User-Centric Credentialing and Personal Data Sharing

VISION PAPER

Foreword

This vision paper presents a practical approach to user-centric data sharing through credentialing. It explores how verifiable credentials can make trusted data universally accessible, giving individuals control and self-custody over their personal data and digital assets while unlocking economic opportunities. It serves as a simple primer for countries seeking to improve citizens' lives through secure and scalable data-sharing models. It also serves as a universal architecture approach for the industry to implement data credentialing to drive innovation and efficiency across various sectors.

This paper is a result of global collaboration, and brings together development partners, DPG community, standards organizations, and the private sector, anchored by the Centre for Digital Public Infrastructure (CDPI).

This paper is an important step in the journey of unlocking personal data as an economic asset for individuals and businesses. It will be followed by sandboxes, articles providing technical guidance, and other community-driven initiatives to drive adoption. We invite you to share your feedback and participate in this journey to make trusted and secure personal data sharing accessible to billions worldwide.

Share your comments using info@cdpi.dev and also watch https://cdpi.dev for future efforts.

Acknowledgments

We are grateful to colleagues worldwide who have been instrumental in this work, offering peer reviews and valuable insights to the previous version of the paper published for public consultation.

This work is a result of contributions from the following people:

1. Anusree Jayakrishnan, Centre for Digital Public Infrastructure
2. Carlos Santiso, OECD
3. Cecilia EMILSSON, OECD
4. Christine Kim, CoDevelop Foundation
5. Chrissy Martin, DIAL
6. David Eaves, University College London – Institute for Innovation and Public Purpose (UCL IIPP)
7. Daniel Abadie, Centre for Digital Public Infrastructure
8. Daniel Amewor, Centre for Digital Public Infrastructure
9. Daniel Goldscheider, Open Wallet Foundation
10. Edward Duffus, OpenCRVS
11. Jacob Arturo RIVERA PEREZ, OECD
12. James Stewart, Public Digital
13. Jon Crowcroft, The Alan Turing Institute
14. Julia Clark, World Bank
15. Kamya Chandra, Centre for Digital Public Infrastructure
16. Kanwaljit Singh, Gates Foundation
17. Kathleen McGowan, DIAL
18. Kunjbihari Daga, Microsave consulting
19. Lindsey Crumbaugh, CoDevelop Foundation
20. C V Madhukar, CoDevelop Foundation
21. Manish Srivastava, egov Foundation
22. Marika Popp, GovStack
23. Mitul Thapliyal,Microsave consulting
24. Neha Narula, MIT Media Lab / MIT Digital Currency Initiative
25. Pete Herlihy, Amazon Web Services
26. Pramod Varma, Centre for Digital Public Infrastructure
27. Prem Ramaswami, Google
28. Priya Jaisinghani Vora, DIAL
29. Priyanka Yadav, Deloitte
30. Ramesh Narayanan, MOSIP
31. Ritul Gaur, DIAL
32. Sanjay Jain, Gates Foundation
33. Sasikumar Ganesan, MOSIP
34. Siobhan Green, (formerly) US Agency for International Development
35. Surendra Singh Sucharia, Dhiway
36. Tanushka Vaid, Centre for Digital Public Infrastructure
37. Tejas Ji, Deloitte
38. Vijay Vujjini, Centre for Digital Public Infrastructure
39. Ville Sirviö, Nordic Institute for Interoperability Solutions
40. Vineet Bhandari, Centre for Digital Public Infrastructure
41. Vyjayanti T. Desai, World Bank
42. Yash Koli, Deloitte

Table of Contents

Data is one of the most valuable resources in the 21st century

Interactions of individuals with society create a lot of data. This is even more true in the digital world, where each interaction captures rich, granular, and valuable data. This data, on our behavior, entitlements, relationships, transactions, affiliations, and more, is perhaps **one of the most important assets an individual or small business has to unlock economic opportunities.**

Today, such personal data and documents are in silos spread across the many institutions and systems with whom they interact. Hospitals have medical data, universities have academic transcripts, financial institutions have money movement data, governments have data about citizens and businesses, social media giants have data on preferences, e-commerce platforms have data on purchase/sale history, employers have data on work experience and performance, and so on.

Today, some of this data is given back to users mostly in paper, cards, and digitized formats – PDFs, MS Word documents, spreadsheets, papers, smart cards/ plastic cards, and papers with holograms, among others. These are the 'currency' every individual or small business has to get access to various services and unlock newer opportunities.

Unfortunately either data stays locked in silos or these paper/digitized copies shared with users **remains high cost, low trust** due to ease at which data can be faked.

The need for trusted personal data has led to a dependence on institutions to directly share it

Most of the forms of data we see around us (pdfs, spreadsheets, paper-based, etc) are not inherently trustworthy due to lack of verifiability. If an individual receives a PDF of their bank statement and then submits it to a potential lender, how does the lender know that the data was not modified/faked by the individual? In the physical world, notarization was a common practice, where a trusted, well-respected person (often a government employee) attested to the authenticity of the documents/copies. This was no better when it came to ensuring trust given such physical attestations can also be easily faked. How was someone to trust the notary's judgment or the veracity of the document itself?

Technological advancements have made forgery effortless, making it impossible for any verifier to adequately verify paper/cards/digitized-docs/etc that the data is authentic and has not been tampered with.

One way to guarantee trust in the data is to get it directly from the data provider/ custodian.[1]

In old, paper-based days, **one would physically send someone (background verification) to the data provider institution to verify the information submitted by the user.** The physical verification processes were **expensive, time-consuming, painfully manual,** and limited the scale and scope of any innovation.

In the digital world, data provider institutions can share information digitally with the data seeker/consumer institution. **This model, which is reliant on the data provider institutions to provide non-tampered, trusted data, requires two digital systems to talk to each other** using what's known as an **Application Programming Interface (API).** Two digital systems, under agreed business contracts, can share data between them by leveraging the relevant APIs through technical provisioning of APIs and integration between their systems.

