WORLD ECONOMIC FORUM

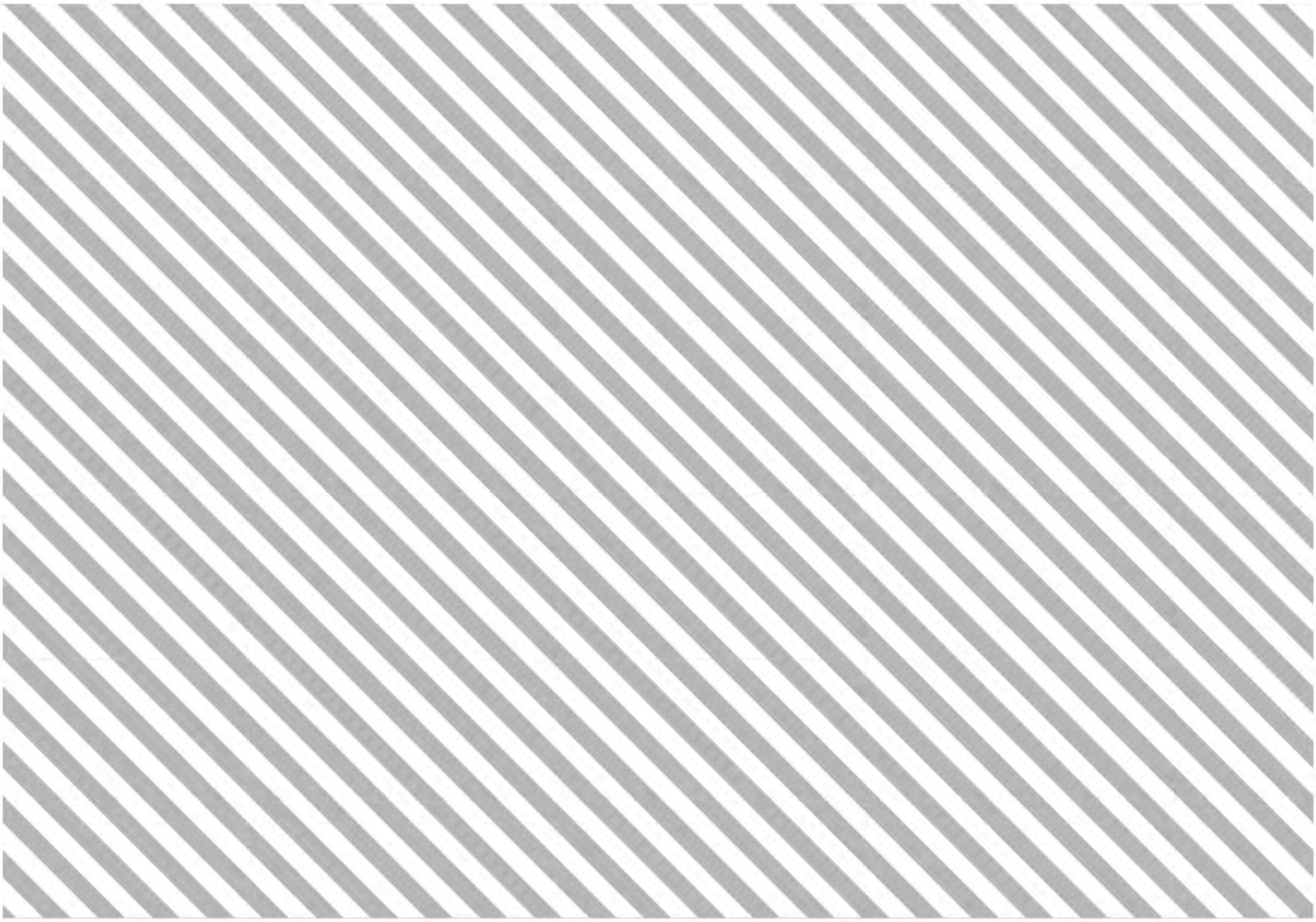
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

# Known Traveller Digital Identity
## Specifications Guidance

In collaboration with Accenture

March 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.:
Fax:
Email @weforum.org
www.weforum.org

# Contents

# 1. Foreword

In January 2018, the World Economic Forum introduced its Known Traveller Digital Identity (KTDI) concept, an initiative co-designed by public- and private-sector partners that aims to anticipate the challenges, and take advantage of the immense opportunities, that emerging technologies will present in the cross-border movement of people. The KTDI concept seeks to address the changing behaviours and expectations of travellers, the growing volume of global travellers, and the increasing focus on risk-based security to promote more seamless and secure travel.

The KTDI concept relies upon a trusted, decentralized and interoperable identity platform enabled through technologies including blockchain, biometrics, mobile devices and cryptography. The Forum and its partners are currently piloting components of the KTDI concept in a real-life, cross-border context between the Netherlands and Canada. The pilot is testing various elements of the KTDI concept's policies, processes and technologies to further enhance the concept and inform future pilots and the development of best practices and standards in collaboration with international regulatory and standards-setting bodies and industry. In future iterations, multiple pilots can run – potentially in parallel and with different use cases, partners, technologies and geographies – to enrich the outcome and scalability of the KTDI concept.

As the pilot is under way, this White Paper documents the standards, open specifications and industry best practices that have shaped the initial pilot and that provide guiding principles for the KTDI concept and any related future pilots towards the end-state vision of global interoperability. The document references applicable standards, capabilities and functionalities that comparable solutions should consider in order to interoperate with the KTDI concept.

This paper is the result of collaboration between the World Economic Forum, Accenture and our partners to inspire active multistakeholder action in this fast-moving landscape. It serves two aims: first, to inform ongoing initiatives and pilots to advance the convergence and harmonization of global developments and, second, as a tool to compare and align KTDI and other complementary approaches and technologies with the ambition to secure maximum interoperability and global adoption. The Forum welcomes engagement from other organizations advancing secure and seamless travel, and looks forward to further collaboration on this subject.

# 2. Executive summary

In January 2018, the World Economic Forum's Platform for Shaping the Future of Mobility introduced its Known Traveller Digital Identity (KTDI) concept, an initiative co-designed by public- and private-sector partners that seeks to anticipate the changing behaviours and expectations of travellers, the growing volume of global travellers, and the increasing focus on risk-based security to promote more seamless and secure travel.

The Forum and its partners are currently piloting components of the KTDI concept in a real-life, cross-border context between the Netherlands and Canada. The pilot's lessons will help to further enhance the KTDI concept and to inform future pilots and the development of best practices and standards in collaboration with international regulatory and standards-setting bodies and industry. In future iterations, multiple pilots can run – potentially in parallel and with different use cases, partners, technologies and geographies – to enrich the outcome and scalability of the KTDI concept.

This White Paper describes the technical foundation of the KTDI concept and documents the standards, open specifications and industry best practices that have shaped the initial pilot and that provide guiding principles for the KTDI concept and any related future pilots.

The KTDI concept was designed to adhere to the values and principles of decentralized identity, including ownership and control of identity attributes, privacy and disintermediation. As such, the KTDI solution is built upon the decentralized identity model, leveraging the emerging World Wide Web Consortium (W3C) verifiable credentials (VC) and decentralized identifier (DID) standards. This model allows travellers to self-manage digital identity attributes that are attested to and provided by issuing authorities (both public and private) so the individual may share them through selective disclosure.

