Docnr 140

KNOWN TRAVELLER DIGITAL IDENTITY

PILOT SOLUTION SUMMARY

August 2019

5.1.2.E

Contents

1. Glossary
2. KTDI Pilot Context
3. Decentralised Identity Benefits
4. KTDI Pilot Process Flow
5. KTDI Detailed Pilot Journey
   i. Netherlands – Canada
   ii. Canada - Netherlands
6. Pilot Solution Platform
   i. Public Permissioned vs Private Permissioned
7. Pilot solution Summary
   i. Attestations, Credentials and Proofs
8. Pilot Interaction Summary
   i. Netherlands
   ii. Canada
9. Pilot Solution Hosting
   i. Partner Hosting Requirements
10. Connectivity

Glossary

Glossary

Term	Equivalents	Definition or reference
Decentralised Identity	Self Managed Identity	Decentralised identity systems don't depend on a single system owner or set of owners to establish and manage identities. Instead, they usually consist of a digital device, owned by an individual, and an identity data store, also managed by the individual. This data store holds attestations from trusted authorities, such as governments. The individual chooses which attestation or data attribute to share and with whom to share it. Distributed Ledger Technology (DLT) can provide a means for establishing and maintaining a root of trust without the requirement for a centralized authority and simultaneously avoiding the existence of a single point of failure.
Blockchain	Distributed Ledger Technology	Whilst often used interchangeably, blockchains are a specific taxonomy of technologies within DLT. This is reasonably explained here. A blockchain is a consensus-based ledger replicated across a peer-to-peer network which synchronises and updates itself independently without central authority.
Attribute		A characteristic of an individuals identity, e.g. the travellers gender or age, which is represented within an Identity Credential.
Credential	Claim	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). See here.
Attestation	Verifiable Claim / Verifiable Credential	Is defined as 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. Seehere.
Issuer	Issuing Organisation / Authority	Issuers are organisations that provide attestations concerning an identity owner
Public DID		Globally Unique Decentralized Identifiers which describes an organization for travelers to find and connect with member organizations. Seehere.
Private DID		Globally Unique Decentralized Identifiers which describes an individual – not used more than once. Seehere.

Glossary

Term	Equivalents	Definition or reference
DID Doc		Referenceable via DIDs, documents containing the Verification Key and Partner Agent Service Endpoint of the entity.
Verification Key	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.
Service End Points		Pointers to an organization's service endpoint. The endpoint is the network address the identity holder uses for PRIVATE communication. See here.
Credential Schema		A schema definition is a machine-readable definition of a set of attribute data types and formats that can be used for the claims on a credential. A schema definition can be used by many attestation issuers and is a way of achieving standardisation across issuers. See here.
Credential Definitions		Once a schema definition is written to the [redacted] Ledger, it can be used by a credential issuer to create an issuer-specific credential definition that is also written to the [redacted] Ledger. This data structure is an instance of the schema on which it is based, plus the attribute-specific public verification keys that are bound to the private signing keys of the individual issuer. See here.
Revocation Registry		A data structure written to the [redacted] ledger by the issuing authority. It references the credential definition and contains a cryptographic accumulator which can be checked by relying parties in order to ensure a credential has not been revoked. See here.
Proof	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), a piece of cryptography magic allow proving a piece of information without presenting the underlying data. See here.

KTDI Pilot Context

KTDI Pilot Context

The **Known Traveller Digital Identity Pilot objective** is to:

✓ Operationalize some of the concepts documented in the initial KTDI Concept Paper to determine what could work well in reality, what needs to be adjusted, and what needs to be reconsidered.

To achieve this, the **Known Traveller Digital Identity Pilot** will**:**

✓ Deliver a **pilot for Dutch and Canadian citizens**, ultimately allowing them to **travel between the two countries** using a decentralised, self managed digital identity where information is shared prior to checkpoints **obviating the need to present travel documents to prove identity.**

KTDI will be delivered through collaboration of the following partners:

- **The World Economic Forum**
- **The Governments of the Netherlands and Canada**, including their respective agencies.
- Two airlines: **KLM & Air Canada**
- Three airports
- Accenture
- Vision-box
- IDEMIA

Decentralised Identity Benefits

Identity Redefined

Why Blockchain-based Digital Identity is relevant for the user and organisations

USERS

PORTABLE
Users can take their identity data, verified skills information and credentials with them and be recognised by other organizations

USER EXPERIENCE
Reduce the amount of repeated data input that each user has to fill in for every application

ACCURATE
Data is shared via a more accurate and consistent digital manner

PRIVATE
User is in control of what data they want to share and with whom

ORGANISATIONS

EFFICIENCY
Certifications, background checks & employment history no longer need to refer to source documentation which may be a manual, paper-based, and time-consuming process

VERIFIABLE
Data can be shared confidentially and can be easily verified that it came from a trusted party

TRUST & INTEROPERABILITY
Data can be trusted where there is no need for direct trust relationships & technical integration

COMPLIANCE
Compliance is easier to manage leveraging blockchain's immutability and auditability

Identity Redefined

What Blockchain brings to KTDI

Portability

The user is in control of their data.

Identity attributes are stored in the KTDI wallet. Identifiers are used for verification of claims with consent provided by the individual making the KTDI pilot solution customer centric

Security

No single point of failure

With no Personal Identifiable Information (PII) on chain, centralised 'honeypot' data stores do not exist.

Distributed blockchain nodes provide platform resiliency, whereby the ledger provides a trusted, immutable audit trail

Trust

Know the passenger, Trust the data

Attestations associated with Decentralised Identifiers provide a permanent, tamper-evident record of veracity; empowering KTDI organisations to trust the verifiable claims presented by identity owners through cryptography.

Interoperability

Seamless interoperability with other parties

Blockchain would enable a lookup on the ledger to verify the existence of a previously issued identity credential, simplifying downstream processes and workflows; removing the need for interactions via intermediaries

Extensibility

Use beyond Known Traveler in other Ecosystems

With a decentralised root of trust based on open standards, any party with permissioned access to the KTDI ledger can look up a decentralised identifier in order to validate verifiable claims that could be used to unlock a wide range of use cases, e.g. hotel check in, car rental

KTDI Pilot Process Flow

KTDI Pilot Process Flow

The three phases of the Digital Identity Life Cycle

The KTDI provides the platform on which partners can interchange across Digital Identity Life Cycle:

Issuance – The process of a traveler being issued trusted, verifiable digital credentials. Note that the Issuer may also perform **Revocation** on credentials it wishes to nullify.

