aapti institute

THE CONVERGENCE FOUNDATION
CATALYSING PIVOTAL OUTCOMES

Building a Globally-Recognised Digital Skills Passport

Leveraging India's DPI to Enable International Mobility



This is a work of independent research, co-authored by Aapti Institute and The Convergence Foundation in 2026. Aapti Institute is a research and advisory organisation that works at the intersection of technology and society. Aapti examines the ways in which people interact and negotiate with technology both offline and online. The Convergence Foundation (TCF) is an Indian philanthropic foundation. TCF builds and partners with mission-driven nonprofit institutions working on job creating economic growth, human capital development, and growing the development sector.

Authors:
Antara Madavane, Astha Kapoor, Rihan Shareef, Rohan Pai, Shruti T (Aapti Institute)
Manya Beri, Shivangi Amba, Shriya Sethi (TCF)

No generative artificial intelligence (AI) technologies were used in the research, writing or editing of this report.

ACKNOWLEDGEMENTS

In addition to contributions from the wider Aapti and the TCF team, this report also draws from the expertise of numerous academic and industry experts and practitioners. We are grateful for their input during interviews and rigorous feedback sessions.

Report Design and Cover Illustration: Meher Rajpal

Table of Contents

Executive Summary 4

Abstract 5

What are Verifiable Credentials (VC) and Digital Wallets? How are they related to DPI? 6

- The emergence of VCs signal a shift to decentralised DPI 6
- VCs as critical data-sharing DPI 6
- VCs have uses beyond digital identity 8
- Why India should consider a VC system for cross-border mobility of labour 8

How is India positioned within global labour mobility? 10

- Growing perils of the domestic labour market 10
- Changing geopolitical tides and the demand for Indian talent abroad 11
- Creating the right conditions for international mobility 11
- Existing efforts are not designed for international mobility 12
- This gap is especially costly in the context of global mobility 13

Designing a Global Digital Skills Passport for India 15

- Technology: Adopting globally-accepted standards for DigiLocker and other academic credentials 15
- Governance: what needs to evolve 18
- Ecosystem: Adoption and Incentives 21

Conclusion 23

Executive Summary

> India is likely to add roughly **7-8 million young people to its labour force every year** over the next decade. As per the State of Working India 2026 report, despite rising education levels, **roughly 40% of young graduates remain unemployed.** On the other hand, international mobility is on the rise, both for higher education and labour. The outbound student mobility from India recorded a compounded annual growth rate (CAGR) of 8.84% between 2016 and 2024, with 1.33 million students studying abroad as of January 2024—**making India the second-largest source of international students globally.** On the labour front, it is estimated that nearly 700,000 workers move abroad each year. In 2024 alone, at least 18.5 million Indians were working overseas, across major destinations like the USA and the GCC. As per projections from Global Access to Talent from India (GATI), a non-profit focused on creating an enabling ecosystem for overseas employment from India, it is likely that the **current export of 700,000 workers a year will jump to 1.5 million by 2030.**

As the Government of India improves its diplomatic footprint through **bilateral agreements on migration and labour mobility**, alongside national policy changes such as the Overseas Mobility (Facilitation and Welfare) Bill, 2025, it is critical to evaluate how **India's digital public infrastructure (DPI) capabilities can be advanced for cross-border mobility** of students and workers. Growing calls for a **Global Digital Skills Passport** indicate a need for a secure, portable and tamper-proof record of academic qualifications and skills that are **mutually-recognised and trustable**. A skills passport that moves with a student or worker can also reduce the burden of verification, and overcome persistent issues such as candidates applying with fraudulent documents—that have affected India's reputation globally and proved to be **burdensome in terms of cost and time for foreign employers seeking Indian talent.**

Currently, efforts like **DigiLocker and the National Academic Depository (NAD)** are helping digitise and create standardised, verifiable academic records in India. However, this is currently limited to institutions integrated with DigiLocker. Considering multiple academic and skills credential-issuers fall outside this network, there is **still fragmentation in modes through which learners carry these credentials**—for instance, some credentials stored in DigiLocker, some on other learning platforms or as physical documents. These differing formats lead to additional labour for employers or other institutions that are verifying these claims. Open standards such as the W3C Verifiable Credentials Data Model (W3C VC) have not been implemented for education and work records, in India, even though there is an inclination to use these standards for digital credentials globally. Additionally, documents on

DigiLocker are recognised domestically through government directives, but this has not been extended to other countries globally—requiring **stronger diplomatic agreements that extend to mutual recognition and trust in digital credentials.**

As per our findings, there is an **emerging trend to use W3C VCs to create data-sharing pipelines for identity and other personal credentials** across the world. Even within India, UIDAI launched VCs for Aadhaar earlier this year, and DigiLocker has activated these capabilities for identity documents and driving licenses, and is exploring a pilot project linking DigiLocker with the EU Digital Identity Wallet. However, the **data-sharing ecosystem is still nascent** and there is scope to explore how DigiLocker can evolve to function as a Global Digital Skills Passport in India. This requires a deeper examination of whether VCs are the appropriate technical architecture for a Global Digital Skills Passport, and the necessary **governance structures, regulatory mechanisms, business models, funding and legal protections to implement these in India.**

Abstract

In this paper, we examine the potential for emerging data-sharing architectures such as **Verifiable Credentials (VCs), related trust registries and data repositories** to enable and facilitate **international labour mobility in India.**

THE RESEARCH WAS UNDERTAKEN WITH THE FOLLOWING OBJECTIVES:

- To contextualise VCs and digital wallets within India's digital public infrastructure (DPI)
- Provide an understanding of how these technical architectures are developing globally
- Situating India's labour and skills economy within the global mobility landscape
- Evaluating how VCs and data-sharing infrastructure can be designed for labour mobility in India
- The barriers and limitations of implementing VCs and digital wallets at this stage
- Recommendations for stakeholder groups in India for implementing VCs and digital wallets

What are Verifiable Credentials (VC) and Digital Wallets? How are they related to DPI?

