digiyatra

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

DSCI
PROMOTING DATA PROTECTION

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Self-Sovereign Identity and the Future of Digital Trust

From India to the World

Self-Sovereign Identity and the Future of Digital Trust

From India to the World

Foreword

Vinayak Godse
CEO- Data Security Council of India

The question of identity is, at its heart, who gets to participate. The systems we build to verify who someone is end up shaping what they can access, what they can own, and how visible they are to power. That is why I have never been able to think of digital identity as a purely technical subject. It is a conversation about the architecture of citizenship in a networked age, and over the next decade, it will quietly determine the competitive position of economies, the resilience of institutions, and the terms on which citizens engage with both.

For close to two decades, our answer to the identity question has been to build larger and more capable databases. The reasoning was straightforward enough at the time: more data, held more centrally, would produce more reliable verification. We have run that experiment long enough to see its limits. The institutions that hold identity data carry costs and liabilities that have begun to outweigh the value they extract from it, and the people whose data sits in these systems have the least say over how it moves. The model is not only inefficient. It is becoming a strategic vulnerability for individuals, for firms, and for states.

Self-Sovereign Identity is not a tweak to that model. It is a different starting point. It begins from the idea that verification does not have to mean accumulation. Verifiable Credentials make the idea concrete. A credential issued by a trusted authority can reside on a citizen's own device, be shared selectively, and be verified cryptographically by any party in the world without that party ever having to contact the issuer. A passenger can prove she is over eighteen without revealing her date of birth. A graduate can prove a qualification without handing over a full transcript. A traveller can prove nationality without surrendering a passport. The standards behind all of this, grounded in W3C Verifiable Credentials and Decentralised Identifiers and complemented by ISO mDL, are now stable. The harder work, and the work that will separate countries that lead from countries that follow, is the institutional and governance scaffolding that has to grow around them.

Interoperability is where that work matters most, and where I think it is most often underestimated. A credential that cannot cross a border, a sector, or a wallet is not really a credential. It is a convenience. The strategic value of verifiable credentials only compounds when an issuer in one jurisdiction is recognised by a verifier in another, when a credential built for aviation can be reused in hospitality, and when a wallet from one country can hold attestations from institutions in dozens of others. Without that, we risk building a generation of digital identity systems that are technically modern and structurally fragmented, which is the worst of both worlds. Travel is the clearest illustration of what is at stake. A passenger flying from Delhi to Frankfurt to São Paulo today moves through three regulatory regimes and three institutional databases that will hold copies of her information long after she has landed. Every one of those touchpoints could be replaced by a single credential held on her device, shared selectively, and verified without anyone retaining her data beyond the journey itself. The country that helps design how this works internationally will set the terms for everyone else.

India comes to this moment from a distinctive place. Aadhaar, UPI, DigiLocker, and the Account Aggregator framework have shown what public digital infrastructure can do when it is designed as a common good rather than a closed asset. Digi Yatra has carried that lineage forward into verifiable credentials at a population scale, and in doing so, it has given India something that is genuinely rare in international standards conversations: operational evidence. Most countries are still arguing about what should work. We can speak to what does. That asymmetry is a strategic asset, and it has a shelf life.

The question is what we choose to do with it. The decisions taken at eIDAS 2.0, ICAO, the OpenID Foundation, and Trust Over IP over the next eighteen months will shape how credentials move across borders for the next decade. We can engage with those processes as a contributor whose experience carries weight, or we can wait and adapt to frameworks designed without us. I know which of the two is harder, and I know which is the only one consistent with the ambitions we have set for ourselves. The same logic applies at home. Verifiable credentials will only deliver on their promise if the regulators governing banking, telecommunications, healthcare, and education recognise them, reach citizens who are not early adopters, and treat privacy and inclusion as design constraints rather than aspirations.

My thanks go to Suresh Khadakbhavi and the Digi Yatra Foundation for a substantive partnership at every stage of this work, and to the Ministry of Electronics and Information Technology for its continued support. This report is offered in that spirit: a careful attempt to map where the world stands, where India stands within it, and what the next steps need to look like.

Foreword

Suresh Khadakbhavi
CEO - Digi Yatra Foundation

The Data Security Council of India (DSCI) and Digi Yatra Foundation have partnered to produce this pioneering report on Self Sovereign Identity and the Future of Digital Trust: From India to the World. On 16 April 2026 we will launch it in New Delhi, sharing insights from some of the world's most ambitious digital identity initiatives. I am honoured, as CEO of the Digi Yatra Foundation, to contribute this foreword. Our intent is to celebrate what has been achieved, outline why digital trust matters and offer a forward looking vision for how India can help shape the global identity landscape.

Digital identity has rapidly evolved from fragmented credentials to standards-based, interoperable frameworks. Global efforts, from W3C Verifiable Credentials and Decentralised Identifiers to eIDAS 2.0, ICAO's Digital Travel Credential, and IATA's One ID, underscore a shared direction - trust must be built into architecture, not added later.

India's digital public infrastructure demonstrates this at scale. Aadhaar, DigiLocker, and UPI have shown how identity, data exchange, and payments can work seamlessly while remaining inclusive and consent-driven. The next frontier lies in extending this foundation into interoperable, self-sovereign identity ecosystems.

Digi Yatra represents one of the most advanced real-world implementations of this vision. Built on global standards, it enables a privacy-first, consent-based travel experience where credentials are held by the user, not centrally stored. With deployment across multiple airports and

millions of users, it has demonstrated that efficiency and privacy can coexist, reducing processing times while strengthening trust.

Importantly, this model is not limited to aviation. The same verifiable credential framework can extend to hospitality, mobility, education, and beyond, reducing duplication, enhancing compliance, and giving individuals greater control over their data. Early deployments beyond airports already signal this transition.

This report outlines a clear path forward - strengthening interoperability, aligning with global standards, building sector-wide credential frameworks, and institutionalising governance mechanisms that reinforce trust. India's opportunity is unique, not just to scale domestically, but to shape global digital identity frameworks through collaboration and leadership.

The future of digital trust will not be built by any one institution alone. It will require governments, industry, standards bodies, and civil society to work together, anchored in openness, privacy, and user empowerment.

As we present this report, I invite all stakeholders to participate in this journey. Together, we can build a digital identity ecosystem that is seamless, secure, and inclusive, one that reflects India's strengths and contributes meaningfully to the global digital future.

Table of

CONTENTS

01 Introduction 10

02 Understanding Digital Identity 16

03 Technology Landscape 22

- The W3C-DID and VC Approach 22
- Available Technologies and Implementations 24
- Global Examples and Pilots 26
- National Implementations in India 29

04 Interoperability, & Standardization 31

05 Digi Yatra: Introduction & Technology Driving IT 38

- The Digi Yatra Framework Overview 38
- Key Components and Architecture 39
- The Role of DY SDK 41

06 Verifiable Credentials as a Digital Public Good and Socio-Economic Enabler 43

01 Introduction

India's digital identity journey reflects both nation-scale ambition and consistent execution. Aadhaar established a unified identity layer at a national level and now provides identity for over 1.25 billion Indians.

The Evolution of Digital Identity Systems

Digital identity has evolved from siloed credentials to regulated, standards-based infrastructure. Over the past decade, key technical and policy milestones, such as NIST SP 800-63, ISO/IEC 18013-5 (the mobile driving licence standard), and the W3C's Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs), have established a shared framework for assurance, interoperability, and selective disclosure of credentials. The EU's eIDAS 2.0 Regulation has advanced the digital wallet model at a continental scale. At the same time, the International Civil Aviation Organisation's Digital Travel Credential (DTC) and IATA's One ID framework illustrate cross-border authentication for travel and mobility. On the other hand, at a national level, several countries that have integrated digital identity into everyday citizen and business services, such as India, Estonia, the Nordic nations, and Singapore, demonstrate that policy alignment and ecosystem adoption are as critical as the technology itself.

India's digital identity journey reflects both nation-scale ambition and consistent execution. Aadhaar established a unified identity layer at a national level and now provides identity for over 1.25 billion Indians. Combined with e-KYC and authentication services, Aadhaar has enabled high-volume, low-friction verification, with 2,707 crore authentications in FY 2024–25 and 2,356 crore cumulative e-KYC transactions as of March

2025. Building on this foundation, DigiLocker serves approximately 540 million users, with billions of issued documents accessible for digital verification. UPI has further normalised real-time, consent-based payments, crossing 20.7 billion transactions in a single month (October 2025). Together, these systems form a mature Digital Public Infrastructure (DPI) where digital identity functions as a trusted enabler for service delivery, inclusion, and innovation.

The next evolution of India's identity ecosystem focuses on interoperability and Self-Sovereign Identity. Emerging efforts in verifiable credentials and decentralised identifiers enable a privacy-friendlier way of selective disclosure, offline authentication, and cross-border acceptance. India's opportunity lies in combining its scale and public infrastructure maturity with open standards and interoperable reference designs that can integrate seamlessly with global digital identity ecosystems.

India's digital identity journey reflects both nation-scale ambition and consistent execution. Aadhaar established a unified identity layer at a national level and now provides identity for over 1.25 billion Indians.

Timelines of Digital Identity Systems – Global and Indian

1980s–1990s

- Emergence of online credentials, mostly limited to usernames and passwords for network access; basic authentication silos appear.
- Foundational identification through physical credentials: PAN, voter ID, driving licence, and passport databases developed independently.

2001

- OASIS SAML 1.0 introduced federated single sign-on (SSO) for cross-domain authentication.

2004–2007

- OpenID and OAuth 2.0 established standards for federated consumer identity.

2017

- ISO/IEC 29115 Identity Assurance Framework standardised.
- Aadhaar authentication APIs expand; early work on Digi Yatra concept begins under the Ministry of Civil Aviation (MoCA) for seamless, paperless air travel.
- First Proof of concept of Digi yatra (Then called as Aadhaar Enabled Biometric Boarding System) at BIAL with Jet Airways

2018

- Global discourse on Self-Sovereign Identity (SSI) intensifies; W3C VC 1.0 Working Draft.
- DigiLocker adoption grows; Aadhaar authentication crosses 1 billion monthly transactions.
- Digi Yatra Policy Framework issued by MoCA in August 2018, outlining voluntary biometric-based boarding using consented digital identity.

2019-20

- Digi Yatra Early Go-live with local enrolment at BIAL.
- ICAO Digital Travel Credential (DTC) and IATA One ID frameworks established for travel identity.
- Digi YatraMultiple pilots were conducted at Various airports l
- IATA one ID, SSI, Evernym

2021

- ISO/IEC 18013-5 (mobile driving licence) published; W3C VC 1.0 becomes Recommendation.
- Challenge with NITI Ayog and Atal Innovation Mission to develop DYCE platform

2022

- W3C DID 1.0 becomes Recommendation; pilots for decentralised identity wallets begin.
- Digi Yatra soft launch on 15th August 2022 at Delhi, and Bengaluru airports. Official Launch of Digi Yatra at 3 airports Bengaluru, Delhi and Varanasi on 1st Dec 2022
- MeitY explores interoperability of identity credentials.

2007

- EU STORK project piloted cross-border eID interoperability, leading to eIDAS.

2009

- UIDAI Established; Aadhaar project initiated to establish a digital identity backbone.

2010

- First Aadhaar enrolments begin.

2011

- NIST SP 800-63 Digital Identity Guidelines published, defining assurance levels.

2013–2014

- FIDO Alliance founded; EU adopts eIDAS 910/2014 for trusted electronic identification.
- Aadhaar reaches 600 million enrolments; e-KYC and direct benefit transfer (DBT) introduced.

2015

- India Stack articulated: Aadhaar (identity), e-Sign, e-KYC, DigiLocker, and UPI (payments).
- Early stages of the concept at Bangalore Airport – Face as Boarding Pass concept.

2016

- Aadhaar Act, 2016 passed, providing statutory backing.

2023

- EU eIDAS 2.0 adopted, enabling the European Digital Identity Wallet (EUDI).
- Digi Yatra public rollout across major airports; over 1 million passengers onboarded within months.

2024

- W3C VC 2.0 approved; EUDI wallet pilots expand across EU.
- Aadhaar authentications exceed 2,707 crore in FY 2024–25; UPI crosses 20.7 billion monthly transactions; DigiLocker users exceed 539 million.
- Digi Yatra Scaled to 24 Airports by September 2024

2025

- Critical Mass to Critical scale
- Digi Yatra crossed 18+Million downloads and 76+Million usage until Nov'25.

The Role of Digital Identity in India's Digital Public Infrastructure

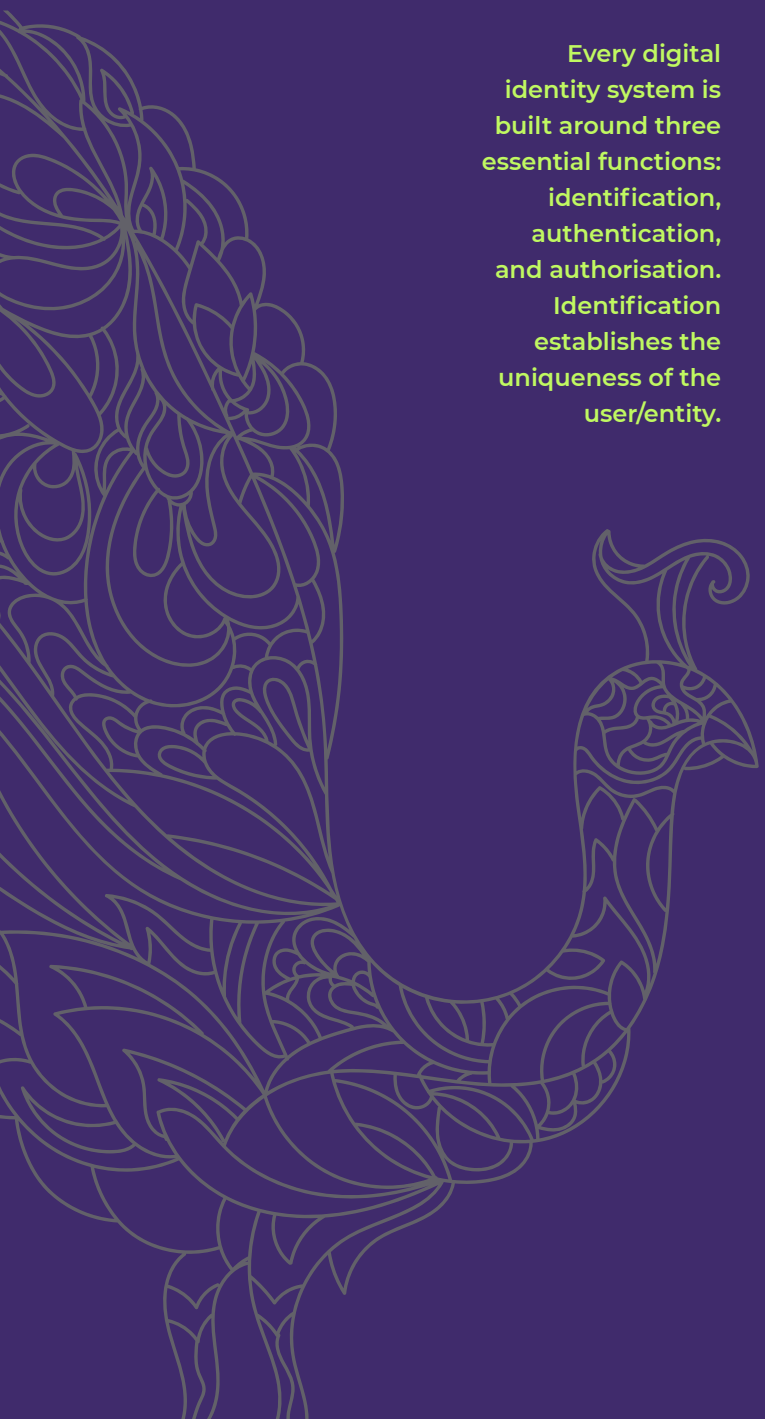
The identity layer serves as one of the critical foundational layers of India's Digital Public Infrastructure (DPI) story, facilitating secure and authenticated connections between citizens, service providers, and platforms to enable large-scale exchanges at a national scale. Sovereign Digital Identity ensures that individuals have a verifiable and unique identity within the digital economy, supporting a wide range of use cases, including authentication for public services, facilitating financial inclusion through verified access, and consent-based data sharing. Its architecture, based on open APIs and interoperable standards, has allowed multiple public and private entities to build on a common trust framework at a national scale.