Sharing – The process of a traveler providing verifiable credentials to service providers

Validation – the process by which a service provider validates travelers credentials

High Level Pilot Process Flow

Issuance

At project initiation, Service Providers Register Public DIDs on the Blockchain

Airline invites traveller to KTDI program and provides instructions on downloading the application

Traveller downloads the KTDI App, accepts T&Cs, creates login

Traveller visits Official and makes identity claim using ePassport; Official can provision standards-based Identity Attestation

Travel Activities

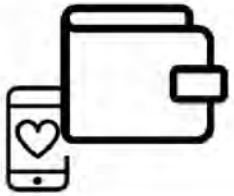
Blockchain activities

Service Providers Public DIDs (similar to country signing certificates)

Traveler's Unique Public Key (Generated from Private Key) added to Accumulator for Issuer

Off-chain activities

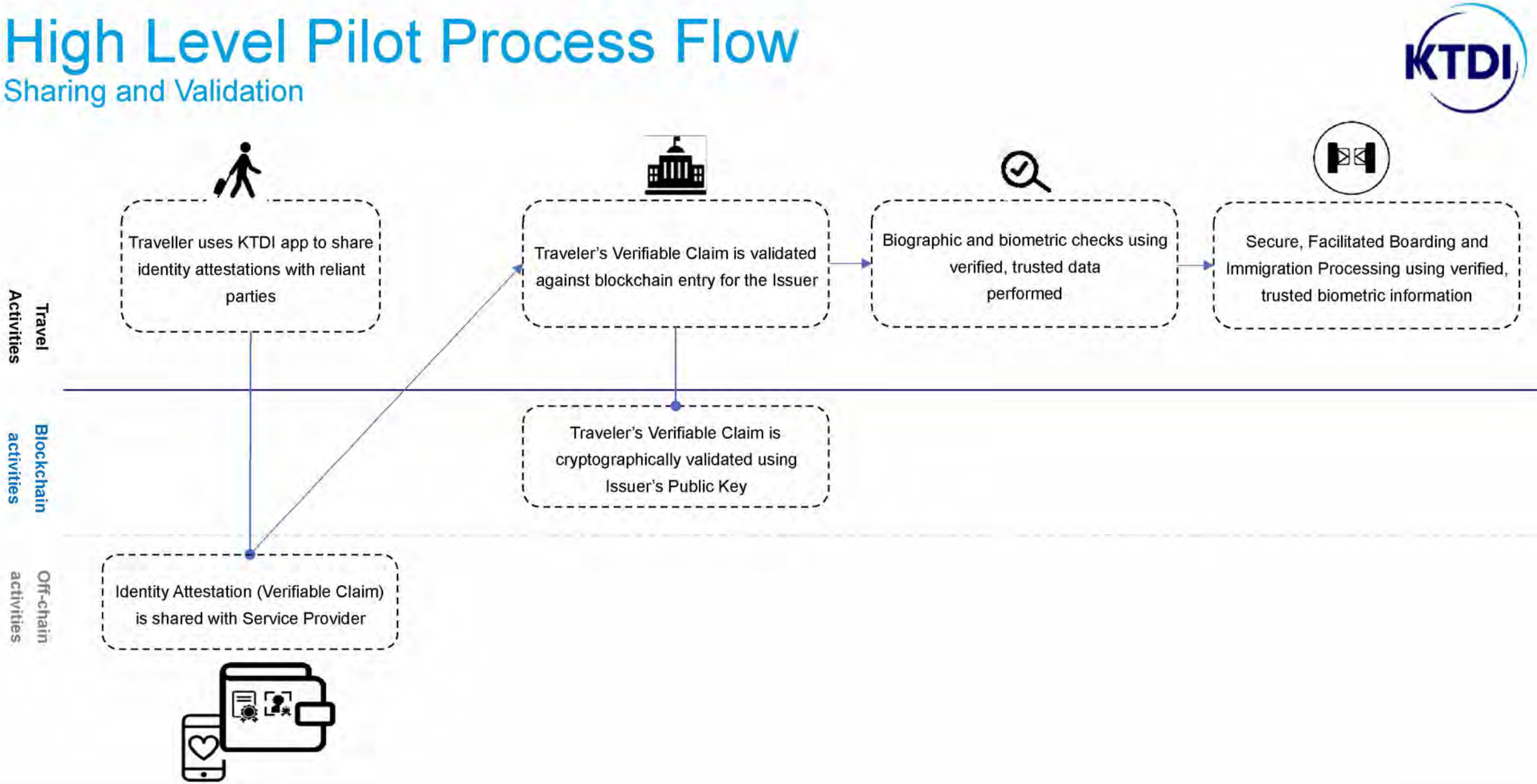
Traveler's Identity Wallet is created



Traveler's [redacted] is updated with the Identity Attestation (Verifiable Claim)

