International Civil Aviation Organization

WORKING PAPER

A40-WP/xxxx
EX/xx
../../19
(Information paper)
English only

ASSEMBLY — 40TH SESSION

EXECUTIVE COMMITTEE

Agenda Item # 14: Facilitation

BI-NATIONAL COOPERATION ON THE WORLD ECONOMIC FORUM KNOWN TRAVELLER DIGITAL IDENTITY

(Presented by the Kingdom of the Netherlands and Canada)

EXECUTIVE SUMMARY	
This paper discusses the Government of Canada and the Kingdom of The Netherlands' involvement in the World Economic Forum's Known Traveller Digital Identity (KTDI) pilot project. The KTDI pilot consortium was formally launched in Montreal alongside the Fifteenth Symposium and Exhibition on the ICAO Traveller Identification Programme (TRIP) Symposium in June 2019. In addition to explaining the concept, the paper aims to identify a relationship between the KTDI Pilot Project and the work of the International Civil Aviation Organization (ICAO) Traveller Identification Program (TRIP). The paper concludes with next steps and a proposed approach for remaining apprised and building on synergies as they present themselves.	
Strategic Objectives:	This working paper relates to Strategic Objective – *Security and Facilitation*
Financial implications:	NIL
References:	NIL

1. INTRODUCTION

1.1 International air travel has evolved in many respects. It has become increasingly accessible and connected; air traveller volumes have grown and continue to grow exponentially; and travellers are beginning to recognize and advocate for improvements to the way they travel and are processed through airports and borders. The aviation industry and immigration and border control agencies have taken note and are struggling to manage the annual growth in air travel. The International [redacted] (IATA) expects 7.2 billion passengers to travel in 2035, a near doubling of the 3.8 billion air travellers in 2016. These growing volumes, coupled with the ongoing threats to the safety and security of air travel, present obstacles that must be managed while still balancing their impact on air traveller facilitation.

1.2 Changes to international air traffic have been accompanied by significant advancements in technology – many of which have been adopted by aviation stakeholders to: securely process passengers (e.g., ePassports and biometric matching); streamline controlled processes (i.e. mobile technology and applications); and improve the customer experience.

1.3 In light of changes to the operating conditions and new opportunities, States and international organizations have been exploring new models for passenger processing that leverage the capabilities of rapidly developing technologies. While some of these emerging models build off the existing systems and tokens in place, others propose changes to the processes/techniques that are employed to move passengers from the travel authorization application process (where needed) to international/domestic arrivals.

1.4 This paper discusses a forward-looking initiative developed by the World Economic Forum (the Forum) that is being tested by the Government of Canada and the Kingdom of the Netherlands through a multi-stakeholder pilot in collaboration with industry partners.

2. BACKGROUND

2.1 The Forum brings together political, business and civil society leaders to cooperate to shape global, regional and industry agendas to drive change and technological uptake. Under the Security in Travel project, the Forum has developed a forward-looking traveller facilitation concept that aims to harness a suite of innovative technologies, including distributed ledger, cryptography, biometrics and mobile technology. The concept would provide travellers with a tool to share information supporting improved screening and decision-making by border authorities and other stakeholders along the air travel continuum, while securely facilitating their travel.

2.2 The Forum's Known Traveller Digital Identity (KTDI) seeks to both: equip government and private sector entities with a traveller's verifiable identity data in order to improve decision-making and risk assessment related to authorizing travel and border crossing; and to empower travellers to facilitate the sharing of their data with security and border screening, or private sector authorities if they choose to do so.

2.3 In the proposed KTDI concept, travellers can voluntarily share their information (e.g. biometric, biographic and travel history) with governmental and private-sector players to build trust in their digital identity. Once achieved, opportunities for facilitated travel would be generated. (Refer to **Annex B** for an overview of the process). For example, a passenger could share specific information contained in their KTDI wallet with government departments and agencies and industry partners resulting in expedited travel procedures. This would allow these government entities to, for example, conduct an advanced risk assessment on the passenger. This advanced assessment could then result in a more efficient and seamless travel experience should the passenger be deemed low risk.