> **Think of APIs as tools one institution/system (API provider) can use to expose services to other institutions/systems (API consumer). The services can vary from accessing data, responding to a query, triggering a task, and so on.**

In the lending example, the lender institution integrates the bank's (in this case the data provider) APIs within their workflows and digitally requests (via API call) the bank to share relevant user information to offer a loan. This type of data sharing is known as **system-to-system data sharing, where the data exchange happens between the data provider and data seeker/consumer** at the request (typically with the consent) of the user. Such system to system API driven digital flows bring **higher trust, lower costs (compared to manual verification), and eliminate delays, as opposed to the paper-based flows.**

At an individual-transaction level, it seems as if we have achieved a seamless flow of trusted personal data between two systems. **Playing out this system-centric data sharing model across sectors and geographies at a global scale makes the impossibility of this approach beyond limited scenarios painfully apparent.**

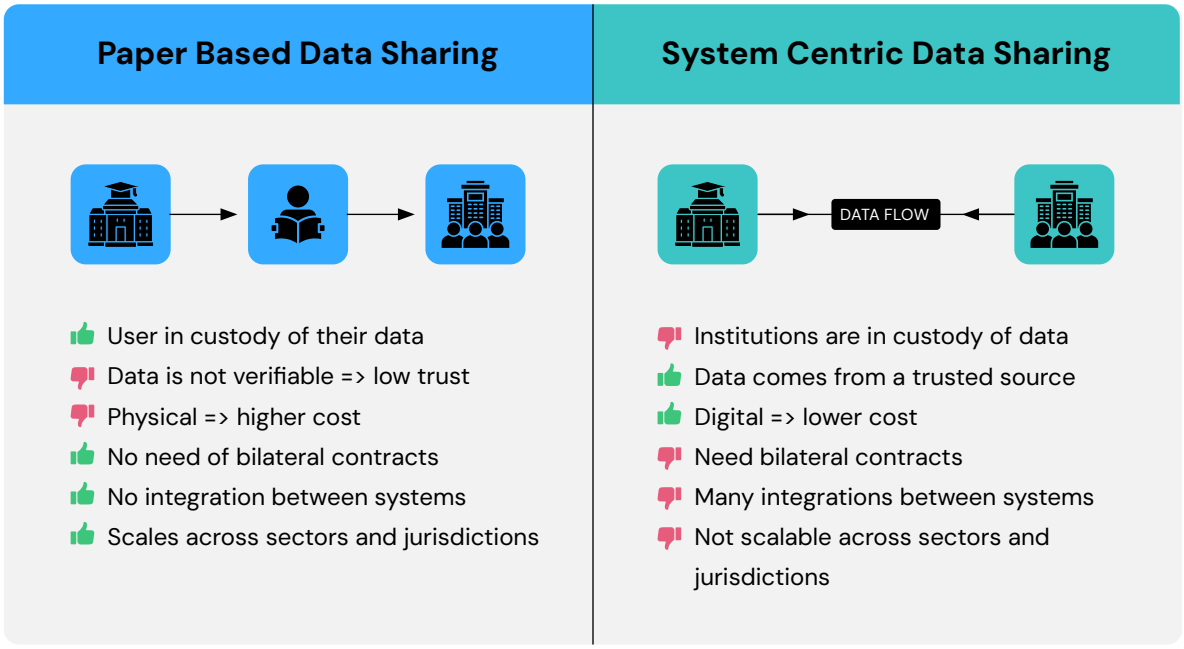
System-centric data sharing is difficult to scale to meet the ever-dynamic needs of 8 billion individuals and 300 million SMEs

Despite its many shortcomings, **paper-based data-sharing systems were inherently user-centric where users held the custody of their personal data (in paper form) and shared with various systems. Individuals had custody and control/agency over their personal data** once they obtained it, enabling them to share it freely with anyone, for any purpose, without further reliance on multiple systems getting integrated.

1 The following terms have been used interchangeably throughout the paper
1. Data issuer/ Data provider/ Data source - to refer to the institution that is the custodian of user's data
2. Data requestor/ Data verifier/ Data seeking/ Accepting party - to refer to the institution that seeks to use data on the user to give them access to a service
3. Data subject/ User - to refer to the person (natural/ legal) whom the data is about
4. System centric/ institution centric - to refer to a type of data sharing between systems

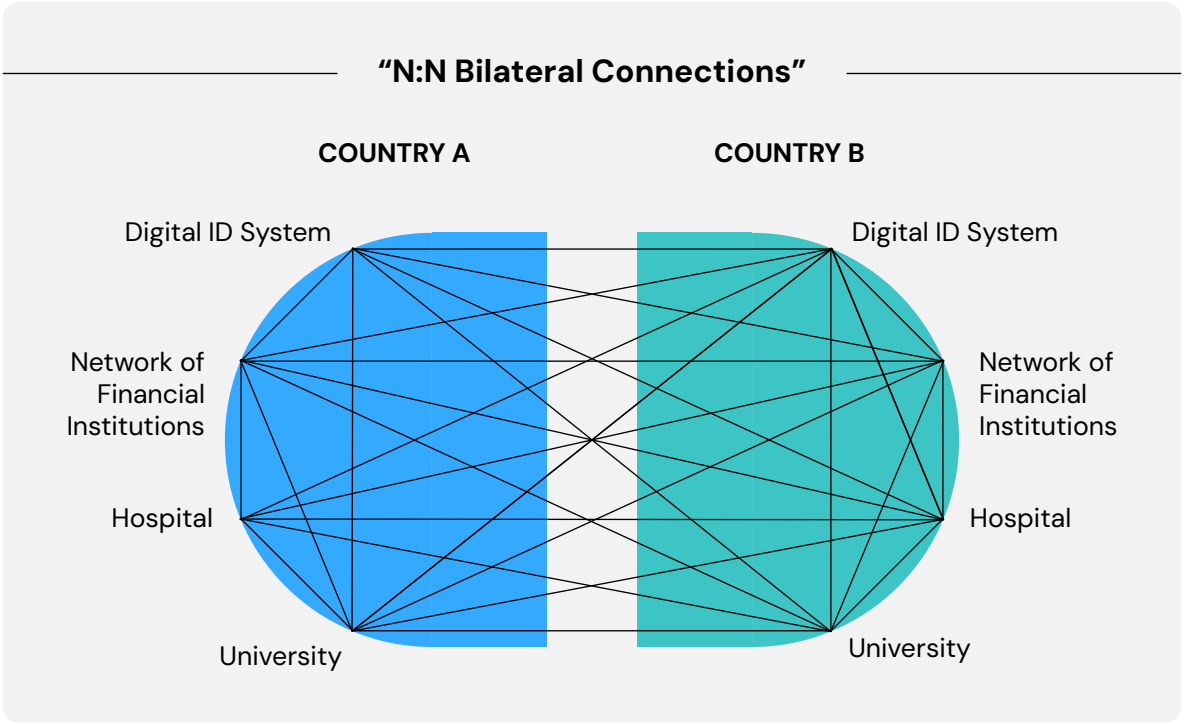
However, as we transitioned to the digital world, this user-centric approach gave way to system-centric models. This shift introduced two key challenges: it **undermined user empowerment** by making individuals dependent on another entity to share their data, and **it lacked scalability.** Restoring **user-centricity is essential for achieving universal scale,** as the user acts as the common link between the two entities in a data-sharing transaction.