Over time, identity has become deeply integrated with other digital layers. Verified documents are now being issued and accepted instantly; eKYC and several other platforms authenticate users seamlessly before a transaction is completed. At a national scale, India has created a self-reinforcing network where digital trust supports every exchange, from government benefits to financial services.

The identity architecture is now entering a phase of decentralisation and selective disclosure. Recent evolutions in frameworks for verifiable credentials and decentralised identifiers enable Self-Sovereign Identity, which allows individuals to hold and share proofs of identity while maintaining complete ownership of the data throughout the data lifecycle. They represent a shift from single-point verification to a distributed trust model that enhances privacy, portability, and interoperability, while giving users absolute control over their data and how they utilise it within its lifecycle.

India's story demonstrates that when digital identity is designed as a public good, it becomes an enabler of innovation. As the DPI evolves, identity will continue to anchor trust while moving closer to a self-managed, user-centric model that supports individual privacy, national priorities and global compatibility.

02 Understanding Digital Identity



Every digital identity system is built around three essential functions: identification, authentication, and authorisation. Identification establishes the uniqueness of the user/entity.

A Brief Introduction to Digital Identity

Digital identity is a verified representation of a person, entity, or device within a digital ecosystem. It works by lining unique and verifiable attributes such as biometrics, physical parameters, credentials, cryptographic keys and other measurable parameters to a unique identifier that can be used to establish trust in digital/digital-led interactions. The purpose of digital identity is not only to confirm someone's identity but also to ensure that digital exchanges are secure, reliable, and traceable.

Every digital identity system is built around three essential functions: identification, authentication, and authorisation. Identification establishes the uniqueness of the user/entity. Authentication confirms that the person or entity using the identifier is genuine and is the same person as per (prior) established credentials. Authorisation determines what level of access or action is permitted once the identity is confirmed. Together, these three functions enable digital systems to manage trust at scale.

As digital economies grow, the demand for secure, scalable, interoperable, and portable identity systems has surged. Effective digital identity framework allows individuals to verify their identity once and use the same across various services. When backed by transparent governance, such frameworks create a foundation for digital inclusion, data protection, and efficient service delivery.

Globally, identity systems are shifting away from centralised models toward architectures that provide users with greater control over their credentials. New standards such as Verifiable Credentials (VCs) and Decentralised Identifiers (DIDs), defined by the World Wide Web Consortium (W3C), enable credentials that can be cryptographically verified and shared selectively across domains while having fundamentally good privacy principles in place. Similar work under ISO/IEC 18013-5 and NIST SP 800-63 Rev.4 reflects this shift toward privacy-preserving, interoperable identity standards. These developments mark a transition from identity as a record in a database to identity as a portable, verifiable trust construct.

Digital identity, therefore, operates as a foundational layer of digital societies. It is the mechanism that links citizens, governments, and service providers through verifiable trust, and it underpins the broader digital public infrastructure on which inclusive, secure, and data-driven economies are built.

Self-Sovereign Identity

Self-Sovereign Identity (SSI) represents the next stage in the evolution of digital identity where individuals and entities gain direct control over how their verified information is held, shared, and used across digital ecosystems. Unlike traditional or decentralised identity models that rely on intermediaries to issue or verify credentials, SSI introduces the principle of user agency: the individual becomes the custodian of their own identity. At the same time, verification remains fully compliant with recognised assurance frameworks.

At its foundation, SSI builds on the Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs) - standards developed by the World Wide Web Consortium (W3C). DIDs enable users to create and control identifiers independently of a central issuing authority, whereas VCs provide a structured, cryptographically verifiable method for presenting credentials issued by trusted entities. SSI extends these capabilities by adding a governance and consent layer, using which individuals can store credentials in secure, standards-compliant wallets, decide which attributes to share, and revoke or update permissions as required, which ensures that authentication is achieved without exposing personal data.

The operational model of SSI follows the issuer–holder–verifier framework. The holder determines how and when their credentials are used, and verification occurs through cryptographic proofs rather than through (API) calls to a centralised database. Every credential exchange becomes a consent-based transaction, improving privacy while maintaining auditability and assurance. This design strengthens both user trust and system resilience, making SSI a viable model for regulated, high-assurance ecosystems.

Globally, the movement toward SSI is gaining institutional traction. The European Union's eIDAS 2.0 regulation establishes European

Digital Identity Wallet (EUDI), which embodies the principles of SSI, including user centric control and cross-border interoperability, while Standards from NIST SP 800-63 Rev.4 and ISO/IEC 18013-5 reinforce these practices within government and industry-led assurance frameworks. In the travel and mobility domain, case studies like Digi Yatra and the IATA One ID programme demonstrates how verifiable credentials and biometric data can enable seamless, paperless journeys while ensuring regulatory compliance.

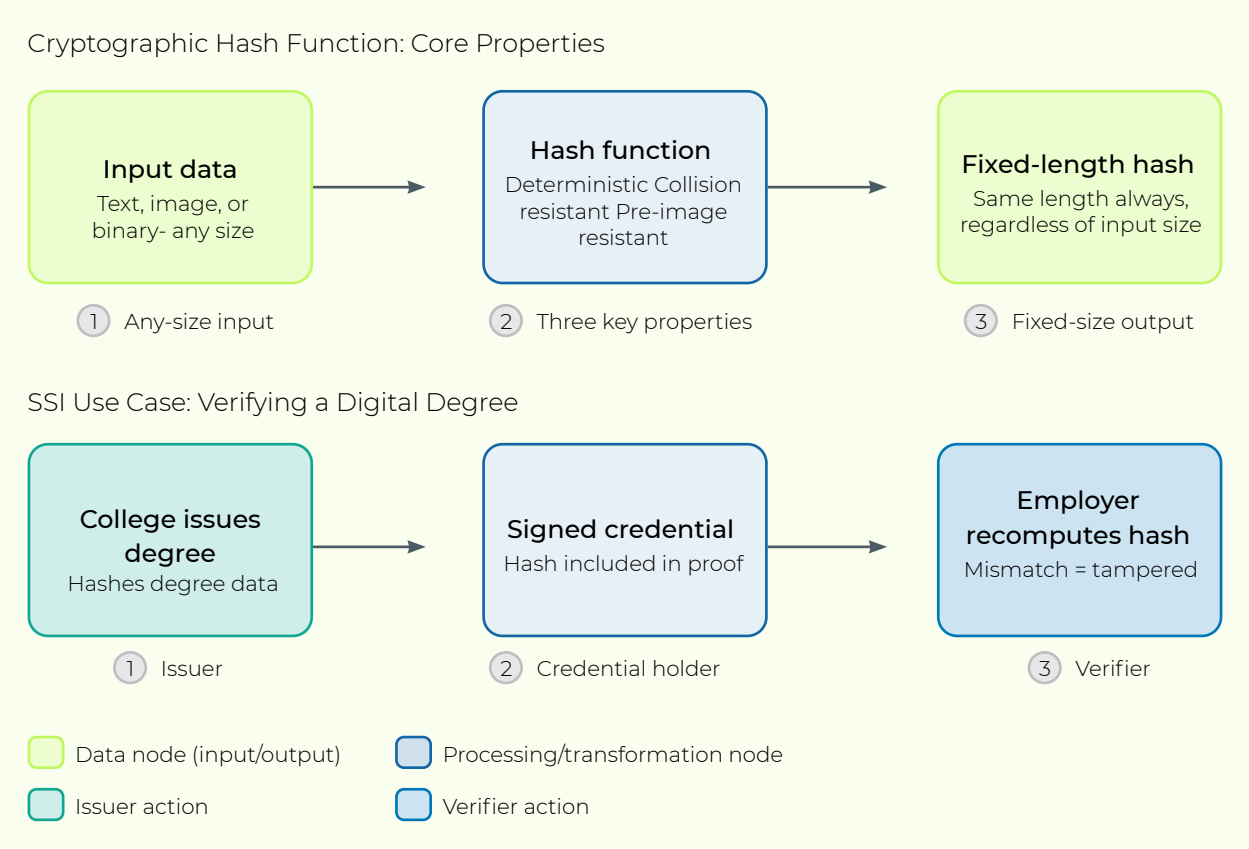
For India, SSI offers an evolutionary path for its Digital Public Infrastructure (DPI), complementing existing identity systems such as Aadhaar, DigiLocker. Integrating SSI principles can make digital identity more portable, consent-driven, and globally interoperable, supporting cross-sector use cases in education, finance, mobility, and healthcare and many other industries. On a strategic front, SSI offers a pathway for India to lead the discussion in creating scalable, privacy-preserving, and interoperable digital identity architectures.

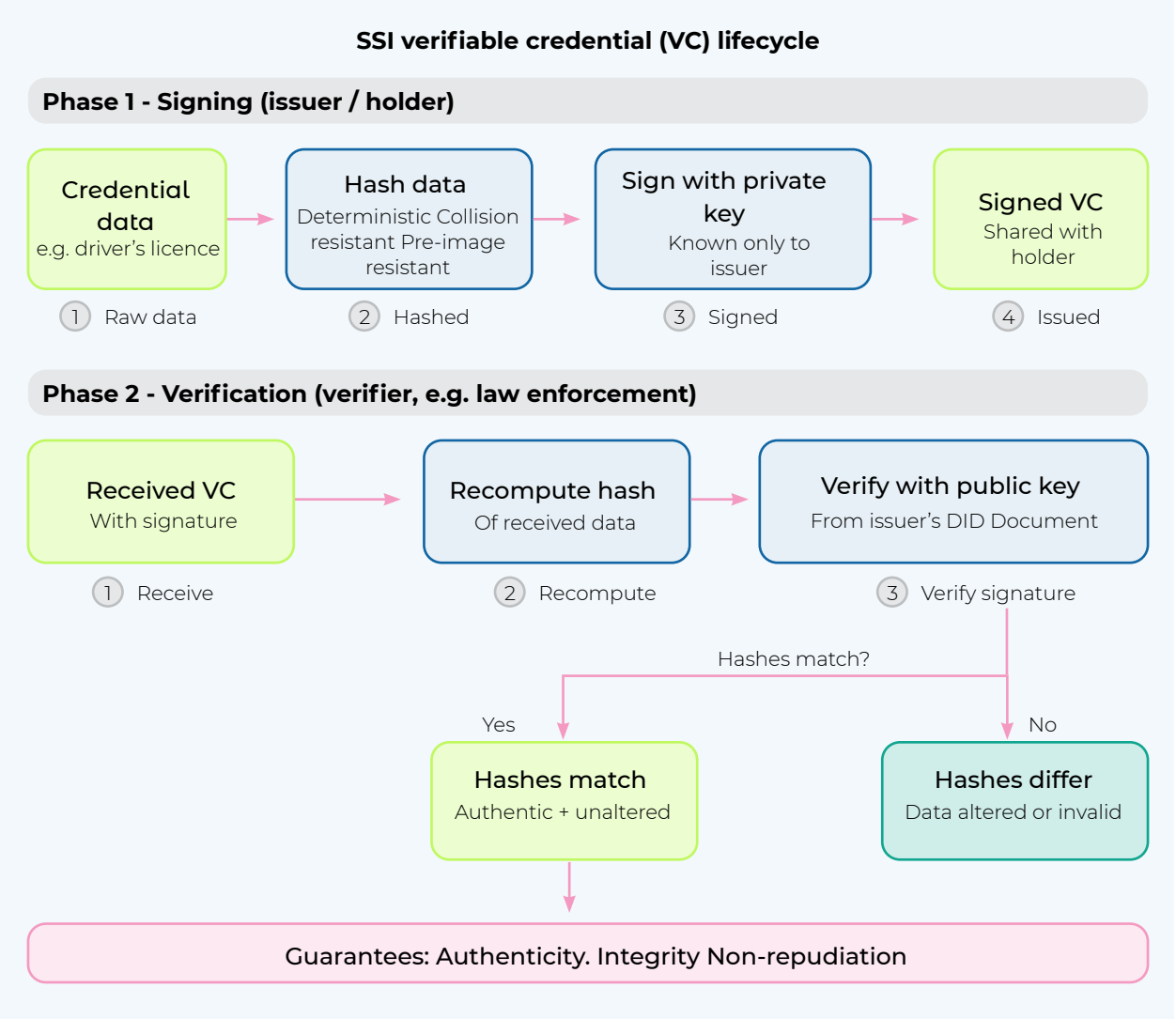
Technology Behind Self Sovereign Identity

Hashing

Hashing is a one-way mathematical function that converts any input (such as text, image, or binary data) into a fixed-length output (Known as a hash). The hash function is:

1. **Deterministic:** The same input always yields the same output and
2. **Collision Resistant:** It is mathematically infeasible for two different inputs to produce the same hash (Unless the hash function is broken).
3. **Image Resistance:** There is no practical way to reconstruct the original input from the hash, which makes it ideal for verifying data integrity.





In the context of SSI, hashing is used to ensure that credentials, DID Documents, and transaction records remain untampered. For example, when a college issues a digital degree, the system computes the hash of the degree data and includes it in the signed proof. When an employer verifies the degree later, they recompute the hash and compare it to the one provided in the credential. Any mismatch in hash values signals manipulation. Hashes are also used in status lists for revocation checks, where each credential is mapped to a bit in a hashed array, allowing for privacy-preserving validation at scale.

Digital Signatures

A digital signature is a cryptographic mechanism that, uses hashing and cryptographic keys, binds a signer to a specific piece of data, ensuring that both the signer's identity and the integrity of the data can be independently verified. It provides three essential properties:

- **Authenticity:** The signature confirms the identity of the signer.
- **Integrity:** Any modification to the signed data invalidates the signature.
- **Non-repudiation:** The signer cannot deny having created the signature.

In SSI, issuers sign Verifiable Credentials using their private keys, and holders sign Verifiable Presentations when sharing credentials with verifiers. For example, when a licensing authority issues a digital driver's licence, the licence data is hashed and digitally signed. A verifier, such as a law enforcement officer, can validate this signature using the public key published in the authority's DID Document. If any information in the licence has been altered, the signature will fail to verify. This mechanism ensures end-to-end trust in the authenticity of credentials across decentralised ecosystems.

Selective Disclosure and Zero-Knowledge Proofs (ZKPs)

Selective disclosure refers to the ability of users to reveal limited and specific pieces of information without exposing unrelated personal data itself. This capability is often enhanced through Zero-Knowledge Proofs (ZKPs), which are advanced cryptographic techniques that allow a verifier to confirm the truth of a statement without learning the underlying data.

For instance, instead of sharing an entire digital ID that includes PII such as name, date of birth, and address to prove eligibility for age-based access, a digital wallet can use ZKPs to prove simply that the holder is over 18 years old, which caters to the specific use case. The verifier receives a cryptographic proof derived from the credential, not the actual data.

Selective disclosure represents the key privacy-preserving advancement that distinguishes SSI from traditional identity systems.

Verified Credentials (VCs)

A Verifiable Credential (VC) is a tamper-evident digital certificate that represents claims made by an issuer about a subject. Each credential is (cryptographically) signed by the issuer, enabling anyone to verify its authenticity and integrity without needing to contact the issuer directly.

A typical VC includes:

Issuer Information: Identifies the entity that created and signed the credential.

Credential Subject: Entity the credential refers to (person, organisation, or device).

Claims (Attributes): statements such as "Alice holds a master's degree in computer science."

Proof Section: A cryptographic signature/ other methodology for validating the above data.