This paper focuses on describing the various layers of the decentralized identity model and the capabilities, standards and specifications that apply to each and that have been leveraged to build the KTDI solution. The layers are divided into two categories of trust (cryptographic and human) as follows (this paper does not cover layer 4):

| | |
|---|---|
| **Cryptographic trust** | Layer 1: DID Networks |
| | Layer 2: DID Communication Protocol |
| **Human trust** | Layer 3: Credential Exchange |
| | Layer 4: Governance Frameworks |

The intended audience for this paper includes teams supporting chief information or technology officers of organizations interested in exploring the adoption of the KTDI concept or complementary solutions. This paper is not intended to cover specific details, lessons or outcomes from the KTDI pilot that is currently under implementation.

As emerging decentralized identity strategies and technologies continue to develop, it is important to consider alternative or complementary technologies and approaches that may also support KTDI's core principles. The expected advantages and disadvantages of every technological choice must be thoroughly assessed on a use case basis, considering legal, national security, certification, risk and other requirements.

This paper outlines the ambition for KTDI to provide the foundations for a globally accepted decentralized identity ecosystem. Further development and wider adoption depend on maximizing data exchange interoperability and federated trust, for which the best use of international standards, open specifications and industry best practices are essential. Success will rest upon cooperation between world governments, regulators, the aviation industry, technology providers and other players to establish global standards and specifications for compliance by all stakeholders.

As the leading global platform for public-private cooperation, the Forum is committed to strengthening the kind of multistakeholder collaboration needed to achieve interoperability in the new identity paradigm that continues to unfold. The Forum invites interested stakeholders to provide feedback and proposals for new pilots or approaches to enhance or complement the KTDI concept and further this goal.

# 3. Introduction

## 3.1 Background

For decades the cross-border movement of legitimate travellers has enabled and sustained international trade, tourism-driven economic growth and increased tolerance across cultural and social divides. However, global travel systems are under greater pressure from the growing number of travellers, infrastructure capacity limits and ever-increasing risk and security requirements. These pressures hinder a secure and seamless cross-border traveller journey and cause various pain points for governments, businesses and travellers. Experts predict that a combination of these pressures on the international travel experience will reach a tipping point, putting the growth of the industry at risk.

The Known Traveller Digital Identity (KTDI) concept aims to leverage advances in emerging technologies, such as blockchain and decentralized key management systems, to simultaneously enhance the security capabilities in the travel continuum while improving the passenger experience.

*The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel* report describes the KTDI concept and outlines a set of recommendations (Table 1) that serve as the basis for this White Paper:[1]

One of the recommendations was to pilot the KTDI prototype policies, processes and technologies and adapt them iteratively while balancing development with ongoing technological breakthroughs and convergence with other initiatives and models. To this end, in 2018 the Forum convened a Pilot Group to develop the first pilot of the KTDI concept. Pilot Group members include:

- The World Economic Forum
- The Governments of the Netherlands and Canada, including their respective departments and agencies
- The airlines KLM Royal Dutch Airlines and Air Canada
- The airports Amsterdam Airport Schiphol, Greater Toronto Airport Authority and Aéroports de Montréal
- Accenture
- Vision Box
- Idemia

**Table 1:** KTDI concept paper recommendations

| | |
|---|---|
| 1. **Act now** | – Pilot and develop iteratively<br>– Ensure inclusivity to drive scalability<br>– Continuously monitor new developments |
| 2. **Build momentum** | – Focus on traveller-centric requirements to accelerate adoption<br>– Explore new business models<br>– Pilot new use case scenarios to build communities of trust and connect them |
| 3. **Sustain a supportive policy framework** | – Uphold standards and recommended practices<br>– Develop advanced risk profiling to expedite the security process<br>– Prioritize privacy and security |

The Pilot Group is working collaboratively to test critical elements of the KTDI concept (i.e. governance, privacy and security frameworks and the technology) in a cross-border, real-life environment.

The pilot's lessons will help mature the KTDI concept and assess the potential for its use by additional stakeholders, such as other governments, airlines and airports as well as hotels, car rental companies, and other players in the travel and tourism sector. In future iterations of the KTDI concept, multiple pilots can be run – potentially in parallel and with different technologies – to enrich its outcome and scalability.

## 3.2 Purpose and scope

From the outset, the KTDI concept was designed with global interoperability as a core design principle, with a view to maximizing the use of open source technologies, open standards and industry best practices (e.g. for security and privacy) and avoiding vendor lock-in. This paper presents a first step in efforts to continue building upon the recommendations outlined in the concept paper and to promote increased multistakeholder collaboration and dialogue on the path towards global interoperability.

Moreover, since 2018, the International Air Transport Association (IATA) has advanced its learnings on the One ID concept, and the International Civil Aviation Organization (ICAO), which is responsible for setting international standards for aviation, including passport issuance, has been developing specifications for digital travel credentials. Through close observance of and engagement with these organizations, the KTDI concept continues to evolve, such that this guidance document aims to contribute to ongoing discussions for the development, use and exchange of digital travel credentials and interoperability.

This White Paper catalogues the most important and relevant standards, technologies, specifications and best practices that have been leveraged to build the KTDI solution. Some of the standards and specifications listed in this paper come from various working groups aligned with different organizations and may change over time. That said, these working groups often have a similar membership and many groups are making efforts to collaborate. Care should be taken to evaluate each standard and specification, and identify any areas that are not complementary.

Further information on the KTDI concept is available from the KTDI website[2] and concept report.

## 3.3 KTDI principles and core technologies

The KTDI concept was designed to adhere to the values and principles of decentralized identity, including ownership and control of identity attributes, privacy and disintermediation. The core enabling technologies selected for KTDI support these values and are currently being tested by the Pilot Group.

Decentralized identity is commonly referred to as self-sovereign identity (SSI), a term used to describe "the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities".[3] Although it is an industry-accepted term (also adopted by the European Union,[4] among others), some maintain that *self-managed identity* is a more appropriate term because a self-issued identity claim has little value to many relying parties. In the KTDI concept, the core verifiable claim that will be used by travellers is based on a government-issued credential derived from the passport. As such, for the purposes of this document, SSI refers to a decentralized identity that is self-managed and that is based on a government-issued verifiable credential.

As explained in Section 6 in more detail, a blockchain-based platform was selected as the key enabling technology for the KTDI concept and pilot with the goal of better understanding integration requirements between multiple stakeholders in this industry. However, decentralized identity management solutions could be non-blockchain based and other approaches could also be used.

As emerging decentralized identity strategies and technologies continue to develop, it is important to consider alternative or complementary technologies and approaches that may also support KTDI's core principles. The expected advantages and disadvantages of every technological choice must be thoroughly assessed on a use case basis, considering legal, national security, certification, risk and other requirements.

