Centre for Digital
Public Infrastructure

Scope Document

[Country Name]

Verifiable Credentialing Infrastructure

version 2.0

dated: xx-xxx-2026

Table of Contents

1. GLOSSARY....4
2. VERSION HISTORY....4
3. INTENDED AUDIENCE AND PURPOSE....5
4. EXECUTIVE SUMMARY....6
5. COUNTRY CONTEXT....9
5.1 Introduction to the Country Context, its Digital Transformation Journey and its Vision for a Digital Wallet of Verifiable Credentials in [Country Name]....9
5.2 First Use Case: Why [Use case]....9
5.3 Additional use-cases....10
5.4 Rollout Objectives....10
5.5 Post-Rollout Vision....12
6. ACTORS....13
7. COMPONENTS....16
8. REQUIREMENTS MATRIX....19
8.1 Functional (Technical/Program)....19
8.2 Non Functional (Technical)....24
9. ROLL-OUT SCOPE - Program & Technical Deliverables....26
9.1 Program Deliverables....26
9.2 Technical Deliverables....30
9.3 Schedule of Deliverables and Payments....31
9.4 Change Request....32
9.5 Assumptions....32
10. PROJECT GOVERNANCE....34
APPENDIX - 1. Verifiable Credential and its Solution Approach to Credentialing....35
APPENDIX - 2. Qualification & Evaluation Criteria....39
APPENDIX - 3. Technical Proposal Response - Template....44

1. GLOSSARY

i.	DCS	Digital Credentials Stack
ii.	DaaS	DPI as a packaged Solution
iii.	DPG	Digital Public Good
iv.	DPI	Digital Public Infrastructure
v.	Engineering Partner	Organisation who can support open source solutions
vi.	ICT	Information and Communication Technology
vii.	ISV	Independent Software Vendor
viii.	KRA	Key Result Areas
ix.	L1 Support	Level 1 support; setup, configuration, basic troubleshooting
x.	L2 Support	Level 2 support; minor bug fixes to code, test, build and deploy
xi.	L3 Support	Level 3 support; new feature development, test, build and deploy
xii.	SaaS	Software as a Service
xiii.	SDK	Software Development Kit
xiv.	SP	Service Provider
xv.	VC	Verifiable Credential
xvi.	VP	Verifiable Presentation
xvii.	ZKP	Zero Knowledge Proof
xviii.	CI	Credential Issuance
xix.	CV	Credential Verification
xx.	CS	Credential Store
xxi.	PR	Programmatic Requirement
xxii.	NFR	Non Functional Requirement

2. VERSION HISTORY

Version No (Date)	Authors	Remarks
1.0 (23-Oct-2024)	CDPI	draft/working doc version
2.0 (21-April-2026)	CDPI	Revised version based on learnings from in-country implementations

3. INTENDED AUDIENCE AND PURPOSE

The intended audience of this document is:

No	Audience	Purpose
1.	DPG	Contribute and review the scope; respond to ISV/SP queries; Support SP with L3 support for the DPG / ISV product offering
2.	DPG Delegate (i.e. anyone acting on behalf of the DPG)	
3.	DPI Owner (e.g., main government focal point)	Contribute and review the scope; respond to ISV/SP queries
4.	Issuers (i.e. public/ private entity responsible for credential issuance, if different from DPI Owner)	
5.	Accepting Entities (ie: public/ private entity responsible who will be the accepting parties or verifiers)	
6.	ISV	Respond to RFQ, meet ISV responsibilities of this scope doc; Support SP with L3 support for the ISV product offering
7.	Engineering Partner	Support SP with L3 support for the DPG / ISV product offering
8.	SP	Respond to proposal, meet SP responsibilities of this scope doc

4. EXECUTIVE SUMMARY

4.1 Disclaimer: This Country Scope Document, read with the DaaS Legal Framework, sets out the entire agreement between the parties with regard to the scope set out herein. Upon non-compliance of the Service Provider with the requirements outlined in this Country Scope Document, the DaaS DPG Partner may terminate this Country Scope Document.

4.2 Scope: This Scope Document outlines the programmatic and technical framework for implementing a national Verifiable Credential (VC) infrastructure in [name of country] following the DPI as a Packaged Solution (DaaS) approach.

4.3 Strategic Vision and Technical Approach: VC rollout in [name of country] seeks to establish a low-cost, high-trust digital ecosystem by enabling cryptographically signed, user-controlled credentials. The approach leverages modular, standards-based components for issuance, storage, and verification—enabling asynchronous adoption by diverse ecosystem actors. The rollout is aligned with [name of country] broader digital transformation goals and leverages the leadership of [name of DPI owner and/or relevant DPI owner supporter/s] .

For more details on verifiable credentials see **Appendix 1: Verifiable Credential and its Solution Approach to Credentialing**. For further reading, CDPI has also published a Vision Paper on User-Centric Credentialing and Personal Data Sharing.

4.4 Use case overview: The rollout will enable citizens of [name of country] to prove their [name of the selected credential(s), eg: identity, academic certificate, others] and attributes securely and digitally across both public and private platforms, reducing administrative burdens and increasing service inclusion. The first credentials to be deployed is/ are [name of the credential, eg: the digital national identity card (nid) and/or driving license and/or birth certificates, etc]. [Name of the designated credential, eg: the digital national identity card] will support online authentication for [short description of the first use case that will be enabled; eg: digital services of DPI owner or eKYC with a designated national/ local Bank]. Deployment of the use case will bring significant impact [describe the impact/value of the use case against the overall population/ respective segment group].The digital credentials will be accessible via a mobile wallet and as printable formats (PDF with QR). Additional use cases to be quoted separately by the Service Provider.