In SSI ecosystems, Verifiable Credentials replace traditional paper or PDF certificates with data models that can be verified in real time. To revisit the earlier example, when a university issues a digital degree, it signs the credential with its private key. The credential can then be stored in the student's wallet and presented to potential employers. The employer's system verifies the signature using the university's public key retrieved from its DID Document. In this case, with VCs, there is no need for database query or manual verification.

Decentralised Identifiers (DID) and Decentralised Identifier Documents

A Decentralised Identifier (DID), as outlined earlier, is a globally unique, cryptographically verifiable identifier that enables individuals,

organisations, and devices to establish secure and persistent digital identities without relying on a central registry or authority. Unlike traditional identifiers such as email addresses or usernames, which depend on third-party control, a DID can be created and owned directly by the user.

A DID Document is a small, structured data object that describes the cryptographic material, verification methods, and available endpoints associated with a specific Decentralised Identifier (DID). DID Document serves as the "digital business card" of a decentralised identity, containing the information necessary to verify control of the DID.

A typical DID Document includes:

- **Public Keys:** Used to verify signatures and authenticate the DID controller.
- **Verification Methods:** Specifying which keys can be used for signing, authentication, or key agreement.
- **Service Endpoints:** URLs or references that allow interactions such as credential issuance or verification.

For example, when an entity publishes a Digital Identifier (DID), the corresponding DID Document lists essential information about the entity, including its public keys and endpoints. When a verifier receives a credential issued by this DID, it consults the DID Document to confirm that the signature is valid and that the issuer is authentic.

DID Documents therefore act as the trust layer between identifiers and cryptographic proofs, enabling verifiable communication without dependency on a central identity provider.

Verifiable Credentials (VCs)

A Verifiable Credential (VC) is a tamper-evident digital certificate that represents claims made by an issuer. Each credential is cryptographically signed by the issuer, enabling anyone to verify its authenticity and integrity without needing to contact the issuer directly.

A typical VC includes:

- **Issuer Information:** To identify the entity that created and signed the credential.
- **Credential Subject:** The entity the credential refers to (person, organisation, or device).
- **Claims (Attributes):** Information about the subject. For example, statements such as "Bob holds a master's degree in computer science from IIT Kanpur"
- **Proof Section:** a cryptographic signature validating the above data.

In SSI ecosystems, Verifiable Credentials replace traditional paper or PDF certificates with data models that can be verified in near real time. For example, when a university issues a digital degree, it signs the credential with its private key. The credential can then be stored in the student's wallet (in a mobile phone, for example) and presented to potential employers. The employer's system may then verify the signature of the student using the university's public key retrieved from its DID Document. There is no need for a database query or manual verification.

This decentralised verification approach enables trust at scale while reducing friction and operational overhead.

03 Technology Landscape

The World Wide Web Consortium (W3C) has established the definitive standards framework for verifiable digital credentials. On 15 May 2025, the Verifiable Credentials Working Group published seven specifications.

The technology landscape underpinning Self-Sovereign Identity and Verifiable Credentials has matured considerably over the past five years, transitioning from experimental specifications to ratified Web Standards with growing production deployments. This section maps the principal standards frameworks, available implementation technologies, and the most significant global and national deployments that collectively define the current state of the art. Understanding this landscape is essential for positioning India's own initiatives within the global trajectory of digital trust.

The W3C-DID and VC Approach

The Verifiable Credentials 2.0 Family of Specifications

The World Wide Web Consortium (W3C) has established the definitive standards framework for verifiable digital credentials. On 15 May 2025, the Verifiable Credentials Working Group published seven specifications as full W3C Recommendations, the highest maturity level in the W3C standards process, signifying broad consensus, extensive implementation testing, and commitment to royalty-free licensing. This family of specifications provides a complete, interoperable foundation for the issuance, holding, presentation, and verification of digital credentials across any domain.

The Verifiable Credentials Data Model v2.0 defines the core data structures: every credential comprises an issuer identifier, a

credentialSubject containing the claims about the holder, validity metadata (such as validFrom and validUntil dates), and a proof section that cryptographically binds the credential to the issuer. The data model is serialised using JSON-LD, which provides extensibility through linked data vocabularies, enabling domain-specific schemas for educational degrees, travel documents, professional licences, health records, or financial attestations to coexist within a single interoperable framework. Version 2.0 refines terminology and aligns with modern security mechanisms compared to v1.1 (published March 2022), while maintaining backward compatibility with existing implementations.

The cryptographic integrity of credentials is addressed through two parallel approaches. The Verifiable Credential Data Integrity 1.0 specification defines how digital signatures and mathematical proofs are embedded directly within the credential's JSON-LD structure. Two companion cryptosuites: Data Integrity EdDSA Cryptosuites v1.0 (based on the Edwards-Curve Digital Signature Algorithm) and Data Integrity ECDSA Cryptosuites v1.0 (based on the Elliptic Curve Digital Signature Algorithm), provide concrete, standardised signature mechanisms. EdDSA offers high performance and compact signatures suitable for resource-constrained environments, while ECDSA provides compatibility with widely deployed PKI infrastructure.

For ecosystems that prefer token-based or envelope-based securing, the Securing Verifiable Credentials using JOSE and COSE specification enables credentials to be wrapped in JSON Web Signatures (JWS), JSON Web Tokens (JWT), Selective Disclosure JWT (SD-JWT), or CBOR Object Signing and Encryption (COSE) structures. This dual-path approach, embedded proofs via Data Integrity or external envelopes via JOSE/COSE, is architecturally significant because it ensures that the VC data model can be adopted by ecosystems with fundamentally different security architectures without requiring either to abandon its established cryptographic infrastructure.

The Controlled Identifiers v1.0 specification generalises the identifier resolution concepts originally defined in DID Core 1.0 (published as a W3C Recommendation in 2022) to accommodate a broader range of identifier types. A Controlled Identifier resolves to a document containing public keys, verification methods, and service endpoints; the same trust information provided by a DID Document, but without mandating a decentralised resolution mechanism. This pragmatic evolution acknowledges that production credential ecosystems must accommodate both decentralised identifiers (DIDs anchored to distributed ledgers or peer exchanges) and conventional identifiers (such as HTTPS URLs or X.509 certificate hierarchies) within a unified verification framework.

Finally, the Bitstring Status List v1.0 specification addresses credential lifecycle management. Rather than maintaining a queryable revocation database, which would enable issuers to track verification events and compromise holder privacy, the specification defines a compact bitstring in which each credential is mapped to a single bit position. A verifier downloads the status list periodically and checks the relevant bit to determine whether a credential has been revoked, suspended, or otherwise had its status changed. This mechanism preserves privacy while enabling near-real-time revocation, a critical requirement for high-assurance use cases such as government-issued identification and regulated professional credentials.

Decentralised Identifiers and DID Core 1.0

The W3C Decentralised Identifiers (DIDs) v1.0 specification, published as a Recommendation in July 2022, provides the foundational addressing layer for SSI ecosystems. A DID is a globally unique URI that can be created, controlled, and resolved without reliance on any centralised registry. Each DID resolves to a DID Document, a structured data object containing the public keys, verification methods, authentication mechanisms, and service endpoints associated with the identifier's controller.

The specification is deliberately method-agnostic: DIDs can be anchored to a wide variety of trust substrates through different DID methods. The did:web method resolves identifiers through standard HTTPS endpoints, making it immediately deployable on existing web infrastructure. The did:key method embeds the public key directly in the identifier, enabling peer-to-peer exchanges without network resolution. Methods such as did:ion, did:ethr, and did:indy anchor identifiers to distributed ledgers (Bitcoin, Ethereum, and Hyperledger Indy, respectively), providing immutability and censorship resistance at the cost of additional infrastructure complexity. This architectural pluralism has been essential for the standard's broad adoption, as it allows each deployment to select the trust substrate most appropriate to its threat model, regulatory environment, and operational constraints.

Available Technologies and Implementations

Credential Exchange Protocols: OpenID4VCI and OpenID4VP

While the W3C specifications define the data models and cryptographic securing of credentials, the practical exchange of credentials between issuers, holders, and verifiers requires standardised interaction protocols. The OpenID for Verifiable Credential Issuance (OpenID4VCI) and OpenID for Verifiable Presentations (OpenID4VP) specifications, developed under the OpenID Foundation, have emerged as the dominant protocol family for this purpose.

OpenID4VCI defines the protocol by which an issuer delivers a signed credential to a holder's wallet, including mechanisms for credential offer, authorisation, and proof of possession. OpenID4VP defines the complementary protocol by which a holder presents credentials (or selected attributes) to a verifier, incorporating nonce-based replay protection, audience restriction, and consent mechanisms. Together, these protocols provide a complete credential lifecycle at the transport layer, and they are designed to work with both W3C VC Data Model credentials and ISO mdoc credentials, making them a critical interoperability bridge between the two major credential format families.

The significance of OpenID4VP in particular cannot be overstated. It is the protocol specified by the EU Architecture and Reference Framework (ARF) for EUDI Wallet interactions, and major browser vendors have adopted it as the underlying transport for the Digital Credentials API. Google Chrome 141 and Apple Safari 26, both released in September 2025, shipped native support for the Digital Credentials API, enabling web

applications to request and receive verifiable credentials directly through the browser without requiring custom integrations. Chrome's implementation is protocol-agnostic, supporting both OpenID4VP and ISO 18013-7 Annexe C, while Safari's initial implementation focuses on mdoc credentials via the org-iso-mdoc protocol. The browser-native availability of credential presentation represents a significant inflection point for mainstream adoption.

Wallet and Agent Frameworks: Hyperledger Aries and ACA-Py

On the implementation side, the Hyperledger Aries project (hosted by LF Decentralised Trust, formerly Hyperledger Foundation) provides an open-source framework for building interoperable credential wallets, issuer agents, and verifier agents. Aries defines an agent architecture and a set of protocols (collectively known as DIDComm) for secure, peer-to-peer messaging between identity agents. The Aries Cloud Agent-Python (ACA-Py) reference implementation is widely used in government and enterprise deployments, including as the basis for several Digi Yatra backend components.

The Aries ecosystem supports multiple credential formats, including AnonCreds (the original Hyperledger Indy credential format with built-in ZKP support), W3C VC Data Model credentials with Data Integrity proofs, and JWT-based credentials. This multi-format support has made Aries a practical choice for deployments that must bridge between legacy and standards-based credential systems. The Digi Yatra Credential Engine (DYCE), which manages the distributed ledger and trust registry for the Digi Yatra ecosystem, leverages Aries architectural patterns and Hyperledger components for credential lifecycle management.

The Trust Over IP (ToIP) Four-Layer Architecture

Recognising that technical standards alone are insufficient without corresponding governance structures, the Trust Over IP Foundation (a project of LF Decentralised Trust) has developed a comprehensive four-layer architecture for digital trust ecosystems. Layer 1 (Technology) addresses cryptographic trust anchors and DID resolution infrastructure. Layer 2 (Agent-to-Agent) covers secure communication protocols such as DIDComm. Layer 3 (Credential Exchange) defines the issuance, presentation, and verification of verifiable credentials. Layer 4 (Application Ecosystem) addresses the end-user applications and governance frameworks that operate on top of the lower layers.

Crucially, each technical layer is paired with a corresponding governance layer. The Technology Architecture Specification V1.0, published by ToIP as a public review draft, provides reference designs for implementers. The Trust Registry Query Protocol defines standardised interfaces for querying whether a given issuer is authorised within a specific governance framework, addressing the fundamental question of "who is trusted to issue what." In September 2025, ToIP and the Decentralised Identity Foundation (DIF) jointly launched three new Working Groups addressing digital trust for agentic AI: the Decentralised Trust Graph Working Group, the Trusted AI Agents Working Group, and a joint working group on Personhood Credentials. This reflects the growing recognition that verifiable credentials will need to serve not only human holders but also autonomous software agents acting on their behalf.

ISO/IEC 18013-5 and the mdoc Credential Format

Alongside the W3C ecosystem, the ISO/IEC 18013-5 standard (published 2021) defines the mobile driving licence (mDL) application and its associated credential format, commonly referred to as mdoc. The mdoc format uses CBOR encoding and COSE signatures (rather than JSON-LD and JWS/Data Integrity used by W3C VCs) and was designed for in-person verification scenarios using NFC and BLE proximity protocols. Its data model is tightly coupled to the presentation protocol,

reflecting its origins in government-issued physical identification use cases.

The subsequent ISO/IEC TS 18013-7 (2024) extends the mdoc format to remote (online) verification scenarios, bringing it into the same domain as W3C VCs. The EUDI Architecture and Reference Framework mandates support for both mdoc and W3C VC formats, reflecting the reality that neither format alone covers all use cases. Government-issued identification credentials (driving licences, national IDs) tend to use mdoc, while broader-purpose credentials (educational, professional, health, financial) tend to use W3C VCs. OpenID4VP serves as the common presentation protocol bridging both formats, and the Digital Credentials API in Chrome and Safari provides the browser-level integration layer.

The practical implication is that any comprehensive national credential ecosystem, including India's, must plan for dual-format support. Wallets that can hold and present both mdoc and W3C VC credentials, verifiers that can validate both formats, and governance frameworks that can assess assurance levels across both credential types will be essential for achieving meaningful interoperability with both the EU's EUDI ecosystem and the broader global landscape.

Global Examples and Pilots

The transition from standards to operational deployments has accelerated markedly since 2023. Several global programmes now provide concrete evidence of how verifiable credential architectures perform under real-world conditions, each addressing a different scope, governance model, and user population. Three programmes merit detailed examination for their relevance to India's digital identity trajectory.`

Bhutan National Digital Identity (NDI)

Bhutan's National Digital Identity (NDI), deployed nationwide in 2023, represents the most complete example of a Self-Sovereign Identity system implemented as a general-purpose national identity platform. Every Bhutanese citizen receives an app-based digital wallet that stores verifiable credentials for identity, age verification, and other government-issued attestations. Critically, all credential data resides on the user's personal device, secured by on-device biometrics, rather than in a centralised cloud database. The government oversees credential issuance, but citizens themselves control the storage, sharing, and selective disclosure of their credentials.

The NDI's technology stack is built on W3C DID and Verifiable Credentials standards, with digital signatures generated by user-held private keys carrying legal standing under Bhutan's Digital Identity Act. This legislative backing is significant: it establishes the legal equivalence of wallet-based digital signatures with traditional forms of identification, a prerequisite for adoption by regulated sectors such as banking, telecommunications, and government services.

Bhutan's interoperability ambitions are equally notable. The NDI was designed from inception to align with eIDAS interoperability principles. In 2024, Bhutan became a member of the Global Acceptance Network (GAN), a consortium working toward mutual recognition of digital credentials across jurisdictions. GAN membership means that Bhutanese credentials can, in principle, be verified by other GAN participants worldwide, establishing a foundation for cross-border credential portability. Bhutanese officials have articulated a vision of citizens carrying digital identities usable internationally, positioning NDI not merely as a domestic convenience but as a component of a global trust network.

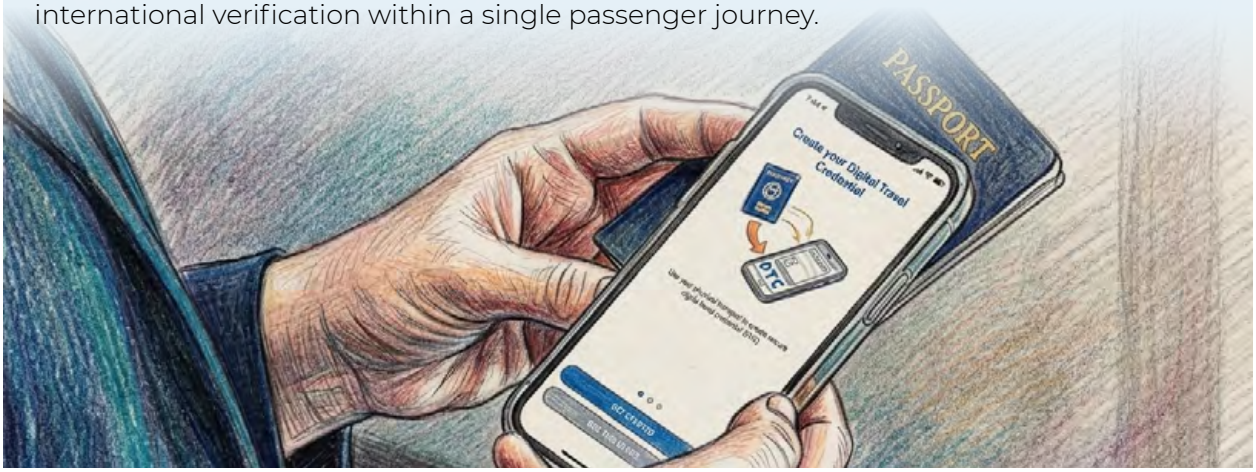
For India, the Bhutan NDI offers several instructive lessons. First, it demonstrates that SSI can be deployed at a national scale even in resource-constrained environments with limited pre-existing digital infrastructure. Second, its early prioritisation of legal recognition for digital credentials provides a model for the legislative framework that India would need to develop to extend VC-based identity beyond voluntary, sector-specific deployments. Third, its GAN membership illustrates a concrete pathway toward international interoperability that does not require bilateral agreements with every individual jurisdiction.

