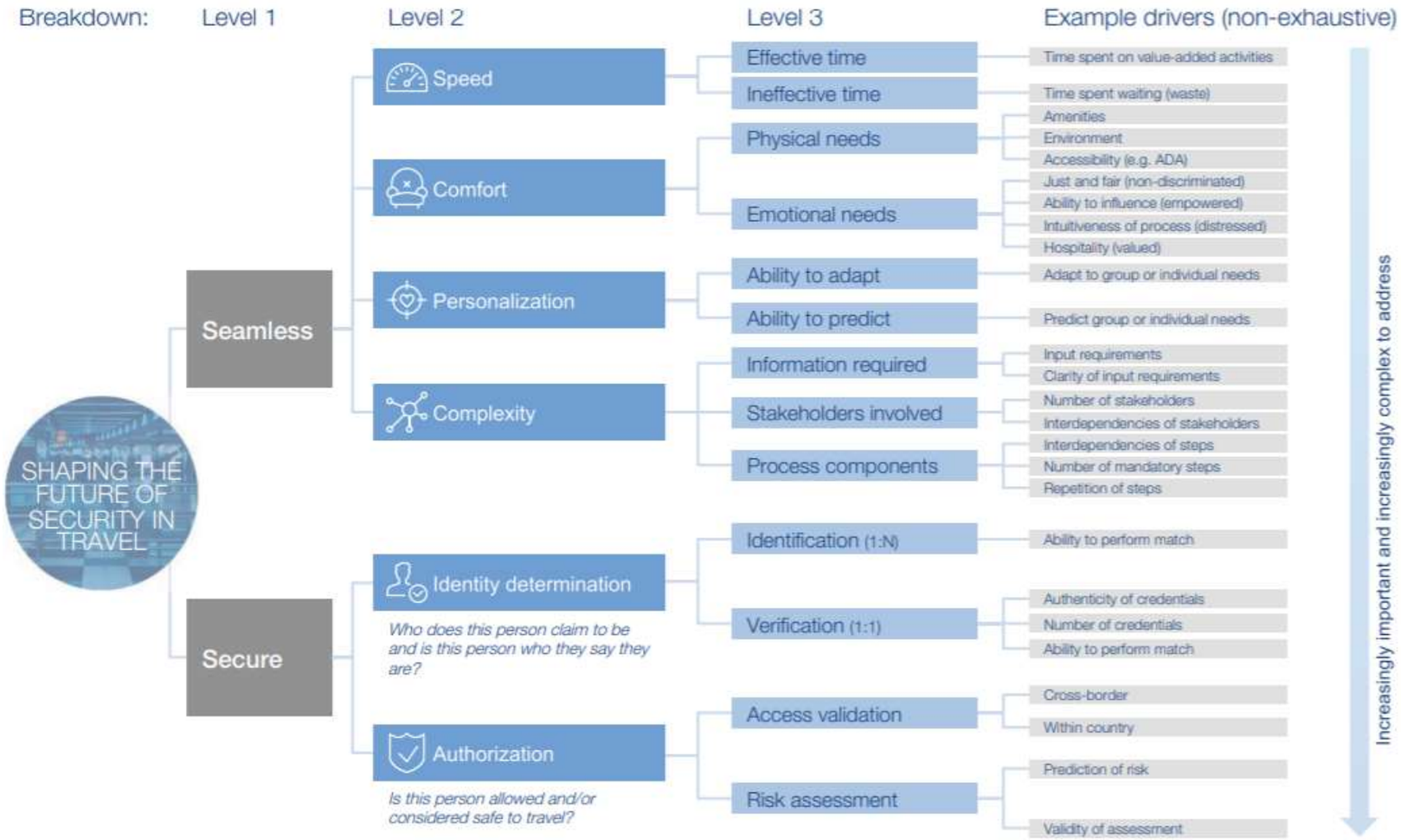
KNOWN TRAVELLER DIGITAL IDENTITY

Hyperledger Identity WG
March 18, 2020

KTDI Context

Improve Security and Facilitation with ever increasing travel volumes



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 physical 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 and contractors.
- Two airlines: **KLM & Air Canada**
- Three airports: **Amsterdam, Toronto and Montreal**
- Accenture

For additional context refer to: KTDI.org

Decentralized Identity Benefits

Identity Redefined

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

USERS

PORTABLE
Users are in possession and control of their verifiable, trusted identity data: biographic, biometric, affinity, registered or trusted traveller programs, etc

USER EXPERIENCE
The user can share information prior to travel obviating the need to present boarding pass or travel document for each service provider

ACCURATE
Data that has been validated and attested is shared digitally; no optical character misreads or key punch errors

PRIVATE
User is in control of what verifiable, trusted identity attributes they want to share and with whom via informed consent