Ongoing work in decentralized identity management, including decentralized public key infrastructure (DPKI), custodianship and zero-knowledge proofs (ZKP), must be assessed and potentially tested in future pilots. Different technology choices may result in diverse trust frameworks that could be linked to co-exist as part of an inter-federation model, thereby meeting the varying yet overlapping requirements of different stakeholders. Further collaboration is needed to explore complementary approaches for SSI to allow for maximum identity reuse and global acceptance.

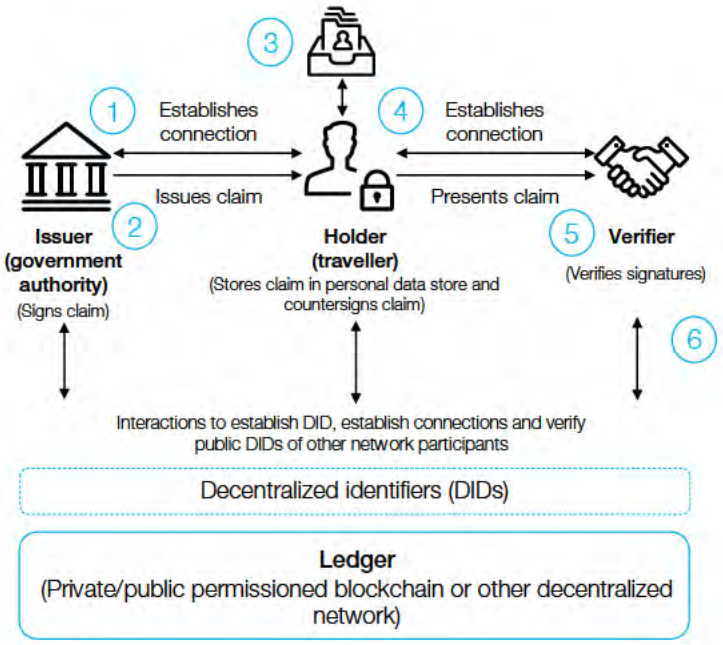
# 4. KTDI: Solution overview

The KTDI solution is built upon the decentralized identity model (described in Figure 1), leveraging the emerging World Wide Web Consortium (W3C) verifiable credentials (VC) and decentralized identifier (DID) standards. As its name suggests, W3C is the main standards-setting body for the World Wide Web and many of the contributors are also members of the Decentralized Identity Foundation, which focuses "on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability between all participants".[5] Its work on VCs and DIDs aims to mature the emerging standards to securely express, exchange and verify claims (i.e. credentials, attestations) via the web.

The KTDI concept is based on a decentralized identity model, allowing travellers to manage digital identity attestations, consisting of verifiable claims conforming to W3C standards and recommendations for the purposes of cross-border travel.

Identity attributes are attested to and provided by issuing authorities (i.e. passport number, bank details) so that the individual may share some, all or even none of their attested identity information through selective disclosure or ZKP. An issuing authority may also revoke a VC that it had previously issued by updating the blockchain-based cryptographic accumulator accordingly.

**Figure 1:** Decentralized identity model




Source: Accenture and World Economic Forum

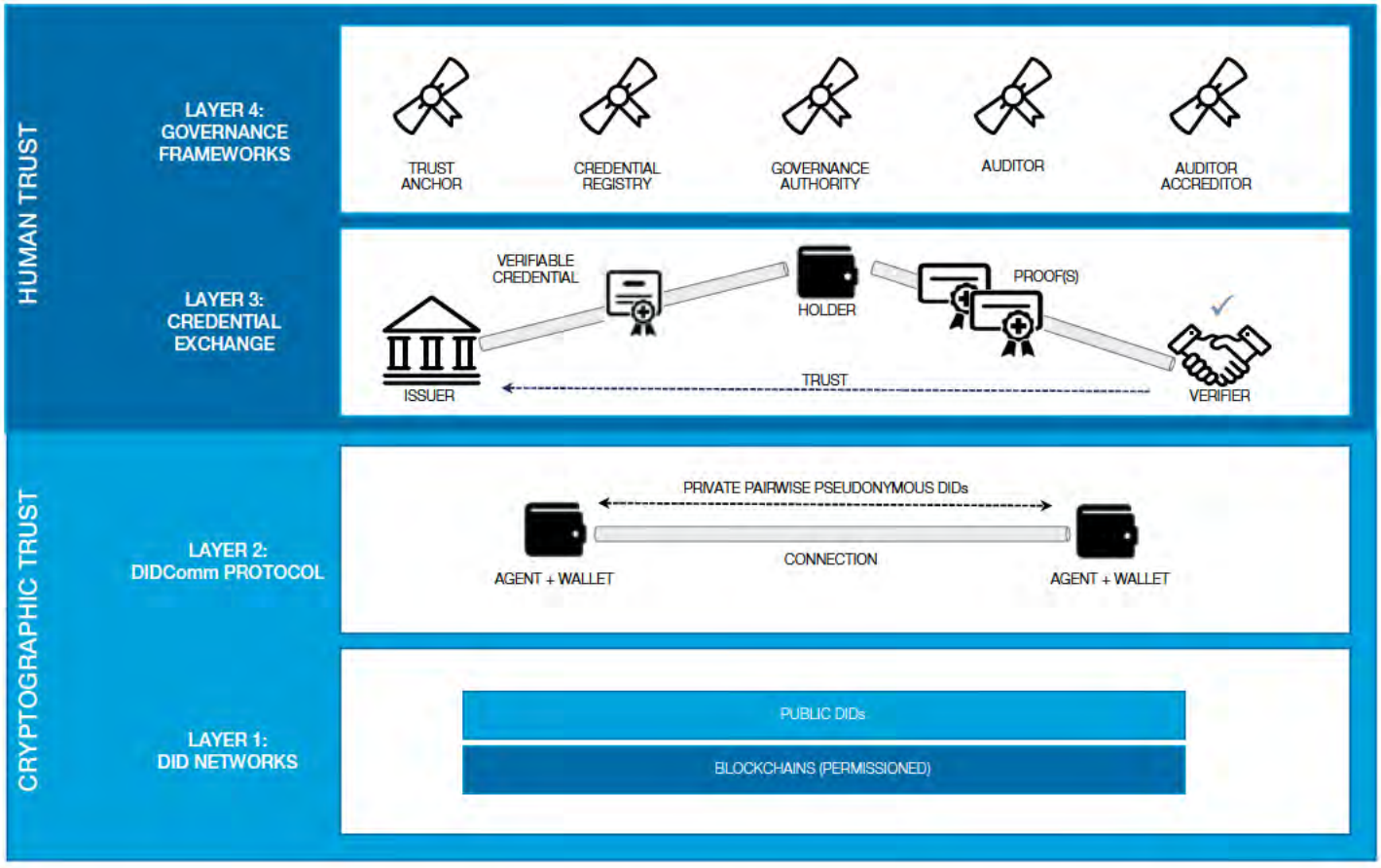
1. **Issuer** and **holder** establish a connection.
2. **Issuer** provides a claim on an identity credential to the identity **holder** (issuer signs the credential with the key associated with the registered DID of the issuer).
3. **Holder** maintains the credential in their private wallet until it must be shared to cross borders or board a flight.
4. **Holder** establishes a connection with the **verifier** (or reliant party) to enable the secure sharing of the identity credentials held in the holder's wallet.
5. **Holder** presents the claim on the identity credential to the **verifier** and countersigns the claim with the key associated with their private DID.
6. **Verifier** looks up the registered DIDs of the **issuer** to resolve DID documents and verify the public key of the **issuer** (the issuer DID resolution is to validate the claim was issued by the issuing authority), and determines if the VC has been revoked through the blockchain-based accumulator.