High Level Pilot Process Flow

Sharing and Validation



KTDI Detailed Pilot Journey

Detailed Pilot Journey

RTP-NL and Canadian eDeclaration not currently captured in process flow

Netherlands -> Canada

Canada -> Netherlands

Traveller | Partner Agent | Phone | eGate | Traveller Journey

Traveller Journey

Netherlands – Canada

Netherlands – Canada Journey

ONE TIME

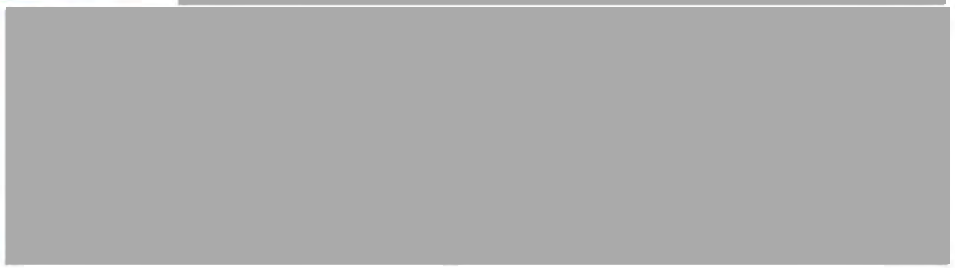
Create Digital ID

1. Enrolment

Netherlands – Canada Journey

EACH TRIP

2. Trip Preparation



Check In

Security

Netherlands – Canada Journey

EACH TRIP

2. Trip Preparation

Exit Immigration

Boarding

Netherlands – Canada Journey

EACH TRIP

2. Trip Preparation

Entry Immigration

Netherlands – Canada Journey

3. Security

EACH TRIP

4. Exit Immigration

EACH TRIP

Netherlands – Canada Journey

5. Boarding

EACH TRIP

6. Entry Immigration

EACH TRIP

Traveller Journey

Canada – Netherlands

Canada – Netherlands Journey

ONE TIME

Create Digital ID

1. Enrolment

Canada – Netherlands Journey

Canada – Netherlands Journey

EACH TRIP

2. Trip Preparation

Boarding

Entry Immigration

Canada – Netherlands Journey

3. Security

EACH TRIP

4. Boarding

EACH TRIP

Canada – Netherlands Journey

5. Entry Immigration

EACH TRIP

Pilot Solution Platform

Pilot Solution Platform

Multiple platforms were considered as the foundation of the KTDI Solution

Hyperledger 5.1.2.E selected for KTDI

KTDI

HYPERLEDGER INDY

corda

uport

sovrin

HYPERLEDGER FABRIC

- Identity focused
- Standards based
- Open Source
- Standalone
- Network type
- Blockchain Development Effort
- Scalability
- Security

Pilot Solution Platform

Hyperledger [redacted]

Whilst Fabric has more production implementations it is not sufficiently developed and tailored for identity use cases and would require significant development and architecture effort to achieve the same functionality.

This effort is likely to be measured in years rather than months due to the feature richness of [redacted] Furthermore, this effort would likely be throw-away since industry is moving forwards with [redacted] implementations.

With regards to security concerns, this is largely down to individual implementations as both platforms offer limited security out of the box. For example, Fabric offers a certificate authority out of the box but this needs exchanging for the organization or consortium certificate authority. [redacted] APIs to expose either platform functionality to consuming services would need to be secured using standards such as OAuth.

Based upon these and the recent progression from 'Incubation' status, **Hyperledger [redacted] was selected as the blockchain platform for the KTDI solution.**

HYPERLEDGER INDY

Pilot Solution Platform

Hyperledger

- Every participant (entity) in KDTI is described by entity records (public data), associated with a **Decentralized Identifier (DID)**
- Each **DID** is associated with a verification key for confidentiality or authentication reasons
- To maintain privacy and prevent correlating the entity's exchanges, each Traveler will have one **DID** per Service Provider and therefore multiple traveller / private DIDs will exist

DIDs

Public DID: Organizations – needed first and foremost by issuers of credentials; stored **on-ledger**

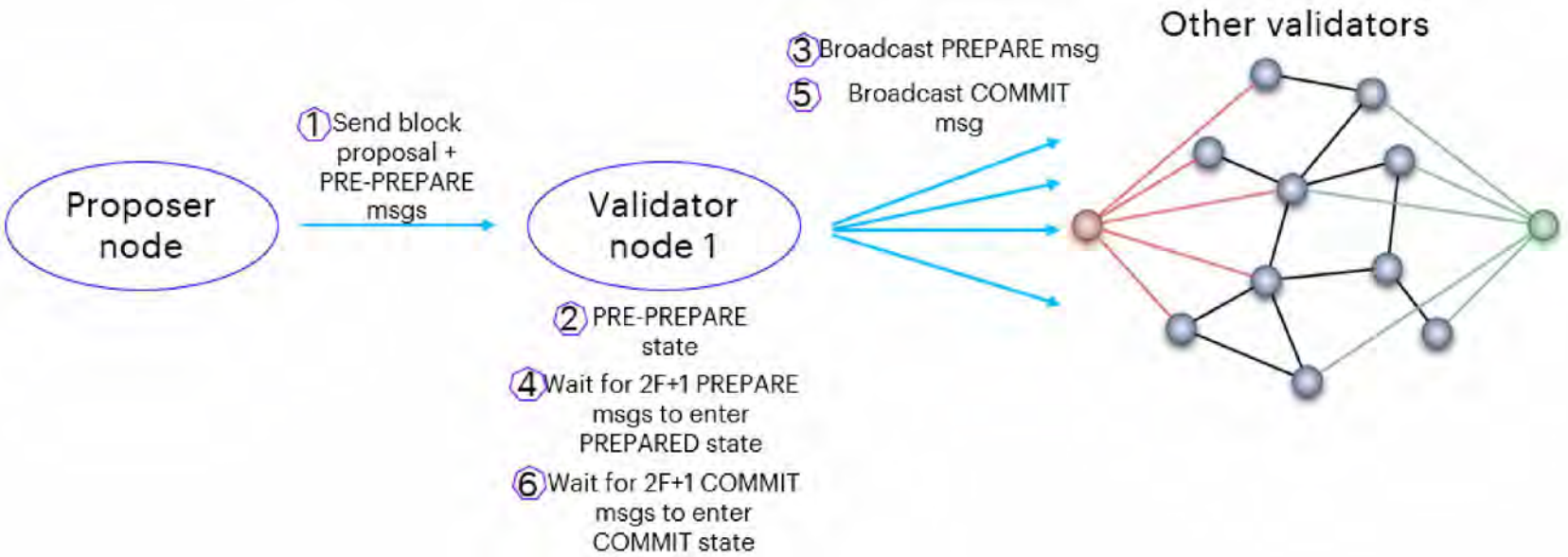
Traveller / Private DID: Pairwise pseudonymous DID shared and stored privately **off-ledger** between the agents for two identity holders

- Associated with their DID, the traveller collects verifiable claims on credentials that consist of identity attributes (this is explained in more detail on the following slides)

Pilot Solution Platform

Hyperledger [redacted]

- KDTI uses the **Plenum Consensus Protocol**: an enhancement of the RBFT (Redundant Byzantine Fault Tolerant) protocol
- The RBFT protocol is a succession of rounds starting with a proposed block and ending with a block commitment with 3 phases in each: **Pre-prepare**, **Prepare**, **Commit**
  - Each node maintains state for ledgers in a **Merkle** [redacted] = a secure storage for cryptographic materials (DIDs, keys ..) held locally
- Fault tolerance: at most F faulty nodes: N = 3F + 1; w*here N is the number of validator nodes*