The emergence of VCs signal a shift to decentralised DPI

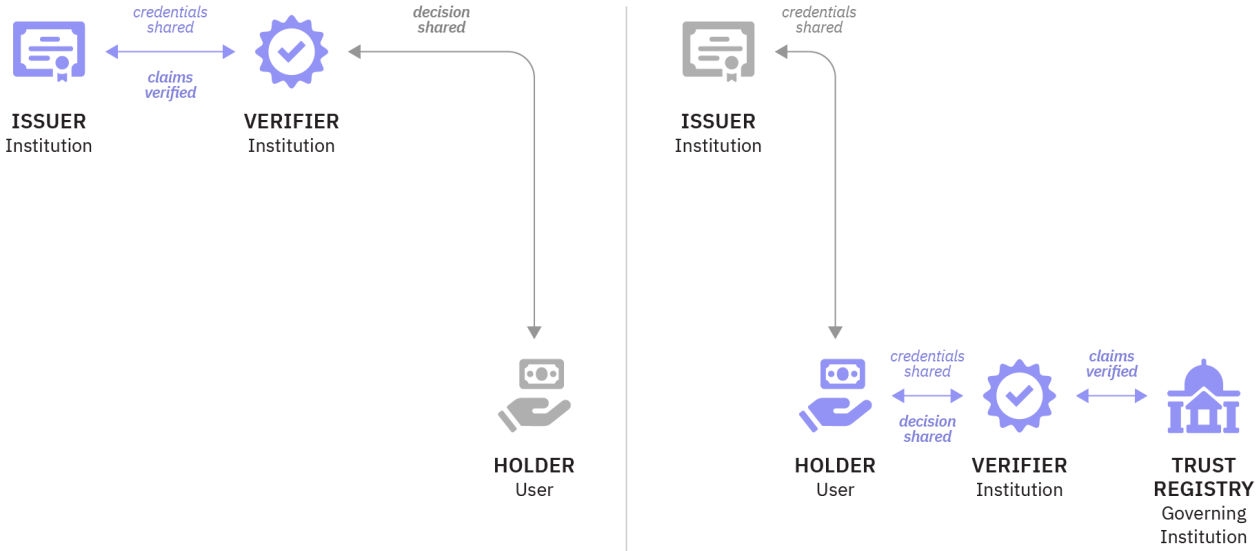
India has been championing the use of Digital Public Infrastructure (DPI) for public service delivery, most notably during its 2023 presidency of the G20. DPI can be understood as shared foundational digital infrastructure that follows 5 core architectural principles: interoperability; reusable building blocks; participatory innovation by market/ecosystem actors; federated and decentralised architecture; and secure and private by design. Although not an exhaustive list, the DPI approach has been centred on 3 building blocks: **digital ID; data sharing; and payments**. Digital ID, in particular, has been the focus of several national efforts globally, and has taken many forms over the years. More recently, a **new infrastructure layer began emerging around the issuance, sharing, and verification of identity data through verifiable credentials (VC).**

Several countries have, or are in the process of, operationalising VC architecture. **India began issuing W3C compliant VCs as part of its Aadhaar digital ID system** earlier this year. Similarly, the EU digital wallet (EUDIW), first proposed in 2021, aims to enable cross-border use of digital identity and credentials. It does this by mandating the use of open standards (like the W3C Verifiable Credential Model) and creating a governance **framework for interoperability and mutual recognition across EU Member States.** A central objective of the EUDI framework is to **give users greater control over their personal data** by allowing them to choose which credentials to share, with whom, and for what purpose. These emerging considerations for implementing VCs as a data-sharing layer within national digital stacks, across foundational layers like ID and for sectoral use-cases such as agriculture, health and education warrants a closer look at its technical architecture.

VCs as critical data-sharing DPI

A VC is a **digitally signed credential** issued by a trusted entity after verifying information against an authoritative source. Together with its ecosystem, it operates as a trusted data sharing mechanism. Unlike conventional digital certificates or scanned documents, **a VC can be authenticated cryptographically without requiring the verifier to contact the issuing**

institution each time the credential is presented. Each credential contains metadata describing its issuance and validity, one or more claims about the holder, and a cryptographic signature that allows the credential to be verified independently of the issuer. VC holders can **selectively disclose** only the information required for a particular transaction while retaining greater control over their personal data.



The VC ecosystem consists of four main functions:

Issuers, create and digitally sign credentials based on trusted information from authoritative sources, such as government agencies, universities, employers, etc.

Holders, or people that receive and store these credentials in a digital wallet, deciding when and with whom to share them.

Verifiers, such as employers, universities, financial institutions and other relying parties validate presented credentials based on shared rules and technical standards (called a trust framework) rather than directly contacting the issuer.

Trust Registry, accrediting institutions that hold public keys for verification.

A defining characteristic of VCs is that they are **built on open technical standards** rather than proprietary platforms. This enables multiple wallet providers, credential issuers, and verification services to operate within the same ecosystem without requiring a single institution to hold or manage all user data. As a result, **VC ecosystems are decentralised by design**, reducing dependence on centralised databases while improving interoperability across organisations.

This growing focus on VCs signals **a shift from building foundational national digital identity systems, to enabling users to securely prove attributes about themselves through an interoperable, data-sharing mechanism** in several different contexts. Rather than simply establishing who a person is, VCs enable users to securely prove specific attributes or qualifications about themselves while retaining greater control over their data. This also reflects a broader evolution in digital identity systems **towards decentralised architectures**, where trust and verification are distributed across multiple actors rather than concentrated in a single authority. In doing so, they embody many of the characteristics associated with the DPI approach—interoperability, modularity, public-interest orientation, and the ability to support multiple public and private sector use cases— and address many of its risks— user control, privacy, and cross-border recognition/interoperability.