Note:

- A use case is defined as a complete end-to-end deployment of a credential, including issuance, storage, and verification workflows, integrated into the relevant systems of at least one issuer and one verifier.
- An issuer is an entity formally authorized to issue verifiable credentials using the infrastructure.
- A verifier is an organization or system formally onboarded to accept and validate verifiable credentials within their operational workflows.

4.5 Service Provider Scope: The selected Service Provider (SP) is responsible for delivering a full suite of programmatic and technical activities as part of the DaaS rollout. The role goes beyond system integration and includes the following four core programmatic objectives. Details of successful rollout criteria for these programmatic objectives is outlined in section 8 requirements matrix

- **Launch the [name of the 1st VC infrastructure, eg; "dnid infrastructure"] and meet all rollout requirements**: Deploy the credentialing infrastructure with full functionality (issuance, storage, verification), including if relevant, delegated access for legal guardians and inclusive display formats. This also includes making necessary adaptations to the product, such as translation into local languages and UX improvements to ensure accessibility for all user groups.
- **Support DPI owner in driving end-user adoption and engagement:** Co-develop an outreach strategy with the government to raise awareness and adoption, delivering inclusive communication materials. The government leads implementation; the SP supports strategy and content design.
- **Enable ecosystem expansion and government capacity:** Onboard new issuers and verifiers from both public and private sectors, while capacitating [name of DPI owner and/or relevant DPI owner supporter/s] to independently manage future onboarding, including through self-service toolkits.
- **Establish institutional sustainability and policy alignment:** Deliver a business and operational plan (including cost recovery models), finalize SOPs, and align the sustainability model with national budgets or multilateral loan operations. Support the creation of a national policy on user-centric credentialing.

4.6 Pricing:

This scope includes confirmed and potential use cases. Vendors are requested to submit a base quote that covers the two confirmed use cases **and** a bonus quote per additional use case, issuer, or verifier onboarded.

The confirmed use cases include:

1. [Name of selected 1st use case]
    - [Number and name of Issuer/s]

- [Number and name of credential types] *(including delegated access for legal guardians in the case of underaged)*
- [Number and name of Accepting Parties/ Verifiers[1]]
- Target population: [Describe the approximate target population of the use cases]

2. [Name of selected 2nd use case]
   - [Number and name of Issuer/s]
   - [Number and name of credential types] *(including delegated access for legal guardians in the case of underaged)*
   - [Number and name of Accepting Parties/ Verifiers]
   - Target population: [Describe the approximate target population of the use cases]

4.7 Additional use cases

The DPI owner is actively exploring opportunities to expand the use of the Verifiable Credentialing Infrastructure beyond the initial credentials. This includes both new issuers (to generate additional credentials) and new acceptors (to enable broader adoption of the [name of the credential type]). These use cases are not yet confirmed and **should be scoped and quoted separately by the Service Provider**. Below is a **reference** list of priority opportunities under consideration:

1. [Name of credential type]
   - Issuer: [The name of issuer]
   - Verifier [The name of verifier/s]
   - Current challenges: [Describe briefly the problem statement].
   - Use cases: [Describe the use cases]
   - Target population: [Describe the approximate target population of the use cases]
2. Same as above if there is more than 1
3. Same as above if there is more than 2

[1] These terms - accepting parties and verifiers - are used interchangeably in this document

5. COUNTRY CONTEXT

5.1 Introduction to the Country Context, its Digital Transformation Journey and its Vision for a Digital Wallet of Verifiable Credentials in [Country Name]

Example: The Ministry for Digital Transformation envisions a verifiable credentials (VC) ecosystem integrated into a national digital identity app, where citizens can securely access and share essential documentation, such as identity documents, certificates, and qualifications. This initiative builds on years of investment in digital public infrastructure to enhance accessibility, transparency, and efficiency in service delivery.

The VC system will streamline processes by reducing dependence on paper documents, minimizing delays, fraud, and administrative costs. Designed with citizen control in mind, it allows users to manage and share their data securely. The Ministry aims for a scalable, interoperable system that aligns with global standards, enabling cross-sector trust and integration. This foundation supports a broader vision where digital credentials expand across sectors, from finance and education to healthcare, fostering a secure, inclusive digital ecosystem. By prioritizing interoperability, security, and inclusivity, the Ministry's VC ecosystem will empower users, reduce bureaucratic barriers, and advance economic growth through more efficient digital interactions.

5.2 First Use Case: Why [Use case]

***Instructions**: At the minimum, this section should include the following details:*

- *Specify the sector (eg: national ID or land registry or health or education)*
- *The problem it addresses, the potential impacts (against total population for example) and the existing user journeys/ the pain points*
- *Scope of the use case rollout/ the rollout objectives*
- *The rollout success criteria(s)*
- *For ease of reference, let's summarize all of the above in a box. Example shown below.*

The use case in a nutshell

Example:

National Land Registry: a mandatory registration system for all rural properties aimed at promoting sustainable land use and ensuring compliance with environmental laws. It collects data on land use, native vegetation, and environmental liabilities, helping the government monitor deforestation and promote conservation efforts.

Land Certificate: a document that proves the registration of the rural property in the national environmental registry. It serves as proof of compliance, allowing landowners to demonstrate their commitment to sustainable practices and access benefits such as credit or incentives for conservation.

Objective: Provide +7M landowners with easy access and control over their land credentials, allowing seamless sharing with banks and other loan providers.