2.4 To build a “Known Traveller” status, travellers need attestations – authenticated claims as declared by a trusted entity – to be added to their KTDI wallet each time a trusted entity (e.g., Canadian or Dutch border authorities) verifies a claim. Attestations serve as the backbone of trust and the basis of reputation and, ultimately, how security decisions (immigration, border clearing, customs and pre-departure screening) can be made. The more a traveller receives attestations, the more confidence is built that the traveller could be assessed as low risk. This results in a known digital identity that facilitates more streamlined and personalised interactions with governments, airlines, and other stakeholders in the travel and tourism industry and thereby contributes to operational efficiencies across government and stakeholder business lines

2.5 In the application for an attestation (the process should follow TRIP best practices for evidence of identity), the identity of the traveller could be authenticated through biometric facial verification and protected by distributed ledger technology and cryptography **(See Annex A)**.

3. RELATIONSHIP TO THE INTERNATIONAL CIVIL AVIATION ORGANIZATION (ICAO) TRAVELLER IDENTIFICATION PROGRAM (TRIP)

3.1 The KTDI model presents a new paradigm for traveller processing. Providing relevant global authorities with access to a platform holding ever-greening digital attestations could fundamentally change the way that “Known Travellers” are managed across the travel continuum (i.e. document issuance/control, inspection systems/tools and interoperable applications).

3.2 As the designated global authority for managing international civil aviation, ICAO should monitor the progress and successes of this initiative. The work of the ICAO New Technologies Working Group (NTWG) around assessing the feasibility, challenges and benefits of developing specifications to support the issuance of globally-interoperable digital travel credentials is particularly important. Both the KTDI and ICAO’s work are being undertaken in line with internationally-agreed upon and respected identity management principles that ensure that identities bound to these credentials are genuine, linked to an identity and used in the community (i.e. Evidence of Identity).

3.3 Canada and the Netherlands are both active participants in the ICAO NTWG and have worked with other international partners to explore linkages between the Forum’s KTDI project and the work of the ICAO NTWG around Digital Travel Credentials (DTC). One notable achievement of these working group members has been to establish the ePassport as the anchor for the digital identity used in the KTDI initiative. Both the DTC and the KTDI will be derived from the physical ePassport to create a verifiable, trusted digital identity whereas the DTC (and ePassport) will utilize a centralized Certification Authority-based Public Key infrastructure to verify the authenticity of the digital identity via the Country Signing Certificate, the KTDI will utilize a blockchain-based decentralized Public Key infrastructure to verify the authenticity of the digital identity.

4. STATUS

4.1 The KTDI pilot consortium was officially launched on 26 June 2019 in Montreal in the context of the Fifteenth Symposium and Exhibition on the ICAO Traveller Identification Programme (TRIP) Symposium. The pilot partners conducted a pilot demonstration at the Montréal Trudeau International Airport which showcased enrolment, biometric boarding and arrival, and immigration.

4.2 The Governments of Canada and the Netherlands signed a binational Letter of Intent and pilot partners signed a consortium Letter of Intent reaffirming their commitment to pilot components of the KTDI concept in partnership with participating airlines and airports throughout 2019-2020.

4.3 The pilot is governed by a consortium governance charter which guides collaboration between the bi-national public and private partners and defines responsibilities for several working groups (legal, technology, performance measurement and communications) to ensure delivery of the pilot.

4.4 The goal of the pilot will be to explore new ways of leveraging the latest technological developments to enable travellers themselves to digitize and share verifiable claims of their identity data with border and aviation security screening authorities, in addition to other industry stakeholders, as early as possible in their journey. It is expected this will result not only in better facilitation for known travellers presenting low risk, but also improved border security by better enabling law enforcement and security screening authorities to focus on passengers who are less known, and who might potentially present higher risk.