VCs have uses beyond digital identity

Although VCs have gained prominence through digital identity initiatives, they are **fundamentally a standardised format for sharing trusted data and can therefore be applied across sectors** wherever verified information needs to move between multiple actors. The African Union's Digital Trade Protocol, under the AfCFTA efforts, requires state parties to adopt certification mechanisms and digital credentials that are interoperable and mutually-recognised, mirroring VC architecture. Similarly, the United Nations Transparency Protocol recommends the use of W3C VCs for cross border trade certificates and sustainability assessments. VCs are especially **useful in sectors that rely on certifications or qualifications that have to be verified**, as it removes the need to cross-check a credential's authenticity with its issuer. This need is amplified when the credentials are intended to be used internationally, as the verifier's ability to trust the issuing institution and confirm the credential's authenticity is further diluted.

Why India should consider a VC system for cross-border mobility of labour

Education and skilling are particularly strong examples, where qualifications are presented across jurisdictions but remain difficult and costly to verify. This is recognised as a use case by the W3C standards body, as it automates and cryptographically presents key information

about this issuing institution— such as a university or a standardised testing body— to an interested party for verification. The **credential itself can take the form of a digital transcript, a skilling certificate, an english proficiency certificate, or a proof of work record** among other use-cases. A VC system would allow the holder—in this case a student or a job-seeker—to store these credentials in their digital wallet, and present them when needed. Several national and regional efforts around VCs for education are underway, with the EUDIW specifically focusing on education credentials for cross-border use. Currently, efforts like DigiLocker and the National Academic Depository (NAD) are helping digitise and create standardised, verifiable academic records in India. However, for **DigiLocker** to facilitate international mobility, **W3C-compliant VCs will be a crucial addition to enhance its existing capabilities** and function as a Global Digital Skills Passport. This will unlock technical interoperability with international verifiers or relying parties (employers, universities and so on), making data-sharing and verification of education and skills credentials more efficient and trustworthy. As of now, DigiLocker does not offer this capability for academic credentials, proving to be a bottleneck for cross-border mobility.



How is India positioned within global labour mobility?

Growing perils of the domestic labour market

India is likely to add roughly **7-8 million young people to its labour force every year** over the next decade, and the 2024 India Employment Report, jointly published by the ILO and the Institute of Human Development, found that **Indian youth account for nearly 83% of the country's unemployed.** More strikingly, the share of unemployed youth with secondary education or higher nearly doubled between 2000 and 2022, indicating a **growing mismatch between qualifications and available work (as opposed to a shortage of qualified professionals).** As per the more recently published State of Working India 2026 report, despite rising education levels, roughly 40% of young graduates remain unemployed, and **a degree no longer functions as a reliable bridge into formal work.**

This is compounded by the type of job opportunities the economy creates. **More than half of India's workforce is self-employed**, but this has been gradually declining and **drifting toward low-productivity informal activity and unpaid family work**. Regular, formal salaried employment remains a narrow slice of total employment. Additionally, figures also point towards a structural skills mismatch: a large share of the workforce entering the labour market each year has had **minimal exposure to vocational or technical training**, even as employers report difficulty finding workers with the specific skills they need.

The result is a **labour market that is simultaneously youth-heavy and job-short**. For a workforce that employs nearly 600 million people (with informal arrangements estimated to be around 79% in rural areas and 67% in urban areas), **outward mobility is perceived as a well-calculated risk**, and not just as an aspiration. Domestically, there are minimal legal protections and avenues for grievance redressal, monthly salaries stand at less than Rs 10,000 for 94% of the registered informal economy on e-Shram, and structural barriers prevent upward mobility. India's demographic dividend is time-bound: the **window in which the working-age share of the population peaks is expected to close within roughly a decade or two**, which means the pressure to convert this workforce into productive employment, domestically or abroad, is a policy goal that needs immediate attention. However, emerging geopolitical trends paint a different picture.

Changing geopolitical tides and the demand for Indian talent abroad

India has moved decisively from ad hoc labour agreements toward comprehensive mobility diplomacy: as of mid-2026, External Affairs Minister S. Jaishankar noted that **India has signed 28 Migration and Mobility Partnership Agreements with 26 countries**, spanning the UK, Germany, France, Australia, Italy, Japan, and others. Trade policy has followed the same logic: the India-EU FTA concluded in January 2026 was signed alongside a separate Mobility and Migration Agreement that **substantially expands legal pathways for Indian students and skilled workers**, while the India-UK Comprehensive Economic and Trade Agreement will ease visa procedures and simplify entry categories for Indian professionals, indicating a broader shift from trade-only agreements toward talent-driven partnerships. This is not simply India pushing its youth outward: it **reflects a convergence of interests, as destination economies facing their own labour shortages—Japan, the UK, Portugal, and several EU states among them—actively court Indian workers through structured, legal channels.** Supporting these trends are government and international mobility datasets that have consistently recorded a sharp rise in the number of Indian students pursuing education abroad in the post-pandemic period.