This is a complex process not covered in this document but included in Hyperledger Indy documentation.[6]

The decentralized identity model (Figure 1) can be broken down into four layers between **two categories of trust: human and cryptographic**, as detailed in Figure 2. This paper covers only layers 1-3, which focus on technology. The governance framework in layer 4 is business focused and is not covered herein. Work is continuing to further define and develop appropriate governance frameworks for the KTDI concept and will be discussed in future reports.

The high-level functionality of each layer in the SSI architecture shown in Figure 2 is described in Table 2. The capabilities within each layer and relevant standards (draft or approved), open-specifications and related industry guidance are described in Section 5.

**Figure 2:** Four-layer self-sovereign identity model



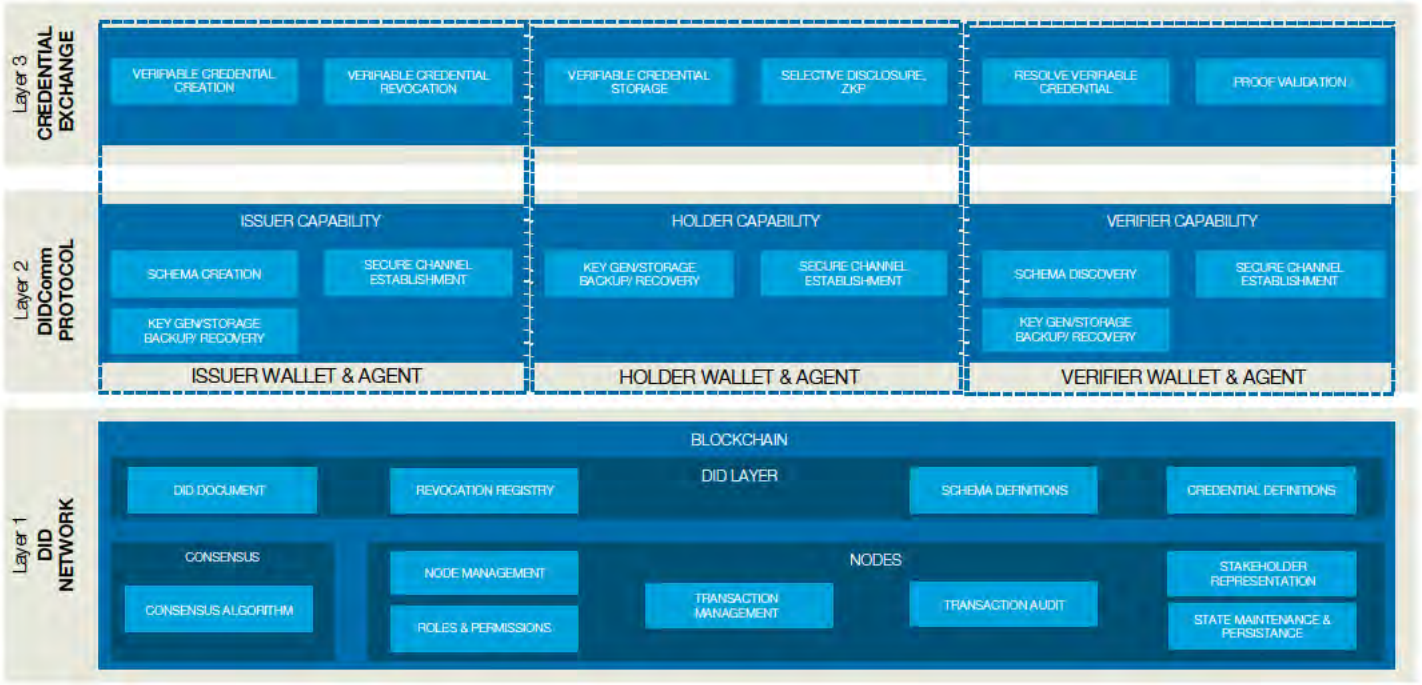

Source: Adapted from Reed, Drummond, "Hyperledger Aries: The Next Major Step Towards Interoperable SSI", Evernym, 30 May 2019, https://www.evernym.com/blog/hyperledger-aries

**Table 2:** Four-layer self-sovereign identity architecture detail

| Layer | Definition |
|---|---|
| *Layer 1*<br>*DID Networks*<br>*(SSI Ledger)* | The bottom layer – the foundation of SSI infrastructure – is the SSI ledger layer where public identities, which are usually organizational rather than individual identities, are rooted in public DIDs. Public identities need to be rooted at this layer by issuers who need their credentials to be publicly verifiable. To protect the privacy of individuals, the KTDI concept does not support storing any private DIDs in layer 1. The SSI ledger also includes publicly available schemas, credential definitions and accumulators (aka, Revocation Registries). Sovrin Ledger Layer Roles are described in Appendix E of the Sovrin Glossary;[7] these roles are generic and not Sovrin specific. |
| *Wallets and Agents, covering:* | An identity wallet is a digital container for data needed to control identity information and is typically realized in a cloud and/or mobile application. A common framework for wallets is Hyperledger Indy (now Aires), which aims to be a ledger agnostic agent framework. It includes an agent-to-agent messaging protocol, called DID Communication (DIDComm), which allows agents to talk to each other with encrypted messages.[8] |
| – *Layer 2*<br>*DID Communication (DIDComm) Protocol (Agent-to-Agent)* | From both a privacy and scalability standpoint, it is critical that each entity (natural person, legal entity, thing or process) be able to form connections, maintain wallets and exchange credentials over direct, off-ledger, peer-to-peer relationships. This is the job of the DIDComm protocol (or Agent-to-Agent) layer. Agent-to-Agent Protocol Layer Roles are described in Appendix F of the Sovrin Glossary; these roles are generic and are not Sovrin specific. |
| – *Layer 3*<br>*Credential Exchange* | Taken together, layer 1 (DID networks) and layer 2 (the DIDComm protocol) only establish cryptographic trust – trust that a set of machines (man-made things) operating cryptographic algorithms will behave as expected. They do not establish human trust – trust that a set of people (individuals and/or organizations) will behave as expected. This is the job of the next two layers (credential exchange and governance frameworks).<br><br>The credential exchange layer is where issuers issue credentials (describing subjects) to holders (which may or may not be the subject). Holders then act as provers to present proofs of those credentials to verifiers, who use the ledger to look up the issuer's DID to get the public key needed to verify the proof. Proofs, in turn, provide a means for the verifier to determine that the VC has not been altered.[9] Credential Exchange Layer Roles are described in more detail in Appendix G of the Sovrin Glossary.<br><br>These credentials are core to the DID standards and must be accepted by the parties involved in the ecosystem as is the case for KTDI where, for the pilot, each stakeholder had a say in defining the VCs they will issue along with which proofs are required for verification. This challenge is reflected in a recent EU report: *"Whereas trust in paper-based or digital files/ records comes from accepting mutually and internationally recognised bodies (certification organisations, governments, other members of the network), the key for international data flows is enabled by trusted mechanisms of participants gaining membership of or partnership to an ecosystem, which would allow them to verify and authenticate the person or documents/ records behind the actions, records and documents."*[10] |
| *Layer 4*<br>*Governance Frameworks* | Establishing human trust in any widely-used credential (e.g. KTDI, ePassport) requires developing business and legal agreements between issuers – typically a group of organizations, such as credit unions, banks, stores, healthcare providers, universities or governments. As stated previously, this layer is not covered in this document. The governance framework, where stakeholders can deliberate trust frameworks, regulatory constraints, capabilities, schemas and the like for KTDI, has not yet been established and will be covered in a future report. |
| *IT Infrastructure and Supporting Technologies* | This layer is not depicted in the high-level SSI architecture shown in Figure 2, but it refers to the IT infrastructure required to support the application, communications and security layers both functionally and non-functionally. |