Public Permissioned vs Private Permissioned

Pilot Solution Platform

Pilot Solution Platform

Pilot Solution Summary

Pilot Solution Summary

Solution Principles

TRAVELER INFORMATION

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

PRIVATE DIDS

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

WHAT'S ON THE CHAIN

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

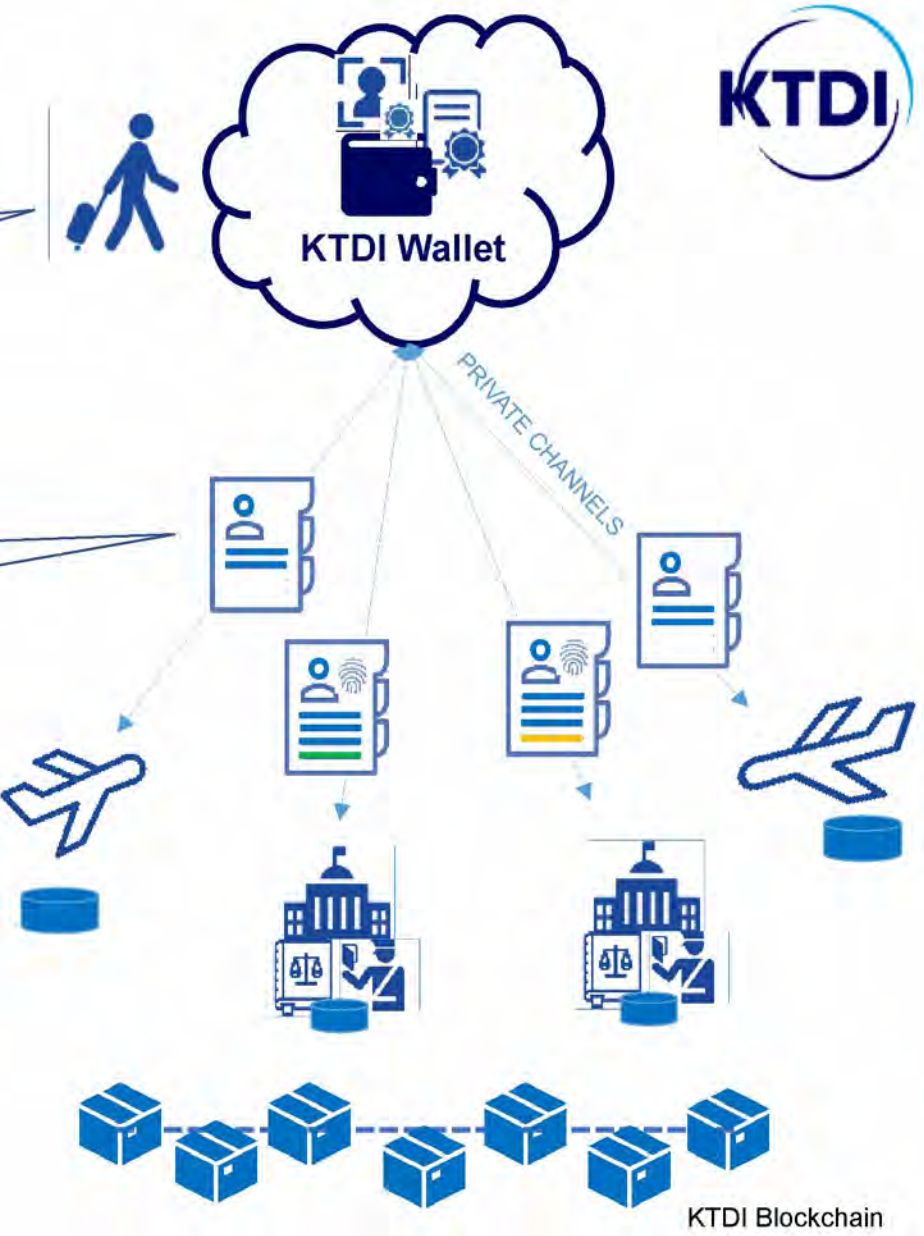
PRIVATE CONNECTIONS

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



Pilot Solution Summary

What's on the Blockchain

Only the following is written to the Blockchain – Note that no transaction information is written to the blockchain When an Issuer creates an attestation there is an underlying key management activity that updates the Accumulator* on the blockchain – but this does not contain transactional identifiers.

- **Public DIDs + DID Docs**
  - Registered Public DIDs of Service Providers (e.g., NOID, IRCC)
  - DID Docs containing [redacted] Key, Partner Agent Service Endpoint
    - *No Private / Pseudo DIDs are on the Blockchain, these are considered Personal Identifiable Information (PII)*

- **Credential Schemas Definitions**
  - A schema definition is a machine-readable definition of a set of attribute data types and formats that can be used for the claims on a credential. A schema definition can be used by many attestation issuers and is a way of achieving standardisation across issuers

- **Credential Definitions**
  - Once a schema definition is written to the [redacted] Ledger, it can be used by a credential issuer to create an issuer-specific credential definition that is also written to the [redacted] Ledger. This data structure is an instance of the schema on which it is based, plus the attribute-specific public verification keys that are bound to the private signing keys of the individual issuer.

- **Revocation Registries**
  - Data structure associated with revoked DIDs (see following slide)