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

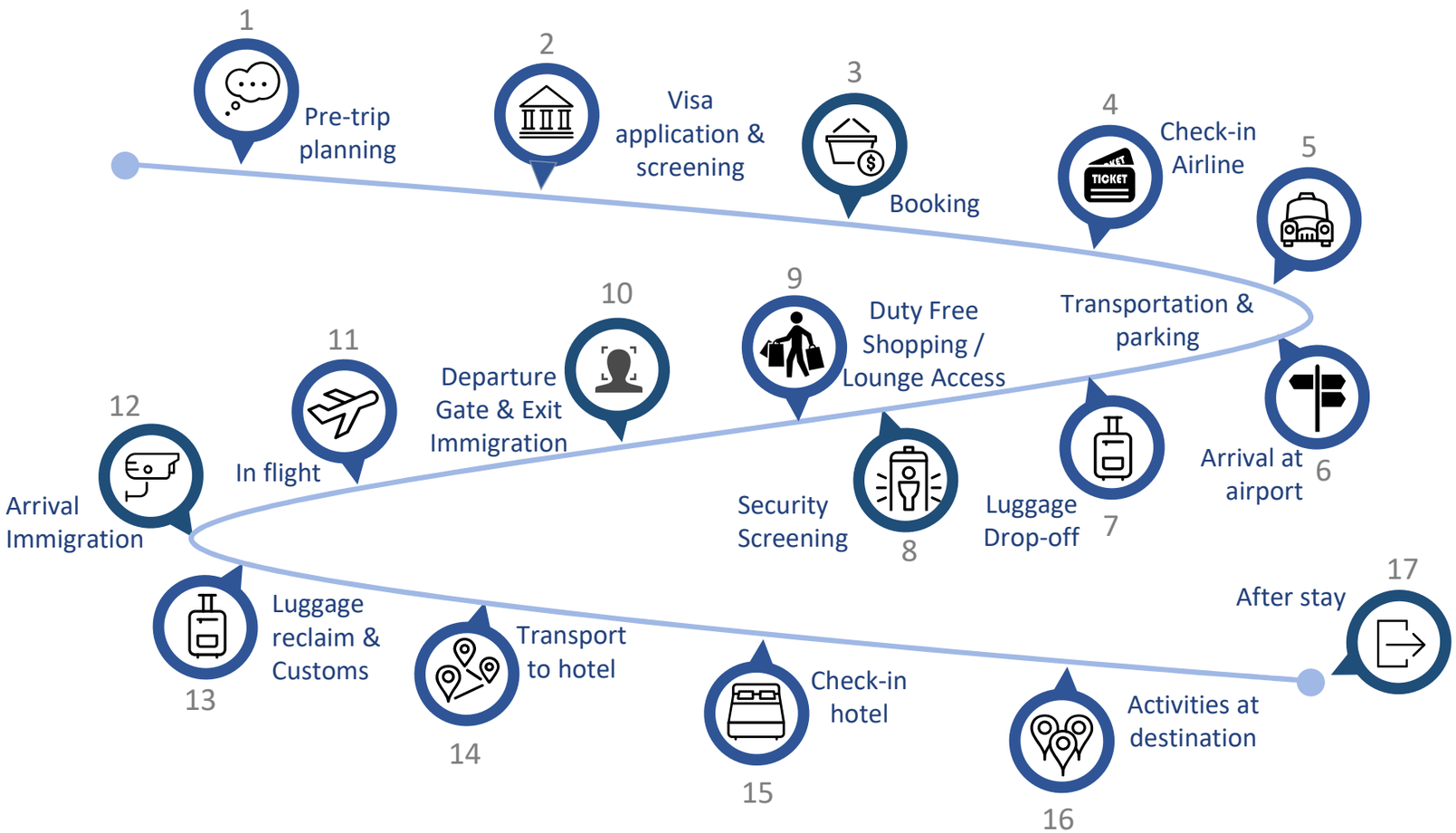
VERIFIABLE
Data can be shared confidentially and can be easily verified that it came from a trusted party

TRUST & INTEROPERABILITY
Verifiable credentials are cryptographically signed and validated via blockchain for integrity and revocation; interop through sstandards-based protocols

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

Secure Facilitation

Once Trusted, Verifiable Claims are shared.... "Your Face is Your Passport"



