WORLD ECONOMIC FORUM

Accelerating the Transition to Digital Credentials for Travel: Lessons from KTDI – a Public-Private Collaboration for Secure and Seamless Travel

WHITE PAPER

OCTOBER 2021

Cover: Phive2015, Getty Images – **Inside:** Getty Images

Contents

Foreword

Pedro Gomez
Head of Shaping the Future of Mobility; Member of the Executive Committee, World Economic Forum

Christine Leong
Global Digital Identity & Biometrics Lead and Managing Director, Accenture

As the demand for cross-border travel resumes in the wake of the COVID-19 pandemic, the need for a more coherent, touchless, efficient, safe and secure travel continuum is more important than ever before. The travel ecosystem needs to adopt efficient and touchless solutions to address the challenges of sharing and verifying travel documents and credentials in an increasingly digital world. Where digital credentials were first identified as an innovative and future-looking approach to addressing concerns about border security, the pandemic has brought that future forward – along with an urgent need to address public health security in cross-border travel.

Multistakeholder collaboration is crucial in moving towards more secure and resilient international travel. Actors from across border agencies, travel partners, public health departments and technology providers will need to work together to create a trusted, widely accepted system of digital credentials for travel that will help facilitate the reopening of international travel and move the industry towards safer, more efficient travel.

The World Economic Forum, together with its partners, has been exploring solutions to improve seamless and secure travel challenges through the Known Digital Traveller Identity (KTDI) concept, introduced in January 2018, as part of its Shaping the Future of Security in Travel project. As the travel sector urgently looks for approaches to establish travel credentials that are trusted, widely accepted, interoperable and adopted across sectors and borders, as well as by travellers themselves, the KTDI concept is now more relevant than ever.

This paper is the result of collaboration between the World Economic Forum, Accenture and industry and government partners to boldly envision a new future for cross-border travel and co-design a trusted, shared and mutually beneficial system, with the traveller at the centre. Multistakeholder efforts such as these are never simple, but they are necessary if we are to address shared challenges. Based on the lessons learned and best practices captured from the KTDI journey so far, we have put together this playbook to facilitate global public-private collaboration efforts on the deployment of digital travel credential solutions. The playbook proposes opportunities for collaboration as well as considerations for those embarking on the process of introducing digital credentials in travel.

We are grateful to the public- and private-sector partners who provided the testing environment for the KTDI concept, and for their long-standing support of the Known Traveller Digital Identity Consortium. Having championed this transition to a traveller-centric, security-enhancing and technology-forward travel system, the Forum and its partners are excited to collaborate further with organizations that share the KTDI vision, within the travel sector and beyond.

Executive summary

The Known Traveller Digital Identity (KTDI) concept was introduced in 2018 to explore how emerging technology innovations could promote more efficient, secure and seamless travel against a backdrop of increasing traveller volumes, security requirements and constraints on resources and infrastructure capacity. Since then, the World Economic Forum and its partners have designed and built the first government-led public-private ecosystem to test these new processes and technologies in a cross-border context and embark on the development of a globally accepted digital travel credentials ecosystem.

The COVID-19 pandemic has upended global aviation, travel and tourism and accelerated the digital transition on which the sector had already begun to embark. As the use of verifiable documents (e.g. government-issued identity vaccination certificates, proof of negative COVID-19 tests) becomes a requirement for safe cross-border movement, global demand for trusted digital credentials across sectors and borders has surged. Many governments have leveraged existing capabilities to meet the need for digital credentials that enable domestic and cross-border movements. Numerous other initiatives have also been launched as a result of the pandemic to meet this gap. This has led to a proliferation of different approaches. Governments globally need to collaborate and employ emerging solutions to enable a more cohesive ecosystem for the industry and the wider public. Public-private as well as cross-sector collaboration is more crucial than ever before to set a clear path forward and establish a trusted framework that can adapt to changing conditions and scale quickly.

The ecosystem of digital travel solutions and approaches has significantly expanded since the inception of KTDI, with decentralized identity, biometrics and decentralized ledger technologies becoming more widespread and increasingly referenced in leading industry policy guidance and frameworks. Despite this progress, the ecosystem remains deeply fragmented, in part due to the lack of a globally accepted trust framework, with disparate solutions often causing confusion and stagnation in the market. Additionally, these new capabilities must be complementary to those that already exist; they will have to work with current capabilities such as essential public key infrastructure if they are to augment their reachability and scalability to sectors beyond border control.

KTDI is unique compared to other consortia efforts in that it is government-led and rooted in a common vision and set of values shared by all partners. While pilot efforts have been affected by the pandemic, the consortium's achievements and expertise serve as a valuable blueprint to inform other similar efforts being developed globally.

This report outlines the main achievements, lessons learned and best practices from KTDI efforts so far. Furthermore, it aims to facilitate multistakeholder dialogue and the development of actionable strategies that help improve border and health screening, touchless traveller processes and more effective use of traveller data. As more governments seek to explore digital credentials for travel, this report is also intended to serve as a "playbook" for policy-makers and industry leaders to guide decision-making and assess important considerations in the areas of governance, legal regulation and technology as they relate to the wider travel continuum.

The success of any public-private travel ecosystem relies on robust government leadership and action, effective intergovernmental collaboration and participation by multiple private-sector partners and international organizations, with a strong focus on serving the traveller at the centre. The World Economic Forum and KTDI partners are committed to promoting such multistakeholder collaboration, which is needed in an increasingly complex and rapidly evolving travel ecosystem.

KTDI's vision is to achieve global collaboration between partner organizations interested in working together on globally trusted digital credentials that are widely accepted, interoperable and adopted across sectors and borders and by travellers themselves. The Forum and its KTDI partners invite interested stakeholders who share a similar vision to explore further collaboration and shape the future of secure and seamless travel.

1 Restoring trust in travel: the need for digital credentials

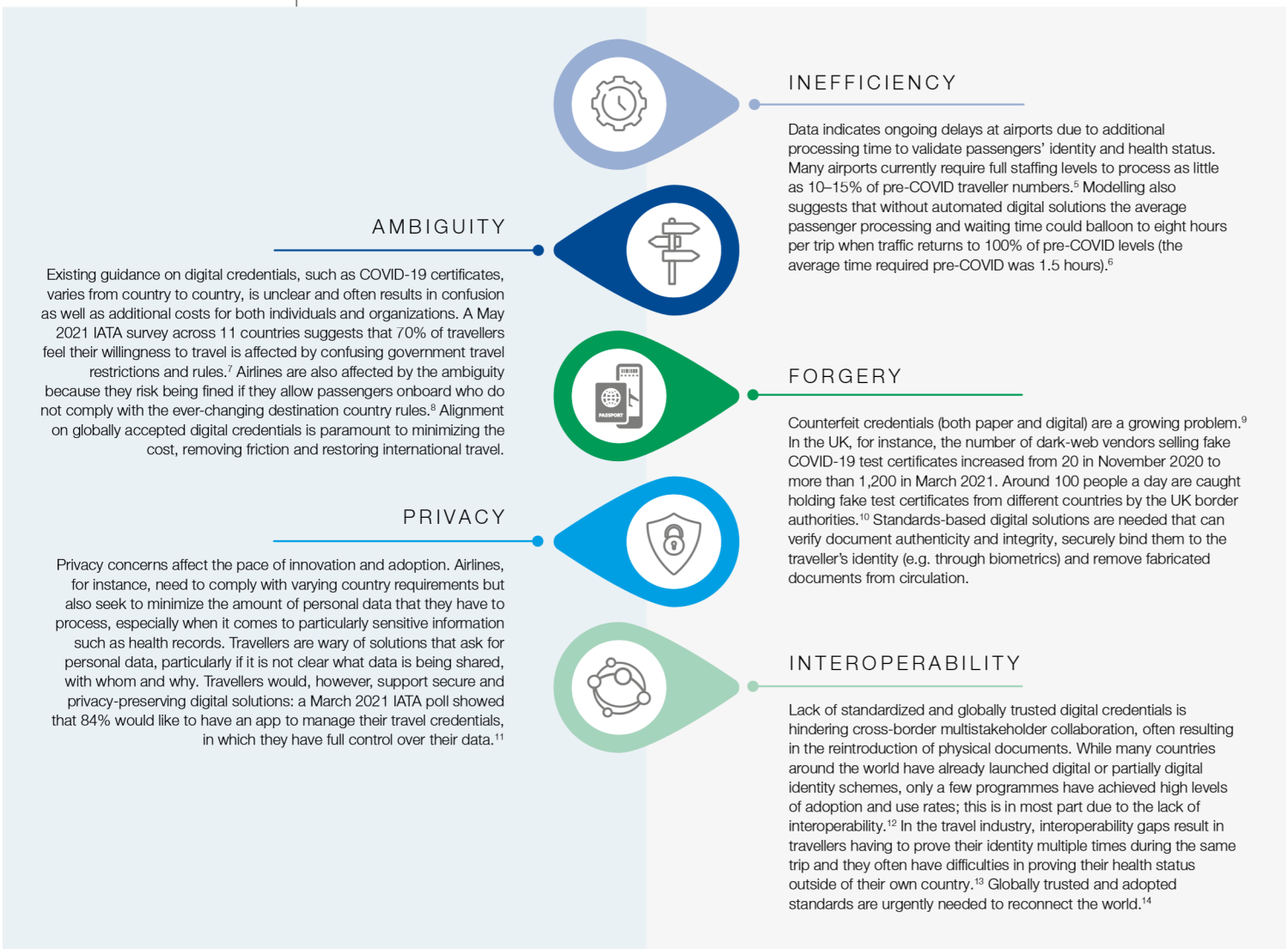
Before the COVID-19 pandemic, the travel industry was already under increasing pressure from a rise in traveller volumes, enhanced security requirements, limited physical infrastructure, and ageing processes and systems.[1] Cross-border travel was expected to grow by 50% over the ensuing decade and reach 1.8 billion international arrivals by 2030.[2] While COVID-19 has heavily affected the travel industry, borders have started to reopen due to the increasing number of vaccinated individuals and advances in testing. In fact, international passenger numbers are now expected to grow and exceed pre-pandemic levels by 5% as soon as 2023.

Having said that, as a result of the pandemic, airlines and border officials now have to manually verify additional documentation that is often paper-based, easy to lose and not difficult to fake. This causes longer queues at airports, making travel increasingly confusing for travellers and all stakeholders involved. For instance, airport processing times have doubled, reaching three hours during peak times despite travel volumes hovering at around 30% of pre-COVID-19 rates, i.e. 2019 levels.[3] In addition, travellers want to have certainty that their documents will be accepted before they leave home, that they won't have to spend much time at the border and that they will be able to board their flight. Digital credentials and touchless borders are needed more than ever to restore confidence in travel, enable efficient traveller processing and prepare for the industry recovery.

Travellers, who now need a number of different documents to travel, also expect and support digital innovation to enable a seamless travel experience. A March 2021 International Air Transport Association (IATA) poll showed that 89% of travellers support globally standardized digital certifications.[4] However, the proliferation of various digital solutions for travel in the past year has actually made cross-border movement even more confusing and cumbersome, especially as many countries and industry players have developed their solutions in siloes. The ecosystem remains deeply fragmented and lacks common standards, and the market often favours speed to market over functionality, consistency, safety and fraud prevention. This can lead to digital "passes" and "certificates" falling short of user expectations and becoming a hotly debated political topic, with many countries facing an intense public backlash.