Problem statement

Instructions: *Provide a brief overview of the current problem, and how a DPI building block can unlock that use case. Use data or policy statements to highlight the urgency of these issues, the potential impacts it is driving (against total population of the country/ the specific use case for example). If possible, also include a brief overview of the existing user journeys.*

Example: The financial services market in [Country Name] is estimated at USD 15-16 billion. However, due to inefficiencies and barriers in accessing financial products, a large portion of this potential remains untapped. Many rural landowners face challenges in securing financial resources for sustainable agricultural practices or conservation initiatives due to reliance on physical documents, which are costly and time-consuming to verify. This gap in financial accessibility not only limits rural economic growth but also hampers environmental efforts reliant on funding.

5.3 Additional use-cases

Instructions: *Provide a brief overview of the other potential use-cases.*

5.4 Rollout Objectives

Instructions: *Define the **Target Population** — the groups that will benefit most, explaining how the solution meets their needs and improves service access. Then, outline the **main programmatic objectives** for the six-month rollout along with measurable indicators.*

In general there are four main objectives the DaaS program would like to achieve, these include:

- *Successful launch of the agreed VC infrastructure and meet all rollout requirements*
- *Support DPI owner in driving end-user adoption and engagement*
- *Enable ecosystem expansion and government capacity to independently manage future onboarding*
- *Establish institutional sustainability and policy alignment*

These objectives could vary depending on the country's context. Details for each objective and their respective successful rollout criterias (KPIs), and supporting key activities will be different for every country DaaS implementation and will be further elaborated in Section 9.1.

Example:

The proposed rollout phase will equip **landowners** with secure, digital credentials, allowing them to store, manage, and share their essential documents (such as property certificates) directly with financial institutions, facilitating seamless access to loans and subsidies. For **financial institutions**, this digital credentialing system will simplify and streamline verification processes, reducing costs and enhancing reliability. For the **government**, it will alleviate administrative burdens and enable decentralized, efficient issuance and verification of credentials.

Over the six-month rollout, the main objectives include:

- **Technical Implementation and Scalability:** Successfully deploy and operationalize the Verifiable Credentialing Stack for the initial use case, with the capability to quickly scale to additional use cases. This will establish the necessary infrastructure to support digital credentials across various sectors. The infrastructure should support the following criteria:
    - **User Access and Convenience for Target Population:** Equip landowners with secure, verifiable digital credentials for essential documents, such as land certificates, that they can manage and share directly with banks or loan providers. This will include:
    - **Formats:** Digital credentials in signed QR codes, signed PDF documents, and machine-readable formats like JSON and XML.
    - **Access Channels:** In-person collection, web portals, mobile applications, and digital wallets to ensure multi-modal access.
    - **Storage Options:** Support for both physical and digital storage methods to accommodate different user needs.
    - **Efficiency and Cost Savings for Verifiers:** Enable financial institutions to verify land certificates quickly and reliably, reducing verification costs and enhancing the accuracy and authenticity of documents. This streamlined process will facilitate loan applications and approvals, providing faster, more affordable access to financial products for the target population.
- **Operational Optimization for issuers and verifiers:** Reduce administrative workload for the government and private entities by simplifying the issuance, storage, and verification of digital credentials. This system will lower operational costs, improve workflow efficiency, and enhance the credibility of participating institutions by offering multiple methods and channels for credential issuance and verification.

The rollout will be carried out in coordination with *[mention the name of the Implementing Ministry/ies]* to align hosting and infrastructure. A hands-on training component will ensure that *[mentioned the*

relevant implementing government partners] can maintain, scale, and add new certificate types independently after project closure.

5.5 Post-Rollout Vision

Instructions: *Outline the long-term goals and impact of the digital infrastructure beyond the initial rollout. Describe the infrastructure's potential for expansion to other sectors or use cases. Also include how the infrastructure will be maintained and scaled.*

Example:

The land registry credentialing system is a first step towards a comprehensive verifiable credentials system. Future phases will include digital wallets for additional government and private sector services, enabling broader participation and streamlined access across sectors. In the next few years, the infrastructure aims to cover various public and private services, from health to education, fostering a secure and inclusive digital environment.

6. ACTORS

6.1 Anchors and focal points

Ministry/ Department/ Organization	Focal point	Designation	Contact
Ministry for Digital Transformation	Ms First Name Last Name	Deputy Secretary for Digital Government	example@mdt.gov
eGov LTD	Mr First Name Last Name	CEO	example@egov.gov
Ministry of Agriculture	Ms First Name Last Name	Project Manager	example@mg.gov

6.2 Institutions and roles

***Instructions**: If a role is not applicable for a country, please state Not Applicable in the column - Entity Information (rather than deleting the row)*