Existing Trusted, Verifiable Credential

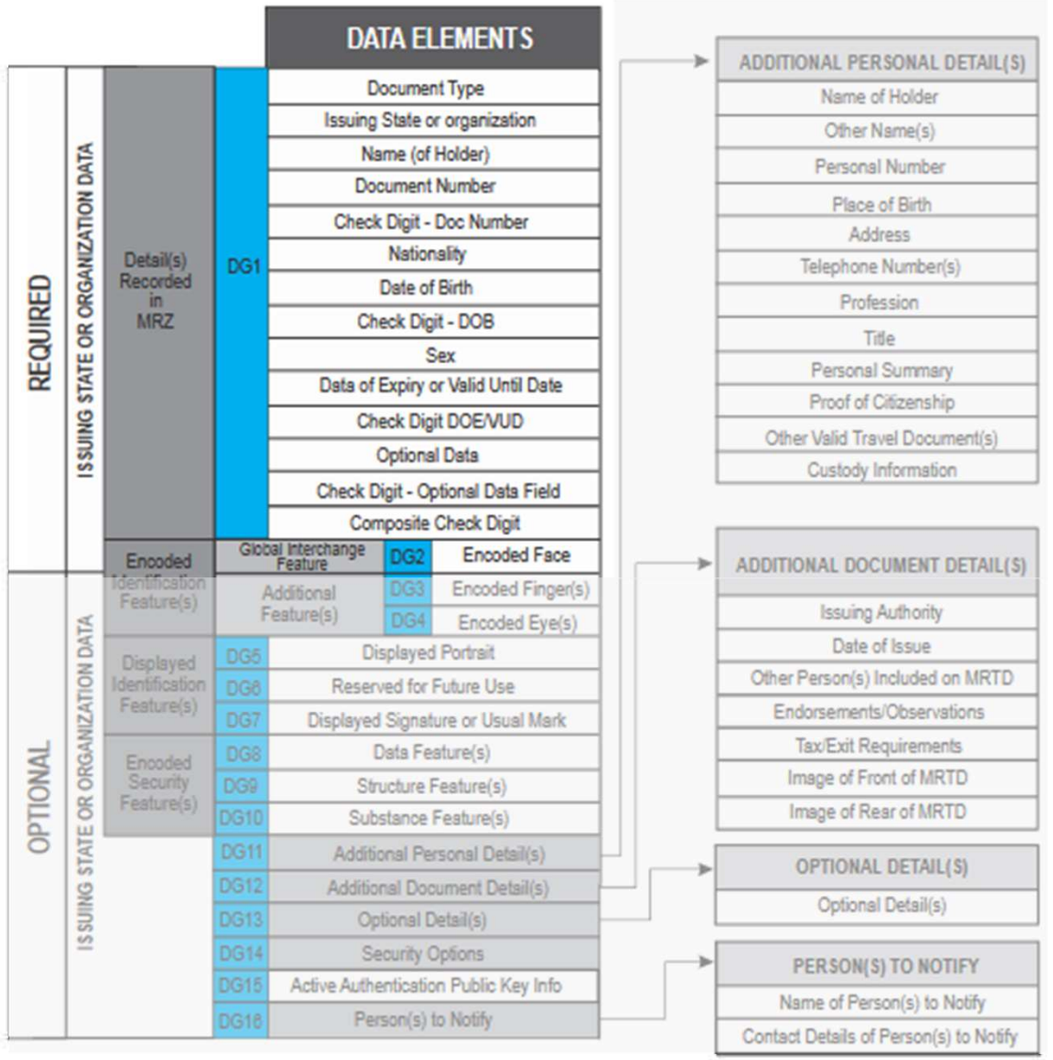
ICAO ePassport

Logical Data Structure

2.1 Security
Data integrity and authenticity are needed for trusted global interoperability.

Data Groups 1 to 16 inclusive SHALL be write protected. A hash for each Data Group in use SHALL be stored in the Document Security Object (EF.SOD).

Only the issuing State or organization shall have write access to these Data Groups. Therefore, there are no interchange requirements and the methods to achieve write protection are not part of this specification.



Other Related Initiatives

ICAO Digital Travel Credential (DTC)

Next generation "virtual" credentials securely stored in mobile devices or cloud hosted and accessed via biometric authentication giving travelers the opportunity for document-free travel between participating countries.

https://www.icao.int/Meetings/TRIP-Symposium-2016/Documents/Cole.pdf

KTDI	DTC
Supports multiple verified, trusted attestations from government or non-government issuers	Supports one verified, trusted attestation from a government issuer
Supports Selective Disclosure of verified, trusted attestations	Supports all or nothing disclosure of verified, trusted attestations
Allows the issuer to revoke a specific attestation that it issued to an individual	Supports revocation of Country Signing Certificates which typically affects thousands of identities
Utilizes a Decentralized Public Key Infrastructure so no intermediary is needed to determine if a credential is valid or if it has been revoked	Utilizes a Centralized Public Key Infrastructure which must be consulted to determine if a credential is valid or if it has been revoked

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 digital credentials to service providers

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

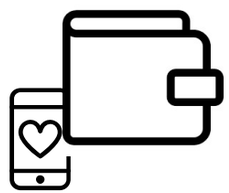
Travel Activities

Service Providers Public DIDs (similar to country signing certificates)

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

Blockchain activities

Traveler's Identity Wallet is created

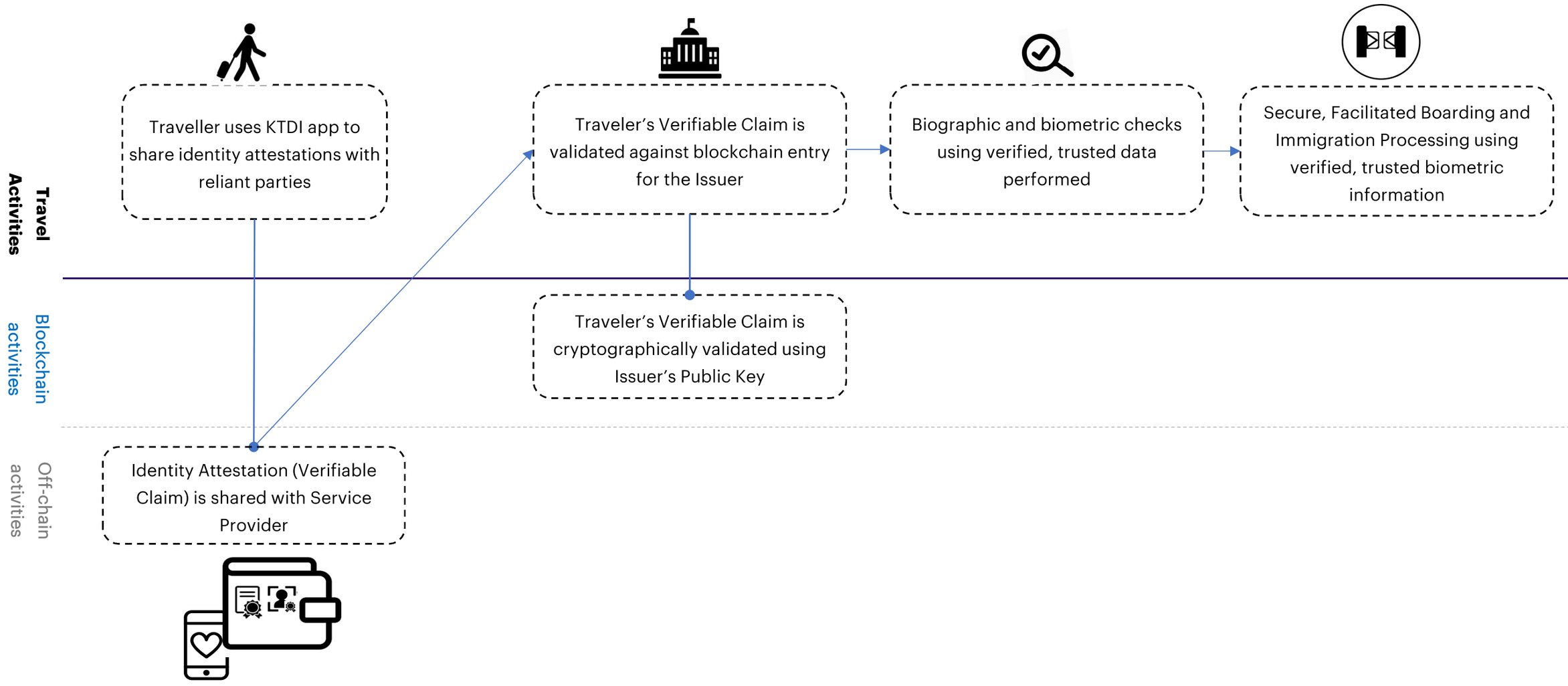


Traveler's Identity Wallet is updated with the Identity Attestation (Verifiable Claim)