In the healthcare world, it is easy for someone to carry their medical records by themselves (self-custody) and present them to another hospital/institution in another country (or a use within another sector in the same country, say employment or insurance) with ease whereas the probability of all hospitals and institutions across the world integrating and sharing personal healthcare records is near zero! Same pattern be seen in the financial world where it is easy to carry cash (money) across institutional and geographic boundaries and use it with ease whereas in the digital world, it is inefficient, expensive, many times impossible for the same due to high business, contract, and technological complexity of every system integrating with every other system across the world.



In system-to-system (or system-centric) data sharing, **each request for data has to be processed by the data source (issuer) under a business and technological arrangement with the data seeker/consumer.** This means the data provider must trust the seeker/requestor, have business/contract arrangement, usually by being part of the same trusted network, community, or group. For example, banks under the same regulator in a limited jurisdiction may trust each other. Government departments may trust other Government or regulated institutions in a particular jurisdiction. Such integrations can also happen when these institutions have the capacity and financial might to implement API based business integrations.

However, it is nearly impossible for all these institutions and other smaller, non-similar institutions to be part of the same network where they can exchange data. For example, a country's digital ID system might not provide access to its data to a small Bed & Breakfast (BnB) owner who needs to do an ID verification. It is impractical for an overseas employer to integrate with a foreign third-tier academic institution to request data of a prospective employee.



Even for institutions that are of high legitimacy or are trusted enough to be part of the formal infrastructure, **there are many bilateral integrations and business agreements required to connect each new institution, new sector, and new country.** API endpoints need to be exposed, authentication mechanisms need to be established, stringent cybersecurity measures need to be put in place, all the organizations need to have business agreements and contracts, and policy alignment is required if the participating organizations fall under different jurisdictions.

It will take years just to connect a country's digital ID system or healthcare or other systems to all the verifying institutions even within the country, that is, if they get access at all. Even after 100+ years, this mammoth task will remain incomplete due to the fundamental need of trust and contract between all these institutions and Governments! How would this scale to cross border and cross sectoral scenarios? It starts becoming apparent that this model of system-system data sharing via API integration, is highly limiting (among types of institutions and geographies) **creating high cost, high friction, and low innovation for users to truly make their personal data an economic asset.** This creates reliance on only those institutions with high capacity to implement APIs and business agreements, on intermediaries, thus adding delays, raising service delivery costs, and **holding millions of individuals and institutions back from unlocking data driven opportunities.** Further, disadvantaged sections of the population will be disproportionately affected by not being able to produce trusted data, as more well-to-do sections of society might have other signals and necessary connections to attest to their eligibility for a service.

So what is then the universally scalable model for trusted personal data sharing? We need to adopt best practices from both worlds and go back to the future! We need to flip the model from institution-centric to user-centric by truly giving the user the custody and control/agency of their personal data.

A universally scalable model for personal data sharing via credentialing and user custody

When envisioning such an infrastructure, it is essential to consider the direction in which the world is moving. We observe several **converging trends**—digitization is accelerating, software-driven solutions are becoming more prevalent, cloud computing is on the rise, and increasing numbers of people are gaining access to connectivity and smartphones. The latest shift we see is the availability of intelligence "on tap," becoming more accessible and cost-effective.

Advancements in cryptography have made it affordable and efficient for any data packet to be secured in a tamper-proof, portable, and non-repudiable manner. Regardless of how many times "the data packet" is shared or moved from one system to another, cryptographic protections ensure its integrity.

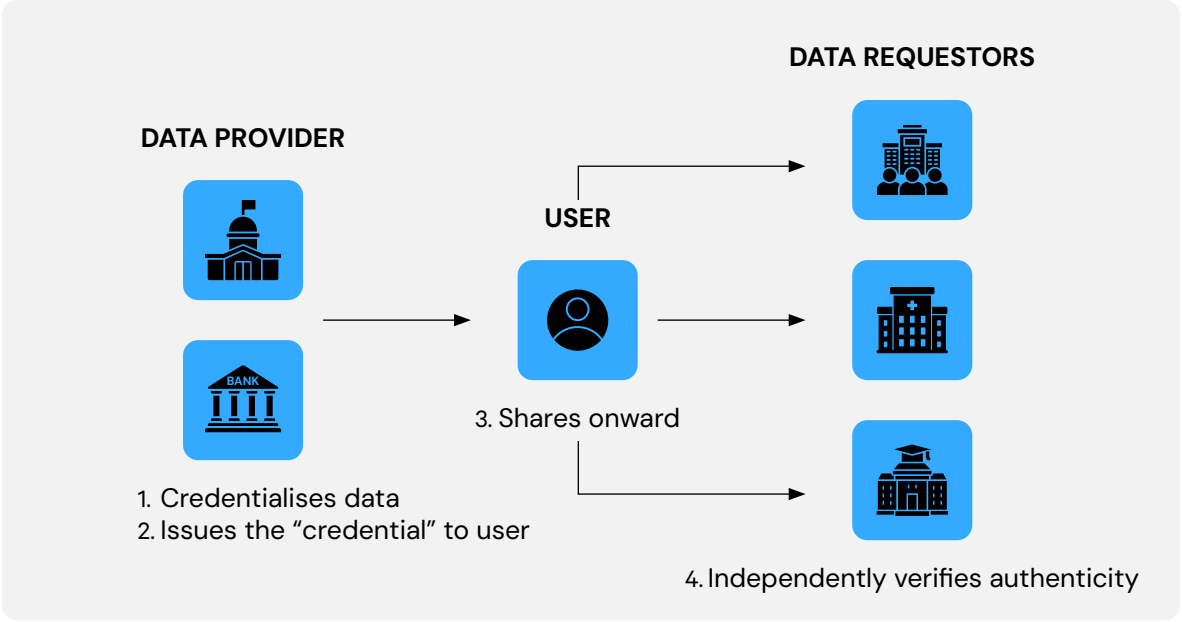
By aligning these technological trends with our need for a viable universal model that is low-cost and high-trust, we arrive at a **user-centric, self-custodial model for personal data sharing using credentialing of all forms of personal data.**