The confusion and fragmentation in the market reiterates the need to focus on innovation and global collaboration to address some of the biggest challenges in border reopening and industry recovery, which include:

FIGURE 1 **Key challenges in restoring cross-border travel**



BOX 1 | **The importance of interoperability – ICAO example: globally accepted travel documents**

The International Civil Aviation Organization (ICAO)'s machine-readable travel documents (MRTD) and electronic machine-readable travel documents (eMRTDs) are globally interoperable because all participating stakeholders (member states) agreed to conform to the corresponding technical specifications for their issuance and verification as prescribed in ICAO governance and trust frameworks. ICAO's eMRTD is the most widely used, globally interoperable digital credential in use today.

These challenges prove that the benefits of using digital credentials in travel cannot be realized through isolated or one-off approaches. Multistakeholder collaboration on globally trusted and accepted digital credentials is fundamental to moving the industry towards more secure and seamless travel.

1.1 Emerging approaches for digital credentials in travel

As a result of COVID-19, multiple solutions have started to emerge that try to meet the global demand for trusted digital credentials for travel. Ecosystems will derive the most value by recognizing that different approaches will have their respective advantages and limitations but that they also can and should work together. Above all, a scalable and sustainable approach should be driven by a common vision and the willingness to collaborate and create an interoperable ecosystem rather than by focusing purely on the technology itself. Piloting globally trusted digital credentials should also **not mean committing to one approach exclusively**, or replacing one system with another, but rather serve to encourage stakeholders to look for ways to build upon and integrate with existing solutions.

In the increasingly crowded and complex ecosystem of digital credentials for travel we are seeing two major approaches that could work together: **centralized public key infrastructure (PKI)** and **decentralized digital identity**.

When COVID-19 hit, the International Civil Aviation Organization (ICAO)'s Public Key Directory (PKD) was already using the well-established PKI approach to support its eMRTDs. Due to the pandemic, international organizations and governments around the world started to further explore the capabilities of PKI-based solutions to address new challenges being faced by the travel industry – specifically, to augment existing foundational identity information with health status information in a globally interoperable, privacy-preserving, secure, verifiable, digital fashion. The ICAO Visible Digital Seal (VDS), the European Union (EU) Digital COVID Certificate (DCC) and the World Health Organization Digital Documentation of COVID-19 Certificates (DDCC) specification are a few examples of the efforts in the trusted digital credentials space.

However, while PKI-based digital identity approaches such as ICAO's eMRTD have established governance frameworks and work well for border control, their extensibility remains a

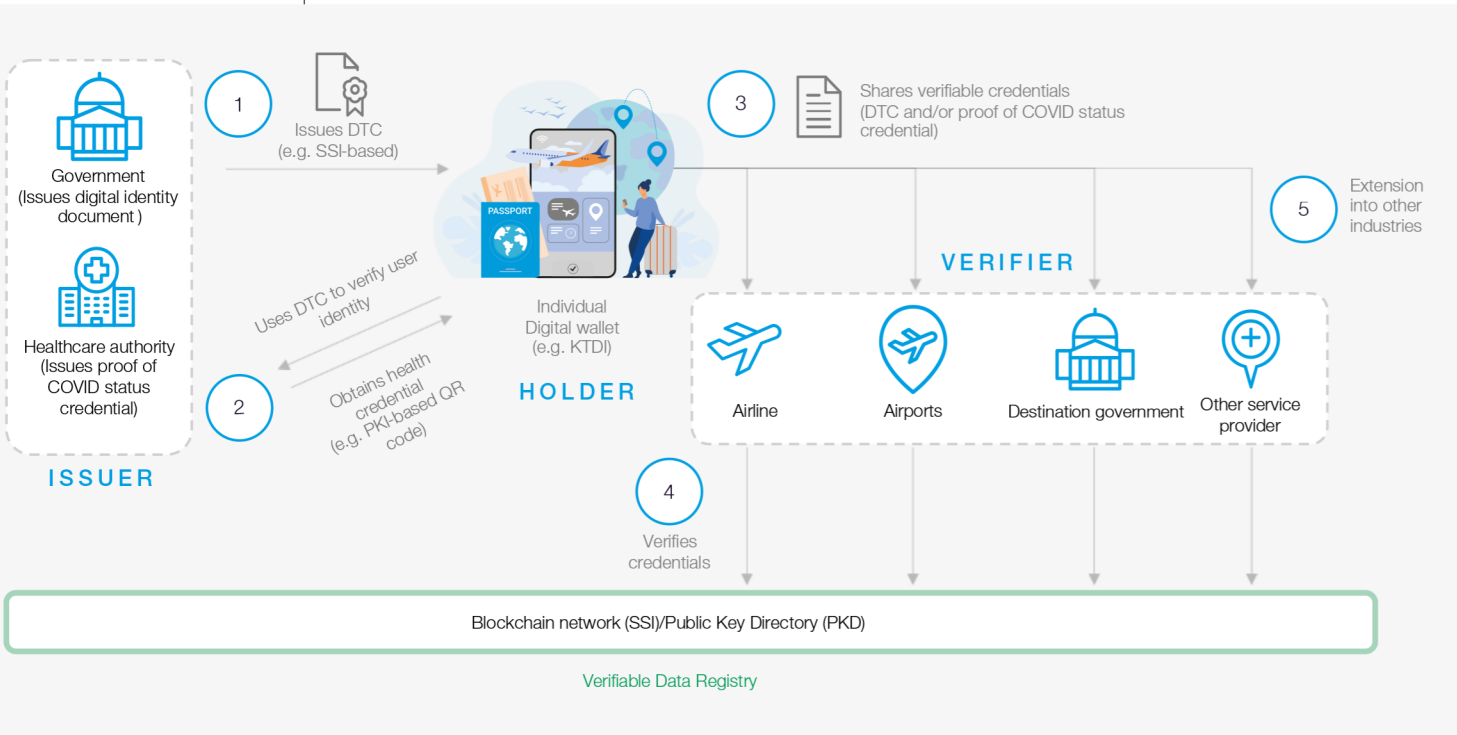
challenge. As access to the ICAO's PKD is limited to member states, the ICAO's eMRTD or, in the future, Digital Travel Credentials (DTC) cannot easily be extended to support private-sector use cases such as boarding, hotel check-in, access to venues, etc.[15] Moreover, PKI-based digital credentials do not support selective disclosure. In the context of QR code-based COVID credentials, they require a portal or similar means to facilitate pre-travel sharing and may need to be presented again during travel. QR -based COVID credentials used today are neither secure nor private. They contain PII and PHI, which can be read (they are not encrypted) and duplicated, so do not resolve the issue of fraudulent credentials in the market.

Decentralized digital identity systems, also known as self-sovereign identity (SSI) systems, started to gain popularity before COVID-19 due to their focus on user control over personal data, as well as the increasing maturity of the open standards that such systems are based on. Decentralized digital identity initiatives, such as KTDI or the IATA's Travel Pass, allow secure sharing of trusted, verifiable data with multiple public and private ecosystem participants, facilitating global cross-border and cross-sector collaboration. This emerging approach also enables users to selectively disclose verifiable credentials securely and under informed consent with verifying parties in advance (e.g. prior to travel) and subsequently allows users to benefit from touchless travel and seamless verification.

While solutions based on decentralized digital identity allow for extensibility, it is important to acknowledge that a fully established governance framework for decentralized identity ecosystems does not yet exist and standards are still evolving.

All in all, centralized PKI-based digital identity and decentralized digital identity solutions both have important advantages and limitations, but they do not have to be mutually exclusive. Below is a high-level example of how centralized PKI-based digital identity and decentralized identity solutions could work together, incorporating the ICAO's eMRTD or DTC into decentralized identity verifiable credentials.

FIGURE 2 **Emerging approaches for digital credentials in travel (example/illustrative only)**



Key roles:

- **ISSUER:** Creates and issues an identity credential based on a set of identity claims made by users
- **HOLDER:** The person or entity that uses an issued digital identity to access services
- **VERIFIER:** The entity that consumes an identity credential from an issuer and trusts that information to make business or service delivery decisions, or to enable access to services[16]

Key activities:

1. The government validates the ICAO eMRTD (or DTC) and issues the foundational identity verifiable credential to the individual's KTDI wallet based on W3C standards.

- Additional W3C-compliant verifiable credentials can be added to the wallet; e.g. a proof of COVID status verifiable credential issued by a healthcare authority or a QR code-based COVID credential.

2. The traveller selectively discloses required information from the foundational identity verifiable credential to verify their identity with the healthcare authority and requests the proof of COVID status verifiable credentials. The healthcare authority issues the **proof of COVID status verifiable credentials** into the user's wallet.

3. The traveller individually consents to selectively disclose the required foundational identity information and **proof of COVID status information** with their airline, airports and destination government.

    - **Decentralized digital identity benefit:** Unlike QR code-based passes, which do not support selective disclosure and expose personal identifiable information (PII) and protected health information (PHI) when exchanged, verifiable credentials enable the individual to selectively disclose only the information required by the relaying party and perform these exchanges through encrypted channels.

4. **Each verifiable credential is validated** (authenticity, integrity and revocation status) using a decentralized Verifiable Data Registry. In the case of centralized PKI-based verifiable credentials, an authorized verifier would ultimately need access to the ICAO master list or PKD to authenticate the eMRTD or DTC itself, and revocation status is not on an individual basis – it typically covers thousands of credentials.

5. Extension into other industries (for any credential).

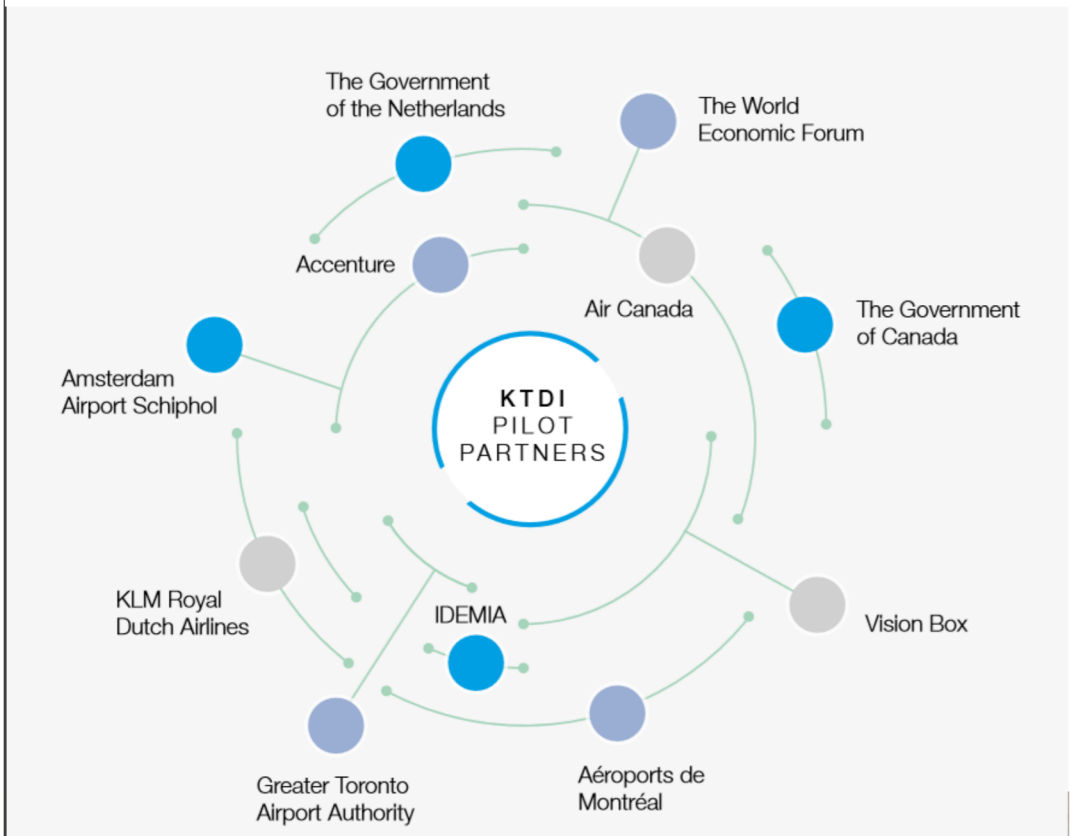
Scalable and globally accepted solutions will have to be extensible to support various emerging standards and approaches to enable seamless domestic and international travel. We can expect the world to end up with multiple centralized and decentralized solutions for travel digital credentials that will ultimately need to work together.