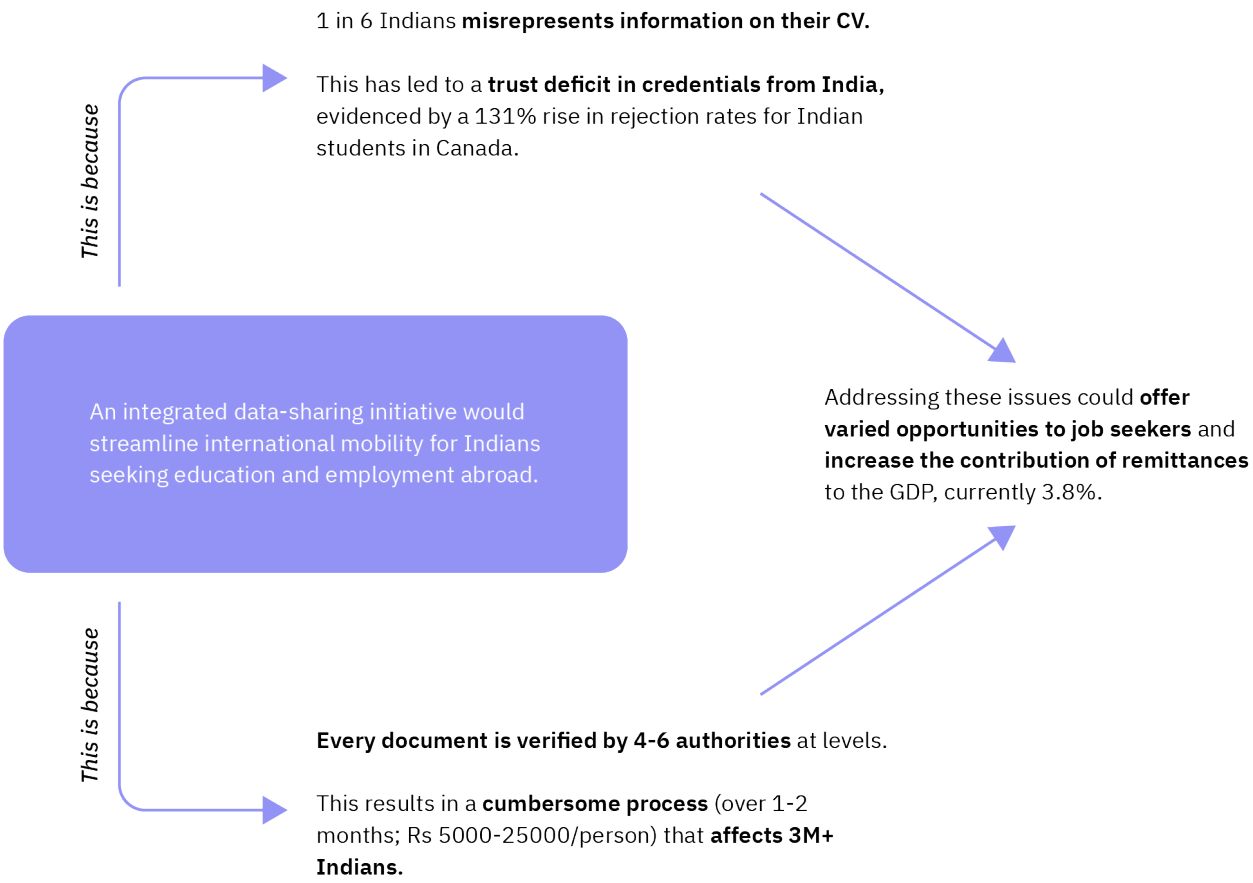
The result is a **policy environment newly favourable to international mobility, at precisely the moment domestic job creation is falling short**. This raises the stakes on the infrastructure and conditions meant to support that mobility considerably. However Indian workers seeking employment overseas continue to face a landscape defined more by informal networks than by institutional infrastructure. Nevertheless, the Indian government is interested in rethinking its role and modernising the regulatory environment, and platforms such as eMigrate that facilitate Emigration Check Required (ECR) passports for workers traveling to any of the 18 notified ECR countries are growing efforts in this direction.

Creating the right conditions for international mobility

A growing number of legal pathways will need to be complemented with **mutually-recognised legal protections and credentialing systems** that allow workers to leverage mobility agreements through portable qualifications and a verifiable proof of skills. The current nature of these agreements risk creating demand that Indian workers are structurally unequipped to meet due to **gaps in cross-border standardisation of skills-recognition, credential-verification formats and labour protections.**

Beneath these requirements are structural weaknesses that affect cross-border mobility for students and workers in various contexts. **Data on education and skilling remains locked in formats that do not travel: physical mark sheets, scanned PDFs, and institution-specific databases that neither employers abroad nor foreign credential evaluators can easily read or trust.** Even where digitisation has occurred, it has rarely produced a standard that different

systems can speak to one another in. This fragmentation in formats for education credentials makes **verification costly and time-consuming for institutions and employers alike.**



Cross-border checks on Indian degrees and certificates still typically involve **manually contacting the issuing institution**. Skill India Digital Hub (SIDH) identifies this as a shortcoming, and cites the lack of a fast, low-cost verification method as a core gap in the ecosystem. Discoverability is a related but distinct failure: workers with genuine skills and employers with openings frequently cannot find each other except through informal intermediaries, and this **absence of a trusted matching layer creates space for intermediaries (background verification, migration agencies) to extract value**. Underlying all three is a **deficit of trust**—between institutions, between employers and workers, and between Indian systems and the foreign systems meant to recognise them.

Existing efforts are not designed for international mobility

DigiLocker has made document storage and domestic verification meaningfully faster, and its **National Academic Depository (NAD)** allows verifying entities (including some overseas employers) to check academic records with consent. But DigiLocker's design is Aadhaar-

anchored and India-specific; as one comparative analysis notes, its **standards are difficult to translate into other national systems**, which limits its usefulness for people pursuing opportunities abroad. The **Skill India Digital Hub (SIDH)**, launched in 2023, goes further by integrating enrolment, assessment, certification, and portable verified credentials on a single platform, and has onboarded over 1.5 crore candidates to date. Yet SIDH too is built around domestic schemes, domestic issuers, and Aadhaar-based identity; it was **not designed with cross-border recognition as a first-order use case**. Both platforms solve for storage and domestic verification; neither solves for interoperability with the credential systems Indian workers and students actually encounter abroad.