These layers can be broken down into the corresponding capabilities, as shown in Figure 3.

**Figure 3:** Relevant capabilities of the four-layer self-sovereign identity model




Source: Accenture and World Economic Forum

While the DID networks (layer 1), including blockchain and DID layers, can be broken down cleanly, the DIDComm protocol (layer 2) and credential exchange (layer 3) are intertwined with the concept of digital identity wallets and agents.

Not shown, but underpinning these components and capabilities, is IT infrastructure and supporting technologies, as with any technology solution. Each of the capabilities depicted in Figure 3 are described in tables in Section 5.

# 5. KTDI solution components: Capabilities and standards

As shown in Table 2, the core of the solution can be broken down into:

- Layer 1: DID networks
- Wallets and agents, covering:
  - Layer 2: DIDComm protocol
  - Layer 3: Credential exchange
- IT infrastructure and supporting technologies.

This section details the capabilities within each layer as well as relevant standards (draft or approved), open-specifications and related industry guidance.

The wallet and agent structures sit across layers 2 and 3 and provide for the peer-to-peer communications at the heart of decentralized identity. Due to their matrix nature, wallets and agents are covered in this paper in detail, with the capabilities per layer and per actor broken out specifically.

## 5.1 Layer 1: DID networks

DID networks are split into the underlying blockchain network and the decentralized identity overlay.

### 5.1.1 Blockchain network

The capabilities required of the underlying ledger are like any other decentralized ledger technology platform. While the list in Table 3 is non-exhaustive, it provides an outline of the capabilities expected.

These capabilities guided the search for the standards that were relevant to this implementation. The standards listed in Table 4 were accounted for and applied during the design and execution.

**Table 3:** Ledger capabilities

| No. | Capability grouping | Capability | Definition/description |
|---|---|---|---|
| 1 | Consensus | Consensus mechanism | The established protocol to maintain the shared ledger in which a transaction is cryptographically signed and chained to a previous transaction |
| 2 | Nodes | Roles and permissions | Roles at the node level that are often platform dependent but could, for example, refer to genesis nodes versus non-genesis nodes or, alternatively, nodes that participate in the consensus mechanism against those that simply observe and replicate |
| 3 | | Transaction management | The ability to orchestrate transactions but also perform more complex actions such as archiving |
| 4 | | Node management | Management and operation of the node itself, such as software updates, availability and monitoring |
| 5 | | Transaction audit | Support across the topology for a complete history of data origination and exchange, access or change across the network |
| 6 | | Stakeholder representation | Representation of a stakeholder's identity on the network in the form of a node they own (NB: a stakeholder may own a node but may not necessarily host or maintain that node) |
| 7 | | State maintenance and persistence | The ability to establish, persist and change states across the nodes/network such that data and the changes to that data are not lost |
| 8 | DID layer | DID document | A set of data that describes the DID subject, including the mechanisms, such as public keys and biometrics, that the DID subject can use to authenticate itself and prove its association with the DID (a DID document may also contain other attributes or claims describing the subject) |
| 9 | | Schema definition | A machine-readable definition of the semantics of a data structure (schemas are used to define the attributes used in one or more credential definitions) |
| 10 | | Credential definition | A machine-readable definition of the semantic structure of a credential based on one or more schemas |
| 11 | | Revocation | The act of an issuer revoking the validity of one or more verifiable claims of a verifiable credential that it had previously issued |

**Table 4:** Applicable standards

| No. | Capability grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| 1 | Decentralized identity | W3C verifiable credentials data model | 1.0 | https://www.w3.org/TR/vc-data-model/ | W3C |
| 2 | Blockchain | ISO/CD 23257.3 – Blockchain and distributed ledger technologies – Reference architecture | *Under development* | https://www.iso.org/standard/75093.html?browse=tc | ISO TC 307 Committee Draft |
| 3 | | ISO/CD TR 23245 – Blockchain and distributed ledger technologies – Security risks, threats and vulnerabilities | *Under development* | https://www.iso.org/standard/75062.html?browse=tc | ISO TC 307 JWG4 Draft Technical Report |
| 4 | | ISO/PRF TR 23244 – Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations | *Under development* | https://www.iso.org/standard/75061.html?browse=tc | ISO TC 307 JWG4 Draft Technical Report |
| 5 | | ISO/DIS 22739 – Blockchain and distributed ledger technologies – Terminology | *Under development* | https://www.iso.org/standard/73771.html?browse=tc | ISO TC 307 Draft International Standard |
| 6 | | ISO/AWI TS 23635 – Blockchain and distributed ledger technologies – Guidelines for governance | *Under development* | https://www.iso.org/standard/76480.html?browse=tc | ISO TC 307 New Project |

Notes: AWI - Approved new work item; CD - Committee draft; DIS - Draft international standard; ISO - International Organization for Standardization; PRF - Proof of new international standard; TC - Technical committee; TR - Technical report; TS - Technical specification

## 5.2 Wallets and agents

Wallets and agents provide a peer-to-peer communications protocol to enable credential exchange. The following tables outline the general capabilities with actor-specific capabilities per layer.

### 5.2.1 General

Table 5 illustrates the general capabilities required from wallets and agents across users.

Since the wallet and agent components are nascent, no specific standards can be applied to these components. The Hyperledger Foundation has several blockchain projects, each open source, that align to different applications; Hyperledger Indy (and its successor Aires) is aligned to identity applications and has built-in wallet and agent capabilities, whereas other technologies require custom code. There are, however, standards and/or specifications that could be applied to the overall IT infrastructure and related technologies, as shown in Table 6.

In addition to these standards, additional international, national and regional standards and regulations may apply to the security and privacy of the IT infrastructure and related technologies.

### 5.2.2 Issuer

In addition to the general capabilities outlined in Section 5.2.1, issuers also require additional wallet capabilities (Table 7).