#	Ecosystem Actors (Roles)	Further context	Entity Information
1	DPI Owner	The DPI owner serves as the primary anchor for the DaaS rollout. The DPI owner will also own, maintain and scale the infrastructure in the country.	**Example:** The Ministry for Digital Transformation (MDT) will sign a Letter of Intention with the DPG and serve as the primary anchor for the DaaS rollout, progressively scaling the infrastructure and incorporating new use cases. eGov LTD, the national provider of IT services for public administration, will be responsible for the technical and operational deployment of the DaaS solution, under oversight of MDT.
2	DPI Owner Supporter	The DPI Owner Supporter is a government agency/ies that works with the DPI owner to help deploy the verifiable credential infrastructure in the country. Their role is crucial to the successful launch of the first few use-cases in the country.	**Example:** Population registrar, if the first use is an ID credential. Other entities depending in country's use case context could include for example: Integrator, Technical Implementation, Data management
3	DPG Owner	The DPG owner is responsible for keeping the core product code updated and aligned with	Example: Owner of DPG that builds and maintains the Verifiable Credential Stack

		global best practices by providing regular, automatic upgrades to all countries. When necessary, the owner will also offer technical support, including bug fixes and addressing implementation queries that the DPG delegate is unable to resolve.	Web wallet, Mobile Wallet, Issuance module , Verification module Any credential issuance/verification offering from ISV that meet guidelines stated in section Solution Approach to Credentialing DPI, overall requirements and deliverables of this scope document are allowed. The selected ISV solution providers are called out in respective actor categories.
4	DPG Delegate	The DPG delegate is affiliated to the DPG owner and acts as the mission anchor throughout the implementation process and beyond. Its role is to act on the behalf of the DPG owner.	**Example:** Centre for Open Societal Systems (COSS)
5	Issuers	The infrastructure must be built for scale, allowing multiple issuers to be on-boarded at short notice.	**Example:** *The National Land Registry operates within the Ministry of Agriculture and will act as the first digitally verifiable credentials issuer institution.*
6	Accepting Entities / Verifiers	The infrastructure must be built for scale, allowing multiple accepting parties or verifiers to use the infrastructure at short notice.	**Example:** *Depending on the use case(s), to identify who will be the accepting entities/ the one(s) that will be verifying documents.* 1. Banks 2. xx 3. yy
7	Subject / Holder	The infrastructure must be capable of supporting multiple simultaneous log-ins and requests for credentials from the holders of the credentials.	***Example:*** *Depending on the use case(s), to identify who will be the main holder of the documents.* 1. Land owners
8	Service Provider (SP) - Program Mgmt	The SP is responsible for the entire Program Management, collaborating with and operating under the oversight of the DPG, DPG delegate (if applicable) and the DPI owner. They must use the open-source DPG code for the Credential Store module as a baseline for technical implementation and contribute back to the code during the course of DaaS implementation. The SPs / ISVs must train and support the country to manage the credentialing infrastructure and integrate it into the national digital infrastructure, and empower them with a strong, clear transition plan from the date requested by	To be selected as part of the outcome of this procurement

		the country. Responsible for a. Overall program mgmt b. Roll out initial and additional use cases c. Scale issuance/verification rollouts through adoption d. End to end ownership (deployment, integration, training, support, etc.,)	
9	Independent Software Vendor (ISV) - Credential Issuance	Responsible for a. Stable product offering b. Integrate with all the other components c. L1, L2 and L3 support	***Instructions:*** *Any vendor specific ISV offering already selected and/or being considered by the issuers as part of this engagement* *If no ISV is listed, SP should consider default components supported by the DPG owner.*
10	Independent Software Vendor (ISV) - Credential Verification	Responsible for a. Stable product offering b. Integrate with all the other components c. L1, L2 and L3 support	***Instructions:*** *Any vendor specific ISV offering already selected and/or being considered by the issuers as part of this engagement* *If no ISV is listed, SP should consider default components supported by the DPG owner.*
11	Independent Software Vendor (ISV) - Credential Store	Responsible for a. Stable product offering b. Integrate with all the other components c. L1, L2 and L3 support	***Instructions:*** *Any vendor specific ISV offering already selected and/or being considered by the issuers as part of this engagement* *If no ISV is listed, SP should consider default components supported by the DPG owner.*
12	Engineering Partner Organisation	DPG Software support. Responsible for a. Provide L2, L3 support to SP b. Provide hot fix and other minor bug fixes	The following engineering partner organisation names, as suggested by the DPG owner, are: a) Cyberpwn b) Technoforte c) Ooru d) xx
13	Cloud Service Provider	Responsible for a. Support ISVs to provide integrated product offering through SaaS and Hosted options b. Provide required credits to DPI Owner and Issuers to host credential solutions	Please see section 7.1 Engagement model for public cloud-hosted solution offering

7. COMPONENTS

***Instructions**: If a component is not applicable for a country, please state "Not Applicable" in the column - Product Information (rather than deleting the row)*

#	Component / Functionality	Product Information
1	Credential Issuance	**Issuance**: ☐ Inji Certify ☐ ISV SDK ☐ ISV SaaS Offering ☐ Credebl ☐ Walt.id ☐ Quark.id **Standard**: ☐ W3C-VC ☐ SD-JWT VC ☐ ISO 18013-5 mDL ☐ AnonCreds (ZKP) **Schema**: - Custom json schema (as agreed with Issuer) Priority is to align with schema.org for interoperability **Formats**: - Signed .pdf doc with signed QR - .json file
2	Credential Verification	**Verification**: ☐ Inji Verify ☐ ISV SDK offering ☐ Credebl ☐ walt.id ☐ Quark.id **Integrations with accepting entity for verification:** - Accept credentials from any credential store - SDK / Library integrated in web portal/mobile app - Issuer hosted API support and integrate with accepting party web portal/mobile app **Credential formats:** - Upload pdf on accepting entity web portal / mobile app - QR Scan through mobile app - Share machine readable credential via deep linking, bluetooth, file upload, etc.,