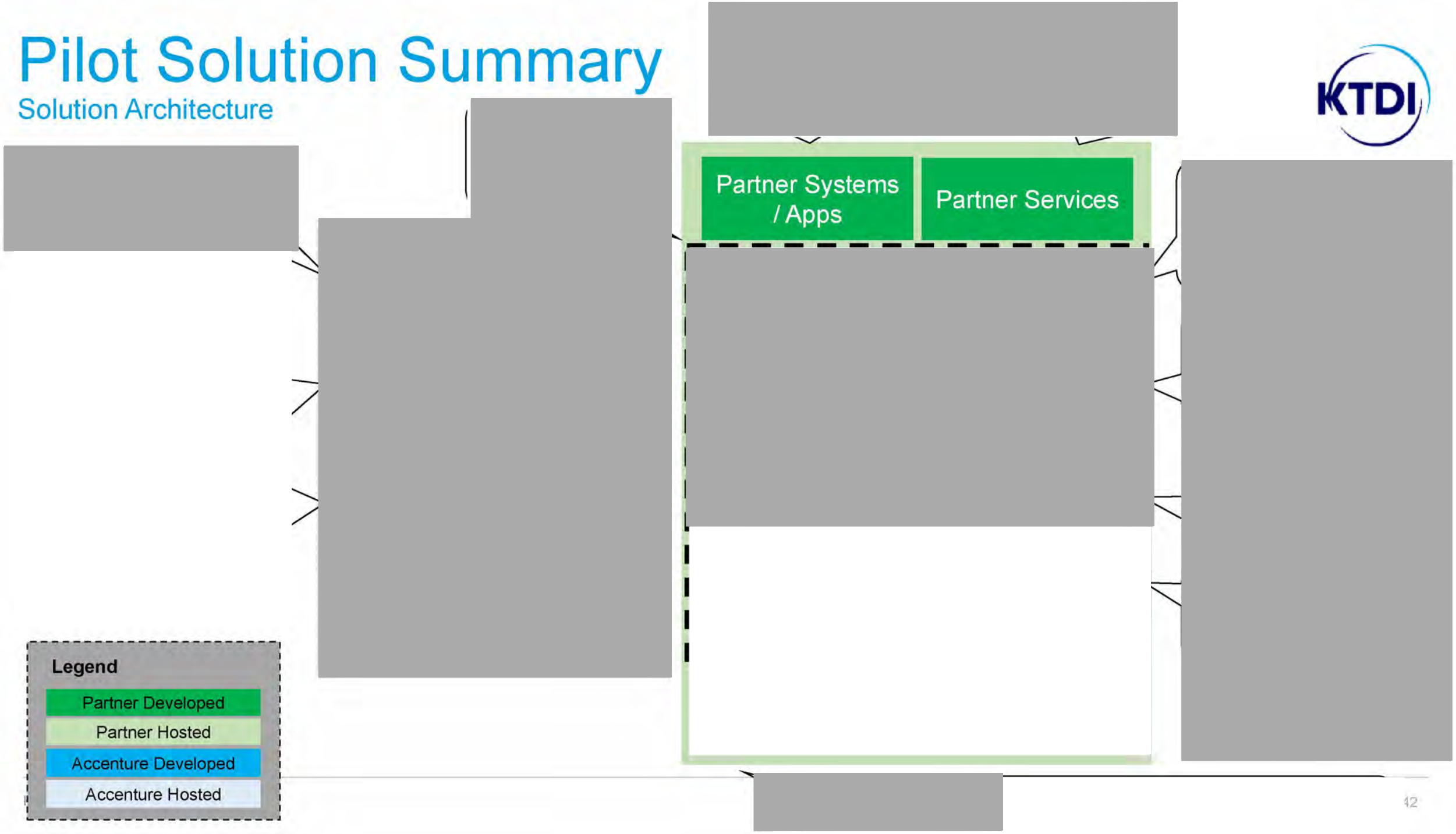
Pilot Solution Summary

What's on the Blockchain

- **A Revocation Registry** is data structure written to the [redacted] ledger by the issuer. It references the credential definition and contains a single (long) number called a cryptographic accumulator. This number can be checked instantly by any relying party when it needs to ensure a data in a proof it has been given hasn't been revoked by the issuer. It uses zero-knowledge cryptography to prove set membership
    - You can think of it as a type of compound hashing function—the number's value changes when hashes of valid credentials are added to or removed from the list, but from the number itself it is impossible to know whether any particular credential is included in the list unless you are the credential holder
- Only the credential holder, using their knowledge of which credential belongs to them, can create a zero knowledge proof of non-revocation, i.e., a proof that their credential belongs to the set of valid credentials (without disclosing which one it is). A relying party that needs to know that a credential has not been revoked can use this proof of non-revocation, together with the cryptographic accumulator the issuer placed on the [redacted] ledger, to instantly determine whether the credential is still valid
- When an issuer needs to revoke a credential, all the issuer needs to do is "subtract" the credential hash from the cryptographic accumulator and post the new number to the [redacted] ledger. The moment that happens, the credential holder will no longer be able to produce a valid proof of non-revocation

Pilot Solution Summary

Solution Architecture



Attestations, Credentials and Proofs

Pilot Solution Summary

Attestations: Granularity & Blockchain Transactions

An Attestation is defined as 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

An Identity Attribute is a characteristic of an individuals identity, e.g. the travellers gender or age, which is represented within an Identity Credential.

Granularity of Verifiable Claims allows for certain data elements to be selectively shared.

1.
2.
3.
4.

Pilot Solution Summary

Credentials and Proofs

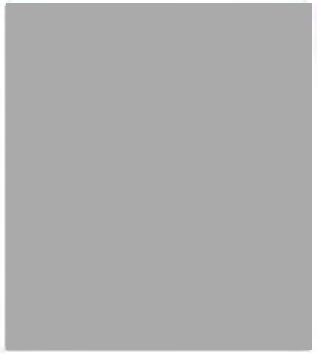
- **Credential Schema (on-chain)** – A schema definition is a machine-readable definition of a set of attribute data types and formats that can be used for the claims on a credential. A schema definition can be used by many attestation issuers and is a way of achieving standardisation across issuers
- **Credential Definition (on-chain)** – Once a schema definition is written to the Ledger, it can be used by a credential issuer to create an issuer-specific credential definition that is also written to the Ledger. This data structure is an instance of the schema on which it is based, plus the attribute-specific public verification keys that are bound to the private signing keys of the individual issuer. This approach enables an issuer to re-use an existing schema and enables a verifier who receives a proof containing data from the issuer to look up the issuer's credential definition on obtain their verification key(s) and verify the origin and integrity of that data.
- **Proof** – Cryptographic verification of an attestation. Proofs are one of two types: Transparent or Zero Knowledge. Transparent Proofs reveal all the information in an attestation. Zero Knowledge Proofs enable selective disclosure of the information in an attestation

Credential schema

Name	Version	Attribute Name
travel-document-holder	1.0	given_names
travel-document-holder	1.0	surname
travel-document-holder	1.0	nationality
travel-document-holder	1.0	date_of_birth
travel-document-holder	1.0	sex
travel-document-holder	1.0	facial_image
travel-document-holder	1.0	org_avatar (organization icon)
travel-document-holder	1.0	cred_avatar (credential icon)

Credentials

Attribute Name
given_names
Surname
Nationality
date_of_birth
sex
facial_image
org_avatar
cred_avatar