5. NEXT STEPS

5.1 The KTDI platform will be integrated with consortium partners' systems and tested internally throughout 2019 with the goal of completing the first passport-less end-to-end journey in 2020. It is envisioned that the pilot project could include up to 10,000 passenger end-to-end trips facilitated by KTDI over a six-month period.

5.2 The pilot group will document and share lessons learned regarding the policies, processes, and technologies used in the pilot and how these can be adapted or improved to mature and further scale the KTDI concept.

5.3 Canadian and Dutch ICAO participants will continue to keep ICAO informed of pertinent KTDI developments and pilot outcomes, as well as continue to explore synergies as they present themselves.

— END —

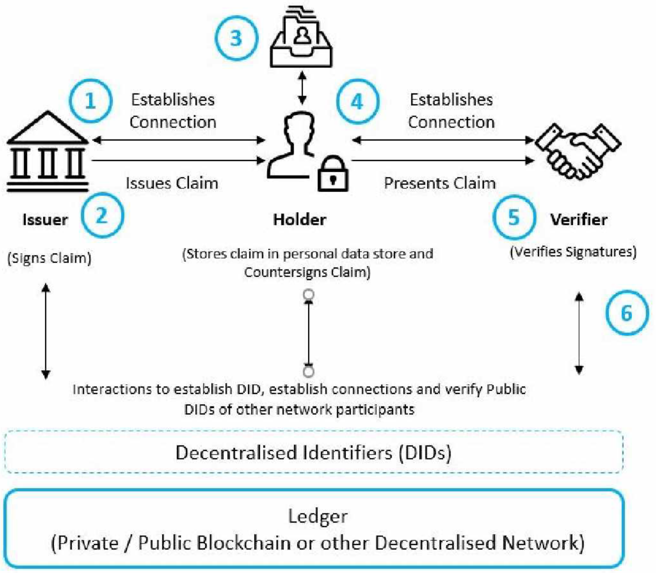
ANNEX A

High Level Overview of Pilot Solution

Verifiable Claims Model:

The KTDI pilot solution is built upon the emerging [redacted] Consortium (W3C) Verifiable Claims standards. As their name suggests, W3C is the main standards-setting body for the World Wide Web. Their work on Verifiable Claims[1] aims to address the current lack of standards to securely express, exchange, and verify claims (i.e. credentials, attestations) via the Web.

Below is a high-level overview of the model and the primary interactions between the three main actors: Issues, Holder, and Verifier. It is important to note this diagram is not exhaustive and does not represent all the interactions that could take place.


3
1
Establishes Connection
4
Establishes Connection
Issues Claim
Presents Claim
Issuer
2
Holder
5
Verifier
(Signs Claim)
(Stores claim in personal data store and Countersigns Claim)
(Verifies Signatures)
6
Interactions to establish DID, establish connections and verify Public DIDs of other network participants
Decentralised Identifiers (DIDs)
Ledger
(Private / Public Blockchain or other Decentralised Network)

1. **Issuer** and **Holder** establish a connection.
2. **Issuer** provides a claim on an identity credential to the Identity **Holder** (Issuer signs the credential with the key associated with the registered DID of the Issuer).
3. **Holder** maintains credential in their private wallet until it is required to be shared in order to cross borders or board their flight.
4. **Holder** establishes a connection with the **Verifier** (or reliant party), to enable the secure sharing of identity credentials held in the Holder's wallet.