		- Show pdf print to an authorised agent etc.,
3	Credential Store	**eLocker**: ☐ Inji Web ☐ ISV SDK offering ☐ Credebl ☐ walt.id ☐ Quark.id **Channels**: - In person collection - Download from the portal using demo auth (what you know) and/or OTP based authentication. **Wallet**: ☐ Inji Mobile ☐ ISV SDK offering ☐ Credebl ☐ walt.id ☐ Quark.id ☐ Any open standard compliant wallet **Support for additional stores to hold credentials:** - Holder personal computer/mobile device - Cloud storage - Physical print
4	Single Sign-On	**SSO:** ☑ eSignet ☐ Wso2 identity server ☐ Keycloak ☐ Custom SSO in country **Integrations with Functional ID provider:** ☑ Integrate with Student registry ☑ Integrate with xx registry **Login options:** ☐ Knowledge based auth ☐ OTP auth ☐ Biometric auth

Additional Information: Engagement Model for Public Cloud-Hosted Solution Offering

#	Topic	Details
1	Primary Cloud Account Ownership	The country will own the primary cloud account.
2	Existing Cloud Account Usage	If the country already has an existing cloud account, the same master account will be used to create sub-accounts.
3	Sub-Accounts Setup	Sub-accounts will be set up with the assistance of the Service Provider.
4	Ownership and Administrative Access	The Service Provider will ensure that nominated government team members receive ownership and administrative access to the sub-accounts
5	Geographical Territory Storage	The setup for geographical territory storage will mirror the existing account configuration.

8. REQUIREMENTS MATRIX

8.1 Functional (Technical/Program)

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
CI-01	Issuance platform must provide self-service issuer onboarding portal with configurable approval workflows (manual approval, automated verification, hybrid)	SP (ISV)	
CI-02	Issuer onboarding must collect and validate key details eg Legal entity name, registration number, authorized signatories, technical contact details, DID/signing key configuration, geographic jurisdiction	SP (ISV)	
CI-03	Role-based access control must support minimum roles: a. Super Admin (platform management), b. Issuer Admin (schema/template/user management), c. Credential Officer (credential issuance only) d. Auditor (read-only access to logs)	SP (ISV)	
CI-04	Issuer profile must auto-generate or allow upload of: DID document (eg did:web, did:key), X.509 certificates, or public keys with automatic trust registry registration	SP (ISV)	
CI-05	Issuance solutions must be offered in at least one of the offerings: a) SDK b) SaaS offering c) Hosted solution	SP (ISV)	
CI-06	Issuance solutions must provide options to configure the following: a) Language options b) Credential docs (pdf/svg) templates (logo, colour themes, etc.,) c) QR code content d) Machine readable schema formats (.json, .xml) across multiple VC standards e) Data schemas to support multiple credential types	SP (ISV)	
CI-07	Issuance solutions must provide capability to generate and store signing keys secure vaults. Additionally, corresponding verification keys must be made available for verification SDKs to verify credentials.	SP (ISV)	

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
CI-08	Issuance solutions must support issuance in signed qr (svg, etc), signed docs (.pdf, svg, etc) and machine readable format(s) (.json .xml, etc) using popular VC standards (e.g W3C-VC)	SP (ISV)	
CI-09	Issuance solutions must generate credentials in batch/on-demand through standard / popular APIs.	SP (ISV)	
CI-10	Issuance solutions must facilitate excel/csv file upload (of attested individuals' data) to generate credentials and return credential artefacts back to the issuer.	SP (ISV)	
CI-11	Issuance solutions must support issuance of credential in print format with signed QR e.g pdf, svg etc.,	SP (ISV)	
CI-12	Issuance solutions must support issuance of the credentials to user controlled credential store either on cloud (eLocker) or mobile (wallet)	SP (ISV)	
CI-13	Issuance solutions must allow issuers to revoke credentials	SP (ISV)	
CI-14	Issuance solutions may optionally allow workflow based credential mgmt for issuance/revocation	SP (ISV)	
CI-15	Issuance solutions must support UI/UX customization, including templates, logo, language and colours, based on issuer requirements	SP (ISV)	
CI-16	Issuance solutions must support delegated access to credentials. The system must allow a parent or legal guardian to receive, view, and present the credential on behalf of a minor, and linkage to the child must be validated using authoritative registry data	SP (ISV)	
CI-17	L1, L2 and L3 Support of credential issuance solution **IMPORTANT**: 1. SP team must be trained for L1 and L2 support and certified with the credential issuance solution owner. 2. SP may sign-up with an empaneled/trained/certified tech software vendor for L3 support by credential issuance solution owner (recommended). SP and L3 software vendors should have a back to back agreement. In absence of such an arrangement, SP must demonstrate L3 capabilities.	SP (ISV)	

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
CI-18	L3 Support of credential issuance solution in the language requested by the country team for 6 additional months post-rollout, (totaling 12 months).	SP (ISV)	
C1-19	Batch issuance performance: minimum 10,000 credentials/hour with <2 second latency per credential for on-demand issuance	SP (ISV)	
CI-20	Go-live by integrating all the above issuance capabilities with all the identified issuers and respective issuer systems.	SP (ISV)	
CV-01	Verification solution must support offering credential verification in below channels: a. SDKs / Libraries / Utilities (mandatory) b. APIs c. Web portals / Mobile apps	SP (ISV)	
CV-02	Verification must validate: a. Cryptographic signature using issuer's public key from trust registry, b. JSON-LD proof chains for W3C VCs, c. Certificate path validation for X.509-based credentials d. Revocation status via CRL/OCSP/StatusList2021, e. Credential expiry timestamps, f. Schema compliance validation	SP (ISV)	
CV-03	Verification solution must support online/offline validations. All interfaces and documentation must be delivered in {select local language as default). Bilingual (xx/EN) support is desirable for interoperability with international verifiers.	SP (ISV)	
CV-04	Verification solution must support in-person/remote acceptance of credentials	SP (ISV)	
CV-05	Verification solution must support self/assisted use cases	SP (ISV)	
CV-06	Verification solution optionally allow ZKP based selective disclosure based credential acceptance	SP (ISV)	
CV-07	Implementing credential verification flows: ● SDK integration in accepting entity mobile app ● Web app hosted by accepting entity (and/or issuer)	SP	
CV-08	Notification infrastructure through multiple channels - Mobile, Email, App based etc., to notify individuals during	SP	