Off-chain activities

High Level Pilot Process Flow

Sharing and Validation



KTDI Detailed Pilot Journey

KTDI Video

Pilot Solution Platform

Pilot Solution Platform

Multiple platforms were considered as the foundation of the KTDI Solution

Hyperledger Indy selected for KTDI

	HYPERLEDGER INDY	corda	uport	sovrin	HYPERLEDGER FABRIC
Identity focused	Yes	No	Yes	Yes	No
Standards based	Decentralized Identity Foundation	Decentralized Identity Foundation	Decentralized Identity Foundation	Decentralized Identity Foundation	No
Open Source	Yes	Partial	Yes	Partial	Yes
Standalone	Yes	Yes	Yes	No	Yes
Network type	Private **permissioned**	Private **permissioned**	Public **permission-less**	Public **permissioned**	Private **permissioned**
Blockchain Development Effort	DID focused logic	Java virtual machine	Ethereum virtual machine	DiD focused logic	Stateful business logic virtual machine
Scalability	High scalability	High scalability (potential issues with notaries)	Constrained by Ethereum network	Nodes require Sovrin approval	High scalability *(potential issues with channels)*
Security	Wallet / agent controlled	Wallet / agent controlled	Wallet / agent controlled *(identity is public to some degree)*	Wallet/agent controlled	Custom

Pilot Solution Platform

Hyperledger Indy

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 Indy. Furthermore, this effort would likely be throw-away since industry is moving forwards with Indy 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. Likewise, REST 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 Indy was selected as the blockchain platform for the KTDI solution.**

HYPERLEDGER INDY

Pilot Solution Platform

Hyperledger Indy

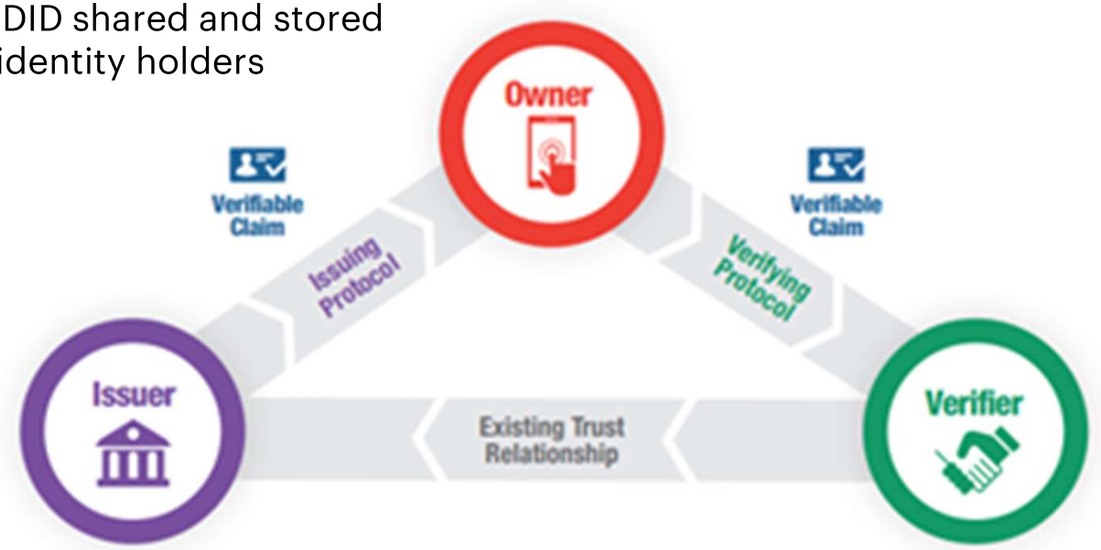
- Every participant (entity) in KDTI is described by entity records (public data), associated with a **Decentralized Identifier (DID)**
- Each **DID** is associated with a verification key for confidentiality or authentication reasons
- To maintain privacy and prevent correlating the entity's exchanges, 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