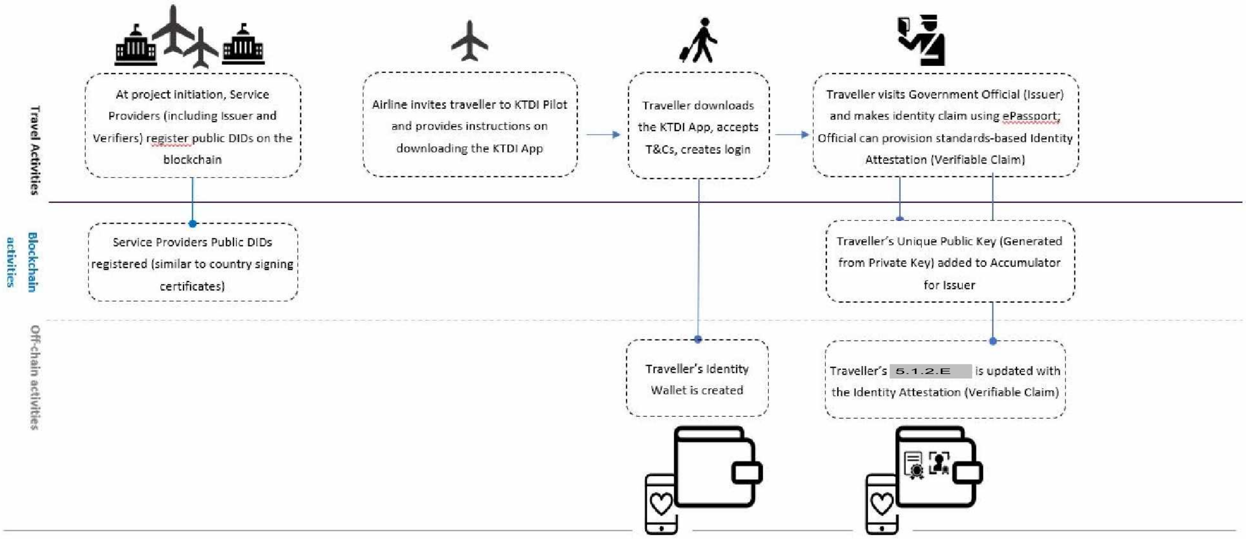
[1] Verifiable claims form credentials (or attestations) which may *"refer to a qualification, achievement, personal quality, aspect of an identity such as a name, government ID, preferred payment processor, home address, or university degree typically used to indicate suitability"*. https://w3c.github.io/webpayments-ig/VCTF/charter/charter-motivation.html

5. **Holder** presents claim on identity credential to the **Verifier** and countersigns the claim with the key associated with their private DID.
6. **Verifier** looks up registered DIDs of **Issuer** to resolve DID documents and verify the public key of the **Issuer** (Issuer DID resolution is to validate the claim was issued by the issuing authority).