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
	issuance, storing and verification as defined by respective module admins.		
CV-09	L1, L2 and L3 support of credential verification solution in the language requested by the country team. **IMPORTANT**: 1. SP team must be trained for L1 and L2 support and certified with the credential issuance solution owner. 2. SP may sign-up with an empaneled/trained/certified tech software vendor for L3 support by credential issuance solution owner (recommended). SP and L3 software vendors should have a back to back agreement. In absence of such an arrangement, SP must demonstrate L3 capabilities.	SP (ISV)	
CV-10	L3 support must extend 6 months beyond project completion, totaling 12 months, to guarantee post-transition technical continuity and maintain solution integrity.		
CS-01	Credential store solution must allow below options with seamless integration with issuance and verification solutions across: a. Digital - Personal Computer Local store b. Digital - Cloud Store c. Digital - eLockers Svc d. Mobile - Wallet	SP (ISV)	
CS-02	Credential store solutions must support import of credentials to user controlled stores either on cloud (eLocker) or mobile (wallet) and with one or more authentication modalities. E.g. a. Knowledge based auth b. OTP auth c. Biometric auth d. Face auth	SP (ISV)	
CS-03	Credential store solutions must support holding of various types of credentials across issuers and in multiple standards.	SP (ISV)	
CS-04	Credential store solutions must support delegated storing of credentials. The system must allow a parent or legal guardian to view and present the credential on behalf of a minor, and linkage to the child must be validated using authoritative registry data		

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
PR-101	Meet Technical, Programmatic and Strategic Rollout objectives. More Info Rollout (KRAs) Scope	SP	
PR-201	Go live on two use-cases[2] (end to end) as identified in section 6.1. More Info Program Deliverables (KRAs) Scope	SP	
PR-202	Onboarding of at least one additional end-to-end use case and identification of three additional issuer institutions. More Info Program Deliverables (KRAs) Scope	SP	
PR-203	Outreach Strategy documented in a playbook, including a roadmap of adoptions by issuers and acceptors beyond the six-month rollout. More info Program Deliverables	SP	
PR-204	Publication of a Whitepaper on the Impact of Credentialing as a DPI. More info Program Deliverables	SP	
PR-301	Technical deliverables. More Info Technical Deliverables	SP (ISV)	
PR-401	Meet the overall Delivery Schedule. More Info Schedule of Deliverables	SP (ISV)	
PR-901	DPG owners must support SP and ISVs to provide timely release of stable and critical updates to the open source code base and carry out vulnerability and resilience assessments, as well as end-to-end penetration tests on the deployed solutions, in accordance with the NIST cybersecurity framework.	DPG Owner	
PR-902	DPI owner must align required personnel identified during kick off meeting for successful execution of the roll out	DPI Owner (SP)	
PR-903	DPI owner must make sure required program, technical and operational personnel to take over the solution with a skill transfer as agreed during the kick of meeting	DPI Owner (SP)	
PR-904	DPI owner must lead to facilitate additional roll-out use cases and connect SP and ISVs to successfully implement the program	DPI Owner	

[2] End-to-end use cases includes one issuance model and one acceptance model for the said use-case

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
PR-905	DPI owner must lead to facilitate reliable and resilient hosting of data schema and trust registry of issuers and verifiers in well known place for ecosystem to leverage	DPI Owner (SP)	
PR-906	DPI owner must enable required policies (if any) to enable issuance, revocation, store and acceptance of credential solutions with-in the country.	DPI Owner (SP)	
PR-907	Issuers must provide attested data files and/or access to the data store to generate credentials.	Issuers (SP)	
PR-908	Accepting entities must provide support to integrate verification SDKs in web portals and mobile apps to allow credential acceptance.	Accepting Entity (SP)	

8.2 Non Functional (Technical)

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
NFR-01	The ISV/SP should do thorough integration testing, failover testing and fix any critical/major bugs to ensure the smooth running of the system during the rollout	SP (ISV)	
NFR-02	The ISV/SP should ensure the integrity of the data and the accuracy of credentials.	SP (ISV)	
NFR-03	The ISV/SP should adhere to data, information and systems security through industry best practices.	SP (ISV)	
NFR-04	The ISV/SP must provide cloud hosting and technical support for 12 months from the date of implementation kick off. This includes a 6-month post-rollout period to ensure seamless continuity, monitoring, and bug resolution, particularly for L3 support and cloud infrastructure stability.	SP (ISV)	
NFR-05	The ISV/SP should monitor the availability and security of the systems.	SP (ISV)	
NFR-06	The ISV/SP should ensure an uptime SLA of 99.9% for the system.	SP (ISV)	