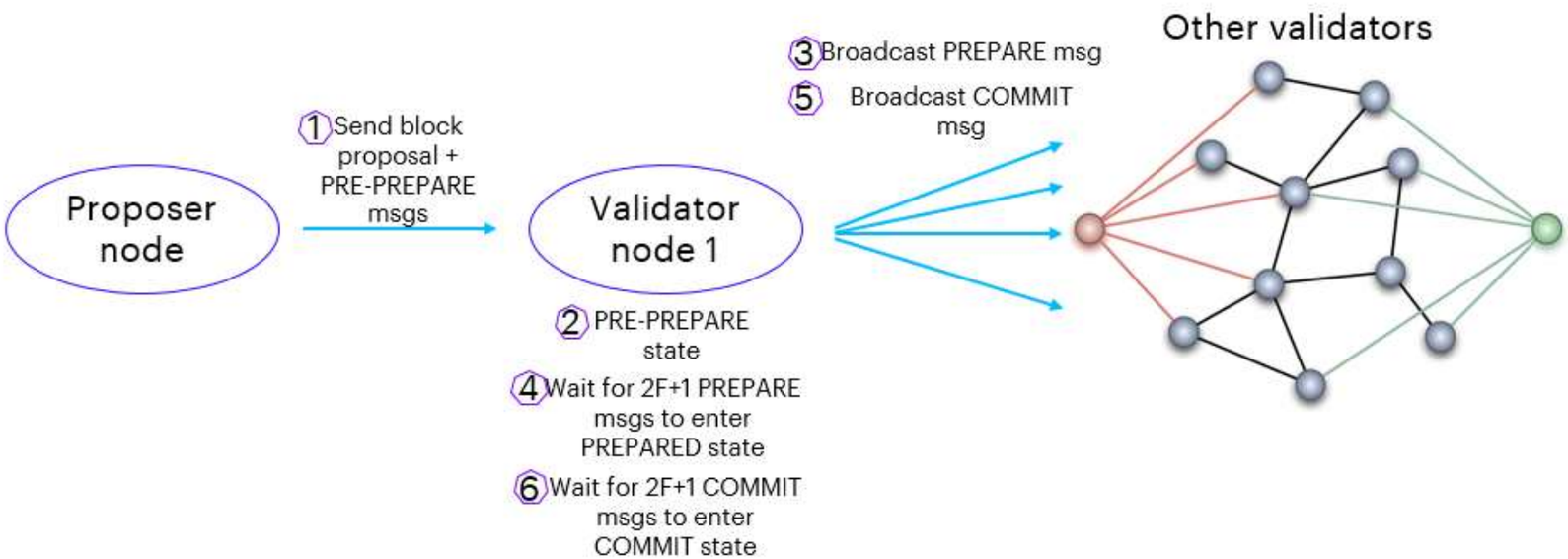
- Associated with their DID, the traveller collects verifiable claims on credentials that consist of identity attributes (this is explained in more detail on the following slides)



Pilot Solution Platform

Hyperledger Indy

- 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 Patricia Tree Wallet** = 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*



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

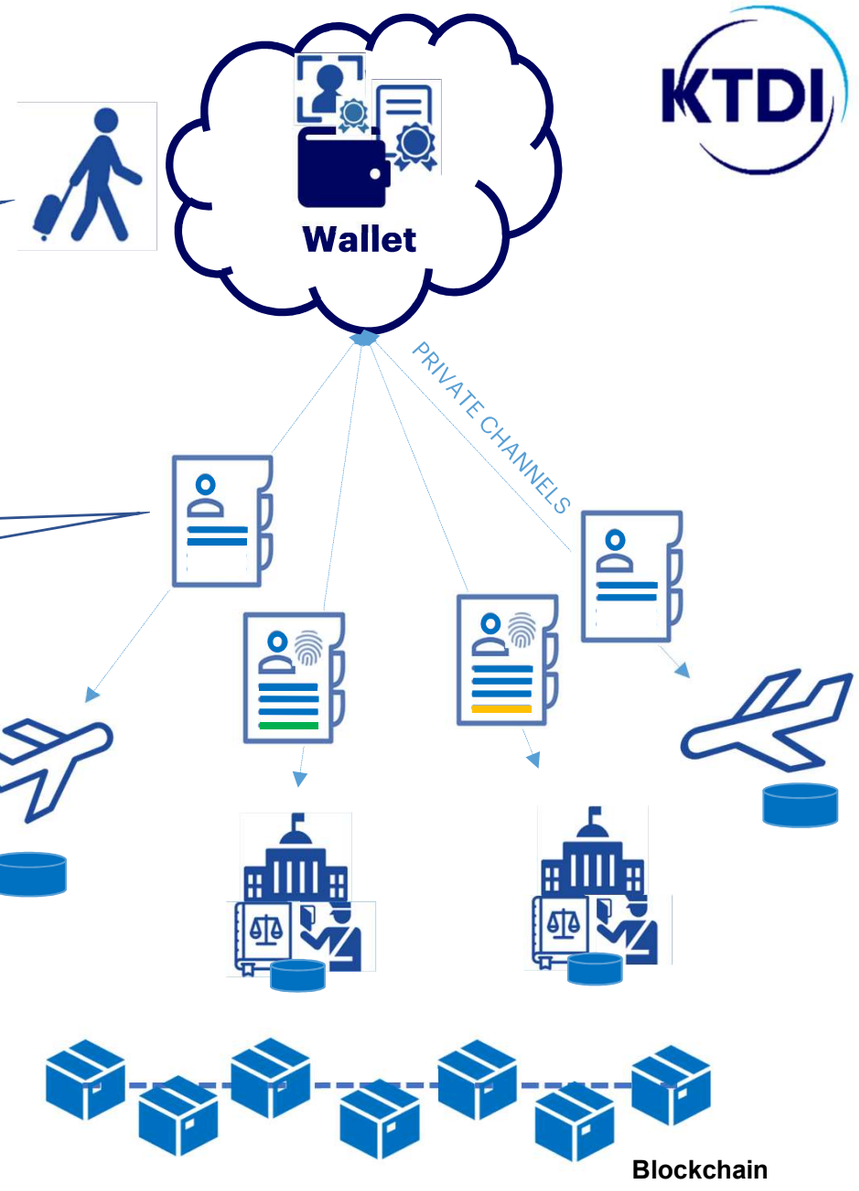
PRIVATE CONNECTIONS

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 Verification 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 standardization across issuers

- **Credential Definitions**
  - Once a schema definition is written to the Indy Ledger, it can be used by a credential issuer to create an issuer-specific credential definition that is also written to the Indy 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 Indy 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 Indy 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 Indy ledger. The moment that happens, the credential holder will no longer be able to produce a valid proof of non-revocation

WHY STANDARDS

Why do we need IT standards?

For any given technology, industry standards assure the availability in the marketplace of multiple sources for comparable products

- They foster **wide spread adoption**
- They **reduce time-to-market**
- They facilitate **interchange** and /or **interoperability**
- They **reduce risk** to integrators and end users
- They **reduce vendor "lock-in"** effect
- They are a sign of industry **maturity**
- Provide a common means to define, measure, and test:
  - **Quality**
  - **Performance**
  - **Security**

STANDARDS BODIES (PARTIAL)

International

ISO IEC ITU

ICAO

National

NIST

ANSI
American National Standards Institute

afnor bsi.