ICAO Digital Travel Credentials (DTC)

The International Civil Aviation Organisation's Digital Travel Credential (DTC) programme represents a fundamentally different architectural approach from Bhutan's general-purpose SSI wallet: it leverages the existing, well-established e-passport Public Key Infrastructure (PKI) to create digitally signed travel credentials that can be verified at border control without introducing entirely new trust infrastructure. This approach is pragmatic in the extreme; rather than requiring governments to adopt new credentialing frameworks, ICAO builds on the PKI that 150+ countries already operate for machine-readable travel documents.

The DTC framework defines two types of credentials. A Type 1 DTC (Virtual Component) is a digital representation of the passport data page, signed with the issuing country's document-signing certificate, using the same PKI hierarchy used for e-passports. This allows a traveller's identity to be verified remotely (for example, during pre-arrival processing) without requiring physical presentation of the passport. A Type 2 DTC (Physical Component) extends the concept to include a digital component embedded in or linked to the physical passport document itself.

The DTC architecture supports biometric matching for identity confirmation, uses the ICAO PKI trust framework for signature validation, and enables minimal disclosure for non-border use cases, such as age verification or nationality confirmation, without revealing the full passport data set. Several countries have initiated DTC pilots, and the Digi Yatra Foundation has signed a pilot agreement with ICAO to explore DTC integration for international travel from Indian airports. This prospective integration would bridge India's domestic credential ecosystem with the global travel document infrastructure, enabling a seamless transition from Digi Yatra's VC-based domestic verification to ICAO DTC-based international verification within a single passenger journey.



IATA One ID

The International Air Transport Association's One ID initiative takes a broader, industry-led approach to the same problem domain. Unlike ICAO's government-to-government DTC framework, One ID is an airline/airport-led programme that establishes standards for the complete passenger journey, from booking through check-in, security, immigration, and boarding. Its scope encompasses both the Digitalisation of Admissibility (ensuring passengers obtain all required authorisations digitally in advance) and Contactless Travel (enabling biometric-based identity verification at every airport touchpoint without physical document presentation).

What distinguishes One ID technically is its explicit endorsement of decentralised identity and the W3C Verifiable Credentials data model. IATA's whitepapers articulate a clear architectural preference: privacy is positioned as the top priority, passengers maintain full control of their data without any centrally managed database, and disclosure is limited to the minimum information necessary with explicit consent. This represents a deliberate alignment with SSI principles by a major industry governance body, lending institutional legitimacy to the decentralised credential approach within the aviation sector.

One ID envisions interoperability through common APIs, trust registries, and the IATA One ID registry, a coordination layer that enables participating airlines and airports to recognise a passenger's "Ready to Fly" status across carriers and jurisdictions. Technical interoperability is achieved through shared credential schemas and verification protocols; governance interoperability is achieved through the One ID Handbook, which defines standards of practice for participating entities. While full production deployment remains in early stages, the One ID framework represents the most comprehensive industry vision for how verifiable credentials can transform the travel experience on a global scale.

The European Digital Identity Wallet (EUDI) as a Structural Reference

While not a travel-specific programme, the EU's EUDI Wallet initiative merits discussion as the most ambitious, regulatory-driven credential deployment globally. Regulation (EU) 2024/1183, entering into force in May 2024, mandates that every EU Member State provide at least one EUDI Wallet to citizens by late 2026, with regulated private-sector entities required to accept wallets by late 2027. The implementing regulations adopted in November 2024 and July 2025 define technical specifications for wallet integrity, credential formats, protocols, certification, and trust services.

Six large-scale pilot projects have been testing real-world use cases, including mobile driving licences, educational credentials, health data, and travel documents, across twenty-six Member States plus Norway, Iceland, and Ukraine, involving over 350 participating organisations. Several Member States already have operational or near-operational wallets: Austria's Valera, France's France Identité, Italy's IT Wallet, Belgium's eID, and Poland's mObywatel. Germany, Finland, Ireland, and Spain are in active development or piloting phases. The European Commission's target is 80% citizen adoption by 2030.

National Implementations in India

India's digital identity landscape already includes several implementations that either deploy or are converging toward verifiable credential architectures. While each operates within its own sectoral governance framework, together they represent a growing ecosystem of credential-based digital trust that could be unified under a common national VC framework.

Digi Yatra: SSI-Based Airport Identity

Digi Yatra represents India's most advanced deployment of verifiable credential principles in a high-throughput operational environment. Launched in December 2022 and now operational at 38 Digi Yatra airports, ~22.5 million app downloads, and ~93 million journeys have been enabled. The architecture is built on W3C VC and DID standards, with Hyperledger Aries components underpinning the credential lifecycle and AWS infrastructure (including Amazon Cognito) supporting the backend.

The system's credential flow follows the canonical issuer–holder–verifier model. The passenger's identity is verified through Aadhaar-based authentication at enrolment, generating a verifiable credential stored in the mobile wallet. At each airport touchpoint, the credential is presented along with a live biometric (facial recognition optimised for Indian demographic diversity), and the biometric token is matched against the credential's reference data. Shared biometric tokens are purged within twenty-four hours, in compliance with both the Digital Personal Data Protection Act 2023 and the Aircraft (Security) Rules 2023.

Importantly, Digi Yatra's ambitions extend well beyond aviation. The Digi Yatra Foundation's CEO has announced plans to expand the Digi Yatra SDK into hotels, IT parks, online examinations, and hospitality venues. The DY101 specification defines a sector-agnostic credential exchange protocol, and a sandbox environment is already active for transport and hospitality integrations. The India AI Impact Summit 2026 (16–20 February, Bharat Mandapam, New Delhi), with over 250,000 registrations, used Digi Yatra credentials for participant access, demonstrating the system's portability beyond its original aviation context.

Mobile Driving Licence (mDL)

India's exploration of the mobile driving licence (mDL) aligns with ISO/IEC 18013-5, the same standard that underpins the mdoc credential format used across the EUDI ecosystem. While the Indian mDL programme is at an earlier stage than Digi Yatra, it represents a significant convergence point: a government-issued identity credential built on an international standard that could interoperate with both the EUDI ecosystem (through the mdoc format and OpenID4VP) and the domestic Digi Yatra ecosystem (through W3C VC bridges).

The mDL use case is particularly instructive because it involves a credential that must function in both in-person (traffic stops, identity checks) and remote (age verification, online services) scenarios. ISO 18013-5 was designed primarily for the in-person case, using NFC and BLE for proximity verification. The extension defined in ISO/IEC TS 18013-7 (2024) adds remote verification capabilities. India's implementation choices here will have long-term implications for the broader national credential architecture, specifically, whether Indian identity credentials adopt a unified format or maintain parallel mdoc and W3C VC formats with protocol-level bridging.

IIT Kanpur: Blockchain-Based Academic Credentials

In December 2021, Prime Minister Modi launched blockchain-based digital degrees for 1,723 students at IIT Kanpur's 54th convocation, one of India's earliest high-profile deployments of verifiable academic credentials. The technology, developed by CRUBN (an IIT Kanpur-incubated company under the National Blockchain Project),

Prime Minister Modi launched blockchain-based digital degrees for 1,723 students at IIT Kanpur's 54th convocation, one of India's earliest high-profile deployments of verifiable academic credentials. The technology, developed by CRUBN (an IIT Kanpur-incubated company under the National Blockchain Project)

issues tamper-proof, globally verifiable degree certificates with selective disclosure capabilities. A student can prove their degree type, graduation year, or academic performance to an employer without revealing their full academic transcript.

The operational impact was immediate: the system replaced a manual verification process that previously required a fee of approximately Rs. 2,000 and a five-day turnaround with near-instant cryptographic verification. While the IIT Kanpur deployment predates the W3C VC 2.0 Recommendations and uses a proprietary blockchain implementation, its underlying principles, issuer-signed tamper-evident credentials, holder custody, selective disclosure, and verifier self-service are fully aligned with the SSI model. The deployment provides practical lessons for scaling academic credentialing across India's higher education system. It serves as an early proof of concept for broader applications of verifiable credentials in education, professional certification, and skills attestation.

Land Records and Emerging Use Cases

Several Indian states, notably Andhra Pradesh and Karnataka, have been exploring blockchain-based land records systems. While these efforts vary in their technical maturity and alignment with standards, they share a common trajectory: the issuance of tamper-evident, cryptographically verifiable records of ownership and transaction history that can be independently verified without reliance on a single centralised registry. Land title verification, currently a major source of friction, fraud, and litigation in Indian property markets, is a natural application for verifiable credentials, where an issuing authority (the state revenue department) signs a credential attesting to land ownership. Any verifier (a bank assessing a mortgage application, a buyer in a transaction) can independently validate the credential.

Other emerging use cases in the Indian context include health credentials (vaccination records, insurance attestations), professional certifications (engineering, medical, legal licences), and supply chain attestations (food safety, export compliance). Each of these domains involves a trusted issuer, a need for portable and privacy-preserving verification, and a clear benefit from moving away from paper-based or database-dependent verification. The common thread across all these implementations is the need for a unified national framework that defines credential schemas, assurance levels, and governance rules: a role that MeitY, potentially in partnership with the sectoral regulators, is uniquely positioned to fulfil.

04 Interoperability, & Standardization

At the governance layer, trust registries operate in isolation: an issuer recognised by one trust framework may have no standing in another, and the mechanisms for cross-recognising issuers across jurisdictions remain nascent.

Need for Interoperability in Digital Identity Systems

Digital identity systems are being deployed with increasing velocity across jurisdictions, yet the conditions for cross-system recognition remain largely unresolved. Governments, industry alliances, and standards bodies have each advanced frameworks tailored to particular constituencies and use cases, producing an expanding mosaic of credential formats, communication protocols, and trust governance models. The practical consequence is that a credential issued in one context is frequently unreadable, unverifiable, or legally unrecognised in another. This fragmentation does not merely inconvenience users. It structurally limits the value proposition of digital credentials and introduces systemic risks that compound as adoption scales.

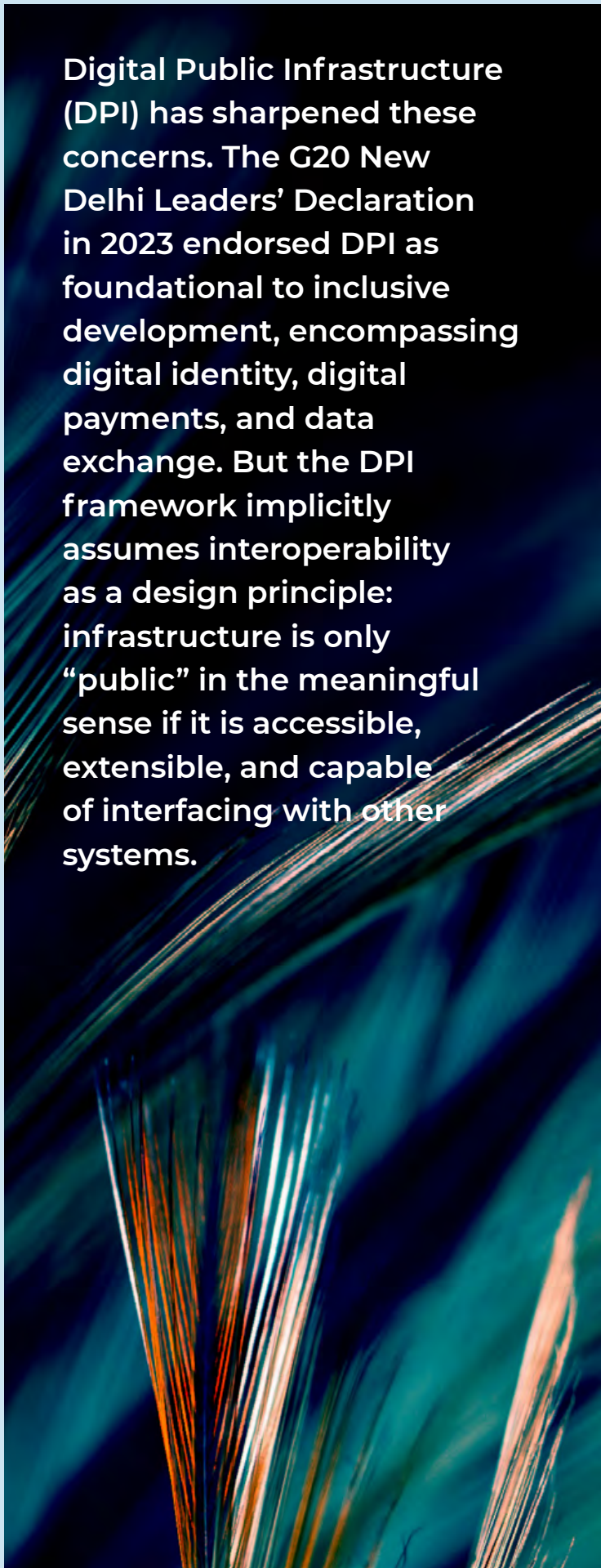
The fragmentation takes several forms. At the technical layer, different systems encode credentials in incompatible formats and exchange them over incompatible protocols. A verifier equipped to process ISO/IEC 18013-5 mdoc credentials, for instance, may have no capacity to interpret a W3C Verifiable Credential encoded in JSON-LD, even when both credentials attest to the same underlying identity attributes. At the governance layer, trust registries operate in isolation: an issuer recognised by one trust framework may have no standing in another, and the mechanisms for cross-recognising issuers across jurisdictions remain nascent. At the legal layer, the conditions under which a foreign digital credential carries the same evidentiary weight as a domestic one are largely undefined outside of specific bilateral or multilateral arrangements.

Vendor lock-in amplifies these risks. Where identity ecosystems are built on proprietary stacks or closed governance arrangements, the cost of switching or bridging systems becomes prohibitively high. This dynamic has been observed in earlier waves of digital infrastructure deployment, from electronic health records to payment networks, and it tends to entrench early movers while raising barriers for new entrants. In digital identity, the stakes are compounded by the sensitivity of the data involved and the sovereignty concerns that governments attach to identity management.

The discourse around Digital Public Infrastructure (DPI) has sharpened these concerns. The G20 New Delhi Leaders' Declaration in 2023 endorsed DPI as foundational to inclusive development, encompassing digital identity, digital payments, and data exchange. But the DPI framework implicitly assumes interoperability as a design principle: infrastructure is only "public" in the meaningful sense if it is accessible, extensible, and capable of interfacing with other systems. Where digital identity systems are deployed as sealed vertical stacks, they function as institutional assets rather than public infrastructure, regardless of the governance rhetoric surrounding them.

The practical challenge, then, is not whether interoperability matters but at what layers it must be achieved and through what institutional mechanisms. Credential-format convergence addresses one layer. Protocol harmonisation addresses another. Trust-framework mutual recognition is a third. And legal enforceability across jurisdictions is a fourth. No single standards body or policy initiative has yet addressed all four in an integrated manner, though several are attempting to address them in combination.