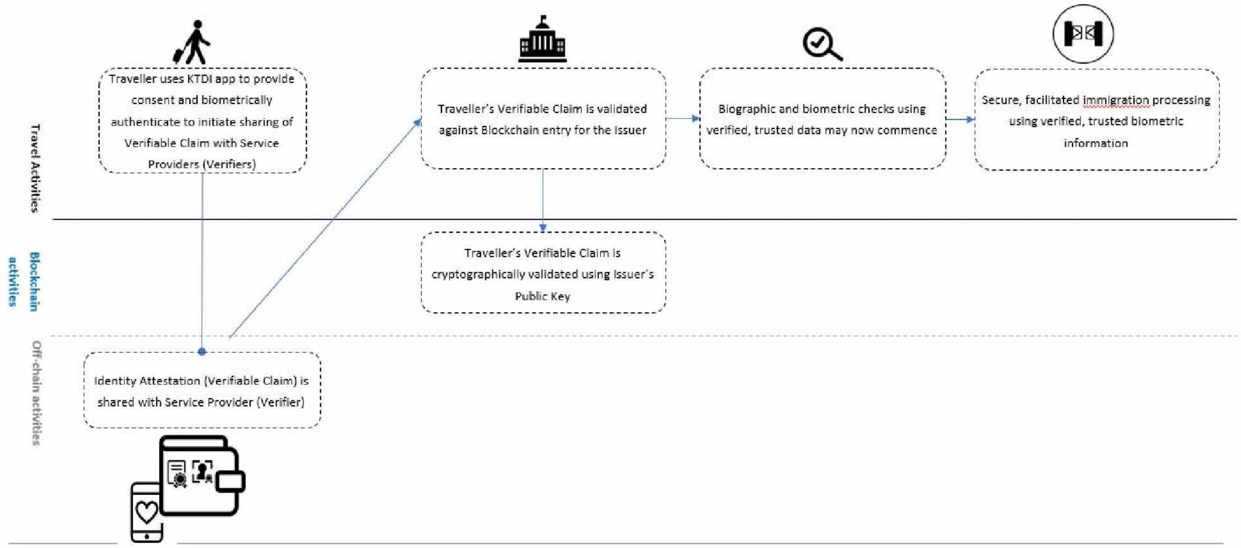
High Level Pilot Process Flow

This section describes the process flows designed for the KTDI pilot based on the Verifiable Claims Model explained above.

Enrolment (done only once):

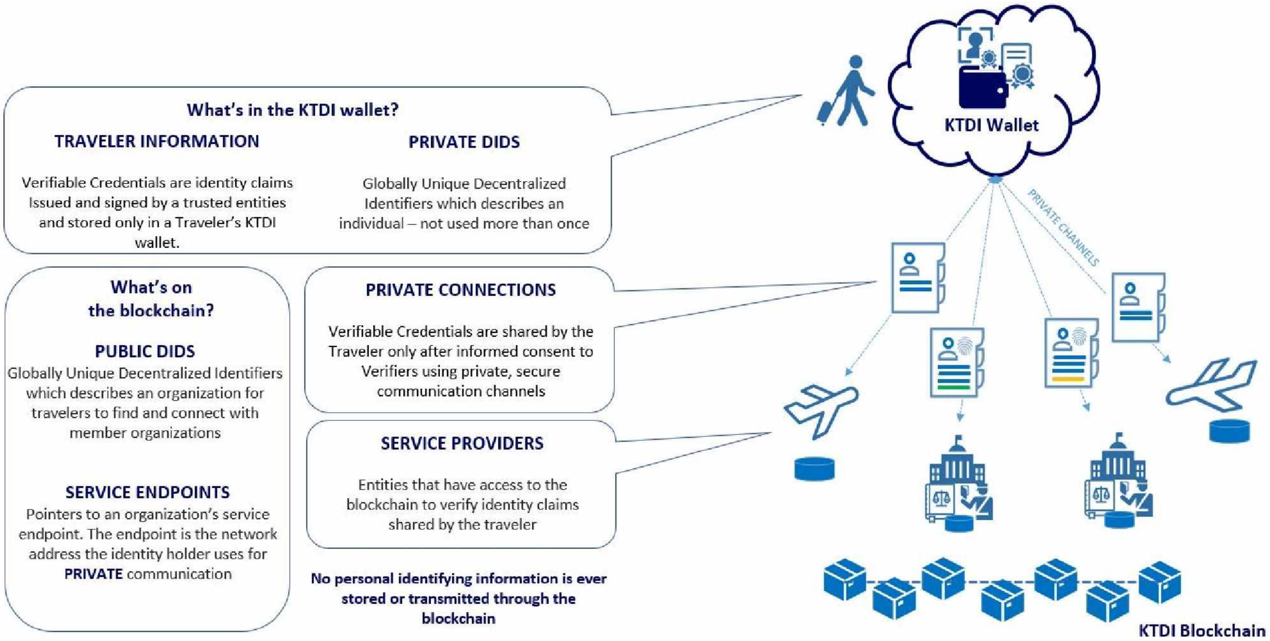

Travel Activities
Blockchain activities
Off-chain activities
At project initiation, Service Providers (including Issuer and Verifiers) register public DIDs on the blockchain
Airline invites traveller to KTDI Pilot and provides instructions on downloading the KTDI App
Traveller downloads the KTDI App, accepts T&Cs, creates login
Traveller visits Government Official (Issuer) and makes identity claim using ePassport; Official can provision standards-based Identity Attestation (Verifiable Claim)
Service Providers Public DIDs registered (similar to country signing certificates)
Traveller's Unique Public Key (Generated from Private Key) added to Accumulator for Issuer
Traveller's Identity Wallet is created
Traveller's 5.1.2.E is updated with the Identity Attestation (Verifiable Claim)