> A Verifiable Credential (VC) is a digital, cryptographically secure representation of claims made by an issuer about a subject (user). It is designed to be tamper-evident and independently verifiable by a third party without relying on the issuer (data provider). This idea of cryptographic protection can also be extended to any forms of personal data including transaction data to ensure all such data packets are verifiable and tamper-evident.

At the core of this approach are two simple interventions:

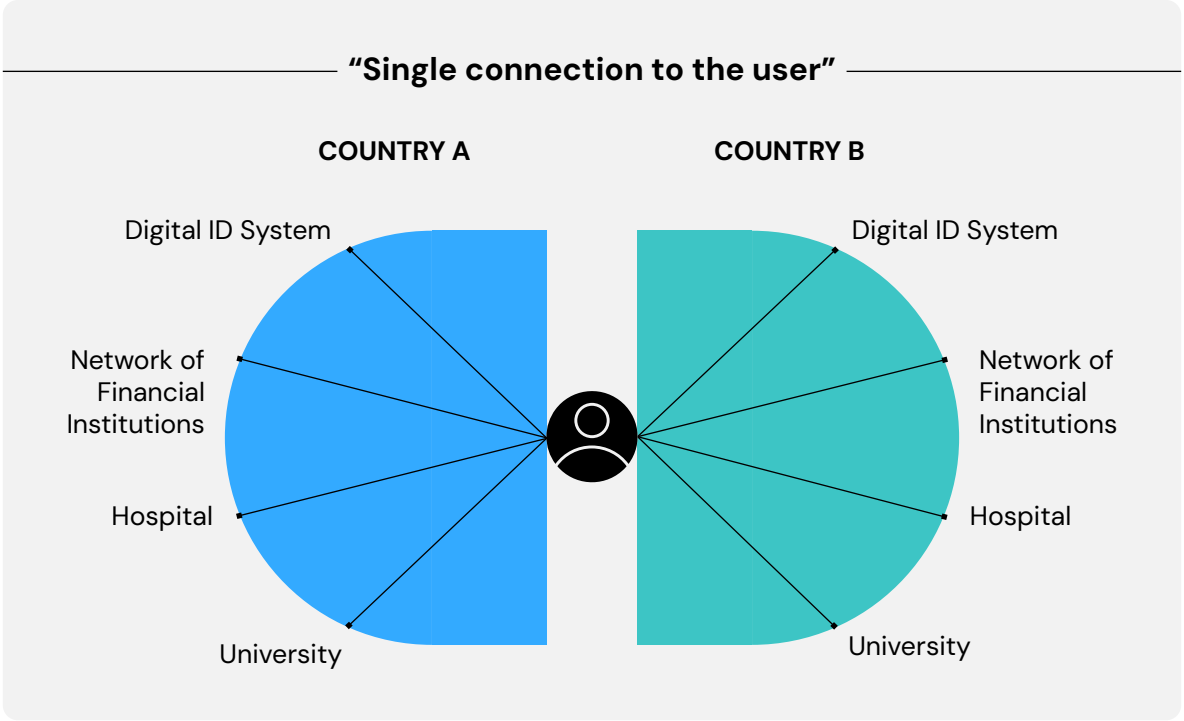
1. **Credentialling** (adding verifiability to data by the issuer/provider using cryptographic techniques)
2. **Giving the credentialled data back to the user** for self-custody and control for subsequent use of such data

The data provider (issuer institution) takes the user's data, generates cryptographically protected data in a verifiable credential form or in any other standard data representation form, and gives it back to the user. Users can use any commonly available tools such as their computers, mobile phones, cloud based personal drives, personal wallets, etc. to store them within their own control. The user is then free to present the credential to any other institution/individual (seeker/ requestor of the data). The requesting party then can independently verify and process the contents for, without having any bilateral integration with the issuer's system, and provide necessary services to the user.



Credentialing ensures that every piece of data is cryptographically secured, no matter who holds it. This shifts the basis of trust in the data from the issuing institution to the credentialled data held by the user, allowing anyone to confidently verify and trust the data's authenticity based on its cryptographic proof rather than relying on one or more institutions every time.

This approach **reduces dependency on the source (data provider) institution to offer APIs and have business contracts with all potential destination (data seeker) institutions, gives control back to the user, and reduces the sharing and acceptance challenge from a many-to-many integration to many-to-one.** Users can now share personal data with any other institution for availing a service and anyone can easily accept and verify it. This is **inherently scalable as the issuers' and verifiers' pre-existing relationships with the user are leveraged,** and there's no need for 1000's of bilateral contracts and integrations. Lastly, issuing a credential is far **less technically complex** and cheaper than maintaining sophisticated real-time APIs and endpoints and hence even smaller institutions with lower capacity can easily implement this model giving it a universally implementable model.