Digital Public Infrastructure (DPI) has sharpened these concerns. The G20 New Delhi Leaders' Declaration in 2023 endorsed DPI as foundational to inclusive development, encompassing digital identity, digital payments, and data exchange. But the DPI framework implicitly assumes interoperability as a design principle: infrastructure is only "public" in the meaningful sense if it is accessible, extensible, and capable of interfacing with other systems.



Convergence of MDOC, W3C VC, and Credential-Formats

Two credential-format standards now dominate the global digital identity conversation; each rooted in different design assumptions and institutional contexts. Their eventual relationship to one another, whether convergence, coexistence, or bridged interoperability, will materially shape the architecture of digital trust systems for the next decade.

The ISO/IEC 18013-5 standard, published in 2021, specifies the technical and operational requirements for mobile driving licences (mDL). The standard defines both a credential data structure (the mdoc format, based on CBOR encoding) and a set of proximity communication protocols for presenting credentials in person via NFC, Bluetooth Low Energy, or WiFi Aware. Its design origin was the in-person verification scenario: a traffic stop, an age-restricted purchase, a physical checkpoint. The standard couples data format and presentation protocol tightly, meaning that a conformant implementation specifies not only what the credential looks like but how it moves from holder to verifier. Verification relies on a certificate hierarchy rooted in Issuing Authority Certificate Authority (IACA) certificates. A verifier need only possess the relevant IACA root certificates to validate a credential offline, with no requirement for real-time communication with the issuing authority.

A complementary standard, ISO/IEC 18013-7, extends the framework to remote (online) credential presentation, addressing scenarios such as opening a bank account or verifying identity for an online service. The addition of this standard reflects a recognition that in-person presentation alone does not capture the full scope of digital identity use cases.

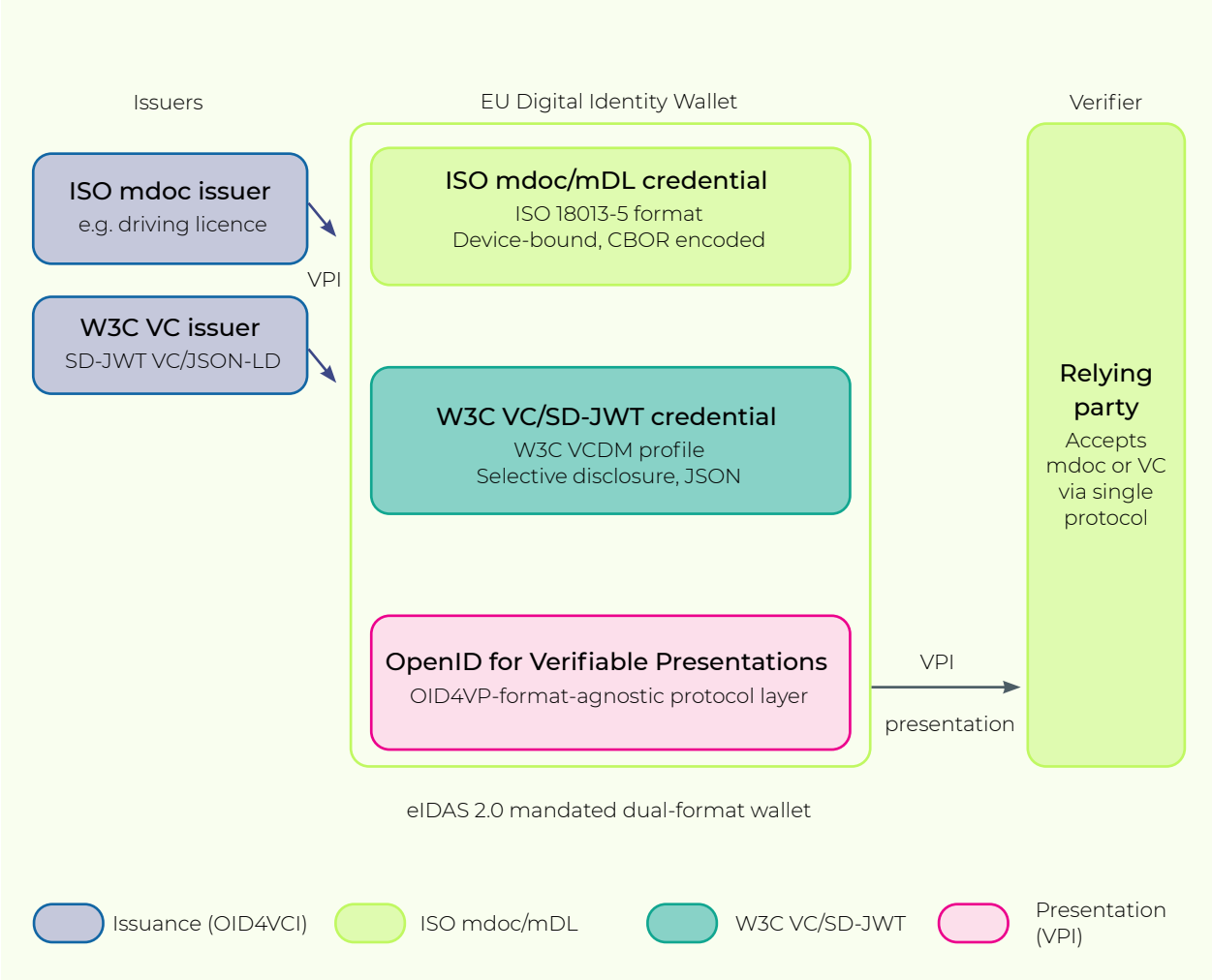
The W3C Verifiable Credentials Data Model (VCDM), by contrast, originated from a fundamentally different starting point. Developed under the auspices of the World

A complementary standard, ISO/IEC 18013-7, extends the framework to remote (online) credential presentation, addressing scenarios such as opening a bank account or verifying identity for an online service.

Wide Web Consortium, the VCDM defines a general-purpose data model for expressing credentials that are cryptographically verifiable, tamper-evident, and capable of selective disclosure. Crucially, the VCDM specifies the structure of a credential but deliberately does not prescribe the communication protocol, the data serialisation format, or the specific cryptographic mechanisms for signing and verification. This flexibility is by design: it allows the VCDM to serve as a common data model across diverse implementation contexts, from government-issued identity documents to educational certificates to health attestations. But this flexibility comes at a cost. Two VCDM implementations that use different serialisation formats (for instance, JSON-LD with Data Integrity Proofs versus SD-JWT), different DID methods, or different trust resolution mechanisms may not interoperate without additional specification work.

The architectural contrast can be stated plainly. The mdoc standard is vertically integrated: it couples a defined data vocabulary, a binary encoding format, and a proximity presentation protocol into a single specification. The VCDM is horizontally extensible: it provides a data-model abstraction layer that sits atop diverse encoding, transport, and cryptographic choices. Each approach carries trade-offs. Vertical integration yields higher baseline interoperability among conformant implementations but limits the range of use cases that can be addressed without modification. Horizontal extensibility enables a wider range of applications but requires additional profiling and conformance testing to ensure that any two implementations can in fact exchange credentials.

The EU's eIDAS 2.0 regulation has made a significant architectural decision by mandating that the European Digital Identity Wallet support both formats: SD-JWT VCs (a profiled subset of the W3C VCDM) and mdoc/mDL credentials. The implementing acts further specify OpenID-based protocols (OID4VCI for issuance, OID4VP for presentation) as the credential exchange layer. This dual-format mandate reflects a pragmatic recognition that neither standard alone covers the full range of required use cases, and that the immediate path forward is coexistence within a common wallet architecture rather than format unification.



Bridging architectures are emerging in parallel. The OpenID Foundation's suite of specifications for Verifiable Credentials, particularly OpenID for Verifiable Presentations (OID4VP), is designed to function as a protocol-level bridge, enabling credential presentation regardless of whether the underlying format is SD-JWT VC, W3C VC with JSON-LD, or mdoc. The Trust Over IP Foundation's Trust Spanning Protocol and the Aries community's work on format-agnostic credential exchange represent additional convergence vectors. None of these efforts has yet achieved the stability and adoption necessary to serve as a universal bridging layer, but collectively they indicate a trajectory toward protocol-mediated format coexistence rather than format consolidation.

Comparative Analysis: IATA One ID, eIDAS 2.0, and Digi Yatra

There are three initiatives, each either already operating at scale or close to it. Together, they illustrate different ways digital identity systems are being used to enable services. They differ in governance structure, geographic scope, standards alignment, trust architecture, and ecosystem maturity. A comparative reading surfaces both common structural patterns and divergent design choices.

IATA One ID is the International Air Transport Association's initiative for streamlining the passenger journey through digital identity and biometric recognition. One ID envisions a process in which travellers share identity and travel credentials in advance, enabling contactless processing at each airport touchpoint. The governance model is industry-led, operating through IATA's Customer Experience and Facilitation Working Group (CEFWG) and the Travel Standards Board, with engagement from airlines, airports, government authorities, and international organisations.

On standards alignment, IATA has endorsed the W3C Verifiable Credentials Data Model as its recommended framework for digital credentials and promotes an open trust framework based on decentralised identifiers and selective disclosure. One ID is designed explicitly for multi-stakeholder, multi-jurisdictional environments, and its architecture accommodates diverse national implementations through a principle of interoperability via shared standards rather than shared infrastructure. A 2024 proof of concept, conducted in collaboration with Neoke on Cathay Pacific flights between Hong Kong and Tokyo Narita, demonstrated a fully digital journey using digital wallets and verifiable credentials with no physical documents.

One ID's maturity should be assessed carefully. Its standards work is well advanced, and its pilot programmes have demonstrated technical feasibility. But widespread operational deployment depends on government adoption of digital travel credentials and bilateral or multilateral agreements on credential recognition, neither of which has reached critical mass. One ID functions as a coordination mechanism and standards catalyst rather than as deployed infrastructure.

The EU's eIDAS 2.0 framework (Regulation 2024/1183), which entered into force in May 2024, represents the most comprehensive regulatory commitment to digital identity infrastructure currently in effect. It mandates that every EU Member State provide at least one European Digital Identity Wallet (EUDI Wallet) to citizens and residents by December 2026. The regulation follows an issuer-holder-verifier architecture that is structurally congruent with self-sovereign identity models, though the trust infrastructure is hierarchical rather than decentralised: issuers and verifiers must be registered on official trust lists maintained by Member States, and the European Commission publishes a List of Trusted Lists (LOTL) that aggregates national registries.

The credential-format choices are technically ambitious. The EUDI Wallet Architecture and Reference Framework (ARF) mandates support for both SD-JWT VC and mdoc formats, with OpenID-based protocols (OID4VCI, OID4VP, ISO 18013-7) for credential exchange. Large-Scale Pilots funded by the EU are testing these specifications across cross-border use cases including identity verification, educational credentials, payment authentication, and travel documents. The regulation also introduces mandatory acceptance requirements: very large online platforms and specified services must accept EUDI Wallet credentials when users present them, creating a demand-side driver for verifier adoption.

The governance model is regulatory-driven, with conformity assessment by accredited bodies and supervisory oversight at the

Member State level. This provides legal certainty and high assurance levels but introduces complexity for non-EU entities seeking to interoperate with the European ecosystem. Cross-border recognition is built into the regulation within the EU but does not yet extend systematically to third countries.

On the other hand, in India, Digi Yatra's operational maturity is notable. With over 38 airports, 22.5 million app downloads and ~93 million passenger journeys enabled, it represents one of the largest SSI-based credential deployments globally. Processing times at entry gates have been reduced from approximately 15 seconds to 5 seconds per passenger. The Foundation has indicated its intent to transition the Verifiable Data Registry (VDR) toward a public, interoperable ledger and to extend the system's applicability beyond aviation.

Comparative observations. Several structural patterns emerge. All three initiatives employ an issuer-holder-verifier model and endorse the W3C Verifiable Credentials Data Model, either directly or through profiled subsets. All three treat biometric verification as a component of the presentation layer rather than the credential layer. And all three confront the fundamental challenge of trust resolution: how does a verifier determine that a credential presented to it was issued by a recognised authority?

The divergences are equally instructive. eIDAS 2.0 addresses trust resolution through a regulated, hierarchical trust-list infrastructure with mandatory acceptance requirements and legal enforceability. IATA One ID relies on a standards-based, voluntary coordination model without binding legal obligations, depending instead on industry consensus and bilateral governmental adoption. Digi Yatra resolves trust within a closed ecosystem by anchoring a single issuer's DID on a private ledger, which provides simplicity and control but limits extensibility and cross-system recognition.

On credential format, eIDAS 2.0 is the only framework that has mandated multi-format support (SD-JWT VC and mdoc). IATA One ID operates primarily within the W3C VC paradigm. Digi Yatra uses Hyperledger AnonCreds and Indy-native credential formats, which are functionally aligned with SSI principles but sit outside the emerging SD-JWT and mdoc convergence path. This creates a potential interoperability gap that would need to be addressed if Digi Yatra's credential infrastructure were to interface with eIDAS-compliant or IATA-aligned systems.

Building a Unified Interoperability Framework and Trust Layer

Achieving interoperable digital identity at international scale is not a matter of selecting a winning standard. It is a problem of layered coordination across technical, governance, legal, and institutional dimensions, each of which presents distinct challenges and involves different stakeholder communities.

Technical standards harmonisation is the most advanced of these layers, though it remains incomplete. The OpenID Foundation's specifications for Verifiable Credential Issuance (OID4VCI) and Verifiable Presentations (OID4VP) are emerging as a lingua franca for credential exchange, capable of operating across SD-JWT VC, W3C VC, and mdoc formats. The Trust Over IP Foundation's four-layer architecture provides a conceptual framework for separating concerns across ledger/VDR operations, agent-to-agent communication, credential exchange protocols, and governance frameworks. The Aries community's ongoing work on DIDComm v2, the did:indy DID Method for cross-network resolution, and support for AnonCreds in W3C VCDM format represent concrete technical bridging efforts. What remains absent is a universally adopted interoperability test suite: a set of conformance tests that can certify that a given implementation will successfully exchange credentials with another across format and protocol boundaries.

Trust registries and certification mechanisms constitute the governance infrastructure without which technical interoperability is insufficient. A verifier must

be able to determine, in real time, whether the issuer of a credential is authorised to issue that type of credential within a recognised trust framework. The EU's approach, a hierarchical system of national Trusted Lists aggregated by a supranational List of Trusted Lists, provides one model. The Trust Over IP Foundation's Trust Registry Query Protocol (TRQP), currently in public review, proposes a decentralised alternative: a lightweight, read-only query protocol for trust registries, described by its authors as "DNS for trust." TRQP is designed to bridge across existing trust infrastructure, including X.509 certificate hierarchies, OpenID Federations, the European Blockchain Services Infrastructure (EBSI) Trust Chains, and the ToIP Trust Spanning Protocol. Whether centralised or decentralised, the core requirement is the same: machine-readable, real-time queryable trust resolution that operates across jurisdictional boundaries.

Legal recognition remains the least developed layer. Within the EU, eIDAS 2.0 establishes legal equivalence for qualified electronic attestations of attributes across all Member States. Internationally, no comparable framework exists. The EU and Canada signed a Memorandum of Understanding in December 2025 on digital credentials and trust services, framing cross-border pilots and standards alignment as an early step toward mutual recognition. Bilateral arrangements of this kind may serve as building blocks for a broader multilateral framework, but the pace of development lags significantly behind the technical standards work. The absence of legal recognition means that even where two systems are technically interoperable, a credential verified by one may carry no legal weight in the jurisdiction of the other.

Cross-certification and compliance models bridge the gap between governance and legal recognition. A cross-certification arrangement specifies that a credential issued under Trust Framework A will be accepted by verifiers operating under Trust Framework B, subject to defined conditions. This is analogous to the mutual recognition agreements that operate in professional licensing and product safety regulation, and the institutional infrastructure for operating such agreements in the digital identity domain is only beginning to take shape. The OIDF's Identity Assurance specifications, which map to government-defined assurance levels including those specified in eIDAS, provide one mechanism for establishing equivalence: if both frameworks specify the same identity assurance level and the verification methods used to reach that level satisfy the requirements of both, then cross-recognition becomes technically and governmentally tractable.