2 A case study for digital credentials in travel – KTDI: the journey so far

Since 2018, the KTDI partners have designed and built the first government-led public-private ecosystem to test a vision of safe and seamless cross-border travel. This vision aimed to reduce touchpoints through the use of emerging technologies, including biometrics and decentralized identity, and inform the future development of a globally accepted decentralized identity ecosystem. While at its inception the KTDI concept or the notion of decentralized identity to facilitate cross-border travel was not yet mainstream or widely understood, KTDI partners worked together to establish a common vision and a core set of values and together found innovative ways to overcome KTDI conceptualization challenges.

While KTDI pilot efforts have been affected by the pandemic, COVID-19 has also created an opportunity to conduct further analysis on how decentralized digital identity and PKI-based approaches could work together. Although the initial pilot employed a decentralized identity approach to trial trusted digital credentials, in the future, KTDI could expand to incorporate additional verifiable credentials (e.g. COVID-19 vaccination certificates) as well as PKI-based digital credentials (e.g. ICAO DTC). The consortium's achievements and expertise can serve as a valuable blueprint to inform other similar efforts being stood up globally.

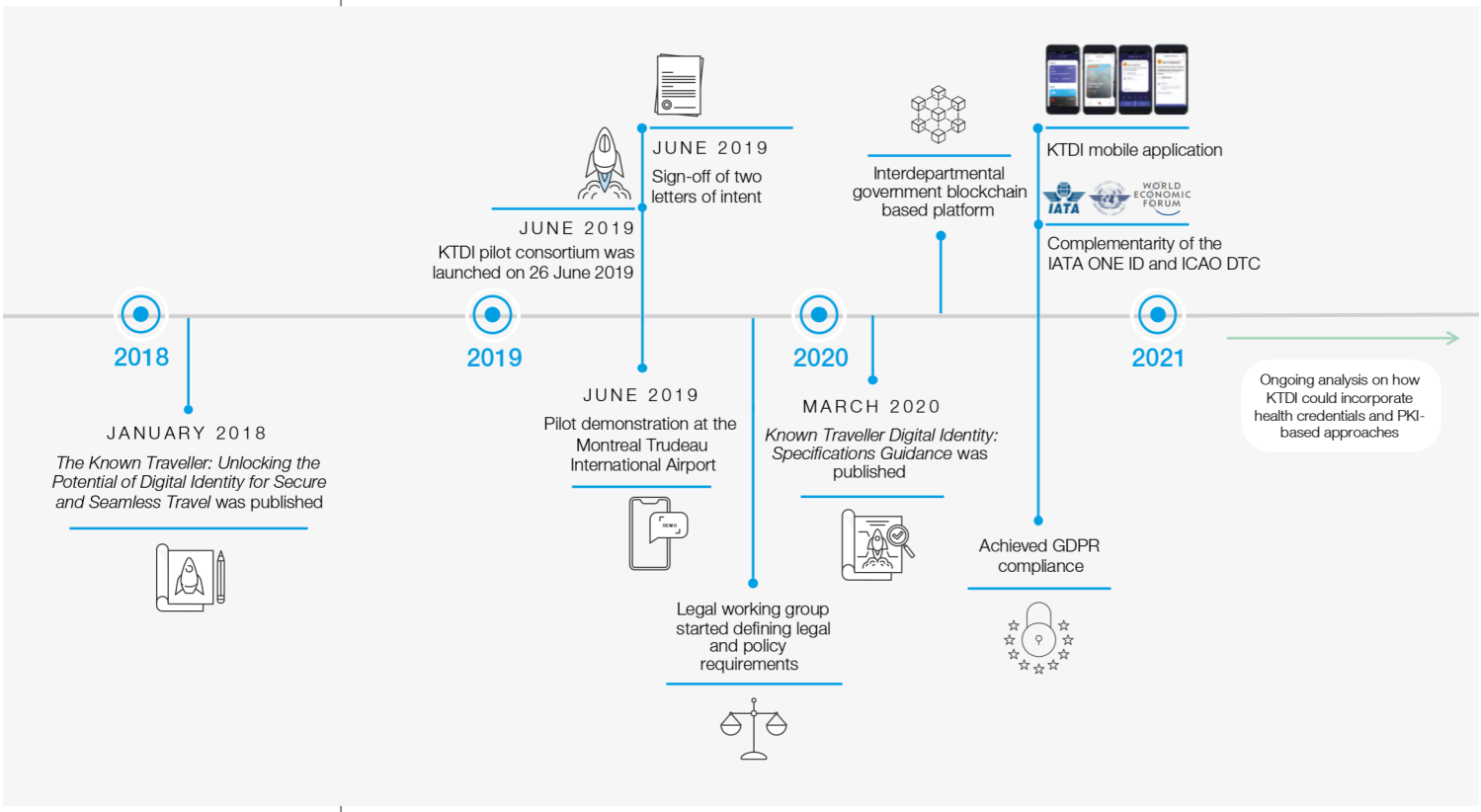
FIGURE 3 **KTDI's pilot partners**



2.1 Timeline and achievements

The high-level timeline below outlines the key KTDI milestones and achievements since its inception in 2018.

FIGURE 4 **KTDI timeline and achievements**



Following the publication of the KTDI concept report and the formation of the consortium, KTDI achieved notable delivery, governance and legal milestones throughout 2020 and 2021, in particular:

- **Establishment of an interdepartmental government blockchain:** The Government of Canada, in collaboration with Accenture, completed the testing of an interdepartmental government blockchain-based digital identity management platform in a simulated environment. Government departments collaborated extensively to illustrate the KTDI proof of concept internally, further facilitating acceptance throughout the various government departments and building trust in the ecosystem. In addition, this proof of concept was the first step towards gaining wider acceptance for using a decentralized digital identity solution for travel within a government setting and driving alignment between several different agencies and departments.

- **Conceptually aligned with the IATA's ONE ID and the ICAO's Digital Travel Credential (DTC) guidance:** When the KTDI concept was initially presented to the broader community of World Economic Forum stakeholders, it was considered to be somewhat futuristic, if not impossible to achieve. The piloting process enabled partners to demonstrate that this radically innovative future state was possible and to show how the concept was directionally aligned with both the IATA's One ID and the ICAO's DTC programmes. The common thread is the ability of travellers to share trusted, verifiable information prior to travel to enable touchless, accurate identity confirmation at airport checkpoints.

- **Definition of cross-border legal and policy requirements:** The regulatory and legal considerations at both the national/interdepartmental level and the binational/cross-border level were the most challenging and complex to navigate, given the multijurisdictional nature of identity and the need to align vision, mandates and policies across all levels. Through the creation of a dedicated legal working group with representatives from each organization, KTDI partners identified the key legal and policy implications and requirements of a decentralized identity ecosystem for cross-border travel, and were able to capture these learnings for

such cross-border efforts in future. This group assessed requirements and issues regarding intellectual property (IP) rights, liability, data sharing and privacy, and compliance with relevant data protection regulations. Specific information is included in Section 4.

- **KTDI mobile application:** All partners are proud of the joint effort to develop the KTDI mobile application, which is based on contributions from industry, governments, legal consultations and vendors, and has received accolades from like-minded initiatives. Co-designing this mobile application meant that individual company or government departmental needs could not take priority over the overall user experience, thus ensuring exceptional user-centricity.

- **Achieved GDPR compliance:** Through multiple review cycles and by working closely with legal and data privacy experts as well as a service design agency, the KTDI partners designed and developed a KTDI mobile application that is fully GDPR-compliant and acceptable for all partners to use. The mobile app's design balances a seamless user experience with informed data-sharing consent, whereby the user remains in control of their personal data.

- **Ongoing analysis of KTDI expansion:** As a result of COVID-19 and the surging demand for globally trusted digital credentials, KTDI aims to continue driving scalability and to pilot new travel use cases. The ongoing pandemic has created an opportunity to conduct further analysis of how KTDI could support health digital credentials, such as COVID-19 vaccination certificates, and how decentralized digital identity and PKI-based approaches could work together to support the future of cross-border travel.

While the KTDI pilot effort is paused as border reopening processes continue, KTDI partners remain committed to collaborating with other like-minded organizations to this end and exploring how KTDI could be expanded to help reopen international travel. The need for trusted digital travel credentials as a result of COVID-19 is paramount and clearly, from the different solutions that have emerged, the pandemic has served as a burning platform urging stakeholders to get the design of trusted digital credentials for travel right.

This is a pivotal moment. Now, more than ever before, public- and private-sector players within the travel ecosystem need to take collaborative action and work towards a common goal of re-enabling people to travel while reducing confusion, anxiety or complexity for travellers, staff and travel authorities. Multistakeholder collaboration is critical to reopening international travel. Organizations have the opportunity to work on digital credentials to make travel safer, more seamless and more efficient.

3 Opportunities for collaboration

Travel and tourism was one of the world's largest sectors in 2019, accounting for 10.4% of global GDP ($9.2 trillion) and 10.6% (334 million) of all jobs – responsible, in fact, for creating one in four new jobs across the world. Although COVID-19 has hampered progress, the effect of the pandemic has emphasized the tremendous importance and positive contribution this industry can have. World Travel & Tourism Council research shows that if international mobility and travel is resumed by 2021, the 62 million jobs (18.5%) lost in 2020 could be recovered before the end of 2022.[17] Existing travel organizations and systems are ill-equipped to deal with the urgent need for touchless borders, the increasingly complex demands on airline, security and border staff, the volume of passenger numbers and increasing security and health requirements – in addition to infrastructure capacity limits.

With the increased pressures and complex requirements, organizations within the travel ecosystem need to evolve. Collaborating with other organizations on integrating seamless and touchless travel mechanisms is essential to enhance the traveller experience and improve efficiencies across a number of processes in different organizations, enabling safe, trusted travel and so reducing some of the burdens that organizations in the travel continuum face today. Operational inefficiencies in handling the increasing demand for global travel will continue to grow if they are not properly addressed in the near future. Collaboration between the public and private sectors is critical to restore international travel and develop the travel and tourism industry.

Establishing digital credentials for travel that are accepted by governments, the private sector, international organizations and travellers is a complex undertaking. With different organizations plus different missions and goals, various barriers become apparent at the start of the collaboration process. However, digital travel credentials will provide value for all organizations within the travel ecosystem. Greater efficiencies can be realized while enhancing the security of both the individual traveller and borders, and consequently improving experiences and processes for both travellers and organizations.