Further, this approach is more scalable because any institution can credentialise the data they hold as well as verify a credential without any need for a central entity or without the need to be a part of a closed network. Since the credential can be verified lifelong or until its validity period, it can still be used many years later even if the issuer organization ceases to exist.

All types of data can be credentialised - be it certificates, ID documents, salary/ payment slips, or more granular records like healthcare records, bank statements, purchase/sale history on an e-commerce platform, and so on.

Simpler forms of Verifiable Credentials can easily be **issued in paper form,** and thus, can function despite digital divide. Verifiable credentials can be in an **electronic format** (PDFs with digitally signed QR codes, or machine-readable files on smartphone apps) **and can be stored in any local or cloud-based storage,** including in digital wallets. This flexibility is crucial in driving inclusion as it allows users with smartphones, those with feature phones, and even individuals without any phone to effectively engage with this infrastructure in both online and offline contexts, whether in a self-service or with assisted mode. While concerns about digital access and literacy are valid—particularly for individuals without smartphones or those who may not be digitally adept—multiple inclusive approaches can address these. Web-based tools, shared family devices, and assisted service models can all be leveraged to ensure access. Even in assisted contexts, users should retain ownership of their digital credentials, for example through cloud-based accounts.

Smartphone or cloud based wallets - one way to store VCs - can even have more privacy-preserving features like selective disclosure and zero-knowledge proofs built in. Users can choose to share a few selected data points of the credential using selective disclosure. Zero-knowledge proofs ensure that any data requestor would reliably get answers to questions about the data without seeing the actual data.
User-centric personal data sharing via verifiable credentials is hence **decentralized, universal, privacy-preserving, and offers a significantly low complexity model.**

Credentials hold the key to to unlocking opportunities in an inclusive and innovative way

Self-custody of personal data in a verifiable and credentialled form is not just a technical solution; **it is a vision for a more connected, inclusive, and empowered digital future.**

Unlocking personal data in a high trust, low cost fashion can have many positive ripple effects, potentially **adding billions in economic value and driving innovation flywheels.** Putting this infrastructure in place does, of course, **streamline and bring efficiency to current processes, decreasing cost and time delays and giving access to economic opportunities to large sections of the population.** A roadside vendor who was denied a loan because her ID or bank statements could not be verified; a farmer who could not sell his produce online as his turnover was too low to undertake expensive background verification; a small trader unable to complete a cross-border transaction as his export papers weren't trusted; a student who couldn't go abroad for better employment opportunities as her academic credential could not be verified - all of them benefit immensely!

While this in itself is momentous, **unlocking low-cost, high-trust data flows in the digital economy can drive hypersonic innovation cycles in new sectors and use cases that haven't been imagined today.**

While some use cases are evident, the **true potential lies in the new innovative applications that will emerge when individuals and small businesses can harness their personal dala in a low-cost, high-trust fashion which then drives new economic opportunities in an accessible and affordable way.**

Fulfilling this vision requires combining robust technology, leveraging open standards, availability of decentralized universal infrastructure along with new models of governance and restructuring market dynamics to trigger innovations.

One proven approach to leapfrogging societal outcomes is the Digital Public[2] Infrastructure model. The DPI movement is inspired by the open standards & specifications that created the Internet (TCP-IP, HTTP, HTML, SMTP, etc) and mobile networks (GSM, SMS, LTE, etc) - which operated as the original digital infrastructure of the late 20th century, catalyzing a wave of public and private innovation that drove inclusion.

The core of a DPI is a framework for sustainable innovation via creating reusable, shared infrastructure that combines;

1. **minimal interoperable technology building blocks,** supplemented by
2. **governance frameworks** that are transparent, accountable, and participatory; and
3. robust **public and private innovation.**

User-centric data sharing via verifiable credentials follows the DPI approach.

All these in a decentralized way to minimize centralized control and data flows.

Globally, nations are advancing their digital transformation agenda with Digital Public Infrastructure (DPI), including Nigeria's NIN (100M+ users), Thailand's Promptpay (3.7M merchants), and Singapore's Singpass. India and Brazil have demonstrated remarkable success through their DPI initiatives - with India's Aadhaar (biometric ID) serving 1.4B users and UPI (instant payment system) enabling 500M+ users to conduct 185billion transactions annually. Brazil's Pix instant payment system has achieved 64 billion transactions across 150 million+ users.

Imagining the possibilities with credentialing

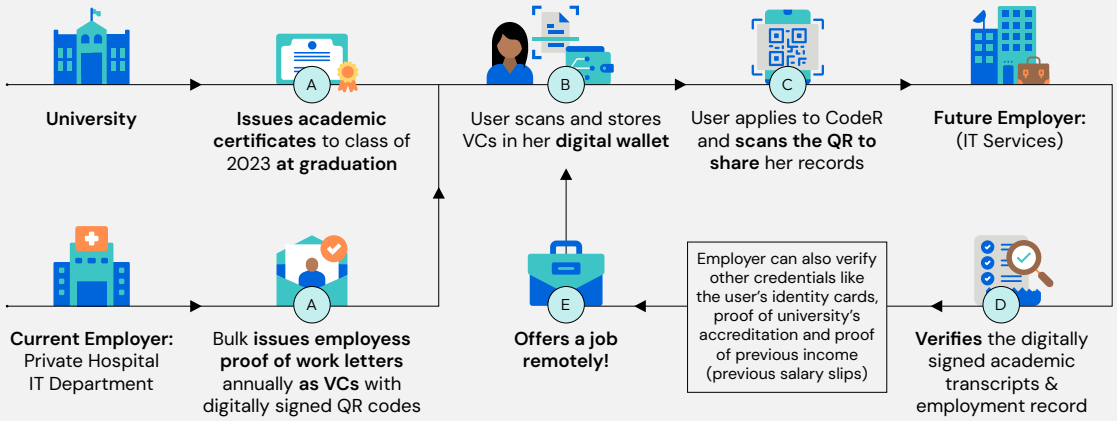
Credentialing infrastructure enables verification of data across sectors, be it with identity documents - from national IDs to purpose-specific cards for farmers and students, or foundational records like birth and death certificates issued by civil registration authorities. The technology can transform any claim into a verifiable credential, encompassing assets (land deeds, vehicle registrations), achievements (degrees, work history), affiliations (memberships, institutional roles), entitlements (tickets, benefits), and transactional records (financial, healthcare), among others[3].