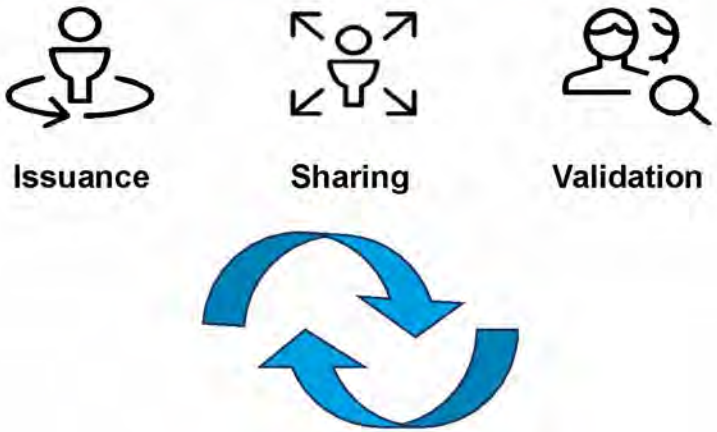


Pilot Interaction Summary

Partner Interactions

KTDI provides the platform on which partners can interchange across the Digital Identity Life Cycle:

- **Issuance** – The process of a traveler being issued verifiable credentials
- **Sharing** – The process of a traveler providing verifiable credentials to service providers
- **Validation** – the process by which a service provider validates a travelers travel credential and allows



It is necessary for Travellers and Partner Organisations to access the KTDI ledger in order to establish private and secure relationships that permit the **issuance** and **sharing** of verifiable claims.

Verifying [redacted] also require access to the KTDI ledger in order to validate the Identity claims presented to them by Travellers.

Typically, an issuing agency provides digital identity attestations once; whereby the traveller can then manage those, and other identity attributes, for sharing and validation as necessary.

Please note that channels, used to send and receive attestations, are not long lived connections and are more analogous to configuration for VPNs in that the same connection can be instantiated based upon that configuration.

Require confirmation as to whether interactions are to be defined for Schiphol for the purposes of Security clearance

Netherlands

NOID

Relationship Establishment

&

Identity Attestation
Reference Issuance

&

Identity Attestation On
Demand Retrieval

NOID – Relationship Establishment

The following diagram and process steps outline **the means by which a connection is established between the Traveller and the NOID**

Process Steps:

1.
2.
3.
4.
5.
6.
7.
8.

NOID – Identity Attestation Reference Issuance

The following diagram and process steps outline **the means by which the NOID Partner issues an identity attestation data Reference for the Traveller**

Process Steps:

1.
2.
3.

NOID – Identity Attestation On-Demand Retrieval

The following diagram and process steps outline **the means by which the NOID issue an On-Demand identity attestation for the Traveller to share with reliant parties**

Process Steps:

1.
2.

3.
4.
5.
6.
7.
8.

KLM

Relationship Establishment

&

Boarding [redacted] /
Attestation Issuance

&

Attestation Receipt /
Verification

KLM – Relationship Establishment

The following diagram and process steps outline **the means by which a connection is established between the traveller and KLM**

Boarding

Process Steps:

1.
2.
3.
4.
5.
6.
7.

KLM – Boarding / Attestation Issuance

The following diagram and process steps outline **the means by which KLM issues a Boarding Pass attestation to the traveller once they have proceeded through boarding**

Process Steps:

1.
2.
3.
4.
5.

KLM – Attestation Receipt / Verification

The following diagram and process steps outline **the means by which KLM receives identity data concerning a traveller that has been attested to**

Process Steps:

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

KMAR

Relationship Establishment

&

Attestation Receipt /
Verification

&

Entry / Exit Attestation Issuance

KMAR – Relationship Establishment

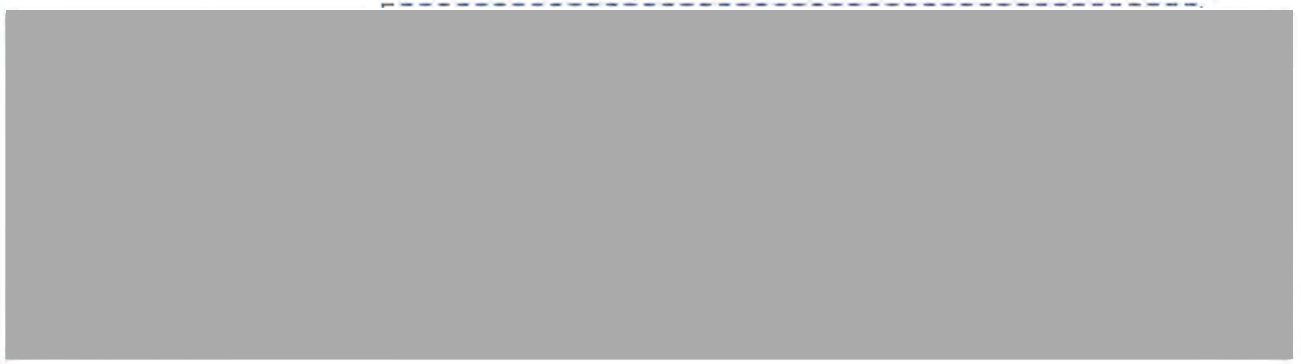
The following diagram and process steps outline **the means by which a connection is established between the Traveller and KMAR**

Process Steps:

1.
2.
3.
4.
5.
6.
7.

KMAR – Attestation Receipt / Verification

The following diagram and process steps outline **the means by which KMAR receives identity data concerning a traveller that has been attested to**



Process Steps:

1.
2.

3.
4.

5.

6.
7.

8.
9.
10.
11.
12.

KMAR – Exit / Entry Attestation Issuance

The following diagram and process steps outline **the means by which KMAR issues an Exit / Entry attestation to the traveller once they have proceeded through Exit Immigration controls**

Process Steps:

1.
2.
3.
4.
5.

Canada

IRCC

Relationship Establishment

&

Identity Attestation Issuance

IRCC – Relationship Establishment

The following diagram and process steps outline **the means by which a connection is established between the Traveller and the IRCC**

Process Steps:

1.
2.
3.
4.
5.
6.
7.
8.

IRCC – Identity Attestation Issuance

The following diagram and process steps outline **the means by which a connection is established between the Traveller and the IRCC**

Process Steps:

1.
2.
3.
4.
5.
6.
7.
8.
9.