DIN
Deutsches Institut für Normung

Federal Agency for
Technical Regulation
and Metrology
(Rosstandart)

Other

W3C®

fido alliance

OASIS
Open standards. Open source.

GSMA

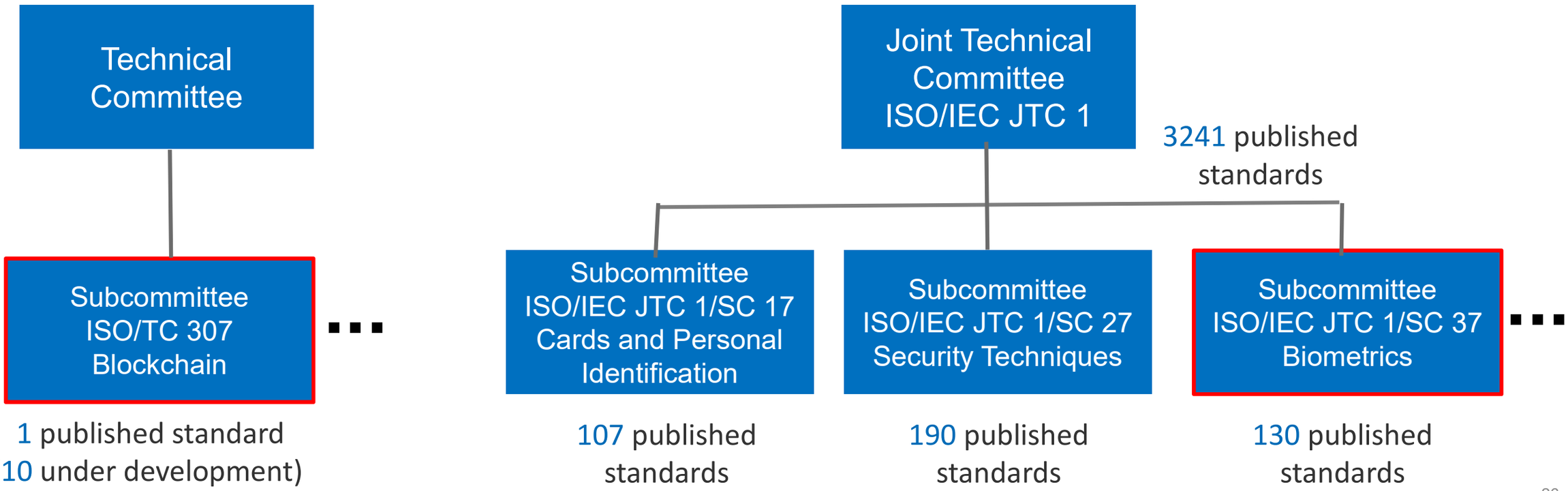
OpenID

STANDARDS BODIES (PARTIAL)

Creation date: 2016

Standardisation of blockchain technologies
and distributed ledger technologies

Participating countries: 44
Observing countries: 13



KEY IDENTITY RELATED STANDARDS

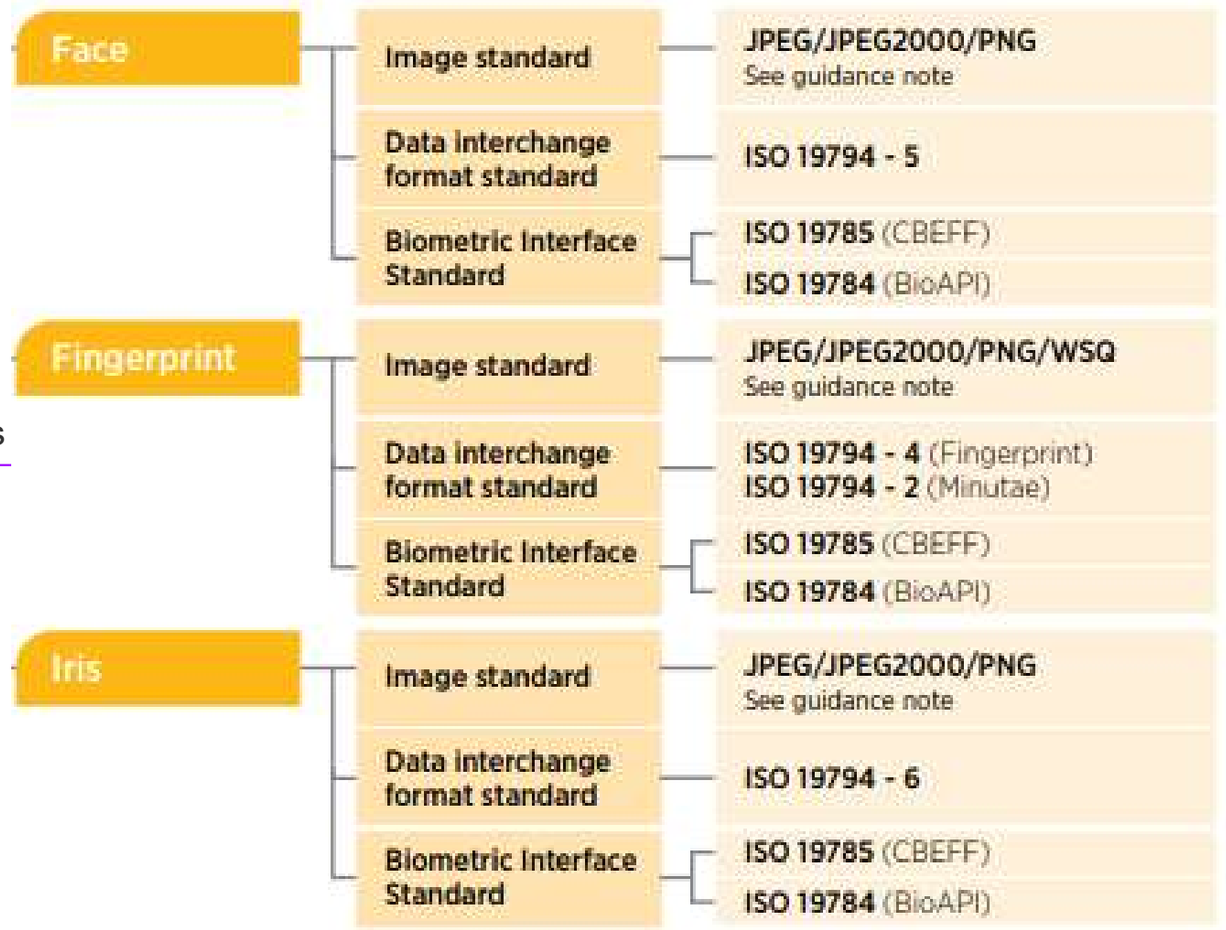
	ISO/TC 307 - Blockchain and distributed ledger technologies
WG 1	**Foundations** ISO/FDIS 22739 Terminology ISO/WD TS 23258 Taxonomy and Ontology ISO/CD 23257.3 Reference architecture ~~ISO/NP TR 23578 Discovery issues related to interoperability~~
WG 2	**Security, privacy and identity** ISO/PRF TR 23244 Overview of privacy and personally identifiable information (PII) ISO/CD TR 23245.2 Security risks and vulnerabilities ~~ISO/NP TR 23246 Overview of identity management using blockchain and distributed ledger technologies~~ ISO/CD TR 23576 Security of digital asset custodians
JWG 4	**Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Blockchain and distributed ledger technologies and IT Security techniques** ISO/NP TR XXXXX Overview of **existing** identity management using blockchain and distributed ledger technologies
WG 3	**Smart contracts and their applications** ISO/TR 23455 Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems ISO/AWI TS 23259 Legally binding smart contracts
WG 5	**Governance** ISO/NP TS 23635 Guidelines for governance
WG 6	**Use cases** ISO/CD TR 3242
SG 7	Interoperability of blockchain and distributed ledger technology systems