Having these documents in trusted, verifiable form can enable access to many services and opportunities - ranging from access to credit, sharing personal health records for access to care, proving eligibility for social benefits, and meeting compliance and regulatory requirements are just a few.

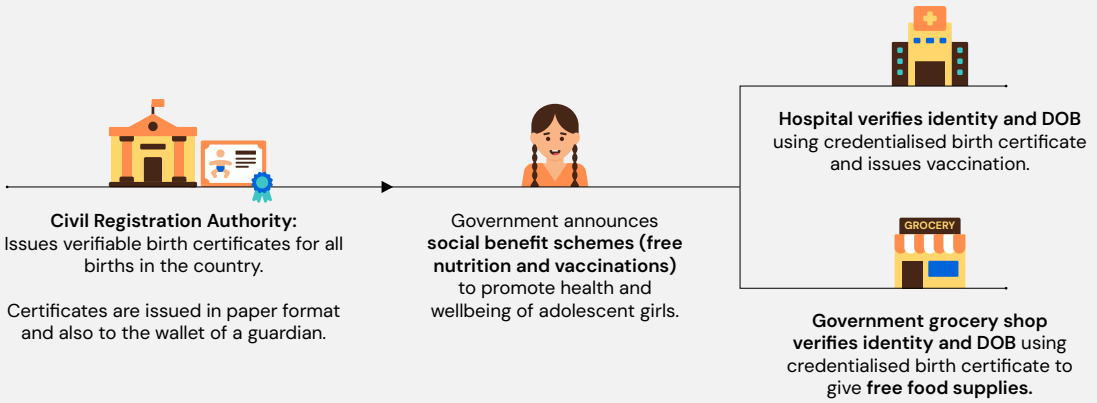
2 What's public about DPI? Public doesn't necessarily mean that the DPI has to be owned/ operated by the public sector. Public speaks to say that they DPI should be governed like a public good and should be open for the rest of the society for innovation.

3 These are only examples and are not meant to be exhaustive.

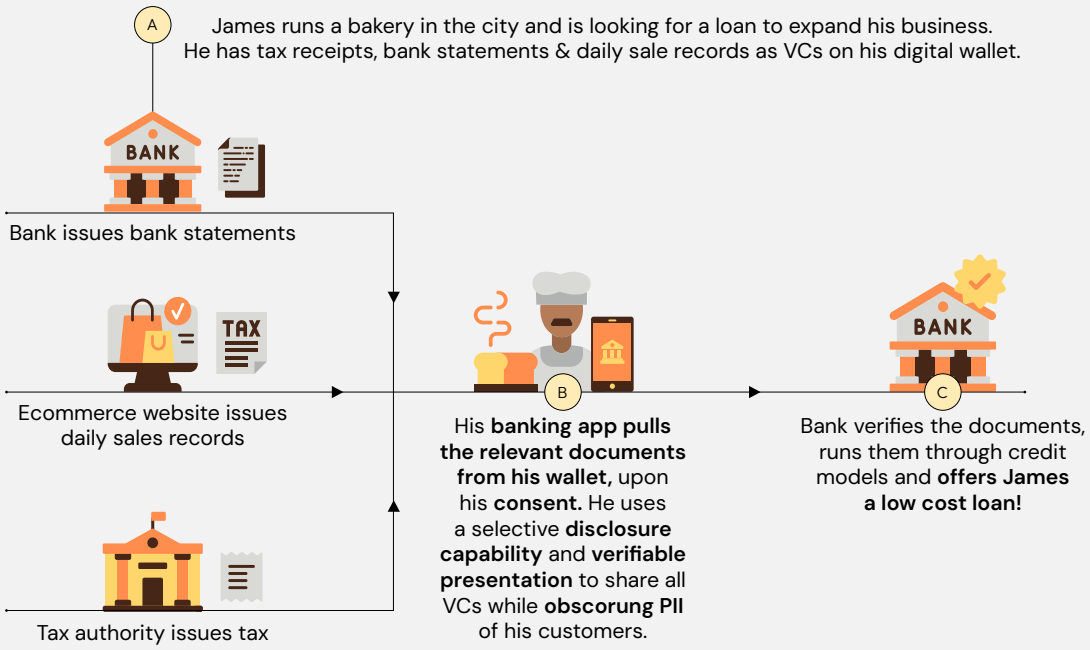
Verifiable Credentials Can Help Drive Trusted Remote Employment



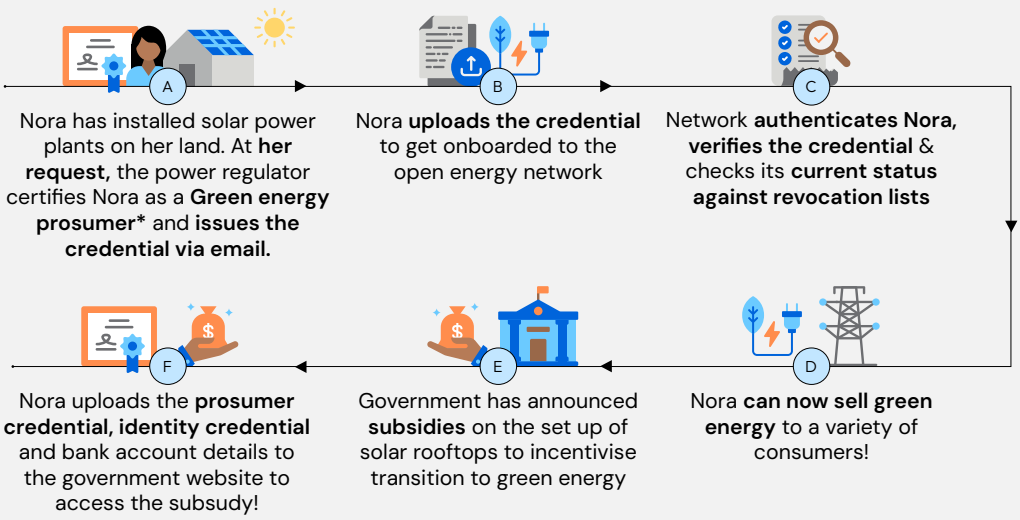
Verifiable Credentials For Access To Social Benefits



Verifiable Credentials for Access to Credit



Verifiable Credentials for Green Energy Trading and Financing



*A prosumer is an individual who produce and consume energy, enabling themselves to participate in energy trading by selling excess solar energy and buying energy from the grid

Design principles to achieve this vision

It is important to note that specific implementation realities are diverse and ever-evolving. Hence, it's imperative to establish a set of design principles that should guide the implementation of this vision.