This gap is especially costly in the context of global mobility

	DOMESTIC	INTERNATIONAL (APOSTILLE)	INTERNATIONAL (ATTESTATION)
Primary verification need	Identity Document, Education Records, Skill Certifications, Criminal Record (certain sectors)	Identity Document (including passport), Education Records, Skill Certifications, Commercial Documents	Identity Document (including passport), Education Records, Skill Certifications, Commercial Documents
Who are the verifiers	Third-party background verification, and employers	**Notary Public, State/HRD, Education Dept, Commercial Dept, Ministry of External Affairs**	**Notary Public, State/HRD, Education Dept, Commercial Dept, Ministry of External Affairs, Embassy**
Time taken to verify	Private Sector: 7 to 30 days Government: 30 to 180 days	SEI/Employer: 15-30 days Notarisation: 1 day State/HRD: 7-15 days MEA: 1-3 days **Total: 24 - 48 days**	SEI/Employer: 15-30 days Notarisation: 1 day State/HRD: 7-15 days MEA: 1-3 days Embassy: 5- 10 days **Total: 29 to 58 days**
Cost of verification	Rs 150 to 5000	**₹5,000-15,000**	**₹10,000-25,000**
Who bears the cost	Skilling and Educational Institutions (SEI)/Employers	**Worker/Student/ Employers/SEIs**	**Worker/Student/ Employers/SEIs**
Cost of trust deficit	Costs of verification are lower due to **informal arrangements** and **lower risk** borne by candidates for domestic jobs.	As per reports, an estimated **10 lakh individuals** from India carry **fraudulent credentials**, affecting the **credibility of Indian institutions globally**, with international employers bearing **high costs in verifying documents**. Due to lower trust, **multiple stakeholder groups are engaged in verification for international mobility.**	

There is no standardised route by which an Indian qualification becomes legible to a foreign employer or institution. **Each corridor, sector, and destination country requires its own bespoke reverification**, often repeating checks that have already been done domestically. Into this vacuum step **recruitment agents and sub-agents**, who research shows routinely **charge migrants fees well above regulated limits**, sometimes more than a month's worth of overseas income. Higher recruitment costs are, in turn, associated with worse outcomes abroad—irregular pay, unmet contract terms, and greater vulnerability to exploitation. This gap in trusted information is what makes middlemen indispensable in the first place.

As a result, there is a need to reconsider how India's DPI capabilities can be advanced to meet the emerging requirements of a growing worker outflow, that is projected to grow twofold by 2030. DigiLocker and other skilling efforts provide a strong foundation, but considerations on technical standards, institutional capacity and ecosystem sustainability are critical factors that will determine India's capabilities to leverage its demographic dividend.



Designing a Global Digital Skills Passport for India

This section examines what India would need to address to meet rising international mobility demand for its students and workers. It does not attempt to settle these questions; rather, it lays out three areas of inquiry that the evidence so far points to as significant: **the technology layer** (what infrastructure already exists and where it appears to fall short), **the governance layer** (questions of ownership, funding, and accountability), and **the ecosystem layer** (whether current incentives are sufficient to bring each stakeholder group in).

A starting hypothesis worth testing is whether DigiLocker, and specifically the National Academic Depository (NAD) built within it can function as the technical basis for a **Global Digital Skills Passport.**

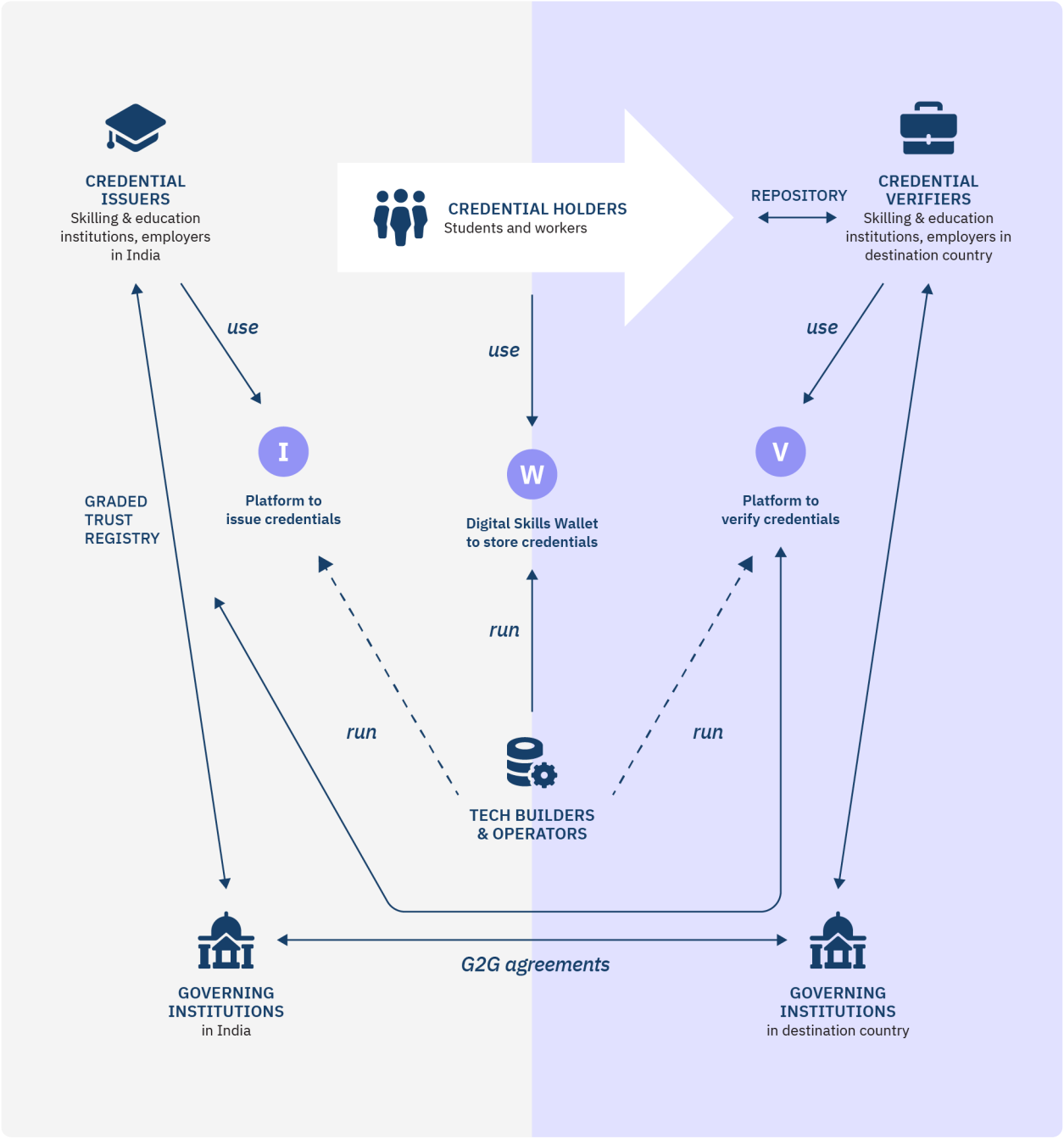
The available evidence suggests DigiLocker and NAD are digitising and standardising academic records, but their coverage appears bounded by which institutions have integrated with the network. A meaningful share of academic and skills-credential issuers likely sit outside it—though the precise scale of this gap does not appear to have been quantified publicly.