Trip (repeated per trip):


Travel Activities
Blockchain activities
Off-chain activities
Traveller uses KTDI app to provide consent and biometrically authenticate to initiate sharing of Verifiable Claim with Service Providers (Verifiers)
Traveller's Verifiable Claim is validated against Blockchain entry for the Issuer
Biographic and biometric checks using verified, trusted data may now commence
Secure, facilitated immigration processing using verified, trusted biometric information
Traveller's Verifiable Claim is cryptographically validated using Issuer's Public Key
Identity Attestation (Verifiable Claim) is shared with Service Provider (Verifier)

ANNEX B

What is stored where?



What's in the KTDI wallet?

TRAVELER INFORMATION

Verifiable Credentials are identity claims Issued and signed by a trusted entities and stored only in a Traveler's KTDI wallet.

PRIVATE DIDS

Globally Unique Decentralized Identifiers which describes an individual – not used more than once

What's on the blockchain?

PUBLIC DIDS

Globally Unique Decentralized Identifiers which describes an organization for travelers to find and connect with member organizations

SERVICE ENDPOINTS

Pointers to an organization's service endpoint. The endpoint is the network address the identity holder uses for **PRIVATE** communication

PRIVATE CONNECTIONS

Verifiable Credentials are shared by the Traveler only after informed consent to Verifiers using private, secure communication channels

SERVICE PROVIDERS

Entities that have access to the blockchain to verify identity claims shared by the traveler

No personal identifying information is ever stored or transmitted through the blockchain

ANNEX C

Glossary

Term	Definition and Reference
Attestation	An attribute or set of attribute(s) contained within an Identity Credential which have been attested to by a trusted entity based on information presented by the traveller that can subsequently be validated by a third party.
Decentralized Identifiers (DIDs)	A globally unique identifier that does not require a centralized registration authority because it is registered with distributed ledger technology or other form of decentralized network. Refer to: https://w3c-ccg.github.io/did-spec/#decentralized-identifiers-dids
Holder	An entity that is in control of a particular credential/claim. A holder is often the entity that initiates the transmission of a credential. In the case of KTDI, the Holder is the traveller.
Issuer (or Issuing Organization, Issuing Authority)	The entity that creates a credential/claim and associates it with a particular subject. In the case of KTDI, the Issuer is the passport-issuing authority or government authority.
Public Decentralized Identifiers (public DID or public identifier)	Globally Unique Decentralized Identifiers which describes an organization for travelers to find and connect with member organizations. A public identifier acts as a unique identifier for an organisation and enables travellers to find and connect with trusted organisations in order to receive and share attestations.
Private Decentralized Identifiers (private DID or private identifier)	Globally Unique Decentralized Identifiers which describes an individual. These are not used more than once.
Proof (or Cryptographic Proof)	Cryptographic verification of a claim. Claims can be selectively disclosed, meaning that just some data elements from a credential are provided in a proof. In addition, zero-knowledge proofs (ZKPs), allows for proving a piece of information without presenting the underlying data.
Service End Points	Pointers to an organization's service endpoint. The endpoint is the network address the identity holder uses for private communication.
Verifiable Claim (or Credential)	A verifiable claim is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, payment provider, home address, or university degree. Such a claim describes a quality or qualities, property or properties of an entity which establish its existence and uniqueness. An identity credential consists of a set of attributes. A credential can consist of a single attribute or multiple attributes (it depends how the credential schema is defined). Refer to: https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential
Verifier	The entity verifying a claim about a given subject.
Verification Key (or Public Key)	Public-key portion of a digital signing key pair, used in the verification of the data signed by its paired signing private-key.