**Table 5:** General wallet capabilities

| No. | Capability grouping | Capability | Definition/description |
|---|---|---|---|
| 1 | Wallet – general | Secure channel establishment | Established through a connection request with another party in the ledger ecosystem – creating a DID and a nonce (an arbitrary number that is used once in cryptographic communication) |
| 2 | | Key generation/storage/back-up/recovery | The life cycle of the set of private keys or entire wallet from creation, to storage, signing, back-up and the subsequent recovery of the set of keys |

**Table 6:** Applicable standards[a]

| No. | Standard grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| 1 | Decentralized identity | Peer DID method specification | Draft 16 | https://openssi.github.io/peer-did-method-spec/index.html | W3C |
| 2 | | Decentralized identifiers (DIDs) | 1.0 | https://www.w3.org/TR/did-core/ | W3C |
| 3 | Identity management | ISO/IEC 24760-1:2019 – A framework for identity management | 1.0 | https://www.iso.org/standard/77582.html | ISO |
| 4 | | Digital identity guidelines – 800-63 | 1.0 | https://pages.nist.gov/800-63-3/sp800-63-3.html | NIST |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Cryptography | Digital signature algorithm – RFC 8017 RSA | 2.2 | https://tools.ietf.org/html/rfc8017 | IETF |
| 6 | | Digital signature standard – FIPS 186-4 | 1.0 | https://csrc.nist.gov/publications/detail/fips/186/4/final | NIST |
| 7 | | Secure hash standard – SHS FIPS 180-4 | 1.0 | https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf | NIST |
| 8 | | Security for cryptographic modules – FIPS 140-3 | 1.0 | https://csrc.nist.gov/publications/detail/fips/140/3/final | NIST |
| 9 | Security and privacy | ISO/IEC 24745:2011 – Biometric information protection | 1.0 | https://www.iso.org/standard/52946.html | ISO |
| 10 | | Guide to protecting the confidentiality of PII – 800-122 | 1.0 | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf | NIST |
| 11 | | ISO/IEC TR 14516 – Guidelines for the use and management of trusted third-party services | 1.0 | https://www.iso.org/standard/31482.html | ISO |
| 12 | | ISO/IEC 27018:2019 – PII protection in public clouds | 1.0 | https://www.iso.org/standard/76559.html | ISO |
| 13 | | ISO/IEC 29101:2018 – Information technology – Security techniques – Privacy architecture framework | 2.0 | https://www.iso.org/standard/75293.html | ISO |
| 14 | | ISO/IEC CD 27555 – Establishing a PII deletion concept in organizations | *Under development* | https://www.iso.org/standard/71673.html | ISO |
| 15 | | RFC 8446: The transport layer security (TLS) protocol version 1.3 (1.2) | 1.3 (1.2) | https://tools.ietf.org/html/rfc8446 (https://tools.ietf.org/html/rfc5246) | IETF |
| 16 | | ISO/IEC 29100:2011 – Security techniques – Privacy framework | 1.0 | https://www.iso.org/standard/45123.html | ISO |
| 17 | | Mobile application security verification standard | 1.2 | https://mobile-security.gitbook.io/masvs/ | OWASP |
| 18 | | Vetting the security of mobile applications – NISTIR 8136 | 1.0 | https://csrc.nist.rip/library/NIST%20IR%208136.pdf | NIST |
| 19 | | W3C verifiable credentials data model | 1.0 | https://www.w3.org/TR/vc-data-model/ | W3C |
| 20 | | ISO/IEC 29115:2013 – Entity authentication assurance framework | 1.0 | https://www.iso.org/standard/45138.html | ISO |
| 21 | | ISO/IEC DIS 27551 – Attribute-based unlinkable entity authentication | *Under development* | https://www.iso.org/standard/72018.html | ISO |
| 22 | | ISO/IEC TS 29003 – Identity proofing | 1.0 | https://www.iso.org/standard/62290.html | ISO |
| 23 | | ISO/IEC 27701 – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines | 2019 | https://www.iso.org/standard/71670.html | ISO |
| 24 | Key management | ISO/IEC 11770-2 – Key management | 2.0 | https://www.iso.org/standard/73207.html | ISO |
| 25 | | ISO/IEC 9594-8 – Public-key infrastructure | 1.0 | https://www.iso.org/standard/72557.html | ISO |

[a] Two TLS specifications have been included as many organizations have not fully migrated from TLS v1.2 yet.
Notes: CD - Committee draft; DIS - Draft international standard; FIPS - Federal Information Processing Standard; IEC - International Electrotechnical Commission; IETF - Internet Engineering Task Force; ISO - International Organization for Standardization; NIST - National Institute of Standards and Technology (US); NISTIR - National Institute of Standards and Technology interagency or internal report; OWASP - Open Web Application Security Project; PII - Personally identifiable information; RFC - Request for comments; SHS - Secure Hash Standard; TR - Technical report; TS - Technical specification

**Table 7:** Additional issuer wallet capabilities

| No. | Capability grouping | Capability | Definition/description |
|---|---|---|---|
| 1 | DIDComm protocol | Schema creation | The creation of a basic semantic structure that describes the list of attributes that one particular credential can contain |
| 2 | Credential exchange | Verifiable credential creation | The creation of a credential that includes proof from the issuer |
| 3 | | Verifiable credential revocation | The ability of an issuer to revoke a credential that it had previously issued |

These capabilities are well defined in standards, specifications and recommendations (Table 8).

**Table 8:** Issuer applicable standards

| No. | Standard grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| 1 | Decentralized identity | Overview of DIDComm | N/A | https://github.com/decentralized-identity/DIDComm-js/blob/master/docs/README.md | W3C |
| 2 | | W3C verifiable credentials data model | 1.0 | https://www.w3.org/TR/vc-data-model/ | W3C |
| 3 | Identity management | ICAO Doc 9303 – Machine readable travel documents: Part 10 | 7th Edition, 2015 | https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf | ICAO |
| 4 | | ISO/IEC 19794-5 – Biometric data interchange formats – Part 5: Face image data | 2011 | https://www.iso.org/standard/50867.html | ISO |
| 5 | | ISO/IEC TR 29794-5 – Biometric sample quality – Part 5: Face image data | 2010 | https://www.iso.org/standard/50912.html | ISO |
| 6 | | ISO/IEC 39794-5 – Extensible biometric data interchange formats – Part 5: Face image data | *Under development* | https://www.iso.org/standard/72156.html | ISO |
| 7 | | Digital identity guidelines – 800-63 | 1.0 | https://pages.nist.gov/800-63-3/sp800-63-3.html | NIST |
| 8 | | ISO/IEC 24760-1:2019 – A framework for identity management | 1.0 | https://www.iso.org/standard/77582.html | ISO |
| 9 | | Decentralized identifiers (DIDs) | 1.0 | https://www.w3.org/TR/did-core/ | W3C |