This unresolved fragmentation appears to keep the verification burden on employers and institutions, who still have to reconcile credentials arriving through different channels. Open standards such as the W3C Verifiable Credentials Data Model do not yet appear to have been applied to education or work records specifically in India, even as the broader inclination—both domestically and internationally—seems to be toward this kind of standard. Some precedent does exist: UIDAI has been piloting Aadhaar Verifiable Credentials and has run a VC "ID'athon" to prototype use cases, but this work appears to have centred on identity attributes rather than skills or academic records, and it is not clear whether or how readily those learnings would transfer.

Technology: Adopting globally-accepted standards for DigiLocker and other academic credentials

Currently, **DigiLocker is structured to be a centralised repository** of citizen documents that is developed over technical specifications like URI pointers, OAuth 2.0, and PKI digital signatures. **Authenticating documents requires validating the issuer's centralised digital signature or querying the live repository**.

On the other hand, W3C VCs allow offline cryptographic verification via decentralised identifiers (DIDs). Global trends already show an uptake of W3C VCs as an accepted standard across regions and sectors, with a strong focus on education records. By building on global and open standards, education records presented on DigiLocker can be verified interoperably by other wallet providers that lie outside its ecosystem—improving the acceptance of its credentials in a global labour market, resulting in **better international competitiveness for candidates from India and reducing the burden of having relying parties integrated in the DigiLocker network**.



A shift to open standards like W3C VCs would require investments in technical service providers and the addition of new data-sharing layers. Suggested here are a set of digital interventions to develop this infrastructure, but as highlighted below, each of these technical choices and its success are closely linked to choices made on the governance of the ecosystem:



ISSUERS: DigiLocker will have to adopt W3C VCs to evolve from **a centralised repository to an issuer** in the ecosystem. Essentially, this would ensure that skilling and educational institutions—that shift to common standards (W3C VC in this case)—are **interoperable with DigiLocker** even if they are not integrated within the application's network. However, this **would require institutions to invest resources and capacity in onboarding technical providers** to digitise and issue VCs.

Whether that onboarding is mandatory or incentivised, and what the associated cost and technical burden looks like, may determine how much of the underlying fragmentation problem is actually addressed.



DIGITAL WALLETS (OR DIGITAL SKILLS PASSPORT): VCs offer a means through which credentials can be user-controlled and decentralised, but it is **important to place such technical architecture within governance structures and regulatory environments that can support this.** In the case of DigiLocker, **MeitY remains both the regulator and the operator**, "as the rule-setter for standards, data protection and privacy, MeitY is responsible for ensuring compliance; yet as the product owner, it also designs, manages, and promotes DigiLocker's growth". An institutional setup of this kind disincentivises other digital wallet providers from participating in the ecosystem, and monopolises the digital pathways toward public trust. As the regulator, it **would be beneficial for MeitY to publish a preferred common standard (W3C VCs), and allow issuers, credential holders, and verifiers to choose technical providers of their choice to implement this**. This will incentivise private participation for the provision of digital wallets and reduce the burden on the State (or initiatives like NAD) to scale the infrastructure.



TRUST REGISTRIES AND REPOSITORIES: NAD's function would need to expand from a repository of participating institutions' records toward something closer to **a trust registry with international interoperability**, aligned to standards such as the W3C VC data model and decentralised identifiers (DID)—a step it does not appear to have taken yet. A **shift toward W3C VCs and a multi-provider wallet model only functions if verifiers can trust who issued a credential,** not just that its signature is valid. This requires trust registries, i.e., publicly queryable lists of which institutions are authorised to issue which categories of credentials. In India's context, bodies like NCVET (for skills and vocational qualifications) and UGC/AICTE (for academic degrees) are natural choices to run and maintain these registries, given their existing accreditation mandates.

ACCREDITATION-AS-PAPERWORK IS DIFFERENT FROM ACCREDITATION-AS-INFRASTRUCTURE: These institutions would need technical and operational capacity to maintain machine-readable registries, issue and rotate DIDs, respond to revocation requests, and audit issuer compliance on an ongoing basis. This is a governance function as much as a technical one, and a **decentralised trust architecture developed over a common standard** can allow academic accreditors to retain their regulatory role—a function that is currently diluted by DigiLocker.

VERIFIERS: This appears to be where the more significant open questions sit, since the verifier base would need to extend **beyond domestic institutions to foreign employers, visa and immigration authorities, and foreign credential-recognition bodies, none of whom currently have an established basis for trusting a DigiLocker-issued document**. While choices on data-sharing standards will determine technical interoperability, **integration will still depend on diplomatic agreements and bilateral policies** that approve these trust mechanisms. At the 3rd India-EU Trade and Technology Council, both sides agreed to explore a pilot linking the EU Digital Identity Wallet and DigiLocker—a preliminary and still-exploratory signal, not yet tied to skills or academic credentials specifically, of what cross-border verifier trust might eventually require.