Req ID	Requirements	Primary Owner (Supported By)	Remarks *(to be filled by the respondent to prove compliance against proposed solution)*
NFR-07	The ISV/SP should train the Country teams and make available the procedures, process documentation, and training materials in the language requested by the country.	SP	
NFR-08	The SP should document the implementation and other relevant integration as part of this rollout and make them available to the DPI Owner.	SP	
NFR-09	The SP must hand over all system components, including the full source code and associated technical documentation, upon the country's request.	SP (DPI owner)	
NFR-10	The SP should follow the best security practices in deploying and maintaining the systems. Wherever applicable, vulnerability assessment and penetration test reports on deployed end to end solutions to be made available adhering to relevant cybersecurity framework in the country.	SP	
NFR-11	The SP must perform iterative UX testing and usability improvements throughout the project lifecycle. This includes collecting user feedback, conducting tests with diverse user groups (e.g., low-literacy, rural, guardians), and implementing enhancements before the transition phase.	SP	
NFR-12	The SP must provide Infrastructure as Code (IaC) using Terraform scripts to enable deployment across multiple cloud providers (AWS, GCP, Azure, OCI) and on-premises infrastructure, ensuring cloud/on-prem agnostic implementation. All components must use cloud-agnostic APIs and services	SP	

9. ROLL-OUT SCOPE - Program & Technical Deliverables

The success of the country rollout will be defined both by programmatic and technical requirements.

9.1 Program Deliverables

The SP will be responsible for delivering the following programmatic deliverables:

Outcomes	KPIs & Deliverables	Key Activities
Programmatic objective N° 1: Ensure the Digital Credentials Stack (DCS) is fully operational and meets all rollout requirements		
-Full deployment of the DCS infrastructure [of x use cases] and live issuance by [name of DPI owner], including credential issuance, storage, and verification modules -Credential infrastructure supports multi-format display (wallet, PDF, printed QR) [if relevant adds: "allows delegated access for parents or legal guardians to manage minors' credentials, ensuring inclusive access and usability."]	**Deliverables** (see section 9.3)**:** -Credential Issuance; number of credentials issued: TBD -Credential Verification; number of credentials verified: TBD -Credential Store -Successful authentication and/or access at Accepting Parties' ends -Citizens can download a wallet app and retrieve their credentials (including those of dependents) in verifiable formats. -Key rollout metrics documented and analyzed.	-Engage with all stakeholders identified in Section 6 to ensure the timely achievement of the schedule outlined in Section 9.3. -Conduct pilot testing and quality assurance to ensure the system functions correctly for both use cases. -Provide training sessions to the DPI owner, to issuers and accepting entities on the use of the DCS for credential issuance and verification. -Execute the go-live, monitoring the system closely and providing immediate support post-launch.

Outcomes	KPIs & Deliverables	Key Activities
Programmatic objective N° 2: Support DPI owner in driving end-user adoption and engagement		
-Widespread adoption of the DCS, supported by a completed outreach strategy documented in a playbook, with a detailed roadmap for issuer and acceptor adoption beyond the six-month rollout.	-Outreach Strategy Playbook completed, launched, and disseminated by the DPI owner to relevant national stakeholders. -Key messages and outreach materials delivered in multiple accessible formats. -Number of users reached: TBD (based on discussions with the country; ideally at a significant proportion against the target population. Eg: 1% of adult population in x country)	-Design and implement an outreach strategy in collaboration with the implementation team, including audience segmentation, messaging strategy, and outreach channels. -Provide strategic direction, visual design, and creative content for campaign materials (e.g., guides, infographics, onboarding flows). -Support government communication teams in preparing campaign assets and adapting messages across formats. -Ensure outreach content is accessible (e.g., low-literacy, disability-inclusive). -Run awareness campaigns for potential issuance and acceptance entities. -Conduct workshops with potential issuance and acceptance entities using the sandbox to demonstrate the value of the credentialing DPI. -Create an outreach playbook documenting the strategy and approach for issuers and verifiers to reuse. ***Note:*** Outreach campaigns will be led and implemented by [DPI Owner]. The SP is not expected to cover costs related to events, media buying social media ads, or campaign deployment.

Outcomes	KPIs & Deliverables	Key Activities
Programmatic objective N° 3: Enable ecosystem expansion and government capacity		
[Name of DPI owner] successfully deploy and onboard additional one use case into the DCS infrastructure Institutional capacity built within [DPI owner and DPI owner supporter, if relevant] to manage issuer and verifier onboarding beyond the initial rollout.	One end-to-end new use case, i.e. a third use-case, fully implemented and anchored by [name of DPI owner]	-Support [name of DPI owner and DPI owner supporter, if relevant] in conducting ecosystem mapping to identify and prioritize high-impact issuers and verifiers. -Hold technical workshops, sandbox demonstrations, and bilateral sessions to explore potential use cases. -Co-develop onboarding materials, including credential schema templates, verification flows, and data mapping guides. -Publish an outreach and onboarding playbook with step-by-step guidance, messaging templates, and issuer enablement content. -Design and implement a **self-service onboarding pathway**, which could include • Intake form for issuer details • Credential schema builder tool • Credential preview generator (PDF/QR) • Access to sandbox and test credentials • Lightweight review and approval flow with [name of DPI owner] -Collect feedback from early issuers to refine materials and tooling. -Provide targeted training and coaching to [name of DPI owner and DPI owner supporter, if relevant] to institutionalize onboarding operations.