| | | | | | |
|---|---|---|---|---|---|
| *10* | Security and privacy | ISO/IEC 24745:2011 – Biometric information protection | 1.0 | https://www.iso.org/standard/52946.html | ISO |
| *11* | | Guide to protecting the confidentiality of PII – 800-122 | 1.0 | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf | NIST |
| *12* | | ISO/IEC TR 14516 – Guidelines for the use and management of trusted third-party services | 1.0 | https://www.iso.org/standard/31482.html | ISO |
| *13* | | ISO/IEC 27018:2019 – PII protection in public clouds | 1.0 | https://www.iso.org/standard/76559.html | ISO |
| *14* | | ISO/IEC 29101:2018 – Information technology – Security techniques – Privacy architecture framework | 2.0 | https://www.iso.org/standard/75293.html | ISO |
| *15* | | ISO/IEC CD 27555 – Establishing a PII deletion concept in organizations | *Under development* | https://www.iso.org/standard/71673.html | ISO |
| *16* | | ISO/IEC 29100:2011 – Security techniques – Privacy framework | 1.0 | https://www.iso.org/standard/45123.html | ISO |
| *17* | | Vetting the security of mobile applications – NISTIR 8136 | 1.0 | https://csrc.nist.rip/library/NIST%20IR%208136.pdf | NIST |
| *18* | | RFC 8446: The transport layer security (TLS) protocol version 1.3 | 1.3 | https://tools.ietf.org/html/rfc8446 | IETF |
| *19* | | ISO/IEC 29115:2013 – Entity authentication assurance framework | 1.0 | https://www.iso.org/standard/45138.html | ISO |
| *20* | | ISO/IEC DIS 27551 – Attribute-based unlinkable entity authentication | *Under development* | https://www.iso.org/standard/72018.html | ISO |
| *21* | | ISO/IEC TS 29003 – Identity proofing | 1.0 | https://www.iso.org/standard/62290.html | ISO |
| *22* | | ISO/IEC 27701 – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines | 1.0 | https://www.iso.org/standard/71670.html | ISO |
| *23* | Key management | ISO/IEC 11770-2 – Key management | 2.0 | https://www.iso.org/standard/73207.html | ISO |
| *24* | | ISO/IEC 9594-8 – Public-key infrastructure | 1.0 | https://www.iso.org/standard/72557.html | ISO |
| *25* | Cryptography | Security for cryptographic modules – FIPS 140-3 | 1.0 | https://csrc.nist.gov/publications/detail/fips/140/3/final | NIST |

Notes: CD - Committee draft; DIS - Draft international standard; FIPS - Federal Information Processing Standard; IEC - International Electrotechnical Commission; IETF - Internet Engineering Task Force; ISO - International Organization for Standardization; NIST - National Institute of Standards and Technology (US); NISTIR - National Institute of Standards and Technology interagency or internal report; PII - Personally identifiable information; RFC - Request for comments; TR - Technical report; TS - Technical specification

#### 5.2.2.1 Identity attestations

Issuers may provision VCs based on schemas already defined or that they define themselves, based on (an) established governance model(s). For cross-border travel, it is assumed that the VCs would encapsulate a government-issued identity. An example of an internationally defined identity schema, from the International Civil Aviation Organization (ICAO),[11] is provided in Figure 4 for reference.

**Figure 4:** ICAO Doc 9303 data group 1 (DG1)

| | | | |
|---|---|---|---|
| Required | Issuing state or organization data | DG1 | Document type |
| | | | Issuing state or organization data |
| | | | Name (of holder) |
| | | | Document number |
| | | | Check digit - doc number |
| | | | Nationality |
| | | | Date of birth |
| | | | Check digit - DOB |
| | | | Sex |
| | | | Data of expiry or valid until date |
| | | | Check digit DOE/VUD |
| | | | Optional data |
| | | | Check digit - optional data field |
| | | | Composite check digit |

Source: ICAO, "Doc 9303: Machine Readable Travel Documents", Seventh Edition, p.4

### 5.2.3 Holder

In addition to the general capabilities in Section 5.2.1, holders also require additional wallet capabilities (Table 9).

**Table 9:** Additional holder wallet capabilities

| No. | Capability grouping | Capability | Definition/description |
|---|---|---|---|
| *1* | Credential exchange | Verifiable credential storage | Storage of a VC within the wallet, presented to the verifier upon receiving a proof request |
| *2* | | Selective disclosure, zero-knowledge proofs (ZKPs) | A privacy-by-design cryptographic technique that reveals only a subset of the data described in the VC (One or more verifiable claims from one or more VCs may be shared through selective disclosure. ZKPs are returned when a request is made for information and a proof that contains no personally identifiable information (PII) will suffice; for example, the proof confirms that the subject is over 21 without revealing birthdate or age. ZKPs may reveal identifying information, so adequate legal/privacy assessments must be considered.) |

As with the issuer capabilities, these are well defined in standard(s) and specifications (Table 10).

**Table 10:** Holder applicable standards

| No. | Standard grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| *1* | Decentralized identity | W3C verifiable credentials data model | 1.0 | https://www.w3.org/TR/vc-data-model/ | W3C |
| *2* | Security and privacy | ISO/IEC 9798-5:2009 – Information technology – Security techniques – Entity authentication: mechanisms using zero-knowledge techniques | 1.0 | https://www.iso.org/standard/50456.html | ISO |

Notes: IEC - International Electrotechnical Commission; ISO - International Organization for Standardization

### 5.2.4 Verifier

In addition to the general capabilities in Section 5.2.1, verifiers also require additional wallet capabilities (Table 11).

**Table 11:** Additional verifier wallet capabilities

| No. | Capability grouping | Capability | Definition/description |
|---|---|---|---|
| *1* | DIDComm protocol | Schema discovery | A credential definition that associates an issuer and their public issuance keys with a particular schema and revocation strategy (The credential definition also specifies the signature scheme used by the issuer, for each attribute in the schema, and references the schema for the credential. Credential definitions are published on the ledger.) |
| *2* | Credential exchange | Resolve verifiable credentials | The ability to receive and process a VC provided by the prover to the verifier, including the ability to resolve the DID documents associated to the VCs |
| *3* | | Proof of validation | Verifier validation of the proof to check that:<br>– It satisfies the request from the verifier<br>– Integrity is achieved/maintained<br>– The digital signature(s) of the issuer(s) of the attestation(s) is (are) present and correct<br>– The attestations contained within the proof have not been revoked. |

As with the issuer capabilities, these are well defined in standard(s) and specifications (Table 12).

**Table 12:** Verifier applicable standards

| No. | Standard grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| *1* | Decentralized identity | W3C verifiable credentials data model | 1.0 | https://www.w3.org/TR/vc-data-model/ | W3C |
| *2* | Security and privacy | ISO/IEC 9798-5:2009 – Information technology – Security techniques – Entity authentication: mechanisms using zero-knowledge techniques | 1.0 | https://www.iso.org/standard/50456.html | ISO |

Notes: IEC - International Electrotechnical Commission; ISO - International Organization for Standardization

## 5.3 IT Infrastructure and supporting technologies

As mentioned in the previous section, as with any other technology, the solution requires underlying infrastructure. As such, only the applicable standards (not the components and capabilities) are listed in Table 13, all of which are well established.

In addition to these global standards, additional international, national and regional standards and regulations may apply.