Recognition abroad sits somewhat outside the technology question itself: DigiLocker documents currently carry weight through domestic government directive, and extending that recognition internationally would likely depend on diplomatic negotiation rather than following automatically from the technical architecture. The next section focuses further on governance and policy choices that will determine the effectiveness of these technological layers.

Governance: what needs to evolve

India's existing DPI systems offer a partial, imperfect basis for comparison on governance questions. UPI, ONDC, DigiLocker, and the Account Aggregator (AA) framework have each taken different approaches to **ownership, participation, business model, and sustainability**, and it is worth analysing these to understand constraints that prevent Indian policymakers and regulators.

	UPI	ONDC	Digilocker	AA	Takeaways For Skills And Jobs Data-Sharing
Ownership	Legal Basis PPP Model Delegation	Weak Basis PPP Model Contractual	Legal Basis State-led	Industry-led PPP Model Regulated	Governance models show that NPOs as an anchor institution balances both state and market interests, balancing adoption, regulatory accountability and public interest. Jobs and skills will require a **multi-stakeholder consortium.**
Participation & Mandates	Top-down Rules-based	Top-down Rules-based	Top-down Mandated	Mandated Incentivised	**Issuers** (training providers, universities, assessment bodies) will need to be **onboarded mandatorily** through a national credential standard. **Verifier** (employers, visa authorities, banks) participation can be designed **through incentives.**
Business Model	Direct Costs Rent-Seeking	Structured Pricing Market-led	Public Good Adoption-led	Structured Pricing Direct Costs	Credential issuance should be **zero-cost to the user** (public good). **Verifiers can be charged API fees** to sustain the infrastructure, but this needs to be **lower than current cost** of verification to keep them incentivised to participate.
Sustain-ability	Public Money Uncertainty	Public Money Uncertainty	Public Money Uncertainty	Donor-funded Incentivised	Limit government to seed-funding, invite **donors once proof-of-concept is established** and draw out an **early roadmap** taking into account current pricing structure and incentives (API pricing + use-cases like international mobility)
Policy Process	Centralised Adaptive Market-led	Delegated Market-led	State-led Closed gov	Delegated Decentralised Nascent	Multiple entities exist—MoSDE/NSDC for skilling credentials; MoLE for labour; NIC/DigiLocker for infrastructure. Primary requirement would be establishing a **coordination framework to prevent policy bottlenecks** and making **room for participation—issuers, verifiers and users.**
Grievance Redressal	Policy-backed Shared Liability	Network-reliant Techno-legal	No Anchor Undefined	Policy-backed Shared Liability	User must retain **sole control on revocation, correction, erasure.** An **independent ombudsman** handles disputes between learners, issuers, and verifiers.



UPI operates on a fairly clear legal basis and a public-private partnership model, with rules-based, top-down bank participation. Policies like zero-MDR have reinforced notions of public technologies, but this comes at the cost of commercial service providers and market entry. Overall, sustainability still appears to depend heavily on public funding and banking infrastructure.



ONDC rests on a comparatively weaker statutory basis, operating through contractual and PPP arrangements rather than dedicated legislation. Its business model also appears unsettled, as **adoption is highly dependent on network participation that is currently low**. Sustainability remains tied to continued public funding, but this can change quickly with better incentives for network participants.



DigiLocker has a clearer legal basis but more state-led ownership than the others, with mandated, top-down participation. It functions as a public good with adoption-led growth. Its most notable gap appears to be governance around disputes—there is **no clearly identified anchor institution, and the grievance-redressal mechanism appears largely undefined**. This profile may be adequate for a domestic document locker, but the evidence suggests it would be tested considerably by the involvement of foreign employers, visa authorities, and cross-border disputes.



The **Account Aggregator framework** presents a comparatively more differentiated model: industry-led but regulated ownership, structured as a PPP; participation split by role (issuers mandated, verifiers incentivised); structured, tiered pricing rather than flat direct costs; sustainability drawing on donor and incentive support; and a grievance framework that is policy-backed with liability assigned between parties. Whether this constitutes a transferable model for DigiLocker's evolution, or simply a different system optimised for a different context, is a distinction worth testing further.

Applying a six-layer governance framework to the specific question of DigiLocker's evolution surfaces where the more significant gaps appear to sit:

1. **OWNERSHIP:** DigiLocker's **current state-led ownership structure may not be well suited to carrying international weight**; the evidence from AA suggests a multi-stakeholder consortium—potentially spanning skilling and labour ministries, the Ministry of External Affairs, and eventually international counterparts—is worth examining as an alternative.

2. **PARTICIPATION AND MANDATES:** The institutions and issuers still outside the NAD network represent the core of the fragmentation problem identified above; how their onboarding is structured (mandate versus incentive) is likely to shape how quickly, or whether, that gap closes. With the inclusion of international institutions and wallet providers, **digital sovereignty will feature as a core concern, but this will have to be weighed against economic competitiveness.**

3 **BUSINESS MODEL:** Keeping issuance free to the learner or worker appears important on equity grounds; a more AA-like structured pricing model for verifiers, **weighted toward the foreign employers and visa authorities who currently absorb the cost of manual verification**, is one direction worth testing. As long as the VC verification fee is priced less than its current manual alternative—which remains high, especially for foreign verifiers—this is unlikely to negatively impact adoption.

4 **SUSTAINABILITY:** Government funding directed toward standard-setting and NAD expansion, with **donor or partner funding introduced once a pilot corridor demonstrates feasibility**, is one plausible sequencing, though it has not been tested in this context.