Getting this process right, however, requires coordinated collaboration on vision, mission, governance, standards and technology. Organizations with a common vision and mission to enable seamless travel can collaborate to establish a scalable and sustainable ecosystem, achieve industry and global adoption and maximize the value of credentials for all partners and travellers.

Above all, to move towards meaningful collaboration on travel credentials, organizations need to adopt a user-centric mentality to deliver genuine value and encourage widespread adoption. Operational efficiency and enhanced traveller experience can be achieved only if the seamless travel solution is embraced by all parties. Each organization may have its own incentives, limitations and objectives, but the entire ecosystem needs a common vision to promote safe and seamless travel for the traveller. Failing this, the travel ecosystem will remain deeply fragmented, with disparate solutions causing confusion and stagnation in the market.

BOX 2 The Importance of collaboration – digital travel credential issuance in Canada

In Canada, valid forms of identification can be issued by federal, provincial and territorial jurisdictions.[18] Canadian citizens are demanding a more integrated process: more than 70% want government and private-sector collaboration on a joint identity framework in Canada.[19] A digital identification infrastructure in Canada and other similar countries could benefit from a collaborative public-private approach, enabling interoperability with different systems in the travel ecosystem to facilitate seamless interactions for the traveller, e.g. at the airport to pass through security, board the plane and cross borders through to car rental and checking into the hotel.

3.1 Value of collaboration

Given the complexity of the travel ecosystem and the diversity of the organizations involved, having stakeholders from both government and travel-sector private partners (e.g. airlines) is critical to fully realize the benefits of digital credentials for travel. These include minimizing risks and costs, helping to transform the user experience and creating efficiencies throughout the end-to-end travel experience. Figure 5 articulates the value enhancements that can be attributed to using digital credentials for travel.

FIGURE 5 **Incentives for collaborating on digital credentials for travel**

Reducing operational inefficiencies:

- Traveller journeys are often slowed by inefficiencies such as repetitive manual checking of information, which result in longer queues and cost impacts for airports, airlines and border management organizations. Currently, travellers must present their identity credentials at least six times from pre-check-in to inbound border control on an international journey.[20] Following the resumption of international travel, 55% of travellers found the process of air travel – booking, getting to the airport and boarding – more stressful than work.[21]
- Digital travel credentials provide a quicker and more seamless way to process and check trusted data such as passports, visa and health status in advance, enabling pre-cleared travellers to quickly continue their journey, while the organization can focus its resources on the right priorities. Organizations can leverage this efficiency to process additional passengers and improve management of staff allocation, benefitting from the reduction in operational and compliance costs.

Establishing cross-border and cross-sector trust:

- Fraudulent travel credentials pose real security risks and operational inefficiencies to travel organizations and border agencies. With more than 100 fake COVID-19 certificates detected per day on entry to the United Kingdom, large amounts of effort and cost are required to validate documents to gain assurance of their trustworthiness.[22]

– With digital travel credentials, passengers can securely provide their trusted identity information, in advance, without needing to present multiple physical documents at each checkpoint. In return, the interacting public and private organizations can verify that the data provided is legitimate, up to date and has not been altered or revoked, and thus pre-clear the traveller quickly.

Enhancing security:

– With the increased number of travellers, and as the world becomes more connected than ever before, security concerns are greater than ever. The Department of Homeland Security's Transportation Security Administration (TSA) has requested $8.9 billion for the fiscal year 2022 to spend on aviation security to accomplish its transportation security mission, an increase of $47.7 million over its previous budget.[23]

– With a trusted ecosystem and travel credentials, businesses can realize greater confidence and security. Digital credentials for travel enable easier identity verification and risk assessment as the information presented is trusted within the travel ecosystem and is often available to border and law enforcement officials earlier in the travel journey, allowing more time to process and assess the information.

Improving the travel experience:

– With the ongoing COVID-19 pandemic, travellers are required to carry and present multiple, often paper-based, documents at various touchpoints. This has resulted in longer queues at airports, with an increase of up to six hours at the peak of the pandemic.[24]

– Advance pre-trip digital sharing of trusted, verifiable information means that an organization is able to quickly validate shared data ahead of time and therefore create a more seamless and less confusing experience for the traveller, ultimately resulting in improved satisfaction.[25]

Resuming safe travel:

– In the aftermath of the COVID-19 pandemic, requirements are in place to ensure the travelling process is as safe as possible. The aviation industry alone lost $370 billion in 2020 due to the pandemic.[26] Recovery from the economic impact will rely on travellers wishing to travel again, and thus travel-related businesses and government departments will need to adapt to new requirements to provide a safe and secure environment.

– Enabling a touchless travel experience can help restore travellers' confidence in cross-border travel in the wake of the pandemic, as well as reduce the risk of transmission for both travellers and staff, given that physical contact is reduced.

3.2 Roles in the ecosystem – adapting to change

Governments, the private sector and international organizations already have well-established roles in the travel ecosystem. Adopting digital credentials for travel, however, requires ecosystem partners to adapt existing mandates, processes, technology and operations. Each organization needs to understand the impact of moving towards digital travel credentials, what this means to their unique role in the ecosystem and furthermore what organizational changes will be required.

FIGURE 6 **Roles in the travel ecosystem**

GOVERNMENT	PRIVATE SECTOR	INTERNATIONAL ORGANIZATION
Take a leadership role to engage other governments and private-sector organizations to drive a digital ecosystem for seamless travel	Collaborate with governments and other private-sector partners to support the ecosystem on relevant standards and technologies to enable seamless travel	Research and evaluate ongoing seamless and touchless travel credential initiatives around the globe to understand emerging and innovative technologies and standards
Collaborate with travel ecosystem partners and other governments on relevant standards and technologies to reduce the need for multiple sets of digital credentials for travellers	Provide meaningful feedback on the legal and regulatory policies and framework for seamless travel credentials	International organizations such as ICAO could consider taking initiatives such as KTDI under their wing to evaluate their existing vision alignment with the global travel industry and interest from member states
Engage with international organizations (e.g. ICAO) to establish seamless travel credential standards and technologies to drive interoperability	Assess an organization's readiness to join the ecosystem and implement seamless travel solutions	Provide direction to standards bodies (W3C etc.) to establish a consensus-driven common set of standards to drive interoperability in the global travel industry
Develop and implement relevant domestic, legal and regulatory foundations that enable the use and acceptance of seamless digital travel credentials	Adopt an open mindset on the digital travel process and relevant innovation	Engage with government and private-sector organizations to provide guidance and education on current and emerging seamless travel standards and technologies to minimize market fragmentation
Provide clear guidance on travel-related policies and regulations to enable easier adoption of travel credentials	Identify common inefficiencies across the ecosystem on which to collaborate	
Open pathways to engage with private-sector organizations to expand travel ecosystems and leverage innovations for public use	Evaluate and engage with other private-sector organizations to join the ecosystem and unlock additional value and reduce inefficiencies	
Promote the use of digital credentials for travellers	Share end-user feedback and operational data with ecosystem partners (e.g. government partners) for improvements	
	Embrace and build new technology capability (e.g. SSI) to support emerging seamless travel standards and technologies	
	Be ready for change with the right skills and training for staff and customers	

3.3 Embarking on your collaboration journey

Once the value of collaborating on travel credentials and the changes required for the ecosystem roles have been outlined, it is vital to understand where you are on your collaboration journey and how you can progress.

All organizations within the travel credential ecosystem will have unique incentives, challenges and capabilities. As organizations embark on the journey towards adopting digital credentials for travel, be this through a pilot, participating in an

industry standards forum or working on regulatory requirements, it is important to start the journey with an organizational vision that is aligned with how the world is evolving towards the introduction of digital travel credentials. Once a vision is set, organizations need to develop a thorough understanding of what digital travel credentials will mean to their organization across a number of different aspects; for example: customer experience; staff interactions; technology; operational support; business interactions with ecosystem partners; intellectual property; regulatory compliance; and the right approach for collaboration across ecosystem partners. Drawing on the KTDI journey and lessons learned so far, this playbook poses questions, considerations and best practices for organizations to support meaningful, focused collaboration towards a vision of globally accepted, trusted, verifiable digital travel credentials.

The following can be used to help policy-makers and industry leaders baseline their organization's capabilities and goals, as well as better understand how to embark on the journey to use digital credentials in travel. This section aims to support organizations to:

- Better understand how their organization's vision and mission can benefit from safe and seamless travel enabled by digital travel credentials
- Identify pain points for the traveller and the organization that can be addressed through more efficient sharing and management of trusted travel credentials
- Determine how existing processes may need to be adapted
- Consider whether the existing standards, policies and regulations sufficiently support their organization in realizing the benefits of a seamless and secure traveller experience by enabling the issuance and acceptance of trusted digital credentials for travel
- Review their role in the travel ecosystem, acknowledge the other organizations on which processes depend and consider collaboration opportunities

The World Economic Forum recently published a digital identity ecosystems guide for executives. It offers a set of tools to help organizations understand their ecosystem and the role they play within it, how to build new ecosystems or engage existing ones, as well as how to define and deliver on value.

Click for more information.

The following key questions have been compiled to enable organizations to understand their collaboration readiness for digital travel credentials, their role within the travel ecosystem, who their potential partners could be and whether there are any existing ecosystems they could leverage. After addressing these, they will be better placed to use the toolkit in Section 4 to help them build your ecosystem for digital travel credentials, enabling people to travel in a seamless and safe manner.

TABLE 1 | **Travel industry key questions**

Questions	Example answer/guidance to support
Is your organization ready to engage and collaborate with other partners in the travel industry to help enable a seamless travel concept?	Leveraging digital credentials for travel can realize multiple benefits that are aligned to my organization's vision and mission – my organization is ready to engage.
Do you have appropriate capability and resources (people, technology and processes) to support technology enabling digital credentials for travel? If not, what and who are you missing?	**People** – I have the necessary technical/business resources to interact with ecosystem partners **Technology** – I have infrastructure and existing systems that can support the adoption of digital credentials, e.g. facial recognition readers, QR code scanners, SSI expertise, etc. **Process** – I have the necessary support capability to operationalize digital credentials for travel
Is your organization familiar with digital travel credential concepts and technology?	My organization previously conducted a digital credential proof of concept/pilot for seamless traveller boarding, border crossing, etc.
How do you currently manage compliance?	My current identity-related compliance programmes are complex and costly, with multiple dependencies on third parties.
How does your organization currently manage fraud related to travellers' identity and credentials?	The risk of identity/credential-related fraud has big implications for my business – e.g. being fined for improper documentation of travellers.
What are you doing to improve the user/traveller experience?	I am currently considering large digital transformation projects to improve the traveller experience at the airport.
Do you hold vast amounts of traveller data?	I am concerned about the amount of traveller data that my organization is currently holding and the potential legal, regulatory and security exposure.
What are you doing to ensure the security and privacy of your users' sensitive data?	I invest a lot of resources to ensure that my processes dealing with traveller data adhere to industry and regulatory standards to keep consumer data safe and ensure privacy (e.g. GDPR).
Does your organization currently process/verify digital travel credentials?	**Governments** – e.g. Verify ICAO VDS to allow entry into the country **Private sector** – e.g. Verify COVID-19 vaccine certificate to provide service/goods
Is your organization ready to accept travel credentials if they are issued by other countries? If not, what needs to be in place to do so?	**Governments** – e.g. I can verify digital credentials issued only by public-sector organizations **Private sector** – e.g. I can verify digital credentials issued only in my country
Are you familiar with emerging digital credential standards for travel and their impact on your organization?	My organization has limited awareness of emerging digital credential standards for travel and their impact on my business and operations. However, we are keen to learn more about them and discuss details and considerations.
What are your current pain points/frustrations from users that could benefit from digital travel credentials?	**Governments** – Improve border-control operations and security **Private sector** – Enhance traveller confidence and recovery of industry data compliance **International organizations** – Research common trust framework and standards to drive global interoperability for digital credential solutions
What is your organization's risk appetite and criteria when selecting partners for collaboration (e.g. leisure, international business, education, etc.)?	I would like to pilot digital credentials domestically first before engaging other governments or international industry players. This would allow me to better understand the benefits of digital credentials in an ecosystem that complies with the same domestic regulations.
Have you considered a pilot use case for digital credentials? If so, who are the ecosystem partners with whom you considered collaborating?	As a government entity, we considered working with private-sector organizations to pilot digital credentials for a touchless airport experience – starting with security and border control and ending with boarding.
Is there an existing ecosystem that leverages digital travel credentials that you considered joining?	My organization is aware of existing digital travel credential ecosystems. We have considered joining a regional effort where government-issued digital credentials are accepted for international travel among a group of countries.