UNIFIED

The infrastructure should promote multiplicity without imposing uniformity or a one-size-fits-all approach. Rather than a single standard or centralized solution, it should allow multiple specific implementations, standards, solutions, and players to coexist seamlessly. This diversity, underpinned by an interoperable framework, enables the entire system to function cohesively.

UNIVERSAL

The core architecture and foundational building blocks must be universally applicable, crossing geographical, sectoral, and jurisdictional boundaries. Avoiding fragmented rebuilding of the infrastructure is crucial—much like the universally adopted model of the Internet—to achieve true global interoperability.

USER-CENTRIC

Users should have complete self-custody, agency, and choice regarding their digital assets, especially their personal data. Although tools, guidance, and educational resources may be necessary to help users manage their assets securely, the ultimate control must remain with the users themselves..

INCLUSIVE

The ecosystem must accommodate a diverse range of user personas and contexts. This includes solutions tailored for users with individual smartphones and high connectivity, as well as those using shared devices or operating in resource-constrained environments. Users without digital access might need printable credentials usable at service points, while users with accessibility needs require specialized tools. Universality is only achieved when affordability and inclusivity are central considerations.

TRUSTED

Security and privacy preservation are fundamental. Leveraging robust cryptographic techniques ensures secure issuance, storage, and verification of credentials. Privacy-preserving technologies, such as selective disclosure and zero-knowledge proofs, alongside strong legislative and regulatory frameworks, reinforce trust within the ecosystem.

OPEN

The entire system must avoid being closed-loop, proprietary, or restricted by bilateral or multilateral contracts, and should not be hardwired to specific sectors or geographic regions. Anyone should be able to issue credentials using their choice of tools, users should manage self-custody using any tools they prefer, and acceptance of credentials should be possible within any workflow using open specifications. This approach requires an unbundled, loosely coupled, and universally accessible open-loop architecture.

INTEROPERABLE

A central goal is a loosely coupled global ecosystem enabling seamless credential sharing. Open, self-describing standards for data schemas, security, and interaction ensure compatibility between issuer tools, user management systems, and acceptance endpoints without restrictive hard-coding or limitations.

DECENTRALIZED

The entire ecosystem should be designed with decentralization at its core to prevent dependency on central authorities or single points of control. Decentralized implementation ensures resilience, avoids monopolization, and facilitates democratic participation and innovation.

ASYNCHRONOUS

The global adoption of credentialing infrastructure cannot rely on synchronized actions or unanimous agreement across all participants. Each subsystem should function independently, enabling stakeholders to implement their parts asynchronously. Collectively, these independent actions converge into a unified and interoperable ecosystem.

INNOVATION-DRIVEN

The ecosystem must promote innovation by encouraging public and private stakeholders to create tailored solutions, applications, and services that meet the diverse and evolving needs of their respective contexts. This approach accelerates adoption by addressing specific sectoral, geographic, and societal requirements effectively.

Implementation guidance: What can you do if you are a...?

A Public Sector Entity

Public sector entities play a vital enabling role in developing an inclusive, sustainable, innovative, and user-centric data-sharing ecosystem. Their support spans multiple functions, including technical assistance, legal frameworks, market acceleration through financial incentives, and advocacy. Specific areas of public sector involvement can include:

1. Issuing verifiable credentials for certificates and documents under their custody.
2. Acting as acceptors or verifiers of credentials within their operational workflows.
3. Establishing credentialing infrastructure accessible to both public and private sector organizations.
4. Curating and publishing relevant standards and schemas.
5. Implementing policies that ensure the legal validity and mandatory acceptance of verifiable credentials.
6. Providing critical utilities such as trust registries, reference implementations, and certification frameworks to strengthen stakeholder trust.
7. Stimulating market adoption through financial incentives for early adopters or high-impact use cases.
8. Advocating for cross-border acceptance of credentials within regional economic zones and multilateral partnerships

B Private Sector: Data Providers/ Issuers

Data issuers should transition from paper-based and unsecured digital documents to verifiable credentials. Banks, universities, healthcare providers, and other institutions can integrate credential issuance directly into existing document generation workflows. Organizations must also discover sustainable business models that balance implementation costs against operational efficiencies gained through streamlined verification processes.

C Private Sector: Credentialling Solution Providers

Private players—including product builders, technology service providers, and hyperscalers—should drive innovation by developing user-friendly interfaces, diversified deployment models, and value-added services. These solutions may encompass sector-specific wallets, standards adapters, quick installers, and other tools that facilitate efficient data conversion and seamless integration into broader systems.

D Development Sector Organizations

Development sector organizations should advocate for the widespread deployment of verifiable credentials across public and private institutions. They can also explore new funding models, conducting impact assessments, and provide crucial feedback on areas of improvement to drive large scale transformation.

E Open Source Solutions/ Communities

Open source communities should continue to deliver high-quality, modular code compliant with leading global standards while remaining adaptable to national and local contexts. The addition of supporting tools as necessary can further enhance system scalability and adaptability.

F Standards Organisations

Standards organisations should lead with thought leadership and technical expertise in the verifiable credentials space. This includes continuously upgrading and versioning standards in an evolvable and extensible manner while supporting multiple schemas to enable interoperability and drive widespread ecosystem adoption.