5 **POLICY PROCESS:** The Overseas Mobility (Facilitation and Welfare) Bill, 2025, proposed to replace the Emigration Act 1983, includes a proposal to establish an **Overseas Mobility and Welfare Council for inter-ministerial convergence**. Whether this coordination mandate would extend to DigiLocker's credentialing function specifically, or remain focused on welfare and facilitation as currently drafted, is not yet clear from the available text. A coordination framework can prevent policy bottlenecks and make room for participation—issuers, verifiers and users—that need access to credentials from a varying set of institutions. For instance, an international employer should be able to access public keys from multiple issuers without contacting them directly.

6 **GRIEVANCE REDRESSAL:** This appears to be the most consequential gap identified in this analysis, particularly once fraud enters the picture. The fake-degree scandal that surfaced in Australia offers a concrete illustration of the **reputational stakes involved in the absence of an independent, cross-border-aware dispute mechanism.**

Ecosystem: Adoption and Incentives

Participation by each stakeholder group appears contingent on distinct, and in some cases untested, incentive structures. The following draws on available labour and education mobility data to assess where those incentives currently look strongest and weakest.

LEARNERS AND WORKERS: A Global Digital Skills Passport could reduce friction and cost for those pursuing opportunities outside the domestic labour market, though the magnitude of that effect cannot be established empirically at this point of time due to digital credentials still being a nascent architectural choice for education and skilling.

SKILLING AND EDUCATIONAL INSTITUTIONS: The incentive here appears more reputational and access-based than financial; issuers within a recognised, interoperable standard may become more attractive to learners and employers, though this could function as the starting point for network effects.

EMPLOYERS AND VERIFIERS, PARTICULARLY FOREIGN ONES: The case rests on time and cost savings relative to current manual verification, and reduced exposure to the kind of fraudulent-document risk that has already affected trust in Indian qualifications abroad.

GOVERNMENT: The GATI Foundation projects that India's annual worker exports could roughly double, from 700,000 to 1.5 million, by 2030. This suggests a credible verification layer could strengthen India's position in the bilateral labour agreements anticipated under the Overseas Mobility Bill, though the projection itself warrants independent scrutiny.

DESTINATION-COUNTRY INSTITUTIONS: A lower-cost trust mechanism may make diplomatic tasks such as mutual recognition agreements more tractable, though discussions such as the EU wallet interoperability remains at an exploratory stage and offers limited evidence either way at this point.

Taken together, the evidence points toward a phased-expansion path as more plausible than a build-from-scratch sequencing. Capacity-building current institutions that fall under NAD to onboard digital VC architecture, and further coverage among institutions most implicated in outbound mobility is the need of the hour. Standard-setting work will rest on participation from issuers, but treating mutual recognition as a parallel diplomatic track rather than a downstream step is necessary. Whether this sequencing holds up, and whether DigiLocker's existing architecture requires more rebuilding than evolution, remains an open question that requires further evidence.

Conclusion

India's working-age population is expected to continue growing over the coming decade, projected to reach 1.04 billion by 2030. This is both a significant opportunity and a policy challenge: as India continues to develop global talent and labour corridors, it must also address the information asymmetries, institutional gaps, and procedural inefficiencies that currently shape international mobility. A Global Digital Skills Passport developed over a W3C-VC compliant ecosystem has the potential to reduce some of these frictions by enabling trusted interoperable credentials that can be verified across jurisdictions, while allowing individuals to retain greater privacy and control over their personal data. These benefits can however only be realised alongside parallel efforts to strengthen labour market governance, improve worker protections, and increase trust between institutions.

Mapping actors & positioning digital interventions	Jurisdiction-specific corridors	Sector-specific use cases
Understanding the **level of digitisation** and involvement of tech players in the global mobility process in India.	Each jurisdiction may have its **own complication in the verification** process. Eg:- In certain countries only the federal government verifies, in others states also verifies.	Each sector has its **own set of standards** that are required in terms of **course verification and eligibility**
Mapping the **digital landscape** adopted by **various stakeholders** involved in global mobility in India.	Each jurisdiction may additionally have its **own standard setting organisation**, that may require more in-depth information.	Each sector may additionally require clearance from **own standard-setting organisation**, and in certain cases clearances of examinations
Devising incentives for these are necessary for the success of the scheme; **barriers could drive workers to more informal routes.**	The **costs and process may vary due to these challenges**, along with **technical capacity to implement the scheme** - understanding the fragmentation is important to solve for it.	The **costs and process may vary due to these challenges**, understanding the complexity and sector-specific needs are required for effective implementation.

There remain many unanswered questions about how this VC system will operate, who are the institutions that will adopt it, what risks it may create for users and non-users, and how the system will sustain itself. An implementation strategy should begin with mapping the existing (global mobility) ecosystem, including relevant stakeholders, the current level of digitisation, prevailing data-sharing practices, and the institutional and technical capacity of participating organisations. Since this is a system that is intended to apply across jurisdictions and sectors—with differing standards and requirements— pilot implementations focused on a specific labour corridor or sector could help highlight existing workflows, verification needs, capacity gaps, and institutional roles. These learnings can then inform the design of a scalable and interoperable VC system. In addition to technical architecture, developing a comprehensive governance model is especially important. This includes establishing trust frameworks, defining institutional roles and responsibilities, creating incentives for issuers and verifiers to participate, ensuring the applicability of data protection and privacy safeguards, providing accessible grievance redress mechanisms, and developing mutual recognition agreements with destination countries. Like with any DPI system—particularly one likely to impact users' livelihoods—these questions of governance and ecosystem-building must be prioritised over technical design choices, as they will decide the success and sustainability of a VC system.





The Convergence Foundation (TCF) is an Indian philanthropic foundation. TCF builds and partners with mission-driven nonprofit institutions working on job creating economic growth, human capital development, and growing the development sector.

connect@theconvergencefoundation.org | www.theconvergencefoundation.org



Aapti is a research and advisory institute that works at the intersection of technology and society. We examine the ways in which people interact and negotiate with technology both offline and online.

contact@aapti.in | www.aapti.in

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 2.5 India License.

View a copy of this license at creativecommons.org/licenses/by-nc-sa/2.5/in/