Air Canada

Relationship Establishment

&

Boarding [redacted]
Attestation Issuance

&

Attestation Receipt /
Verification

Air Canada

Currently under discussion for Air Canada – If integration is incorporated into KTDI, the following interactions will be mapped:

Relationship Establishment

&

Boardin [redacted] */ Attestation Issuance*

&

Attestation Receipt / Verification

CBSA

Relationship Establishment

&

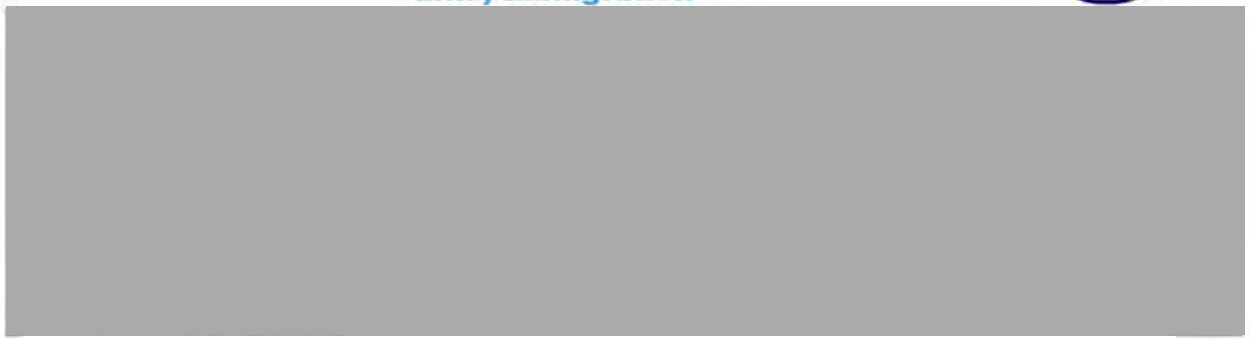
Attestation Receipt /
Verification

&

Entry Attestation Issuance

CBSA – Relationship Establishment

The following diagram and process steps outline **the means by which a connection is established between the Traveller and CBSA**



Process Steps:

1.
2.
3.
4.
5.
6.
7.

CBSA – Attestation Receipt / Verification

The following diagram and process steps outline **the means by which CBSA receives identity data concerning a traveller that has been attested to**

Process Steps:

1.
2.

3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

CBSA – Entry Attestation Issuance

The following diagram and process steps outline **the means by which CBSA issues an Entry attestation to the traveller once they have proceeded through Entry Immigration controls**

Process Steps:

1.
2.
3.
4.
5.

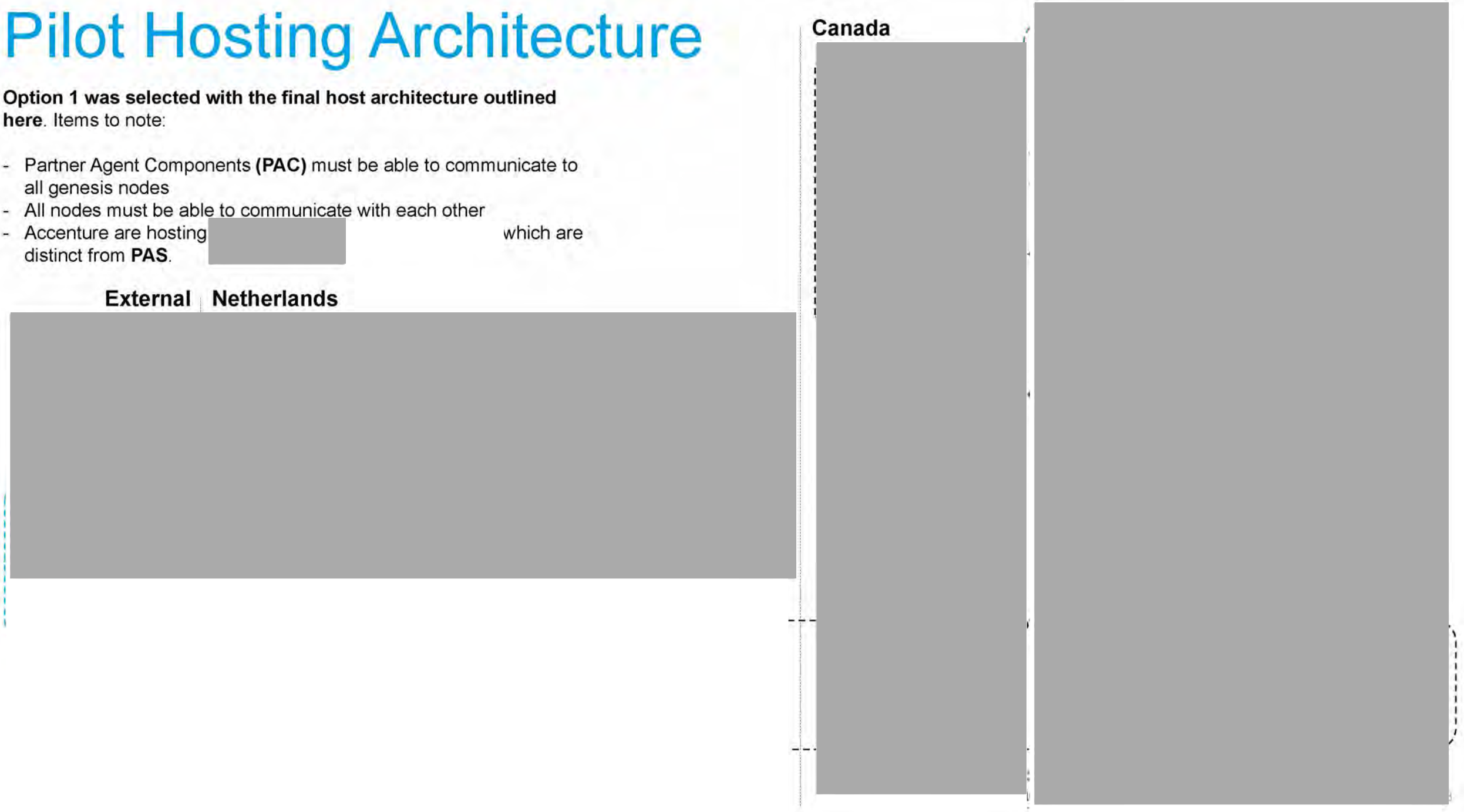
Pilot Solution Hosting

Pilot Minimum Viable Network

Pilot Hosting Architecture

Option 1 was selected with the final host architecture outlined here. Items to note:

- Partner Agent Components **(PAC)** must be able to communicate to all genesis nodes
- All nodes must be able to communicate with each other
- Accenture are hosting [redacted] which are distinct from **PAS**.