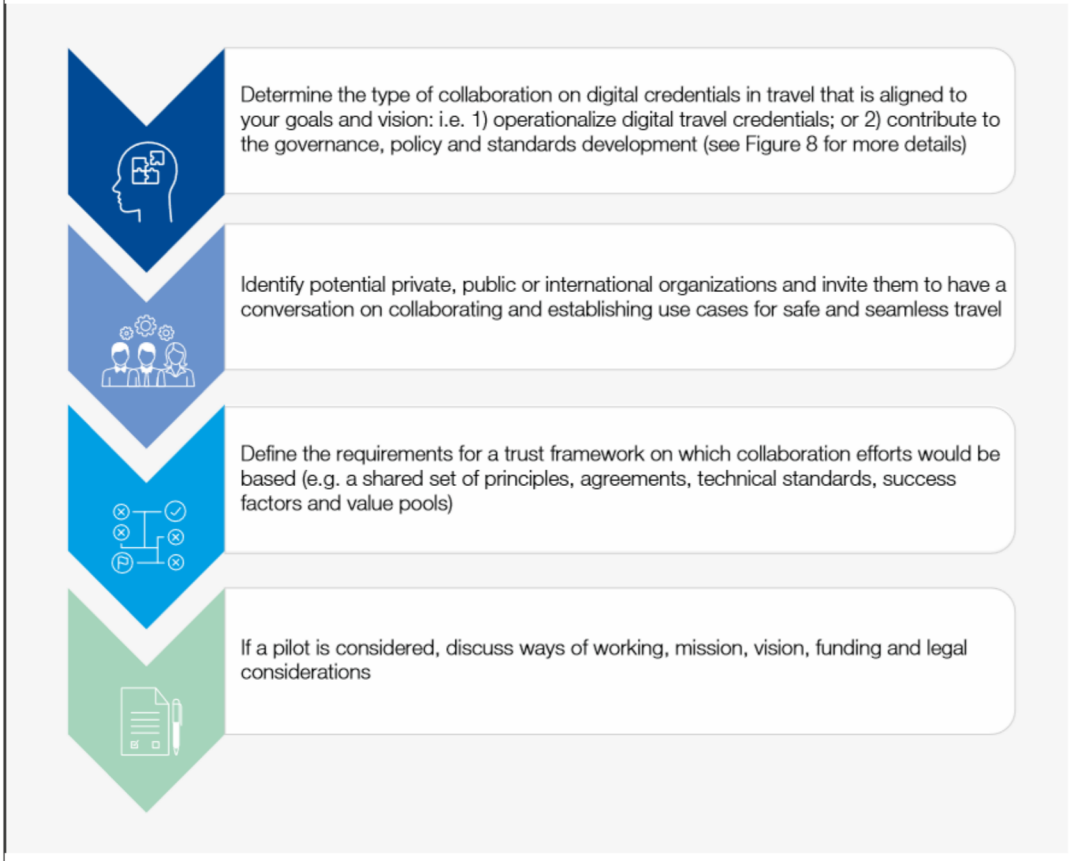
3.4 Opportunities for collaboration to drive the adoption of digital travel credentials

While fully established cross-border, public-private ecosystems for digital travel credentials do not yet exist, countries around the world are collaborating and beginning to look at ways in which these systems can be developed. Spain and Germany, for instance, recently signed a cooperation agreement to exchange methodologies in digital identity at a technical, regulatory and operational level and set up a cross-border pilot for a European ecosystem of digital identities. The pilot aims to contribute to the development of an EU-wide digital identity ecosystem that is targeting 80% of EU citizens using digital ID by 2030 – for which travel is likely to be a key use case.[27,28]

Without collaboration, travellers will probably have to use a whole array of different apps, making their end-to-end travel journey frustrating and confusing and, in turn, lead to a lack of adoption and thus a waste of resources for organizations. Travellers in the US already use seven or eight apps throughout their journey and want a more consolidated experience.[29] Collaboration between organizations will enable trusted verifiable data to be shared and verified in advance, so organizations can benefit from efficiency gains in relation to time, money and resources. With the influx of digital travel credential initiatives that are emerging due to COVID-19, collaboration is critical among interested parties, to provide a better travel experience and ultimately drive adoption success.

When considering opportunities for collaboration (and drawing on the responses from Table 1), governments, the private sector and international organizations can:

FIGURE 7 **Opportunities for collaboration**



Lessons learned from KTDI, outlined in this playbook, can contribute to the foundational blueprint for collaborations and efforts, both new and already under way.

FIGURE 8 | **Two types of collaboration that enable the development of digital travel credentials**[30]

COLLABORATING TO OPERATIONALIZE THE CONCEPT OF DIGITAL TRAVEL CREDENTIALS

Organizations can collaborate to **operationalize** digital travel credentials, **piloting new solutions** for safe and seamless travel

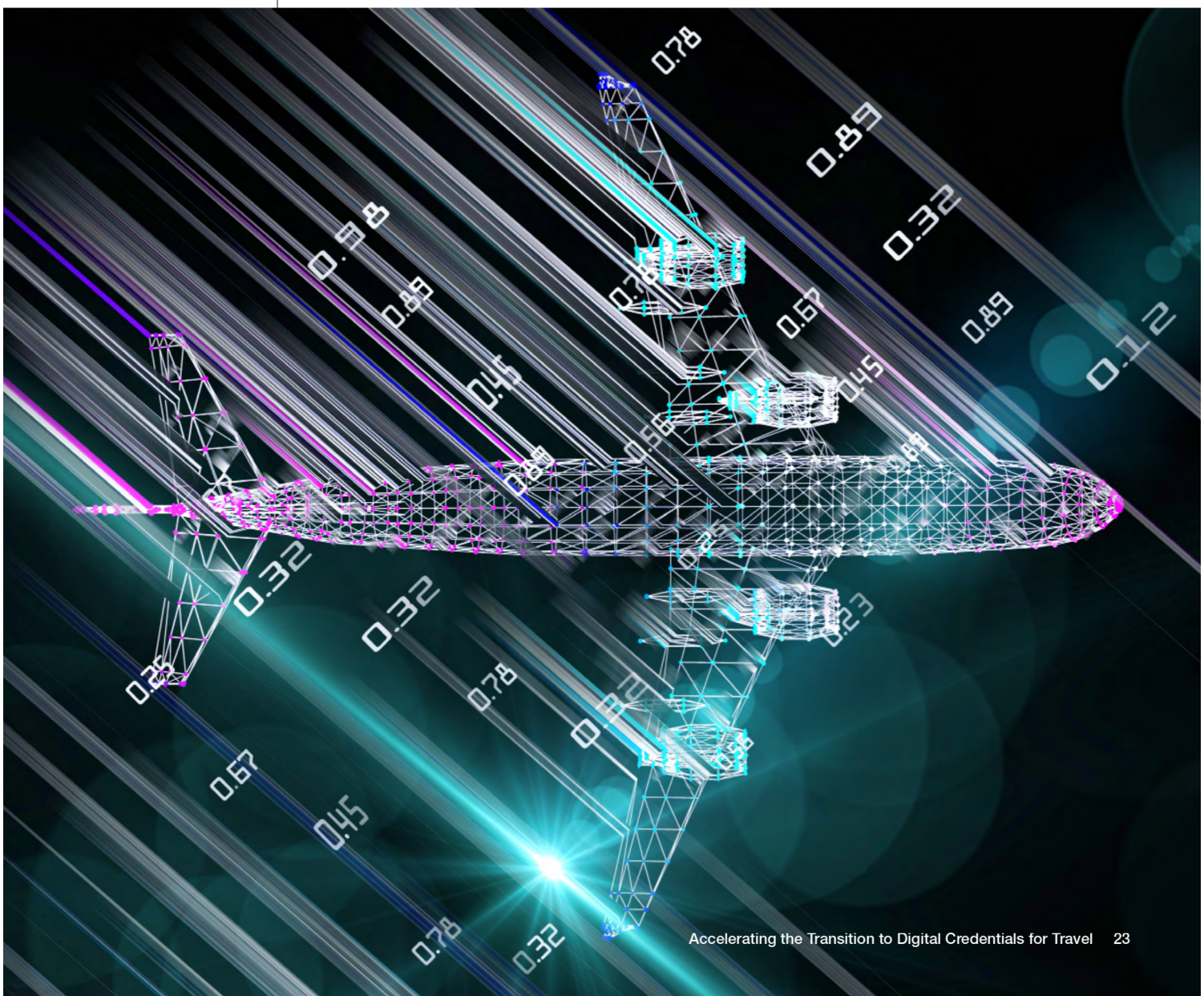
KTDI consortium partners learned many lessons across the technical, regulatory and operational functions that can be carried forward to other travel-related collaborations and initiatives. Consider the principles and considerations that provided the basis for the collaboration on KTDI to facilitate new efforts

COLLABORATING AT THE GOVERNANCE, POLICY FRAMEWORK AND TECHNOLOGY STANDARDS LEVEL

Organizations can collaborate to contribute to the **strategic direction** of digital travel credentials in the travel industry or provide technical thought leadership to help **advance technical and data standards**

Similar efforts may also find KTDI principles, lessons learned and open specifications helpful in developing the future of digital travel credential standards and governance to support seamless travel

Regardless of where an organization currently is in its digital identity journey and which type of collaboration is best for it, KTDI best practices and lessons learned can help guide the process of building a sustainable travel ecosystem that benefits from the adoption of digital travel credentials.