Public-private coordination is the institutional substrate on which all of the above depends. The standards bodies involved, W3C, ISO, the OpenID Foundation, the Trust Over IP Foundation, ICAO, IATA, and the Linux Foundation Decentralized Trust, operate through different governance models with different membership structures. Governments participate unevenly across these bodies. Industry representation varies by sector and geography. Civil society engagement is limited. Building a unified interoperability framework requires not merely technical alignment but institutional coordination across these bodies, creating shared workstreams, common test environments, and aligned publication timelines. The SIDI Hub (Secure Identity Alliance), which convenes stakeholders across government, industry, and standards bodies to address international digital identity interoperability, represents one emerging mechanism for this coordination, though its effectiveness will depend on sustained political and financial commitment from participating governments.

The structural challenge, in sum, is not an absence of standards activity. It is the absence of an integrating mechanism that connects technical specifications, trust governance, legal recognition, and institutional coordination into a coherent system. Individual initiatives are each addressing portions of this problem with considerable rigour. The gap lies in the connective tissue between them.

05

Digi Yatra: Introduction & Technology Driving it

Digi Yatra is an industry-led digital initiative coordinated by the Ministry of Civil Aviation (MoCA), Government of India, designed to provide seamless, paperless, and contactless processing of domestic air travellers through the use of facial biometric verification and decentralised digital identity.

The Digi Yatra Framework Overview

Digi Yatra is an industry-led digital initiative coordinated by the Ministry of Civil Aviation (MoCA), Government of India, designed to provide seamless, paperless, and contactless processing of domestic air travellers through the use of facial biometric verification technology and decentralised digital identity. Launched on 1 December 2022 at Varanasi, Delhi, and Bengaluru airports, the initiative is implemented through the Digi Yatra Foundation (DYF), a not-for-profit Section 8 company incorporated in February 2019, with shareholding distributed among the Airports Authority of India (26 per cent) and five private airport operators (Hyderabad, Cochin, Bangalore, Mumbai, and Delhi) each holding approximately 14.8 per cent.

The foundational architecture of Digi Yatra is explicitly built on W3C (World Wide Web Consortium) open standards, leveraging the Self-Sovereign Identity (SSI) paradigm. The core technical premise is that a passenger's identity credential, verified through Aadhaar-based e-KYC, is issued as a Verifiable Credential (VC), stored locally on the passenger's mobile device in a secure digital wallet embedded within the Digi Yatra application, and presented at airport verification nodes using Decentralised Identifiers (DIDs). No personally identifiable information (PII) is stored in any central repository. The system relies on a Distributed Ledger to provide a decentralised layer of trust among ecosystem participants.

As publicly disclosed by Digi Yatra leadership, the technical stack is built on the Hyperledger Aries framework for the communication and data exchange layer, using DID Communication (DIDComm) protocols between participants: the Issuer (Digi Yatra), the Holder (Passenger), and the Verifier (Airport). The Aries Request for Comments (RFCs) enable Digi Yatra to conform with W3C standards for DIDs and VCs. For the Verifiable Data Registry (VDR), the system uses LFDT Indy (Linux Foundation Decentralised Trust, formerly Hyperledger Indy), an open-source, Apache-2.0-licensed ledger purpose-built to store public DIDs and metadata for issuing verifiable credentials.

According to the Digi Yatra Foundation, the system is currently configured as a private, permissioned network of Indy Ledger nodes, which suffices for the airport validation use case. However, this architecture can support a transition to a public, fully interoperable ledger to accommodate broader use cases and integrations.

Critically, no user information, including individual VC hashes, is stored on the blockchain. What resides on the VDR is the cryptographic hash of the issuer's signing key (the public DID derived from the private DID), along with Credential Schemas and Credential Definitions. Private keys, actual credential payloads, and holder information are explicitly excluded from the ledger. The system has reduced processing time at airport entry gates from approximately 15 seconds to 5 seconds per passenger.

Key Components and Architecture

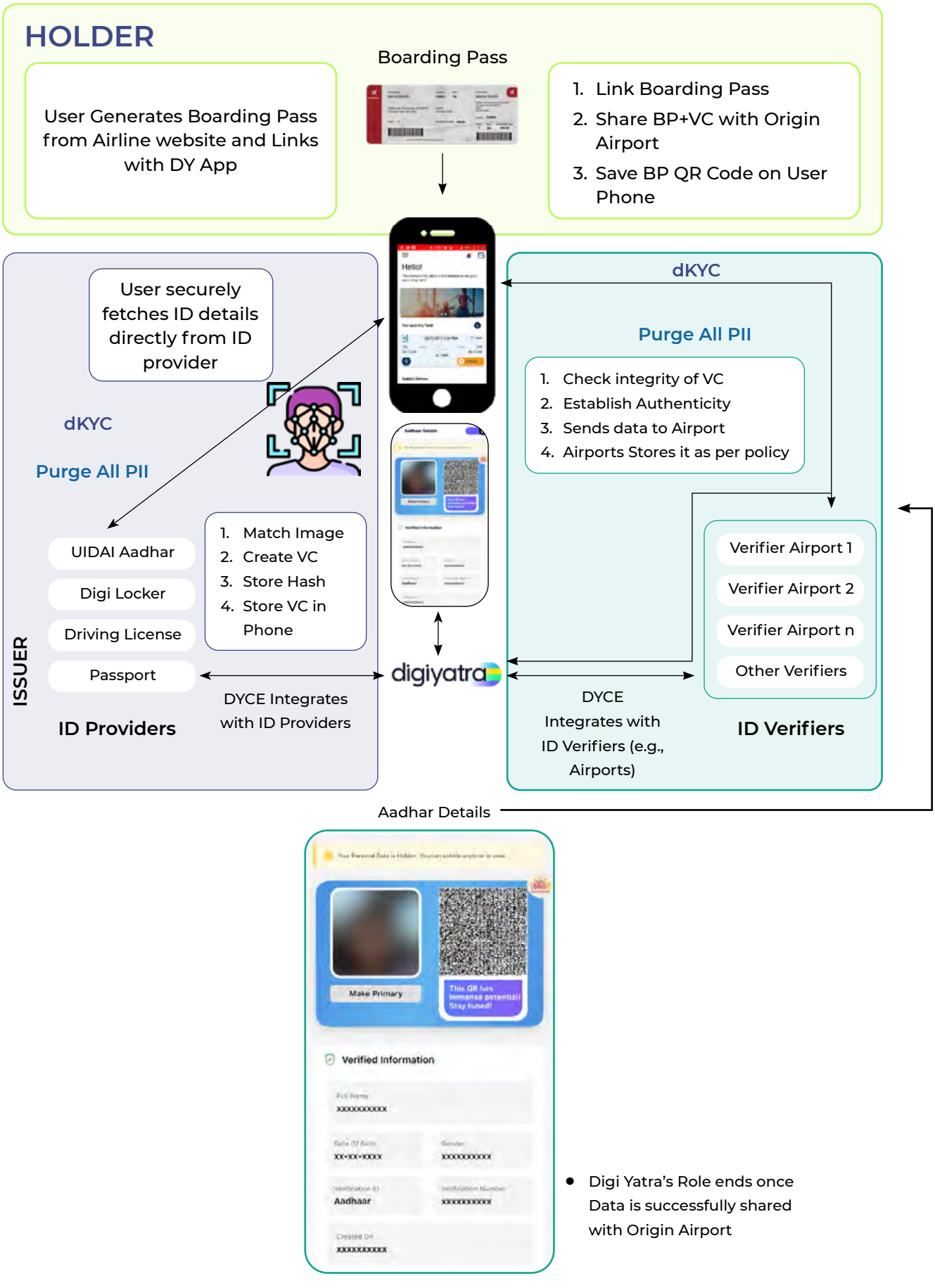
The Digi Yatra architecture follows a three-party trust model, canonical in the SSI ecosystem, involving an Issuer, a Holder, and a Verifier. A shared Verifiable Data Registry underpins it.

The Issuer (Digi Yatra Central Ecosystem)

Digi Yatra serves as the credential issuer. When a passenger enrols through the mobile application, the system fetches only the necessary data from the Unique Identification Authority of India (UIDAI): a facial image, name, gender, date of birth, and the last four digits of the Aadhaar number. This data is used to create a Verifiable Credential, which is digitally signed by Digi Yatra's issuer key. The VC signing process is currently automated and without human intervention, designed to preclude discriminatory actions in credential issuance. The cryptographic hashes of the signing keys are anchored to the Indy VDR.

The architecture is described as serverless, with only minimal configuration storage on the cloud infrastructure. Digital assets are deployed on Amazon Web Services (AWS), using Amazon Cognito for identity and access management, Amazon Simple Notification Service (SNS) for OTP-based authentication, and DigiLocker API integration for Aadhaar e-KYC document retrieval. After the VC is generated and delivered to the passenger's device, the central system no longer retains PII.

Step 1- Creation and storage of VC - One Time



- Digi Yatra's Role ends once Data is successfully shared with Origin Airport

The Holder (Passenger Mobile Wallet)

The passenger's mobile device functions as the credential wallet. Upon installation, the Digi Yatra application provisions a secure, local wallet that conforms to Aries wallet specifications. All credentials: identity, travel, etc., are stored locally. The passenger exercises sovereign control over credential sharing: before travel (typically 60 minutes to 48 hours before scheduled departure), the passenger actively shares relevant credentials with the departure airport verifier node. This consent-based sharing mechanism reflects a core SSI principle: the credential holder governs the disclosure of their own data.

The Verifier (Airport Node)

Each participating airport operates a verifier node. Upon receiving shared credentials, the airport node validates the VC by checking the issuer's public DID and credential definition against the Indy VDR, and performs facial biometric matching at physical touchpoints: entry gates, security checkpoints, and boarding gates. Each verification session generates a new DID, making cross-airport passenger tracking infeasible. Biometric data retained at the airport verifier node is purged within 24 hours of flight departure.

The Verifiable Data Registry (Indy VDR)

The Indy-based VDR serves as the authoritative registry for public DIDs, credential schemas, and credential definitions. It is purpose-built for identity use cases and imposes no storage of PII. The Aries RFCs governing DIDComm communication are designed with the principles of Privacy by Design and Privacy by Default at their core.

Audit and Compliance Framework

The system undergoes multiple overlapping audit cycles: comprehensive CERT-In audits by empanelled auditors covering the whole platform, applications, and airport verifier nodes; STQC (Standardisation Testing and Quality Certification) Safe-to-Host certification; infosec audits by the Centre for Development of Advanced Computing (C-DAC); regular UIDAI infosec audits (as Digi Yatra operates as a UIDAI Sub-KUA); and an external privacy-by-design audit. The Foundation has been awarded ISO 27001 compliance certification and is pursuing ISO/IEC 27701 Privacy Information Management System (PIMS) compliance certification

The Indy-based VDR serves as the authoritative registry for public DIDs, credential schemas, and credential definitions. It is purpose-built for identity use cases and imposes no storage of PII. The Aries RFCs governing DIDComm communication are designed with the principles of Privacy by Design and Privacy by Default at their core.

The Role of DY SDK

The development of Digi Yatra's technology ecosystem was catalysed through the Digi Yatra Central Ecosystem (DYCE) Challenge, organised by NITI Aayog in collaboration with the Digi Yatra Foundation, Atal Innovation Mission, and Amazon Web Services. The challenge sought startup-led solutions that could deliver the Central Ecosystem infrastructure, including the enrolment, credential issuance, and data-sharing stack. A key eligibility criterion for participating teams was demonstrated experience in developing and deploying SDKs capable of integrating with multiple applications, identity management aligned with ISO/IEC 27701, and distributed ledger systems.

In the context of Digi Yatra's ecosystem, the SDK layer serves a critical function: it provides the programmatic interface through which airlines, airport operators, and other third-party service providers can integrate with the Digi Yatra Central Ecosystem. The IndiGo–Digi Yatra app-to-app integration, completed in October 2025, demonstrates this SDK interoperability in practice, enabling seamless

boarding pass sharing between applications while maintaining the consent-based data-sharing model.

Additional Technical Context: In the broader Hyperledger Aries ecosystem, SDKs serve as middleware that enable applications to interact with agents, wallets, and the VDR. The Aries SDK architecture abstracts cryptographic operations (wallet management, key creation, DID resolution, credential exchange) from application logic, allowing diverse frontends to participate in the trust ecosystem without requiring deep cryptographic expertise. This pattern is consistent with the approach described in Digi Yatra's publicly disclosed architecture, where the mobile application embeds an Aries-compatible wallet and communicates with airport verifier agents using standardised DIDComm protocols.

The architectural significance of the SDK layer for digital public infrastructure cannot be overstated. By exposing well-defined APIs for credential issuance, presentation, and verification, the SDK model allows the Digi Yatra trust framework to extend beyond airports into multimodal transport, hospitality, and other identity-verification domains; a trajectory that the Foundation has publicly indicated is part of its roadmap.

06 Verifiable Credentials as a Digital Public Good and Socio-Economic Enabler

How Verifiable Credentials Transform Identity Verification: Mechanisms and Evidence

The conventional model of identity verification is built on repeated disclosure. Each time a person opens a bank account, registers a mobile connection, checks into a hotel, or boards a flight, they submit the same foundational documents to a new verifying party, which then stores and manages copies of that information independently. The result is a sprawling duplication of sensitive personal data across hundreds of institutional databases, each with its own security posture, retention policy, and breach exposure surface. Verifiable credentials alter this model at a structural level by decoupling the act of identity assertion from identity verification and shifting the locus of data control from institutional relying parties to credential holders.

The mechanism operates through a three-party trust architecture. An issuer, typically a government agency or regulated institution with authoritative standing, creates a credential that binds a set of claims about a subject to a cryptographic proof. The subject (or holder) stores this credential in a digital wallet. When a verifier needs to confirm an identity attribute, the holder presents the credential, and the verifier validates the cryptographic proof against the issuer's public

key, which is resolvable through a verifiable data registry such as a distributed ledger or a trust list. At no point does the verifier need to contact the issuer directly, and no copy of the underlying source document needs to change hands.

Selective disclosure is the operational feature that distinguishes this model from earlier approaches to electronic identity. Rather than presenting an entire identity document, the holder can reveal only the specific claim required for the interaction. A verifier confirming age eligibility receives a boolean attestation (over 18: yes) without gaining access to the holder's date of birth, address, or document number. Cryptographic techniques enabling this vary by implementation. SD-JWT (Selective Disclosure JSON Web Token) achieves this by providing individually disclosable claims within a signed token. Hyperledger AnonCreds uses zero-knowledge proof constructions, including CL signatures, to enable predicate proofs without revealing underlying data values. The practical implication is that each verification transaction exposes the minimum data necessary for the purpose at hand, reducing both the holder's privacy exposure and the verifier's data liability.

The evidentiary base for these mechanisms, while growing, remains concentrated in a small number of large-scale deployments. India's Digi Yatra system, operating across approximately 38 airports and enabled over 93 million journeys, has demonstrated that W3C-aligned verifiable credentials can operate at scale in a high-throughput, time-sensitive environment. Gate processing times at entry checkpoints have been reduced from approximately 15 seconds per passenger to 5 seconds. The EU's Large-Scale Pilots under eIDAS 2.0 are testing verifiable credential issuance and verification across cross-border use cases, including identity confirmation, educational qualifications, and payment authentication. IATA's 2024 proof-of-concept on Cathay Pacific flights between Hong Kong and Tokyo Narita demonstrated a fully document-free journey using verifiable credentials in a digital wallet.

What these deployments share is a confirmation that the theoretical privacy and efficiency gains of verifiable credentials translate into measurable operational outcomes: fewer data touchpoints, faster processing, and reduced reliance on physical documents. What they do not yet provide, in most cases, is longitudinal data on fraud reduction, credential revocation performance under adversarial conditions, or user behaviour at scale over extended periods. The evidence base is encouraging but still maturing.