User-Centric Credentialing and Personal Data Sharing complements rather than replaces existing approaches to data sharing

This user-centric approach to personal data sharing through credentials can co-exist with, and meaningfully complement, other approaches to data sharing, including system-centric data sharing. Verifiable credentials may not be optimal in scenarios where real-time data access is critical and any delay is unacceptable. System-centric models are well-suited for such use cases—particularly when data flows between a limited number of highly-structured institutions operating within a closed, regulated ecosystem. For example, sharing citizen data among a few government departments collaborating on a specific project may be more efficiently handled through system integrations. Even in such cases, however, issuing the data back to the user as a verifiable credential is encouraged—enabling self-custody and empowering individuals to use their data as an economic asset. This isn't a question of one approach versus the other; it's about selecting the right infrastructure for specific use cases.

It is also important to note that this approach is specifically designed for personal data sharing—pertaining to both natural and legal persons. In the case of non-personal data, such as weather information or statistical aggregates, conventional mechanisms like APIs or open data hubs remain appropriate and sufficient.

Closing remarks

The path to universal credentialing is one of the most promising revolutions in how we share and verify information. Success demands the **orchestrated efforts of the entire ecosystem:** government ministries and departments establishing the legislative foundations; development and funding agencies providing crucial resources and implementation support; communities and standards organizations[4] creating the technical bedrock for interoperability. Open source solutions builders and digital public goods projects translate these standards into practical tools, while private sector innovators - from software vendors to system integrators - develop solutions that bring the vision to life. Business service providers and last-mile organizations ensure these solutions reach and serve every user, from large institutions to individual citizens.

Way forward with Credentialing and ubiquitous, low-cost, trusted attestations

It is clear that user-centric credentialing and personal data sharing offer substantial benefits. Moreover, these concepts align closely with and actively shape the trajectory of our digital future. We are moving towards a world where there is increasing dialogue and consensus on empowering users to reclaim control over their assets, whether it be personal data or their digital creations. This shift mirrors the evolution of the web from read-only to read-write and now to ownership paradigms.

The tokenization of various assets—including registered assets such as vehicles, user-controlled assets like NFTs, and regulated assets such as securities and insurance—necessitates attestations regarding ownership, authenticity, and other attributes. Verifiable Credentials (VCs) will underpin these attestations, ultimately enabling a future where individuals possess greater choice, autonomy, and control over their digital assets.

Only the collaborative efforts of public-sector leadership, open-source innovation, private-sector expertise, and community engagement can enable users and small businesses to turn digital footprints into economic opportunities. Through their coordinated efforts, we can build an inclusive credential infrastructure that serves everyone - making trusted data sharing not just a possibility but a reality for billions worldwide. **The future of universal credentialing isn't just about technological transformation - it's about creating a more accessible, trustworthy, and empowering digital world for all.**

4 The foundational work toward universal credentialing has been significantly advanced through the contributions of several key organizations, including but not limited to the Linux Foundation, OpenID Foundation, and W3C.This list is not exhaustive and many other organizations have made valuable contributions to this field.

All activities that CDPI is anchoring related to user-centric data credentialing and personal data sharing can be tracked at this link. This serves as a one-stop repository for updates on ongoing sandboxes, technical notes, implementation blogs, practitioner case studies, and more. If you are interested in participating in any of these activities or contributing to the ecosystem, we invite you to contact us here.

References

1. CDPI Wiki | link
2. OpenWallet Foundation | link
3. OpenID Foundation | link
4. W3C VC | link
5. Inji | link
6. Finternet paper | link
7. ISV RFQ procurement | link

Annexure: National Data Sharing Infrastructure Implementations

Many countries[5] have recognised the importance of building rails for data sharing and have made significant strides in improving efficiency, access to services, and economic growth.

CAMBODIA

Verify is a powerful document issuance and verification platform in Cambodia that uses blockchain technology to ensure the authenticity of documents bearing a standard QR code. This platform has been extensively adopted across most public sector documents in Cambodia and has expanded to include cross-border use cases within the Asian region, notably with South Korea and Laos.

ESTONIA

Estonia (with over 25 other countries worldwide) has implemented a whole-of-society data sharing by deploying the digital public good X-Road®, which provides unified and secure data exchange between organisations in a collaborative ecosystem.

INDIA

India has developed a consent framework known as Account Aggregator that acts as the trusted intermediary to prioritise and collect users' consent to share their data between systems to receive services at a lower cost. The AA infrastructure crossed 100 million consents in August 2024. India also provides verifiable credentials for a variety of certificates and licenses across national, state, and private entities (such as identity, driver's license, health, and education) through 'Digilocker'. Over 9.3 billion documents have been issued by 1700+ issuers.

UNITED KINGDOM

The UK's open banking system currently has 9 banks connected to the network, which allows them to share data about an individual's current account and credit card with third parties that are listed as an approved Open Banking provider on the Open Banking Directory.

5 This list is only indicative, not meant to be exhaustive.

ARGENTINA

They have issued over 19 million verifiable driver's licenses in just a few weeks through the 'Mi Argentina' program. Today, more than 27 million users have access to their Digital ID Card, Driving License, and vaccine certificates, among 30 other credentials and 1000 digital services.

BRAZIL

The GOV.br infrastructure hosts over 100 verifiable credentials across sectors that can be reused by citizens to prove their attributes and gain access to services at a lower cost.

EUROPEAN UNION

The EU recently released specifications for their digital wallet that will store documents in a user-centric manner in online and offline modes to access public or private services with high trust. Over 250 private companies and public authorities across 25 Member States and Norway, Iceland, and Ukraine will participate.

NEW SOUTH WALES, AUSTRALIA

Launched in 2023, this state-level digital wallet provides access to the NSW Digital Driver's Licence, Social Benefits Vouchers, Boat driver licences, Individual contractor licences, and other 90 verifiable credentials with legal status.

UKRAINE

The 'Diia' mobile application allows 30 million Ukrainians to access over 120 government services through verifiable digital documents and is available for reuse as an open-source project. All usage of personal data by government entities is tracked, and users are alerted when and why their data has been accessed.

cdpi.dev