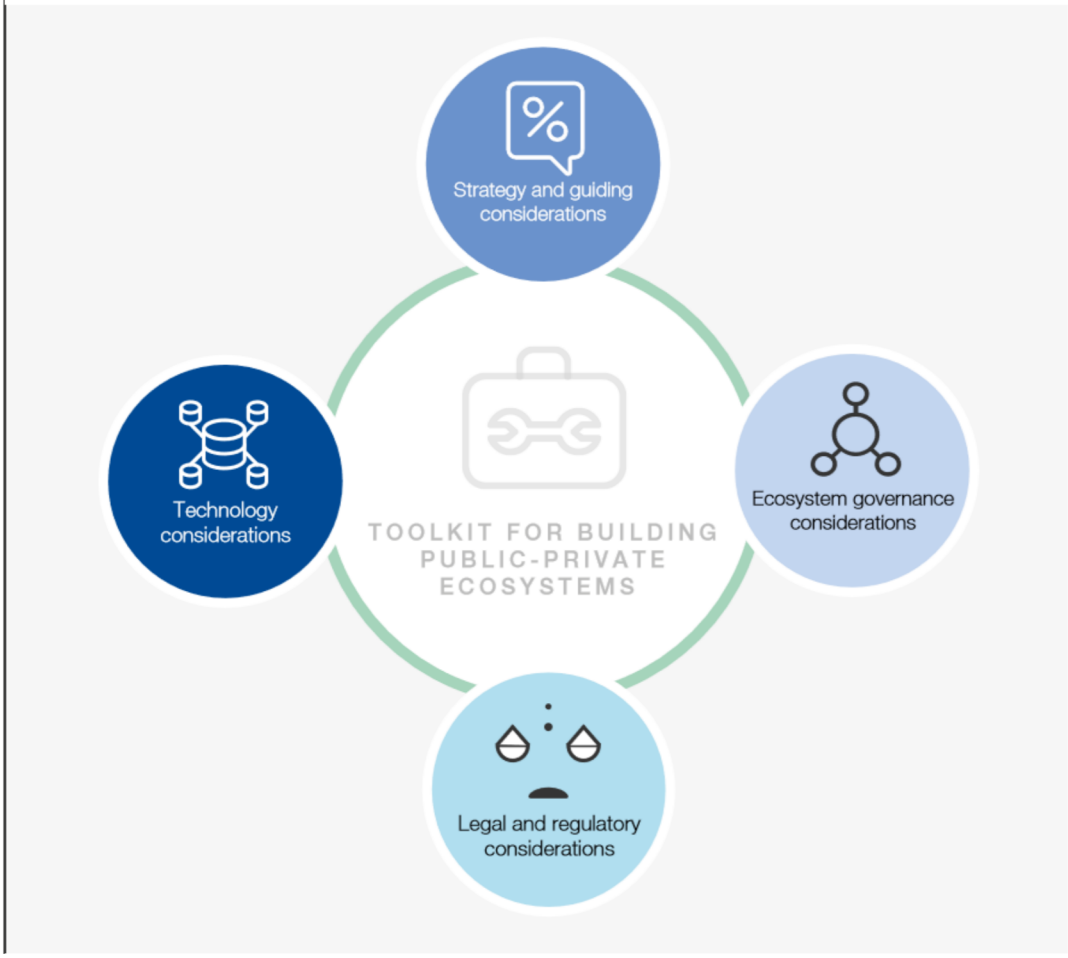


4 **Toolkit for building public-private ecosystems:** lessons learned from KTDI and considerations for deployment

The KTDI cross-border initiative between Canada and the Netherlands contributes important considerations and best practices for policy-makers and industry leaders that may be taken into account for other similar multilateral arrangements. The considerations and best practices outlined in this section are based on KTDI's experience and lessons learned throughout the different stages and areas of the pilot, including the initial conceptualization, governance set-up, legal and regulatory activities, solution design and delivery. They could serve as a blueprint for collaboration efforts that look to adopt trusted, interoperable, extensible and secure digital travel credentials to reopen borders while enabling a seamless and touchless digital experience for travellers and greater efficiencies across organizations in the ecosystem.

The following toolkit has been created to group and consolidate the key considerations learned from KTDI on building collaborative public-private ecosystems. While the KTDI pilot focuses on the travel use case (arguably one of the most difficult and complex to implement), the best practices and lessons learned are applicable to many use cases and can be used by other organizations in their transition towards building a digital identity ecosystem.

FIGURE 9 **Lessons learned and best practices**



4.1 Ecosystem building: strategy and guiding considerations

Getting the ecosystem right at its inception is essential for success. Use the following best practices and lessons learned from KTDI to assist in building a strategy and mission with the correct partners:

1. **Establish a common vision and mission:** this is vital to keep partners united in order to overcome any setbacks and work effectively together throughout the collaboration. As a result of COVID-19, the vision of the emerging

collaborative efforts could include getting people back to travelling while helping the economy, supporting a more touchless and efficient way for border and airline staff to process travellers and protecting people's privacy.

– Obtaining internal support for this vision and mission is crucial, with executive buy-in and sponsorship to secure its future viability.

– Ensure alignment with organizations in the ecosystem so that it is clear what the parties want to achieve and that there is commitment towards working in the same direction.

FIGURE 10 **Lessons learned and best practices**

In KTDI, all partners started with a common mission to promote safe and secure movement of people across borders. To do this, a cohesive vision for the future of security in travel must include user-centricity, digitization and trustful cooperation.

You can read more about this in *The Known Traveller: Unlocking the Potential of Digital Identity for Secure and Seamless Travel* report here.

2. **Evolve the use case with the traveller at the centre:** digital credentials should serve the traveller first as a core focus.

– Public- and private-sector collaboration is crucial in establishing digital travel credential ecosystems that can serve travellers throughout the travel continuum, such that they experience a consistent level of ease and seamlessness from the moment they book a flight, through check-in, airport security and border control upon arrival.

– Each organization will have its own objective for the use case, but ensuring the user remains at the centre will help focus the vision and drive trusted interactions between ecosystem partners to produce an improved travel experience and efficiency gains.

3. **Understand the legal and regulatory landscape:**

– Determine whether any legal or regulatory changes are required for digital travel credential issuance and legal acceptance, as would be similar to the passport today.

– Consider how differing regulations in collaborating countries can also increase the number of requirements to meet jurisdiction compliance for cross-border travel.

4. **Consider the cultural choices and priorities of other governments (and different departments of the same government):**

– Acknowledge that governments will have different mandates and priorities, and that there may be varying appetites for introducing changes.

– For instance, digital credentials for travel might require mandates from many different government departments; sometimes this might involve departments that are not used to working together, e.g. as a result of COVID-19, ministries of health and borders need to collaborate closer than before to align on travel requirements.

– Understand all stakeholders' dependencies and ensure central sponsorship and ownership of the initiative as well as continuous stakeholder engagement to prevent any stalling and to foster ongoing collaboration.

5. **Enable collaboration on digital travel credentials across multiple levels and dimensions:**

– When convening partners, recognize the complexity and interdependencies in the travel ecosystem. Consider domestic (e.g. national aviation regulations, airport operations), international (e.g. IATA guidance, ICAO standards), cross-sector domestic (e.g. data privacy laws) and cross-sector international (e.g. WHO guidance) factors and the diversity of travellers, as well as the relevant technologies and operational processes.

– Identify the private-sector partners, government departments and stakeholders (e.g. international organizations, interest and privacy groups, etc.) that need to be involved to achieve global adoption.

6. **Continuously refine the ecosystem model:**

– Implement continuous refinement to incorporate any legal, technological, standards, social, economic and cultural changes that affect the travel industry so that the ecosystem can extend beyond the original use case and partner organizations.

– Fully established models for digital credential ecosystems do not yet exist. Understand what can be adopted from successful public-private governance ecosystems and where gaps exist, e.g. ICAO's governance model is fully established and can provide helpful methodologies, but it does not extend the framework beyond governments to enable support for the whole travel continuum for credential verification.

4.2 Ecosystem governance considerations

After aligning upon a strategy and mission with ecosystem partners, the next step is to build the appropriate governance to ensure the right choices are made, with agreement by all, across business, operational and policy aspects. These best practices from KTDI may be helpful in setting up the correct governance for the ecosystem:

1. ESTABLISH GUIDING PRINCIPLES:

guiding principles encompass the ecosystem's values and beliefs and provide guardrails that help partners align on how to achieve their vision. The KTDI pilot partners, for instance, agreed on the following guiding principles as the foundation for their collaboration, with the aim of developing an interoperable and scalable solution for trusted digital credentials:

- **Adhere to international standards** – verification of traveller identity will adhere to internationally recognized standards; it will not circumvent existing legislative and regulatory requirements for identity verification or replace current standard operating procedures or regulatory requirements.
- **Agree on a technological and vendor agnostic approach** – participants will adhere to an agnostic approach to technology development, deployment and relevant vendor procurement actions, so as not to preclude pilot participants from integrating their pre-existing activities and infrastructure.
- **Consider technology scalability** – technological innovations that enable further scaling up of the use of technology to facilitate air travel will be employed.
- **Design for interoperability** – with a view to achieving a scalable solution with global reach, the KTDI project must interoperate with partner legacy systems.[31]

2. ESTABLISH ROBUST BUSINESS AND OPERATIONAL GOVERNANCE STRUCTURES:

governance structures are the most important factors if a member of a digital trust ecosystem is to successfully build trust, coordinate mutual objectives and maintain operational aspects.

- **Ensure participating stakeholders have appropriate mandates** – ensuring that stakeholders across different government departments have a clear and consistent mandate from government leadership that considers each agency's goals and agenda is critical throughout all stages of the programme. Understanding the structural hierarchy and jurisdictional uniqueness (e.g. federal agency vs. local/provincial agency) is essential when giving a mandate to individual government departments.
- **Empower leadership across governments** – there should be a lead entity in each partner government to identify the relevant stakeholders across different departments and facilitate their engagement in government governance (i.e. governance across different government departments), national governance (i.e. governance across the country and private-sector partners in-country) and binational governance (e.g. governance provided by the KTDI steering and management entities).
- **Align stakeholders at an operational level** – alignment and a shared vision and level of commitment at the operational level are vital to maintaining momentum. Stakeholders must clearly understand their roles and commit resources accordingly. Establish ways of working, communication channels and protocols, as well as collaboration tools to help maintain such alignment.

3. ESTABLISH PROCESSES AND WAYS OF WORKING:

- **Understand that fundamental changes are inevitable** – due to the nature of dealing with a new type of governance to share data across organizations and governments, a degree of flexibility and understanding among partners is required to allow for process changes. Even with the most thorough due diligence in place up front, unforeseen challenges are unavoidable, meaning that organizations need to be prepared to accept and adapt. New policies, regulations and procedures will have to be defined as this way of working matures to enable effective and secure sharing and verification of data in the new manner.
- **When changes come, recentre on the common vision and mission** – when adapting to changes (e.g. new ways of issuing and verifying an identity), the common goal needs to be kept at the forefront. In a non-binding consortium setting, it is not only important to have standard processes, such as change management and conflict resolution, but also to ensure that these processes consider the vision and mission of the ecosystem.

BOX 3 | **Business governance and operational governance – what does it mean?**

Business governance provides the foundation for mutual trust between parties with a shared vision for unlocking the value of an ecosystem. Business governance is provided by a dedicated "ecosystem business entity". This is the case with the ICAO, for instance, an entity funded by 193 national governments to govern the overall mission of the civil aviation ecosystem.[32] Business governance may initially be provided by a collection of staff from individual ecosystem members (e.g. a steering committee and a project management committee were established for the KTDI pilot). However, as the ecosystem matures, this should transition into a full-time function that operates as a stand-alone entity or be delegated to a third-party service provider with a relevant reporting structure in place.

Operational governance provides network participants with the "rules of the road" that govern the technological and operational aspects underpinning the ecosystem. A dedicated function is also required to manage the technology within the ecosystem and maintain its operation and reporting. Again, this can be created by the existing membership operating as a stand-alone entity (such as the technology and architecture working group established for the KTDI pilot) or delegated to a third-party service provider.