> India's **Digi Yatra system,** operating across approximately **38 airports** and enabled over **93 million journeys** enabled and **~22.5 million app downloads** has demonstrated that **W3C-aligned** verifiable credentials can operate at scale in a high-throughput, time-sensitive environment. Gate processing times at entry checkpoints have been reduced from approximately **15 seconds** per passenger to **5 seconds.**

Sectoral Use Cases:

Travel | Banking | Telecom | Hospitality

Travel. The aviation sector has been the earliest and most visible proving ground for verifiable credentials in service delivery. IATA's One ID initiative envisions a passenger journey in which identity and travel documents are shared as verifiable credentials in advance, enabling contactless processing at check-in, security, and boarding. The architecture accommodates both domestic and international scenarios. However, the latter depends on bilateral or multilateral acceptance of digital travel credentials by border control authorities, a precondition that remains largely unmet at scale. India's domestic aviation deployment has demonstrated the operational mechanics within a closed national system: credential issuance against Aadhaar-linked identity, biometric matching at airport nodes, and automatic data purging after flight completion. Maritime travel presents an analogous use case, with cruise operators increasingly exploring digital embarkation credentials that could streamline port-of-call identity checks across multiple jurisdictions.

Banking and financial services. The banking sector bears some of the highest regulatory costs associated with identity verification. Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance requires institutions to collect, verify, store, and periodically re-verify customer identity information. These processes are costly, time-consuming, and duplicative: a single customer opening accounts at multiple institutions must undergo substantially similar verification at each one. India's Central KYC Registry (CKYC), managed by CERSAI, represents an early centralised approach to reducing this duplication by assigning each customer a unique KYC Identifier. Verifiable credentials offer a structurally different path: rather than centralising identity records in a shared registry, they enable institutions to accept a cryptographically verifiable KYC credential issued by an authorised entity, eliminating the need to re-collect documents.

The regulatory landscape is evolving to accommodate this possibility. Indicio, a verifiable credential infrastructure provider, recommended in a December 2025 submission to the U.S. Treasury that regulators define how verifiable credentials satisfy AML and sanctions obligations, and called for supervised pilots aligned with NIST and FATF guidance. In the EU, the eIDAS 2.0 regulation's mandate that financial institutions accept EUDI Wallet credentials by December 2027 creates a concrete regulatory demand for credential-based identity verification in the banking sector. The AU10TIX and Microsoft collaboration on Reusable ID, built on Microsoft Entra Verified ID, is designed to reduce repeated identity verification at critical onboarding junctures. These developments are at varying stages of maturity, and the shift from pilot to production-grade deployment in regulated banking environments will require clear supervisory guidance on credential acceptance and liability allocation.

Telecommunications. SIM card registration represents one of the highest-volume identity verification touchpoints globally. In jurisdictions with mandatory SIM registration laws, telecom operators must verify customer identities at activation, creating a mass-market identity verification requirement that is often handled through manual document inspection. The Alliance for Telecommunications Industry Solutions (ATIS) has published an analysis on the application of verifiable credentials within telecom ecosystems, proposing a governance framework in which a telecom VC governance authority endorses credentials issued by external bodies, such as those managing Legal Entity Identifiers or government-issued personal credentials, provided their policies meet telecom-specific standards. This would enable verifiers across the call path, from service providers to end-user devices, to authenticate presented identities without maintaining direct relationships with every issuing authority.

The Decentralised Identity Foundation's Hospitality and Travel Working Group has begun surveying identity requirements across hospitality, travel, and entertainment providers. The potential application is straightforward in concept: a guest presenting a verifiable credential at hotel check-in could satisfy both regulatory registration requirements and property security protocols without surrendering a physical identity document for photocopying or manual data entry. AU10TIX's collaboration with Palladium Hotel Group and Microsoft on Reusable ID has explored this in practice, aiming to enable remote check-in, digital room access, and identity verification within a privacy-preserving framework.

Hospitality. The hotel sector's identity verification practices remain among the most manual in regulated industries. Guest registration in many jurisdictions requires the collection of government-issued identification, which is typically photocopied and stored by the property. This creates both a data-liability burden for operators and a privacy concern for guests. CLEAR's identity verification platform, deployed across U.S. hospitality properties, has reported over 50 per cent reductions in fraud through biometric matching and document authentication at check-in. While CLEAR's system is not built on verifiable credential standards, it demonstrates the demand for digital identity verification in hospitality. The DIF Working Group's survey of sector-specific identity needs is expected to map these requirements more precisely and identify where verifiable credentials could reduce both compliance cost and guest friction.

Across these sectors, a typical pattern emerges: identity verification is a recurring, high-cost, high-friction activity that generates duplicative data holdings. Verifiable credentials address this pattern by enabling reusable, cryptographically verified identity assertions. The rate at which each sector adopts this model will depend on regulatory clarity, the maturity of standards, and the development of sector-specific credential schemas.

Impact on Ease of Living, Economic Inclusion, and India's Digital Public Infrastructure Vision

India's Digital Public Infrastructure ecosystem has evolved through a sequence of interconnected layers, each building on the one before. Aadhaar established the identity layer: a biometric-backed unique identifier covering over 1.3 billion residents. The Unified Payments Interface (UPI) established the payments layer, processing over 100 billion transactions in 2024 with a total value exceeding ₹150 trillion, and reaching into rural markets where cash had previously been the sole medium of exchange. DigiLocker provided a document storage layer. The Account Aggregator framework introduced consent-based financial data sharing. Each of these systems was designed around principles of openness, interoperability, and extensibility, enabling private sector innovation on top of public digital rails.

Verifiable credentials fit into this architecture as a potential trust layer: a mechanism for asserting and verifying identity attributes across contexts without relying on a single centralised database for every transaction. The DPI model's distinguishing feature has been its capacity to reduce the unit cost of service delivery. Aadhaar reduced identity verification costs from an estimated $10–20 per transaction to approximately $0.27 per transaction. UPI eliminated merchant discount rates for most small-value transactions, enabling adoption among street vendors and rural merchants. If verifiable credentials achieve comparable cost reductions in identity assertion, the implications for financial inclusion, regulatory compliance, and service access are substantial.

The inclusion dimension is particularly significant. For populations that lack stable addresses, conventional employment records, or extensive documentation histories, the ability to present a verified credential rather than a portfolio of physical documents lowers the threshold for accessing banking, telecommunications, and government services. Selective disclosure mechanisms provide an additional layer of protection for vulnerable populations: a domestic worker presenting a credential for SIM registration needs to reveal only the data elements required by regulation, without exposing information that could be exploited in other contexts.

There are, however, structural constraints that temper optimism. First, the DPI ecosystem operates on the assumption of smartphone access, which, while expanding rapidly, is not universal. According to survey data, only 45-50% of rural adults in India report confidence in using digital platforms for banking or government services. A trust layer built on verifiable credentials inherits this digital-literacy constraint. Second, India's data protection framework, enacted through the Digital Personal Data Protection Act of 2023, establishes consent-based data processing principles but grants the central government broad discretionary powers, creating tension between the DPI model's promise of individual data control and the regulatory reality of state access. Third, extending verifiable credentials beyond aviation into banking, telecom, and hospitality requires not only technical integration but also the development of sector-specific credential schemas, trust frameworks, and liability models that do not yet exist in production.

India's DPI experience demonstrates that population-scale digital infrastructure can be built and adopted when design principles align with institutional incentives. Whether the trust layer follows the same trajectory depends on whether the enabling conditions, regulatory, technical, and institutional, are assembled with comparable coherence.

The "UPI Moment" for Identity: Conditions for Scaling Verifiable Credentials Beyond Aviation

The comparison between UPI's trajectory and the potential scaling of verifiable credentials is instructive, but it should be handled with analytical discipline rather than analogical

enthusiasm. UPI succeeded not merely because the technology worked, but because a specific set of structural conditions aligned: a regulatory mandate from the Reserve Bank of India, interoperability requirements enforced through the National Payments Corporation of India (NPCI), zero or near-zero transaction costs for small merchants, integration across competing banks through a shared protocol layer, and a massive existing demand for low-cost digital payments that the formal banking system was not meeting. The question for verifiable credentials is whether an analogous configuration of conditions can be assembled in the identity domain.

Interoperability is a non-negotiable precondition. UPI's defining characteristic was that it worked across all participating banks and payment applications from the outset. A user of one bank's UPI application could transact with a merchant using a different bank's application without friction. For verifiable credentials to achieve a comparable scale, a credential issued by one authorised entity must be verifiable by any conformant verifier, regardless of the specific technology stack, wallet application, or trust framework under which either party operates. This requires convergence at multiple layers: a standard credential format or a format-bridging protocol, a shared or interoperable trust registry for issuer resolution, and consistent presentation mechanisms. The OpenID Foundation's OID4VP and OID4VCI specifications, the Trust Over IP Foundation's TRQP protocol for trust registry interoperability, and the Aries community's work on DIDComm are all addressing portions of this requirement. None has yet achieved the level of universal adoption that UPI's single-protocol layer enabled.

Regulatory mandate and institutional orchestration. UPI's adoption was not organic in the sense of emerging from voluntary market coordination. It was orchestrated through NPCI with regulatory backing from the RBI. Banks were required to participate. Merchants were incentivised through zero MDR. For verifiable credentials, no equivalent regulatory orchestrator currently exists in India. The Ministry of Electronics and Information Technology (MeitY) has authority over digital governance policy, and the Digi Yatra Foundation has demonstrated operational capability within aviation. But there is no entity with a mandate to require credential acceptance across sectors or to enforce interoperability standards across issuers and verifiers. The establishment of a National Centre of Excellence for Decentralised Digital Identity, as proposed in policy discussions, could serve this function. Still, it remains a prospective institutional mechanism rather than an operational one.

Ecosystem incentives and demand-side drivers. UPI solved a problem that millions of users and merchants experienced daily: the cost and inconvenience of cash transactions. The demand was pre-existing; UPI provided the infrastructure to meet it. The demand for verifiable credentials is less immediately legible to end users. Most individuals do not perceive repeated KYC processes or document submission as problems amenable to a technology-mediated solution; they see them as bureaucratic friction that is simply part of how institutions work. Shifting this perception requires demonstrating tangible benefits, faster onboarding, reduced paperwork, and greater control over personal data in contexts that users encounter frequently. Aviation has served as one such context. Banking and telecom, where KYC processes are both universal and repetitive, represent natural next frontiers, but only if regulatory frameworks recognise verifiable credentials as satisfying existing compliance obligations.

Governance architecture and credential schema development. UPI required a single protocol specification. A multi-sectoral verifiable credential ecosystem requires a more complex governance architecture: authorised issuers for different credential types, defined schemas for sector-specific attributes, revocation and renewal procedures, liability allocation between issuers and verifiers, and mechanisms for dispute resolution. India's DPI track record suggests that such architectures can be developed through a combination of government initiative, industry

consultation, and iterative deployment. The Account Aggregator framework, which required coordination across the RBI, financial institutions, and technology providers, provides a partial precedent. But the breadth of a cross-sectoral identity credential framework, spanning travel, banking, telecom, hospitality, healthcare, and education, exceeds the scope of any prior Indian DPI initiative.

The "UPI moment" for identity, then, is not something that arrives through technological readiness alone. It requires the deliberate construction of regulatory mandates, interoperability standards, institutional coordination mechanisms, and demand-side incentives, all aligned around a common governance framework. India's DPI history offers reason to believe that such alignment is achievable. It does not guarantee that it will occur, nor does it specify the timeline over which it might unfold. The conditions are identifiable. Whether they are assembled is a matter of policy will, institutional design, and sustained coordination across government, industry, and standards bodies.

07 Closing

Digi Yatra is an industry-led digital initiative coordinated by the Ministry of Civil Aviation (MoCA), Government of India, designed to provide seamless, paperless, and contactless processing of domestic air travellers through the use of facial biometric verification technology and decentralised digital identity.

This report has traced a structural shift in how digital identity systems are conceived, built, and governed. The arc runs from centralised identification databases, designed to answer the question of who someone is, to distributed credential architectures that allow individuals to prove specific attributes without surrendering control over the underlying data. That shift is not yet complete. But the technical standards, regulatory frameworks, and operational deployments surveyed across these sections confirm that it is underway, and that the pace of convergence is accelerating.

The foundational layer of this transition is now stable. The W3C Verifiable Credentials Data Model 2.0, published as a formal Recommendation in May 2025, provides a shared vocabulary for credential representation. The W3C Decentralised Identifiers specification, approved in July 2022, provides a mechanism for identifier creation and resolution outside of centralised registries. ISO/IEC 18013-5 defines the mobile driving licence as a tightly coupled credential-and-protocol specification for in-person presentation. These are no longer experimental proposals. They are published standards with institutional backing, conformance testing regimes, and growing implementation communities.

What distinguishes the current moment from earlier phases of digital identity discourse is the emergence of binding regulatory commitments built atop these standards. The EU's eIDAS 2.0 regulation mandates that every Member State provide a European Digital Identity

Wallet by September 2026, with private-sector acceptance requirements for financial institutions and telecom operators taking effect by December 2027. The POTENTIAL pilot tested this architecture across 19 Member States, demonstrating technical feasibility for banking, SIM registration, and e-government services. ICAO's Digital Travel Credential programme has moved from specification to pilot deployment, with live implementations in Aruba and Finland generating measurable evidence on border processing efficiency. These are not aspirational roadmaps. They are implementation timelines with legal force, procurement implications, and compliance consequences.

The interoperability challenge, examined in detail in this report, remains the most consequential unresolved structural problem. Two credential formats, the W3C VC ecosystem (encompassing SD-JWT VC, JSON-LD with Data Integrity Proofs, and Hyperledger AnonCreds) and the ISO mdoc format, coexist without a universal bridging mechanism. The EU's pragmatic decision to mandate support for both SD-JWT VC and mdoc within the EUDI Wallet reflects an acknowledgement that format unification is not imminent and that coexistence within a common wallet architecture is the tractable near-term path. Protocol-level bridging work, through the OpenID Foundation's OID4VP and OID4VCI specifications and the Trust Over IP Foundation's Trust Registry Query Protocol, is advancing but has not yet achieved the stability or adoption necessary to serve as a universal interoperability layer. The trust registry federation, the mechanism by which a verifier in one jurisdiction can determine the authoritative standing of an issuer in another, remains nascent. The EU's hierarchical Trusted Lists model and ICAO's Public Key Directory provide established approaches within their respective domains, but a cross-domain, cross-jurisdictional trust resolution protocol does not yet exist in production.

Governance and legal recognition lag behind technical progress. Within the EU, eIDAS 2.0 establishes legal equivalence for qualified electronic attestations of attributes across all Member States. Internationally, no comparable framework exists. The EU-Canada[GU12.1] Memorandum of Understanding on digital credentials, signed in December 2025, represents an early bilateral model. Beyond this, the institutional infrastructure for cross-border credential recognition is largely absent. The gap between technical interoperability, which is increasingly achievable, and legal mutual recognition, which requires diplomatic and regulatory negotiation, defines the current bottleneck in global credential system maturation.

India occupies a distinctive position within this landscape. Its Digital Public Infrastructure ecosystem has demonstrated that identity, payments, and data exchange systems can be built and operated at a population scale. Aadhaar has enrolled over 1.3 billion residents and processed more than 150 billion authentication transactions. UPI processed over 100 billion transactions in 2024. DigiLocker serves approximately 540 million users. The Account Aggregator framework has introduced consent-based financial data sharing across regulated institutions. These systems have generated institutional knowledge about high-throughput architecture, inclusion design for low-literacy

populations, public-private coordination at a national scale, and iterative deployment in environments characterised by linguistic diversity and variable connectivity.