KEY IDENTITY RELATED STANDARDS

	W3C
DID	Decentralized Identifiers - Self-sovereign identifiers
VC	Verifiable Claims - A standard way to express claims on the Web
WebID	Web Identity and Discovery - Provides globally unique, dereferenceable identifiers
WebID-OIDC	Extends Open ID Connect to support WebID's
WebACL	Access Control Lists for web-based resources, e.g. user profiles, segments within them, or individual data items
LDP	Linked Data Platform - Platform to allow reading and writing of data on the Web
RDF	Web-native abstract data model allowing for data integration and independent extension [Resource Description Framework]
JSON-LD	Serialization of RDF as JSON
	OTHER
OpenID	OpenID Connect - Identity layer on top of OAuth 2.0
IETF IETF	OAuth 2.0 - Authorization framework JSON Web Tokens - For representing claims to be transferred between two parties
Schema.org	Google, Microsoft, Yahoo and Yandex (http://schema.org) –De-facto vocabulary for describing 'things' of interest to search engines, expressed as RDF

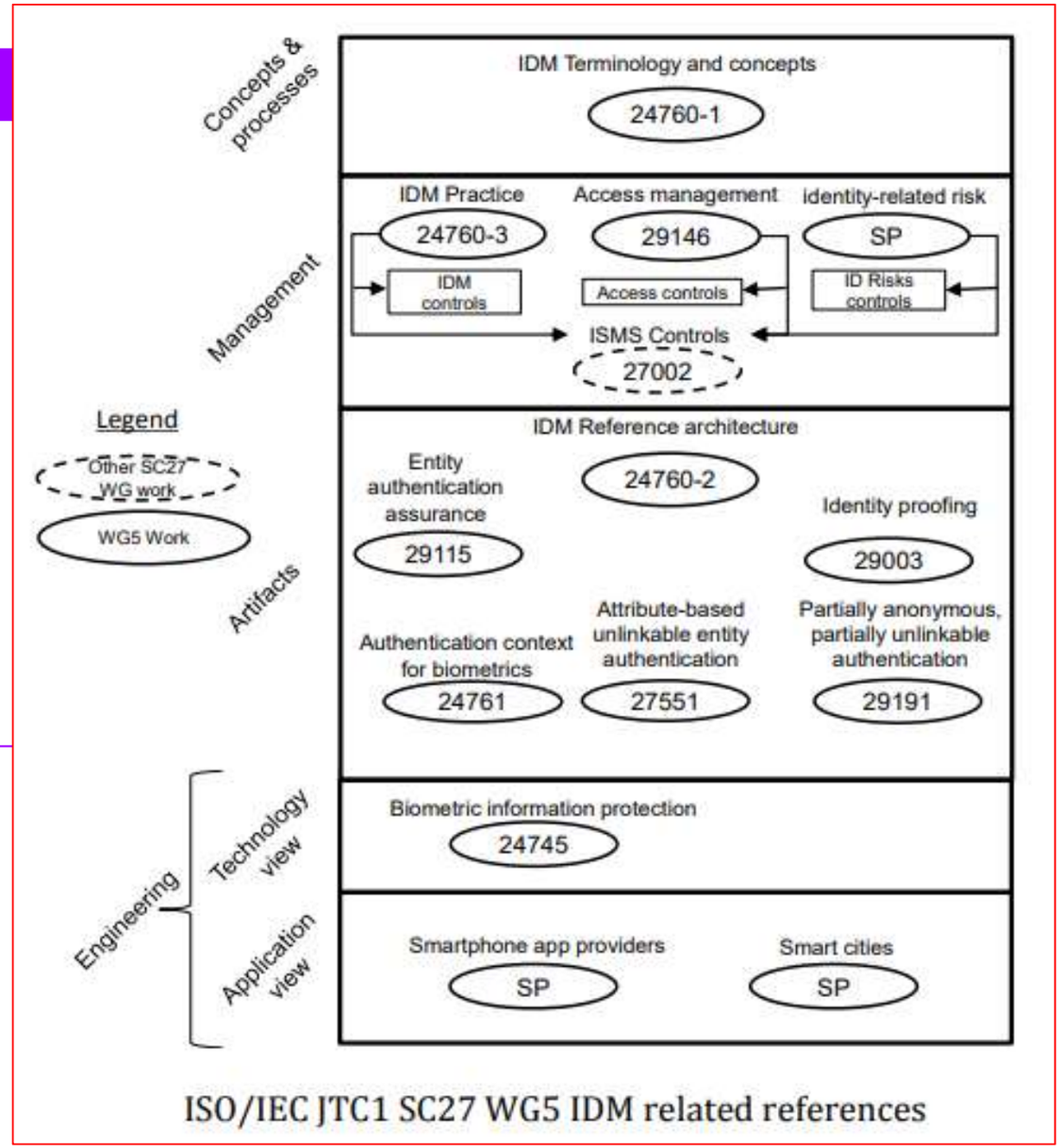
KEY IDENTITY RELATED STANDARDS

ISO/IEC JTC 1/SC 37 - Biometrics	
WG 1	Harmonized biometric vocabulary
WG 2	Biometric technical interfaces
WG 3	Biometric data interchange formats
WG 4	Technical Implementation of Biometric Systems
WG 5	Biometric testing and reporting
WG 6	Cross-Jurisdictional and Societal Aspects of Biometrics



KEY IDENTITY RELATED STANDARDS