4.3 Legal and regulatory considerations

After establishing a digital trust ecosystem, members of the ecosystem must agree on business and social policies and follow the legal requirements and regulations to achieve their trust objectives. The following best practices from KTDI may assist organizations in considering how to achieve compliance with legal and privacy requirements.

1. **Legal involvement**

- **Identify key legal personnel and understand legal and regulatory considerations from the outset** – the appropriate legal subject matter experts (e.g. regulatory, intellectual property, contracting and data privacy) need to be involved from day one in order to both highlight legal considerations to be addressed and ensure legal and regulatory buy-in for the initiative. Legal representatives from each participant should align on legal principles and be part of the business and operational planning and governance as opposed to working in isolation. This is essential to avoid roadblocks and apply changes or exemptions, or provide the required regulatory flexibility to make a pilot work.

- **Start with a baseline assessment of the legal framework** – an initial understanding of the existing domestic and international legislative and regulatory frameworks as well as ways of working by all parties, and the obligations therein, is essential to identify and work through potential roadblocks in advance.

  - A sound understanding of the landscape in all disciplines early in the business development stage is key to ensuring that ancillary elements such as privacy regulations and ethical decision-making frameworks are not overlooked. In addition, this will identify any gaps where the legal and regulatory framework needs to be considered and updated to support self-sovereign identity.

  - Collaborate and, if possible, update legal regulatory language to support self-sovereign identity and the use cases considered.

- **Continuously monitor legislative and regulatory frameworks** – pilot projects such as KTDI take time and are transformative in nature. Partners need the ability to continuously monitor the legislative and regulative frameworks that could potentially affect the project.

2. **Operational agreements**

- **Create, negotiate and execute the necessary legal agreements** – the consortium should have binding agreements (e.g. multiparty NDAs, IP agreements, evaluation licences) that outline the responsibilities, commitments and milestones for each type of partner. This binding documentation is essential to clarify the roles of the parties, their benefits and obligations and overall accountability.

- **Address potentially sensitive legal topics early on** – for instance, IP ownership and licensing considerations should be addressed at the very beginning of consortium members' discussions. It is important for each consortium member to communicate how use of their pre-existing IP is permitted by the other parties and the consortium as a whole, as well as how they can and cannot use other parties' pre-existing IP or new IP created by the consortium of participants, within their own organization. Consortium members need to determine how new IP will be owned and licensed and whether any of it will be distributed outside the consortium (e.g. via open-source licensing or other licensing vehicle).

3. **Data privacy and compliance**

- **Conduct data privacy assessments and understand the resources and timeline required** – all partners, including governments and public-sector organizations, need to complete their data privacy assessments because the understanding of respective roles and proposed use of data must be aligned. This will help partners ensure that they meet legislative requirements and identify the impact that the programme will have on individuals' data privacy.
  - In Canada, for instance, two federal privacy laws are enforced by the Office of the Privacy Commissioner of Canada: the Privacy Act covers **how the federal government handles personal information** and the Personal Information Protection and Electronic Documents Act (PIPEDA) covers **how businesses handle personal information**. For KTDI, the Government of Canada initiated a comprehensive assessment of its process to ensure full compliance with the Privacy Act. Industry partners were required to comply with separate legislated criteria, as outlined in PIPEDA. Industry partners also had to comply with additional privacy regulations depending on where their business was conducted, e.g. GDPR.
- **Design to comply with relevant data privacy regulations:**
  - It is recommended that other similar efforts build an intuitive and transparent consent management mechanism that clearly explains to the user why data is needed, how it will be used and how consent can be withdrawn. This will not only increase user trust but also help achieve compliance with any relevant data protection regulations.
  - If there are multiple parties across different geographies (cross-border), partners should aim to comply with the most stringent data privacy regulation available. In the case of KTDI, GDPR compliance was a key requirement.

4.4 Technology considerations

As technology capabilities, standards and specifications continue to evolve, it is critical for participants to monitor developments as well as new technology approaches and innovations that could be employed. The following best practices from KTDI may be helpful in considering technology solution implementations.

- **Establish common IT principles across partners:**

  A central governance structure (e.g. an architecture and technology working group was established for the KTDI pilot) should define a common set of principles and standards before any development begins. This will help to future-proof the solution, drive interoperability and ensure that it will be capable of scaling beyond the original use case.

- **Incorporate digital inclusion:**

  Consider accessibility and inclusion by design, taking into account geographic, demographic and socioeconomic factors, so that the needs of all people are reflected and the effects of the digital divide are minimized. It is important to consider fall-back processes and to gradually introduce new technology that meets the needs of all traveller groups.

- **Choose open-source and adaptable technology and standards:**

  Consider technologies and specifications that are built on open standards for easier adaptability and upgrades as the technology evolves.

  For instance, built on an open-source capability, KTDI allows for easy adaptability and upgrades, as the technology is still being developed at a fast pace.

  Using open-source software can also help avoid vendor lock-in, allowing more flexibility to enable the solution to evolve.

- **Consider each partner's technology maturity, skills and capabilities:**

  Partners are likely to have varying technical skills, different technical capabilities and disparate levels of maturity. Define the technology principles and support models that works for all collaborating parties.

  It is critical that each partner has the appropriate technical skills and expertise to support ecosystem technologies, whether in-house or outsourced.

For instance, while larger organizations such as large government departments or airports might prefer to deploy and host solution components themselves, smaller organizations such as smaller airlines or hotel chains might prefer to integrate applications via their APIs (application programming interfaces) or use managed services options. This allows organizations to use the functions of the systems without the need to manage the complexities of the underlying technology, given that skills in a particular technology (e.g. biometrics or SSI) might be very difficult to find.

Consider conducting proof-of-concept and testing real-life scenarios in a lab setting before going live. This can help to identify and address potential gaps and risks before the solution is launched.

– **Embed security from the start:**

Robust security is critical: a vulnerable link in an ecosystem can endanger every other element within it and significantly affect trust.

When building a secure ecosystem, bear in mind that information security requirements for government systems such as borders will look different from the security requirements for an airline, for instance.

Engage security experts early to address different partners' security considerations and concerns, as well as to ensure alignment on overarching security architecture.

– **Marry user experience and technology:**

To achieve adoption, technology requirements must include user-experience requirements.

Collaborate with user experience and user interface experts; also gather end-user feedback to ensure that the technology is designed to meet traveller expectations.

For instance, an intuitive consent management mechanism that clearly explains why data is needed, where it is used and how consent can be withdrawn encourages traveller trust and reduces ambiguity.

– **Choose technology partners:**

Consider using technology partners to develop and set up core capabilities (e.g. via API, SDK, etc.) so that each organization can easily integrate with its existing systems (e.g. bookings and reservations, security control, immigration control and other systems) for quicker deployment.

Before choosing technology partners, assess their experience and expertise in implementing the chosen technology in similar settings and scale (e.g. cross-border travel between a certain number of countries and, more critically, experience in working with governments and border systems as these are unique and highly specialized).

Ensure that all technology partners have their own innovation and capabilities roadmap to anticipate the evolving technology and travel industry landscape.

For each technology partner, it is critical to consider the level of commitment required to support the ecosystem objectives. Ensure all technology partners have the capability and capacity to provide the appropriate resources and teams to deliver the ecosystem progress.

As the technology and the ecosystem mature, managed services capabilities might be required to ensure services are consistently delivered across the ecosystem, especially in supporting some of the smaller organizations.

Conclusion

In the interests of protecting public health, the demand for trusted, interoperable, secure, privacy-preserving digital credentials for travel has significantly increased. Digital credentials will become the norm in a future of touchless and seamless borders. These capabilities will support the reopening of cross-border travel and set the example for a future of trusted digital documents as various use cases emerge in travel and beyond. This is in much the same way as the passport was developed for trusted cross-border travel and is now used for many other identity-proofing transactions, from renting accommodation to checking in to a hotel.

International and national standards, frameworks and multilateral agreements were formed to enable people to travel effectively across borders. As the world becomes increasingly digital, the travel ecosystem has an opportunity to lead the way towards the development and adoption of trusted digital travel credentials that are accepted beyond a single sector and country. The development and adoption of such capabilities is built upon a strong will and commitment in governments and the private sector to collaborate on a global scale, from governance structures, legal and regulatory frameworks, standards harmonization and consumer adoption to issuing and accepting digital travel credentials. The capabilities and the demand are already here. The time for collaboration among governments is now.

This report is intended to serve as a playbook for policy-makers and industry players to inform their decision-making regarding collaboration on and the deployment of digital solutions for seamless travel at this critical time. It proposes opportunities for collaboration and considerations for embarking on the journey to use digital credentials in travel, as well as the KTDI pilot lessons learned and best practices.

The World Economic Forum and its KTDI partners invite interested stakeholders who share a similar vision to explore further public-private collaboration and transform the future of secure and seamless travel through the use of trusted, verifiable, digital travel credentials.

Glossary/abbreviations

Term	Definition
Certificate	An electronic document combining data that is associated with the user (e.g. identity name, public key, a validity period, etc.) to establish a digital identity
Decentralized digital identity/self-managed identity/ self-sovereign identity (SSI)	In a decentralized identity system, entities are free to use any shared root of trust. Globally distributed ledgers, decentralized P2P networks or other systems with similar capabilities provide the means of managing a root of trust without introducing a centralized authority or a single point of failure. In combination, DLTs and decentralized identity management systems enable any entity to create and manage their own identifiers on any number of distributed, independent roots of trust. Entities are identified by decentralized identifiers (DIDs) and may authenticate via proofs (e.g. digital signatures, privacy-preserving biometric protocols, etc.). A fuller explanation can be found here
Decentralized identifiers (DIDs)	DIDs are identifiers consisting of numbers and alphabets that are unique and mapped to a DID document located in a certain distributed ledger. They are a type of unique identifiers that enable entities to generate and control their identifiers in the digital world. A fuller explanation of the latest DID definitions and standards can be found here
Digital credential	Credential issued to individuals by organizations that have verified the individual and can attest to their identity claim. Additionally, they can also detail a qualification, competence or authority for an individual. Examples include passports, national identity cards, driver's licences, etc.
Digital divide	Distinction between those who have internet access and are able to make use of new services offered on the world wide web, and those who are excluded from these services[33]
Digital identity	A collection of individual attributes associated with a uniquely identifiable individual (e.g. name, date of birth, occupation, health status) – stored and authenticated in the digital sphere – that is trusted and used for transactions, interactions and representations online[34]
Distributed ledger technology (DLT)	Software that uses a blockchain or similar data structure shared over a network of participants who distribute and verify information about transactions
General Data Protection Regulation 2018 (GDPR)	Regulation number 2016/679 entitled Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
Harmonization	The process of minimizing redundant or conflicting standards by finding commonalities and identifying critical requirements that need to be retained to provide a common standard. For example, data harmonization involves transforming datasets to fit together in a common architecture, while semantic harmonization ensures the meaning and context of data remains uniformly understood by all interacting actors, regardless of how the data was collected originally
ICAO Digital Travel Credential (DTC)	Digital Travel Credential (DTC) is a virtual credential derived from a state-issued document such as a passport. It is an exact representation of the electronic machine-readable travel document (eMRTD) that includes the holder's facial image, biographical data and security features[35,36]
ICAO machine-readable travel documents (MRTD)	The MRTD is an official travel document issued by a state or organization, used by its holder for international travel. It contains, in a standardized format, various identification details of the holder, including a photo (or digital image) with mandatory and optional identity elements. The mandatory elements, apart from the photo, are reflected in a two- or three-line machine-readable zone (MRZ)[37]
ICAO master list	List that contains the Country Signing Certificate Authority (CSCA) public key certificates of ICAO PKD members that have been passed to ICAO through diplomatic channels and are therefore trusted by ICAO[38]
Interoperability	The capability of different information systems, devices and applications to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organizational, regional and national boundaries, to provide timely and seamless portability of information