India's deployment of verifiable credentials in aviation provides additional, more directly relevant experience. The Digi Yatra system, built on Hyperledger Aries for DID communication and LFDT Indy for its Verifiable Data Registry, implements the issuer-holder-verifier model with biometric matching, consent-based credential sharing, and automated data purging. With over 38 Digi Yatra airports, ~93 million journeys enabled and ~22.5 million app downloads, it constitutes one of the largest SSI-aligned credential deployments globally. The SDK architecture, demonstrated through the IndiGo integration in October 2025, provides a programmatic interface for third-party participation in the trust ecosystem, a pattern with potential applicability beyond aviation.

This report has been careful to distinguish between operational scale and systemic readiness. India's centralised identity infrastructure generates transferable lessons in throughput management, fraud detection, and inclusion design. Its decentralised credential deployment generates lessons in SSI architecture and consent-based verification. But several structural gaps separate current capability from the requirements of a multi-sectoral, internationally interoperable credential ecosystem. The Verifiable Data Registry operates as a private, single-issuer ledger, limiting extensibility and cross-system recognition. The credential format (AnonCreds on Indy) sits outside the SD-JWT VC and mdoc convergence path endorsed by eIDAS 2.0, creating a format-level interoperability barrier. No Indian regulatory body has issued guidance recognising verifiable credentials as satisfying existing compliance obligations in banking, telecommunications, or hospitality. Sector-specific credential schemas, trust frameworks, and liability models do not yet exist in production form. And India's

India's deployment of verifiable credentials in aviation provides additional, more directly relevant experience. The Digi Yatra system, built on Hyperledger Aries for DID communication and LFDT Indy for its Verifiable Data Registry, implements the issuer-holder-verifier model with biometric matching, consent-based credential sharing, and automated data purging.

participation in the international standards bodies where credential formats, trust protocols, and governance frameworks are negotiated, the W3C, the OpenID Foundation, the Decentralised Identity Foundation, the Trust Over IP Foundation, and ISO/IEC JTC 1 SC 17, remains limited relative to its operational scale.

The policy and technical recommendations presented in Section 6 of th[GU14.1]is report address these gaps directly: the establishment of a National Centre of Excellence for Decentralised Digital Identity with a cross-sectoral mandate; the transition of the Digi Yatra VDR to a public, interoperable ledger; the development of multi-sectoral credential schemas aligned with W3C VCDM 2.0; the pursuit of bilateral digital credential recognition arrangements with eIDAS jurisdictions; the alignment of domestic credential formats with international convergence paths; the strengthening of non-discriminatory safeguards and transparency mechanisms; and the institutionalisation of academic-industry accountability dialogues. These are not prescriptions for a distant future. They respond to a compressed convergence window: the EU's eIDAS 2.0 implementation timeline, ICAO's DTC specification maturation, the OpenID Foundation's protocol stabilisation, and the Trust Over IP Foundation's trust-registry work are all advancing within the same two-to-three-year period. India's capacity to shape these processes, rather than merely adapt to

their outcomes, depends on the timeliness of its engagement.

The broader observation that emerges from this report is that verifiable credentials are not a technology in search of a problem. They address a documented, measurable, and cross-sectoral pattern: the repeated collection, storage, and re-verification of identity information by institutions that each maintain independent, often insecure, copies of the same data. The privacy, compliance, and inclusion costs of this pattern are substantial and well-documented. Verifiable credentials offer a structurally different approach: one in which identity assertions are cryptographically verifiable, selectively disclosable, and controlled by the credential holder. The standards are published. The pilots are producing operational evidence. Regulatory mandates in the EU and increasingly elsewhere are creating demand-side drivers.

What remains is the work of institutional coordination. Standards must be harmonised across credential formats, exchange protocols, and trust registries. Regulatory frameworks must recognise verifiable credentials as satisfying existing compliance obligations, not merely as novel technological artefacts. Governance mechanisms must be put in place to manage trust across jurisdictions, including issuer authorisation, credential revocation, and liability allocation. Private-sector participants must invest in interoperability rather than proprietary lock-in. Civil society must be included in oversight processes to ensure that credential systems expand access rather than restrict it, and that data protection commitments are substantive.

This is not work that any single government, standards body, or technology provider can accomplish alone. The evidence surveyed in this report, across the EU, Ukraine, the United States, ICAO, IATA, and India, confirms that progress is distributed and that the ecosystem's[GU15.1] maturation depends on sustained, coordinated engagement across all of these actors. India brings to this effort a distinctive combination of population-scale operational experience, a mature DPI ecosystem, and a live, verifiable credential deployment. Whether that combination translates into meaningful influence on the global architecture of digital trust will depend not on the scale of what has been built, but on the precision and persistence of what is done next.

References

International Standards and Specifications

- W3C – Verifiable Credentials Data Model v2.0 (2025)
  https://www.w3.org/TR/vc-data-model-2.0/
- W3C – Decentralised Identifiers (DIDs) v1.0: Core Architecture, Data Model and Representations (2022)
  https://www.w3.org/TR/did-core/
- W3C – Verifiable Credentials 2.0 Press Release (May 2025)
  https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/
- ISO/IEC – 18013-5:2021, Personal Identification: Mobile Driving Licence (mDL) Application
  https://www.iso.org/standard/69084.html
- ISO/IEC – 18013-7, Personal Identification: Mobile Driving Licence (mDL) Add-On Functions (Online Presentation)
  https://www.iso.org/standard/82772.html
- ISO/IEC – 27560:2023, Privacy Technologies: Consent Record Information Structure
  https://www.iso.org/standard/80392.html
- NIST – Digital Identity Guidelines, SP 800-63 Rev. 4 (2025)
  https://pages.nist.gov/800-63-4/
- IETF – SD-JWT (Selective Disclosure for JWTs), RFC 9449 and Related Specifications
  https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/
- IETF – CBOR (Concise Binary Object Representation), RFC 8949
  https://datatracker.ietf.org/doc/rfc8949/

European Union: eIDAS 2.0 and EUDI Wallet

- European Parliament and Council – Regulation (EU) 2024/1183 Amending Regulation (EU) No 910/2014 (eIDAS 2.0)
  https://eur-lex.europa.eu/eli/reg/2024/1183/oj
- European Commission – European Digital Identity Wallet: Architecture and Reference Framework (ARF)
  https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework
- European Commission – EUDI Wallet Programme and Policy Overview
  https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet
- European Commission – EU Large-Scale Pilots (POTENTIAL, EWC, DC4EU, NOBID)
  https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox
- European Data Protection Supervisor – TechDispatch #3/2025: Digital Identity Wallets (December 2025)
  https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/2025-12-15-techdispatch-32025-digital-identity-wallets_de

Aviation: ICAO and IATA

- ICAO – Digital Travel Credential (DTC) Specifications
  https://www.icao.int/Security/FAL/Pages/Digital-Travel-Credentials.aspx
- ICAO – High-Level Guidance on DTC Implementation (2024)
  https://www.icao.int/Security/FAL/TRIP/Pages/default.aspx
- IATA – One ID Programme Overview
  https://www.iata.org/en/programs/passenger/one-id/
- IATA/Neoke – End-to-End Digital Identity Proof of Concept: Hong Kong to Tokyo Narit[GU16.1]a (October 2024)

https://www.neoke.com/blog/iata-end-to-end-proof-of-concept-digital-identity

- SITA/Indicio – ICAO DTC Type 1 Deployment in Aruba (March 2023)

  https://www.phocuswire.com/IATA-digital-IDs-biometrics-passenger-survey

Standards Bodies, Foundations, and Industry Groups

- OpenID Foundation – OpenID for Verifiable Credential Issuance (OID4VCI)

  https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

- OpenID Foundation – OpenID for Verifiable Presentations (OID4VP)

  https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

- Trust Over IP Foundation – Trust Registry Query Protocol (TRQP), Public Review Draft

  https://trustoverip.org/

- Trust Over IP Foundation – Trust Spanning Protocol and Governance Architecture

  https://trustoverip.org/our-work/

- Linux Foundation Decentralized Trust – Hyperledger Aries, Indy, and AnonCreds Projects

  https://www.lfdecentralizedtrust.org/

- Decentralised Identity Foundation (DIF) – Hospitality and Travel Working Group

  https://identity.foundation/

- SIDI Hub – Interoperable Digital Identity Initiative: Multi-Stakeholder Convening

  https://sidihub.org/

- GS1 – Verifiable Credentials Implementation for Trade Documentation and Sustainability Claims (2025)

  https://www.gs1.org/

- ATIS – Verifiable Credentials Governance Framework for Telecommunications

  https://www.atis.org/

- Credential Engine / Digital Credentials Consortium – Issuer Identity Registry Research Report: Trust Infrastructure for W3C VCs (June 2025)

  https://credentialengine.org/2025/06/09/building-trust-in-a-digital-world-scalable-solutions-for-verifiable-credential-ecosystems/

- 1EdTech – Open Badges, Comprehensive Learner Record (CLR), and Digital Credentials Standards

  https://www.1edtech.org/workstream/credentials

India: Digital Public Infrastructure

- UIDAI – Aadhaar Dashboard and Authentication Statistics

  https://uidai.gov.in/aadhaar_dashboard/india.php

- NPCI – Unified Payments Interface (UPI) Transaction Data

  https://www.npci.org.in/product/upi/product-statistics

- DigiLocker / MeitY – DigiLocker: National Digital Document Platform

  https://www.digilocker.gov.in/

- Digi Yatra Foundation – Digi Yatra: Privacy-Preserving Biometric Processing for Indian Aviation

  https://www.Digi Yatrafoundation.com/

- MeitY – Digital Personal Data Protection Act, 2023

  https://www.meity.gov.in/data-protection-framework

- MeitY – Joint Secretary Bhondve, Global Digital ID Standards Announcement (April 2025)

- MOSIP (IIIT-Bangalore) – Modular Open Source Identity Platform: Deployments in Philippines, Ethiopia, Morocco

https://mosip.io/

- CERSAI – Central KYC Registry (CKYC) and KYC Identifier System

  https://www.cersai.org.in/

- Reserve Bank of India – Account Aggregator Framework

  https://www.rbi.org.in/

- IIT Kanpur / C3i Centre – National Blockchain Project (Funded by National Security Council Secretariat)
- IGNOU – Blockchain-Backed Digital Degrees Issued to 60,000+ Students (2022)

Ukraine: Diia Ecosystem

- Ministry of Digital Transformation of Ukraine – Diia Ecosystem: Digital Identity and Public Services Platform

  https://expo.diia.gov.ua/

- NACES – Digital Ukrainian Credentials Accessible via Diia Digital Application

  https://naces.org/digital-ukrainian-credentials-accessible-via-diia-digital-application/

- Harvard Kennedy School, Centre for International Development – Ukraine's Digital Transformation: Innovation for Resilience

  https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience

- CGAP (World Bank) – Ukraine's Diia: A Digital Lifeline in Times of Crisis

  https://www.cgap.org/blog/ukraines-diia-digital-lifeline-in-times-of-crisis

- New America Foundation – Digital Public Infrastructure in Ukraine: Harnessing Technology for the Public Good

  https://www.newamerica.org/the-thread/digital-public-infrastructure-ukraine-war/

- CMS Law Now – Ukraine Adopts Use of Digital ID Wallets Meeting EU Standards (June 2025)

  https://cms-lawnow.com/en/ealerts/2025/06/ukraine-adopts-use-of-digital-id-wallets-meeting-eu-standards

United States: Education and Workforce Credentials

- North Carolina Community College System – Legislative Report for the Digital Credential Pilot Program (2025)

  https://wordpress.nccommunitycolleges.edu/wp-content/uploads/2025/07/PROG-06-Legislative-Report-for-Digital-Credential-Pilot-Final-071825.pdf

- State of Arkansas / Walmart / Google – LAUNCH: Skills-Based Job and Workforce Training Portal (2025)
- Western Governors University – Skills Library (20,000+ Rich Skill Descriptors) and Unified Credential Framework
- Wyoming Innovation Partnership – Digital Credential Wallet Pilot (2024-2025 School Year)

Other National Implementations

- GovTech Singapore – Singpass and National Digital Identity Programme

  https://www.tech.gov.sg/

- Government of Estonia – e-Governance Academy and X-Road Interoperability Framework

  https://www.ria.ee/en/state-information-system/x-tee.html

Multilateral and Policy Frameworks

- OECD – Building Trust in Digital Identity Systems (2023)

  https://www.oecd.org/digital/

- G20 – New Delhi Leaders' Declaration: Digital Public Infrastructure Framework (2023)
- European Union / Canada – Memorandum of Understanding on Digital Credentials

(December 2025)

- FATF – Guidance on Digital Identity (Updated)

  https://www.fatf-gafi.org/

- UNDP Ukraine – DIA Support Project: Digitalization of Public Services (Phase 2, 2024)

  https://www.undp.org/ukraine/projects/digital-inclusive-accessible-support-digitalisation-public-services-ukraine-dia-support-project

Technical Analysis and Commentary

- Spherical Cow Consulting (Heather Flanagan) – Verifiable Credentials and mdocs: A Tale of Two Protocols (January 2024, Updated 2025)

  https://sphericalcowconsulting.com/2024/01/03/verifiable-credentials-and-mdocs-a-tale-of-two-protocols/

- Pomcor – Overview of ISO/IEC 18013-5: Innovations and Vulnerabilities in the mDL Standard (2023)

  https://pomcor.com/2023/10/27/overview-of-iso-iec-18013-5-innovations-and-vulnerabilities-in-the-mdl-standard/

- NXP Semiconductors – Verifiable Credentials and ISO/IEC 18013-5 Based Credentials (White Paper)

  https://collateral-library-production.s3.amazonaws.com/uploads/asset_file/attachment/36416/CS676613_-_Digital_Credentials_promotion_campaign-White_Paper_R3.pdf

The Data Security Council of India (DSCI) is a premier industry body on data protection in India, set up by NASSCOM, committed to making cyberspace safe, secure, and trusted through best practices, standards and initiatives in cybersecurity and privacy. Bringing together governments, industry sectors such as IT-BPM, BFSI, and telecom, as well as data protection authorities, think tanks, and industry associations, DSCI drives policy advocacy, thought leadership, capacity building, and outreach initiatives.

As part of its commitment to strengthening India's cybersecurity ecosystem, DSCI, in collaboration with the Ministry of Electronics & Information Technology (MeitY), Government of India, established the National Centre of Excellence (NCoE) for Cybersecurity Technology Development. NCoE is dedicated to catalyzing cybersecurity technology development and entrepreneurship, fostering innovation across critical and emerging security domains. With state-of-the-art facilities, including advanced lab infrastructure and test beds, NCoE enables research, technology development, and solution validation for adoption across government and industry. By translating innovation and research into market-ready solutions, NCoE is driving the creation of an integrated technology stack, featuring cutting-edge, homegrown security products and solutions.

DYF is a not-for-profit company incorporated under Section 8 of the Companies Act 2013, for the implementation of a digital ecosystem i.e., Digi Yatra Central Ecosystem ("DYCE") aimed at streamlining air travel pursuant to and in accordance with the Digi Yatra Policy issued by Ministry of Civil Aviation (MoCA).

DYF has developed the Digi Yatra Application and DYCE platform, which provides a unique and memorable digital travel experience for air travellers (passengers/users) using real time selfie-based facial biometric verification.

The DYCE uses the concept of Self-Sovereign Identity (SSI) to enable the creation of digital Verifiable Credentials (VC) and allow sharing of these verifiable credentials for identity and travel for the purpose of achieving a seamless, hassle-free travel at airports in India using a single token face biometric, decentralised identifiers ("DIDs") and the created verifiable credentials (VCs).

DYF is committed to protecting user privacy by adhering to SSI principles which empower users with control over their personal data, ensuring that their information is secure, private, and used only for the intended purposes. These principles ensure that users can manage their digital identities with greater autonomy and confidence, aligning with the highest standards of data protection and privacy.

DATA SECURITY COUNCIL OF INDIA

+91-120-4990253 | ncoe@dsci.in

https://www.n-coe.in/

4th Floor, NASSCOM Campus, Plot No. 7-10,
Sector 126, Noida, UP -201303

Follow us on

@CoeNational

nationalcoe

nationalcoe

NationalCoE