Pilot Components Hosting Requirements

Based on the solution architecture the components can be divided into groups with different hosting for each KTDI Partner:

Partner Hosting Requirements

Pilot Components Hosting Requirements

At a high level, if KTDI Partner wishes to host the solution within their environment then the following requirements need to be met:

Pilot Components Hosting Requirements

Components can be split into multiple security zone and KTDI Partner shall keep this in mind when designing network infrastructure

Specifications

The table below summarises the infrastructure required to support the KTDI components and [redacted] Node.

Infrastructure specifications:

[redacted]

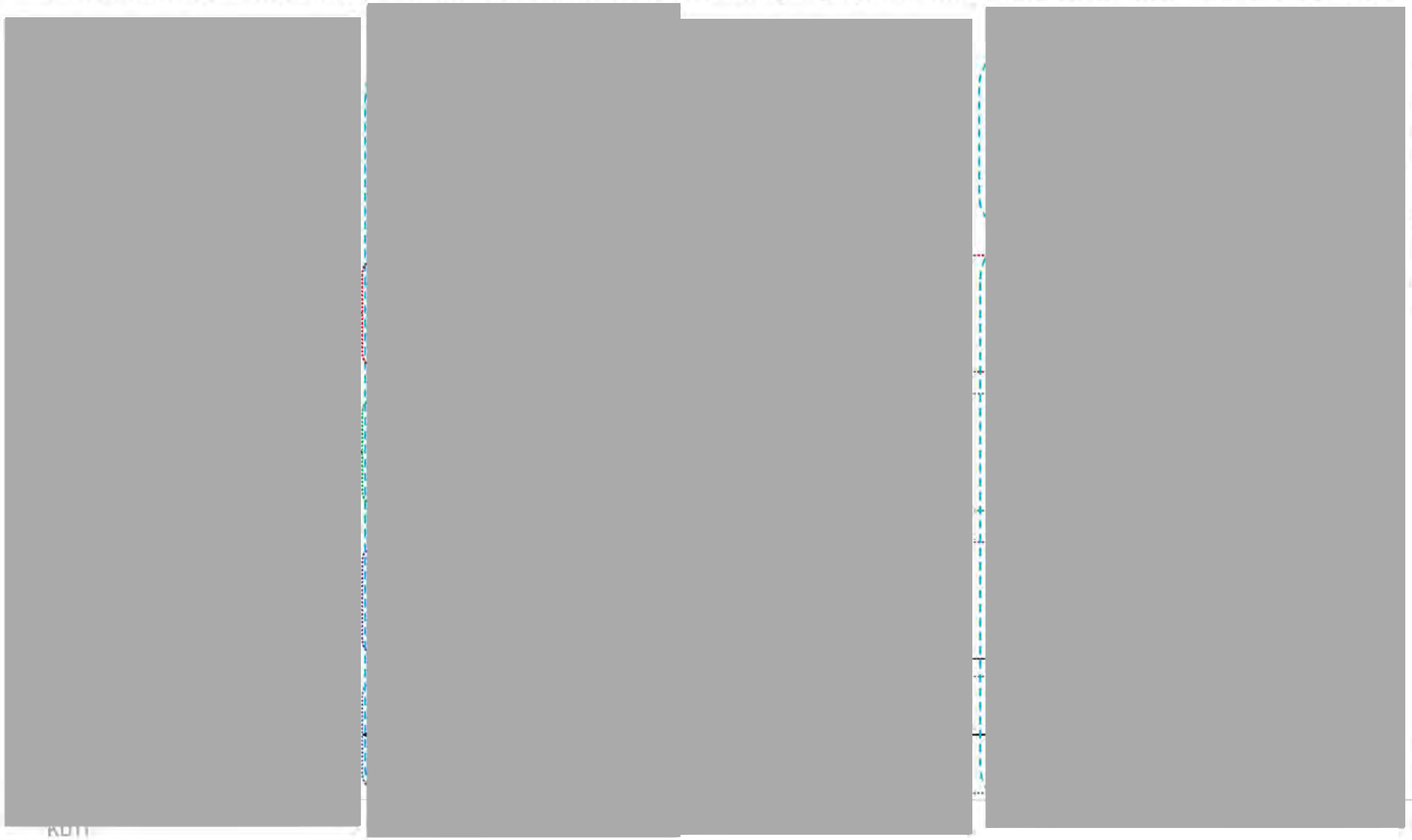
Connectivity specifications:

[redacted]

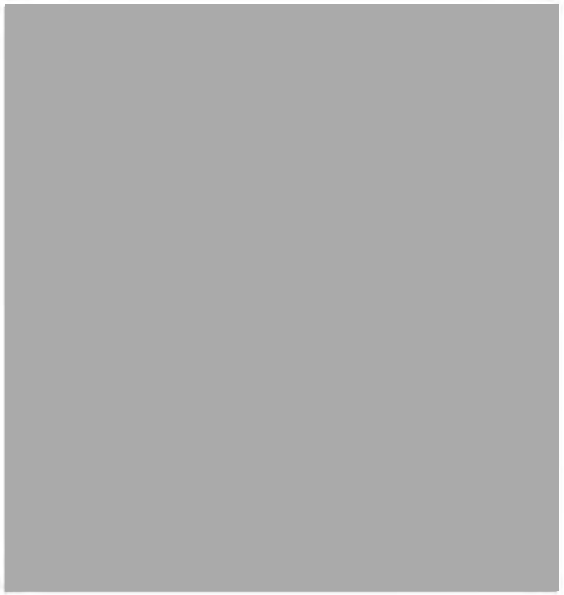
Connectivity

ACN, TRAVELLER & NLD Connectivity

To illustrate the connectivity, the solution has been broken into geographies with reference to Accenture and the Traveller.



The proposed network zones map to the previous slide with each organisation occupying a “column”. Where connectivity is to a ”zone”, it is assumed all components within this zone will have the same connectivity, i.e. Partner Agent Services -> Provider Agent Services.



ACN, TRAVELLER & CAN Connectivity

To illustrate the connectivity, the solution has been broken into geographies with reference to Accenture and the Traveller.

Thank You!

For further information
or any additional queries
please contact or consult:

[redacted]
Delivery Lead
[redacted]@accenture.com

[redacted]
Project Manager
[redacted]@accenture.com