Personally identifiable information (PII)	Information that, when used alone or with other relevant data, can identify an individual. PII may contain direct identifiers such as passport information that can identify a person uniquely or quasi-identifiers (e.g. race) that can be combined with other quasi-identifiers (e.g. date of birth) to identify an individual
Public key directory (PKD)	A central repository for exchanging the information required to authenticate credentials
Public key infrastructure (PKI)	The policies, roles, software and hardware components and their governance that facilitate the digital signing of documents and issuance/distribution/exchange of keys
Selective disclosure	A privacy-by-design cryptographic technique that allows individuals to reveal only a subset of the data described in their verifiable credential. It enables individuals to share a specific piece of their information with the receiving entity, so that only what is needed (e.g. date of birth but not the full ID) is disclosed
Trust framework	A collection of policies and technical specifications that are accepted by multi-organizational participants to satisfy a particular need. In the case of digital identity, trust frameworks provide policy and technical interoperability for the issuers of digital identity credentials, the individuals asserting their identities through the use of the credentials and the organizations relying on the identity assertions linked to the credentials
Validation	The assurance that a verifiable credential or a verifiable presentation meets the needs of a verifier and other dependent stakeholders. This specification is limited to verifying verifiable credentials and verifiable presentations, regardless of their usage
Verifiable credentials	An attribute or set of attribute(s) contained within an identity credential and attested to by a trusted entity based on information presented by the traveller that can subsequently be validated by a third party
Verifiable data registry	A system that facilitates the creation, verification, updating and/or deactivation of decentralized identifiers and DID documents. A verifiable data registry might also be used for other cryptographically verifiable data structures such as verifiable credentials
Verification	The evaluation of whether a verifiable credential or verifiable presentation is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds

Abbreviation	Full form
DCC	Digital COVID Certificate
DDCC	Digital documentation of COVID-19 certificates
DID	Decentralized identifier
DLT	Distributed ledger technology
eMRTDs	Electronic machine-readable travel documents
GDPR	General Data Protection Regulation
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
ICAO DTC	ICAO Digital Travel Credential
IP	Intellectual property
KTDI	Known Traveller Digital Identity
MRTDs	Machine-readable travel documents
PHI	Protected health information

PII	Personally identifiable information
PKD	Public key directory
PKI	Public key infrastructure
SSI	Self-sovereign identity
VC	Verifiable credentials
VDS	Visible digital seal

Contributors

World Economic Forum

Andrea Serra
Lead, Security in Travel, USA

Lauren Uppink Calderwood
Head of Aviation Travel and Tourism, USA

Accenture

Dan Bachenheimer
Global Digital Identity Innovations Technical Lead and Associate Director

Christine Leong
Global Digital Identity & Biometrics Lead and Managing Director

Kotryna Urbanaite
Technology Innovation Strategy Manager

Battsooj Uvsh
Technology Innovation Strategy Manager

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 contribution of members of the Known Traveller Digital Identity Consortium, who have provided the testing and learning environment for the concept and continue to drive innovations in safe and secure travel.

Endnotes

1. Louise Cole, *digital travel credentials*, International Civil Aviation Organization (ICAO) Traveller Identification Programme (TRIP) 15th Symposium, 25 June 2019: https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf.
2. World Economic Forum, The Known Traveller: *Unlocking the Potential of Digital Identity for Secure and Seamless Travel*, January 2018: http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.
3. International Air Transport Association (IATA) press release, "Digitalization Needed for Smooth Restart", 26 May 2021: https://www.iata.org/en/pressroom/pr/2021-05-26-02/.
4. IATA press release, "Accepting Vaccinated Passengers Should Be Best Practice to Reopen Borders", 19 May 2021: https://www.iata.org/en/pressroom/pr/2021-05-19-01/.
5. Good Health Pass Blueprint 2021, 1 August 2021: https://drive.google.com/file/d/1EEiGeFXgNh1S0joHYSt2K2YEr0odsZgC/view?usp=sharing.
6. IATA press release, "Digitalization Needed for Smooth Restart", 26 May 2021: https://www.iata.org/en/pressroom/pr/2021-05-26-02/.
7. IATA press release, "Passengers Confident in Onboard Safety, Continue to Support Mask-Wearing", 21 July 2021: https://www.iata.org/en/pressroom/pr/2021-07-21-01/.
8. Miriam Berger, "Covid-19 Passports Aim to Streamline Travel Requirements. But There's No One-Size-Fits-All Fix", *The Washington Post*, 18 February 2021: https://www.washingtonpost.com/world/2021/02/18/coronavirus-passports-pandemic-travel/.
9. Cecilia Rodriguez, "Covid-19 Passports and Travel: Free, Non-Discriminatory and 'Non-Fakeable'?", *Forbes*, 16 May 2021: https://www.forbes.com/sites/ceciliarodriguez/2021/05/16/covid-19-passports-and-travel-free-non-discriminatory-and-non-fakeable/?sh=11f202a581cb.
10. Jamie Grierson, "Fake Covid Vaccine and Test Certificate Market Is Growing, Researchers Say", *The Guardian*, 16 May 2021: https://www.theguardian.com/world/2021/may/16/fake-covid-vaccine-and-test-certificate-market-is-growing-researchers-say.
11. IATA press release, "Travelers Gaining Confidence", 9 March 2021: https://www.iata.org/en/pressroom/pr/2021-03-09-01/; IATA, "Digital Processes for Testing and Vaccines Critical for Restart": https://www.iata.org/contentassets/204c444a815b4e2b9251a6cda365d671/digital-processes-restart.pdf.
12. Axel Dolmeyer, Mike McCarthy, Simon Pfeiffer and Gundbert Scherf, "How Governments Can Deliver on the Promise of Digital ID", McKinsey, 31 August 2020: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id.
13. Daniel Boffey, "NHS Covid Pass Still Not Recognised in Some EU Countries", *The Guardian*, 24 August 2021: https://www.theguardian.com/world/2021/aug/24/nhs-covid-pass-still-not-recognised-in-some-eu-countries.
14. IATA press release, "EU and UK Digital Covid Certificates Recognized by IATA Travel Pass", 19 August 2021: https://www.iata.org/en/pressroom/2021-releases/2021-08-19-012/.
15. Louise Cole, *digital travel credentials*, International Civil Aviation Organization (ICAO) Traveller Identification Programme (TRIP) 15th Symposium, 25 June 2019: https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf.
16. World Economic Forum, Digital Identity Ecosystems: Unlocking New Value, September 2021: https://www3.weforum.org/docs/WEF_Guide_Digital_Identity_Ecosystems_2021.pdf
17. World Travel & Tourism Council, *Travel & Tourism Economic Impact 2021*: https://wttc.org/Portals/0/Documents/Reports/2021/Global%20Economic%20Impact%20and%20Trends%202021.pdf?ver=2021-07-01-114957-177.
18. Government of Canada, "Documents to Support Your Identity – New Adult Passport Applications": https://www.canada.ca/en/immigration-refugees-citizenship/services/canadian-passports/new-adult-passport/identity-documents.html.
19. FinExtra, "Canada Commences Testing of Digital ID Framework", 16 September 2020: https://www.finextra.com/pressarticle/84093/canada-commences-testing-of-digital-id-framework.
20. IATA/One ID, *Concept* Paper, January 2018: https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-concept-paper.pdf.
21. The Points Guy, "Travelers Report Major Stress While Flying – Here Are 9 Ways to Reduce the Hassle", 26 February 2020: https://thepointsguy.com/guide/air-travel-stress-report/.
22. Sky News, "Covid 19: At Least 100 Fake Coronavirus Test Certificates Are Used by UK Arrivals Every Day, It Is Revealed", 21 April 2021: https://news.sky.com/story/covid-19-at-least-100-fake-coronavirus-test-certificates-are-used-by-uk-arrivals-every-day-it-is-revealed-12282433.
23. Department of Homeland Security, "Department of Homeland Security Transportation Security Administration Budget Overview Fiscal Year 2022": https://www.dhs.gov/sites/default/files/publications/transportation_security_administration_0.pdf.

24. Ilaria Grasso Macola, “How Technology Can Cut Airport Queues”, Airport Technology, 15 July 2021: https://www.airport-technology.com/features/contactless-security-how-technology-cut-airport-queues/.
25. World Travel & Tourism Council, *Travel & Tourism Economic Impact 2021*: https://wttc.org/Portals/0/Documents/Reports/2020/Biometrics%20Importance%20and%20Benefits.pdf?ver=2021-02-25-183021-407.
26. United Nations News, “Air Travel Down 60 Per Cent, as Airline Industry Losses Top $370 Billion: ICAO”, 15 January 2021: https://news.un.org/en/story/2021/01/1082302.
27. Die Bundesregierung press release, “Germany and Spain Join Forces on the Development of a Cross-Border, Decentralised Digital Identity Ecosystem”, 29 July 2021: https://www.bundesregierung.de/breg-de/aktuelles/germany-and-spain-and-join-forces-on-the-development-of-a-cross-border-decentralised-digital-identity-ecosystem-1947302.
28. European Commission, *Europe’s Digital Decade: Digital Targets for 2030*, 9 March 2021: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.
29. Travel Agent Central, “Stats: Nearly Two-Thirds of Travelers Rely on Mobile Apps During Trip”, 19 November 2018: https://www.travelagentcentral.com/running-your-business/stats-nearly-two-thirds-travelers-rely-mobile-apps-during-trip.
30. World Economic Forum, *Known Traveller Digital Identity: Specifications Guidance*, White Paper, March 2020: http://www3.weforum.org/docs/WEF_KTDI_Specifications_Guidance_2020.pdf.
31. Ibid.
32. ICAO, “About ICAO”: https://www.icao.int/about-icao/Pages/default.aspx.
33. Eurostat, “Glossary: Digital Divide”: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Digital_divide.
34. Keith Metcalfe, “The Digital Identity: What It Is + Why It’s Valuable”, Learn Hub, 30 July 2019: https://learn.g2.com/digital-identity.
35. Idemia, *The Digital Travel Credential: Taking Seamless Travel One Step Further by Simplifying the Travel Process While Increasing Security and Privacy*: https://www.idemia.com/wp-content/uploads/2021/07/digital-travel-credential-position-paper-idemia-202107.pdf.
36. Louise Cole, *digital travel credentials*, International Civil Aviation Organization (ICAO) Traveller Identification Programme (TRIP) 15th Symposium, 25 June 2019: https://www.icao.int/Meetings/TRIP-Symposium-2019/PublishingImages/Pages/Presentations/Digital%20Travel%20Credentials.pdf.
37. ICAO, Technical Advisory Group on Machine-Readable Travel Documents (TAG/MRTD)”, ICAO Working Paper, Twenty-Second Meeting, 21–23 May 2014: https://www.icao.int/Meetings/TAG-MRTD/TagMrtd22/TAG-MRTD-22_WP24.pdf.
38. ICAO, “The ICAO Master List”, August 2021: https://www.icao.int/Security/FAL/PKD/Pages/icao-master-list.aspx.

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.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org