with Blockchains*. s.l. IBM Institute for Business Value, 2016.
- 37 **Bitsonblocks.** *A Gentle Introduction to Self-Sovereign Identity*. *bitsonblocks.net*. [Online] Bits on blocks, May 2017. <https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/>
- 38 **RIA.** *Data Exchange Layer X-Road*. *ria.ee*. [Online] Republic of Estonia Information System Authority, 2017. <https://www.ria.ee/en/x-road.html>
- 39 **Credits.** *Terminology*. *credits.readthedocs.io*. [Online] 2017. http://credits.readthedocs.io/en/latest/blockchain_terms.html - distributed-ledger-technology
- 40 **Lewis, Antony.** *What's the Difference between a Distributed Ledger and a Blockchain?* *Bits on Blocks* [Online] 20 February 2017. [Cited: 29 November 2017] <https://bitsonblocks.net/2017/02/20/whats-the-difference-between-a-distributed-ledger-and-a-blockchain/>
- 41 **IDC.** *It Was Only a Matter of Time: Digital Identity on Blockchain*. [Online] 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GIL12346USEN&>
- 42 **Hare, Stephanie.** *HBR: Blockchain Could Help Us Reclaim Control of Our Personal Data*. *blog.accenture.com*. [Online] Accenture, Oct 5, 2017. https://blog.accenture.com/stephanie_hare/2017/10/05/hbr-blockchain-could-help-us-reclaim-control-of-our-personal-data/.
- 43 **Buchner, Daniel, et al.** *Decentralized-identity/hubs*. *github.com*. [Online] Github, 26 July 2017. <https://github.com/decentralized-identity/hubs/blob/master/explainer.md>
- 44 **Lundkvist, Christian, et al.** *Uport: A Platform for Self-Sovereign Identity*.
- 45 **Mattila, Juri.** *The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures*. Berkeley Roundtable on the International Economy, University of California, Berkeley : ResearchGate, 2016., and **Windley, Phil.** *Is Sovrin Decentralized?* *Windley.com*. [Online] 2017. http://www.windley.com/archives/2017/09/is_sovrin_decentralized.shtml
- 46 **Tobin, Andrew and Reed, Drummond.** *The Inevitable Rise of Self-Sovereign*. s.l. The Sovrin Foundation, sovrin.org, 2016.
- 47 **RIA.** *Public Key Infrastructure PKI*. *RIA.ee*. [Online] Republic of Estonia, Information System Authority, 18 April 2017. <https://www.ria.ee/en/public-key-infrastructure.html>
- 48 **O'Higgins, Conor.** *Digital Identity Part II – Proof-of-Personhood*. *Cryptoinsider.com*. [Online] 2017. <https://cryptoinsider.21mil.com/digital-identity-part-ii-proof-personhood/>
- 49 **Reed, Drummond, et al.** *DID (Decentralized Identifier) Data Model and Generic Syntax 1.0 Implementer's Draft 01*. *Github.com*. [Online] Nov 2016. <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2016/blob/master/draft-documents/did-implementer-draft-10.md>
- 50 **IDC.** *It Was Only a Matter of Time: Digital Identity on Blockchain*. [Online] 2017. <https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GIL12346USEN&>
- 51 **O'Higgins, Conor.** *Digital Identity Part II – Proof-of-Personhood*.
- 52 **NIST.** *Face Recognition Algorithms Surpass Humans*. s.l. : NIST, 2016.
- 53 **Accenture.** *Citizen Support for the Use of Biometric Technologies to Facilitate Travel and Secure Borders*. s.l. : Accenture, 2014.
- 54 **NIST.** *Biometrics*. 2017. <https://www.nist.gov/programs-projects/biometrics>
- 55 **Jagers, Chris.** *Digital Identity and the Blockchain*.
- 56 **Lundkvist, Christian, et al.** *Uport: a platform for Self-sovereign Identity*.
- 57 **DIF.** *Identity Foundation*.



**COMMITTED TO
IMPROVING THE STATE
OF THE WORLD**

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: [REDACTED]
Fax: [REDACTED]

[REDACTED]@weforum.org
www.weforum.org