**Table 13:** Applicable standards

| No. | Standard grouping | Standard name | Version | Link | Standards body |
|---|---|---|---|---|---|
| *1* | Security and privacy | ISO/IEC 27001 – Information security management | 2.0 | https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en | ISO |
| *2* | | ISO/IEC TR 14516 – Guidelines for the use and management of trusted third-party services | 1.0 | https://www.iso.org/standard/31482.html | ISO |

Notes: IEC - International Electrotechnical Commission; ISO - International Organization for Standardization; TR - Technical report

# 6. Pilot technology

As previously mentioned, the KTDI pilot is still under implementation and therefore the specific standards and open specifications that have been leveraged may be updated or changed during the course of the pilot. However, the technology platform has been chosen.

Hyperledger Indy[12] was selected as the decentralized identity platform for the KTDI pilot solution. Indy is purpose-built for decentralized identity, providing tools, libraries and reusable components to create and use independent digital identities rooted by blockchains so they are interoperable across administrative domains, applications and any other “silo”.

Hyperledger Indy meets the following functional and non-functional programme requirements:

- Identity focused: it has pre-built identity-related agents and libraries
- Standards focused: it is not a standard, but it aims to align to and use industry accepted standards
- Open source
- Stand-alone: it does not require membership in a particular blockchain network
- Alignment with a private, permissioned blockchain network model
- DID-focused logic
- Scalable.

## 6.1 Technology developments

It should be noted that some Hyperledger Indy components are being migrated to the Hyperledger Aries and Ursa projects to modularize solution components to allow for more tailored solutions and for individual components to mature at different rates. Hyperledger Aries will provide infrastructure for blockchain-rooted, peer-to-peer interactions. It includes a shared cryptographic wallet (the secure storage technology, not the user interface) for blockchain clients as well as a communications protocol for off-ledger interaction between those clients.

Hyperledger Aires uses the cryptographic support provided by Hyperledger Ursa to provide secure secret management and decentralized key management functionality. Hyperledger Ursa is a shared cryptographic library that enables people and projects to avoid duplicating other cryptographic work, potentially increasing security in the process. The library would be an opt-in repository for projects (and, potentially contributors) to place and use cryptography.

Hyperledger Indy will continue supporting Aries and Ursa as portions of the Indy libraries are migrated into Aries core libraries, and Indy-Crypto is being replaced with Ursa in Indy Node. At this time, there is no reason to migrate the KTDI pilot solution away from Hyperledger Indy.

# 7. Conclusion

This White Paper outlines the ambition for KTDI to provide the foundations for a globally accepted decentralized identity ecosystem. Further development and wider adoption depend on maximizing data exchange interoperability and federated trust, for which the best use of international standards (existing and emerging), open specifications and industry best practices are essential. Success will rest upon cooperation between world governments, regulators, the aviation industry, technology providers and other players to establish global standards and specifications for compliance by all stakeholders.

The KTDI concept is not tied to a particular product, is modular, scalable and based on emerging and existing international standards. The World Economic Forum will continue to engage additional stakeholders to launch further pilots and explore new use cases, geographies and technology approaches. Decision-makers may then combine the lessons learned from the pilots to provide the optimum way ahead that maximizes flexibility and benefits, without constraining organizations or nations to specific solutions.

Organizations seeking to test or develop the KTDI concept or complementary solutions should become familiar with the core concepts of decentralized identity as well as the relevant standards and technology approaches available. Stakeholders should also identify potential use cases, their scope, and how the pilot would align with their long-term vision. The development of additional pilots will require addressing practical considerations, including legal, cybersecurity, privacy and national security requirements. National and international assurance models are still emerging for SSI solutions based on blockchain technologies, and to date no countries have adopted such a model for cross-border travel.

The KTDI concept shows great potential for use beyond the travel industry, including applications in healthcare, education, banking, humanitarian aid and other sectors. It will be critical to leverage network effects by earning the trust of users, engaging more government entities and crowding in more private parties to build the concept, continue to broaden the horizon and be at the forefront of disruptive changes.

The Forum and its partners will also continue to conceptualize the appropriate governance frameworks that would promote trust between ecosystem players and establish the premises to maximize interoperability and global adoption in the travel sector and beyond. As some of the standards and specifications catalogued in this White Paper continue to evolve, it is critical to monitor developments as well as new technology approaches and innovations that may be leveraged. Ongoing collaboration with international organizations like ICAO and IATA to develop and use digital travel credentials is also crucial to ensure complementarity towards a common goal.

As the leading global platform for public-private cooperation, the Forum is committed to strengthening the kind of multistakeholder collaboration needed to achieve interoperability in the new identity paradigm that continues to unfold. The Forum invites interested stakeholders to provide feedback and proposals for new pilots or approaches to enhance or complement the KTDI concept and further this goal.

# 8. Contributors

The World Economic Forum acknowledges the valuable contributions to this White Paper of our community of stakeholders collaborating on the KTDI concept and pilot.

# 9. Endnotes


1. World Economic Forum, *The Known Traveller: Unlocking the potential of digital identity for secure and seamless travel*, 2018, http://www3.weforum.org/docs/WEF_The_Known_Traveller_Digital_Identity_Concept.pdf.
2. World Economic Forum, Known Traveller Digital Identity [website], 2019, www.ktdi.org.
3. Sovrin, "What is self-sovereign Identity?", 6 December 2018, https://sovrin.org/faq/what-is-self-sovereign-identity.
4. European Economic and Social Committee, "European Self Sovereign identity framework", 25 June 2019, https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework.
5. Decentralized Identity Foundation, Our Focus [website], https://identity.foundation/#about.
6. Hardman, Daniel, "Credential Revocation", Hyperledger Indy, 2018, https://hyperledger-indy.readthedocs.io/projects/hipe/en/latest/text/0011-cred-revocation/README.html.
7. Sovrin, "Sovrin Glossary V3", in *Sovrin Governance Framework*, 4 December 2019, https://docs.google.com/document/d/1gfIz5TT0cNp2kxGMLFXr19x1uoZsruUe_0gIHst2fZ8/edit?pli=1#heading=h.851bm05lgtfu.
8. GitHub, "Overview of DIDComm", 11 August 2019, https://github.com/decentralized-identity/DIDComm-js/blob/master/docs/README.md.
9. W3C, "4.7 Proofs (Signatures)", in *Verifiable Credentials Data Model 1.0*, 19 November 2019, https://www.w3.org/TR/vc-data-model/#proofs-signatures.
10. European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), *Distributed Ledger Technologies and Blockchain: Perspectives for eu-LISA and the Large-scale IT Systems, Research and Technology Monitoring Report*, 2019, p. 21, https://www.eulisa.europa.eu/Publications/Reports/DLTs%20and%20blockchain%20report.%20Dec%202019.pdf#search=Perspectives%20for%20eu%2DLISA%20and%20the%20Large%2Dscale%20IT%20Systems.
11. International Civil Aviation Organization (ICAO), "Doc 9303: Machine Readable Travel Documents", Seventh Edition, 2015, https://www.icao.int/publications/Documents/9303_p10_cons_en.pdf.
12. Hyperledger, "Hyperledger Indy", Projects, https://www.hyperledger.org/projects/hyperledger-indy.

WORLD ECONOMIC FORUM

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.:
Fax:

@weforum.org
www.weforum.org