	ISO/IEC JTC1 SC 27 - IT Security techniques
WG 1	Transversal Items
WG 2	Cryptography and security mechanisms
WG 3	Security evaluation, testing and specification
WG 4	Security controls and services
WG 5	**Identity management and privacy technologies**
AG 1	Management Advisory Group
SG 1	Data security
SWG-T	Information security management systems



ISO/IEC JTC1 SC27 WG5 IDM related references

KEY IDENTITY RELATED STANDARDS

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLGY (NIST)	
SP 800-63-3	**Digital Identity Guidelines**
SP 800-63-A	Enrollment and Identity Proofing
SP 800-63-B	Authentication and Lifecycle Management
SP 800-63-C	Federation and Assertions
IR 8202	Blockchain Technology Overview
NIST.CSWP.01142020	**A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems**
ANSI/NIST-ITL	**Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information** (used by INTERPOL, RCMP, EU, DOD, FBI, and others)
NIST IR 7151	NIST Fingerprint Image Quality (NFIQ)
NIST IR 8173	Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects
….	Many others

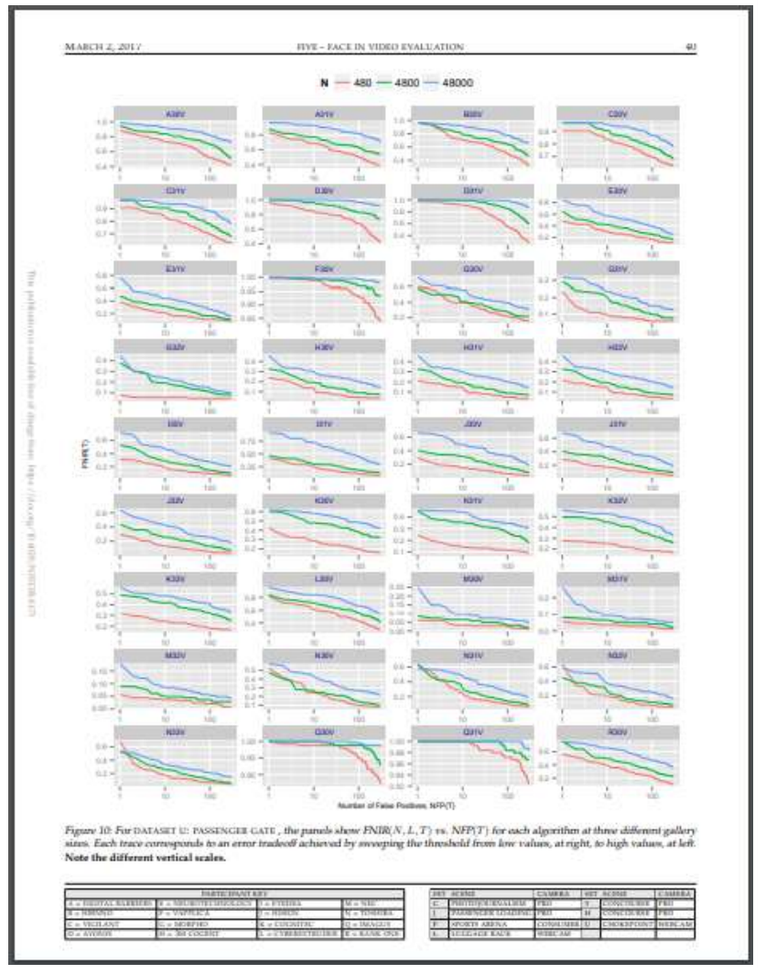


Figure 10: For DATASET 12: PASSENGER GATE *, the panels show FNIR(N, L, T) vs. NFP(T) for each algorithm at three different gallery sizes. Each trace corresponds to an error tradeoff achieved by sweeping the threshold from low values, at right, to high values, at left.* **Note the different vertical scales.**