Outcomes	KPIs & Deliverables	Key Activities
Programmatic objective N° 4: Establish institutional sustainability and policy alignment		
[Name of DPI owner] and relevant government teams are fully trained and capable of independently operating and scaling the credentialing infrastructure. A clear roadmap is established for operational continuity, financial sustainability, and institutional governance beyond the pilot phase.	-[Name of DPI owner and DPI supporter, if relevant] team trained (L1–L3). -Standard Operating Procedures (SOPs) finalized and delivered. -System successfully handed over to [name of DPI owner]. -Operational and business plan developed, detailing functional workflows, cost recovery models, and recommendations for scaling (e.g., issuance models, pricing, support roles). -Alignment ensured with other funding mechanisms identified by the country, such as national budget allocations or loan operations with multilateral institutions. -National Policy on User-Centric Credentialing submitted to [name of DPI owner].	-Co-develop the operational and business plan in close coordination with [name of DPI owner], including scenario-based recommendations for cost recovery (e.g., per credential, annual budgets, potential public-private partnerships) and internal workflows and stakeholder roles required for scale. -Align sustainability plan with national budgets and/or multilateral loan operations (e.g., IDB, World Bank, if relevant) identified by the country. -Support the creation of a National Policy on User-Centric Credentialing (templates will be provided by CDPI). -Design and deliver tailored training sessions (L1–L3 support). -Finalize and transfer all SOPs. -Execute a structured transition plan.

9.2 Technical Deliverables

The success of the Country rollout will be defined by the following key criteria:

1. Deployment and Integration:
    a. Successful deployment of all the listed Components section of this scope document.
    b. Seamless integration of credentials verification modules in accepting entity applications/workflows listed in Components section of this scope document.
2. Functionality and Performance:
    a. Efficient upload and processing of individuals' attested data for credential generation/issuance.
    b. Accurate generation and delivery of credentials, ensuring individuals receive their printable credentials (.pdf) and machine readable formats (.json) via the channels listed in Components section.
    c. Reliable integration and operation across all components of the country's specific solution stack.
    d. Successful email notifications and OTP deliveries across all agreed workflows and interactions.
3. User Experience:
    a. User-friendly admin portal allowing Administrators at Issuer end to easily upload data, generate credentials, and send emails.
    b. Smooth individual login experience using registered email IDs and OTPs.
    c. Verified Administrator and Administrator Credentials marked accurately
    d. Customization with Issuer requirements for UI/UX, including language, theme, templates, logos, and colours.
    e. Hosting and accessibility of issuers' well-known configurations and schemas to enable trust infrastructure for issuance, acceptance and store ecosystem to leverage.
4. Credential Types and Storage:
    a. Support for specific credential types such as Degree Certificates from Administrator and Transcripts from Issuer and the third additional use-cases as required.
    b. Secure cloud storage (e.g., S3, Blob) for VC machine readable files.
5. L1, L2 and L3 Operational Support as stated in the requirements section
6. Stakeholder Satisfaction:
    a. Positive feedback from all stakeholders, including individuals, administrators, and employers.
    b. Effective support and communication between SP, ISVs, Issuers, Accepting Entities, DPI Owner and DPG Owner throughout the rollout phase.
    c. Effective handover to the country teams from the date requested by the country.
7. Continuous Improvement: Regularly update and enhance the platform based on user feedback and technological advancements. Document these approvals in a log book shared with the DaaS convenors post completion of the rollout.

8. Training and Transition Support: SP should provide ongoing training and support to ensure the smooth adoption and transition of the systems/services to all stakeholders identified by Issuer from the date requested.
9. Data Portability: SP should demonstrate the option to export the data from the pilot SaaS offering setup and import it to another Hosted instance of the latest version of the open source stack seamlessly. SP must provide documented export procedures, standardized data formats (JSON-LD, CSV), database migration scripts, and validation tools ensuring zero data loss during cross-platform migration.

9.3 Schedule of Deliverables and Payments

Phase	Description	Key deliverables		Payment Percent (of total amount)
		Programmatic	Technical	
A	Planning/Design (2 weeks) (wk1-2)	Completed deployment of the DCS infrastructure which supports multi-format display(wallet, PDF, printed QR), in [x use cases] and live issuance by [name of DPI owner], including credential issuance, storage, and verification modules	a) Finalise the tech integration & extension requirements b) Finalise the training requirements c) Finalise the outreach requirements	15%
B	DaaS Product Set-up & Pilot Program Go-Live	Outreach strategy playbook completed, publicly launched, and attended by key stakeholders	a) Completion of installation, integration, configuration and extensions b) Stakeholder demonstration (wk 6) - feedback and improvements c) Execution as per the published training and outreach plan including workshops, hackathons etc. d) Publish Project governance mechanism e) Launch of the roll-out by key stakeholders	30%
C	Execution	Successful deployment and onboarding of one end-to-end new use case, i.e. a third use-case,	a) Project execution as per the defined outreach plan and governance	35%

	(14 weeks) (wk11 - wk24)	fully implemented and anchored by [name of DPI owner]	b) Document and share project learnings document with the necessary stakeholders	
D	Transition & closure (Wk11 - Wk24)	-Standard Operating Procedures (SOPs) finalized and delivered. -System successfully handed over to [name of DPI owner]. -Operational and business plan developed, detailing functional workflows, cost recovery models, and recommendations for scaling . -Alignment ensured with other funding mechanisms identified by the country, such as national budget allocations or loan operations with multilateral institutions. -National Policy on User-Centric Credentialing submitted to [name of DPI owner]	a) Submit project closure report b) Prepare & execute transition plans	10%
E	Up till Wk24		Bonus completion	TBD
F	Up till Wk 48	-Completed training to [Name of DPI owner and DPI supporter, if relevant] team trained (L1–L3).	L3 support as part of a post-rollout support service Cloud hosting and support	10%

9.4 Change Request

Please note that change requests to cater for additional requirements other than those captured in this document are not permitted in the DaaS rollout program unless all the key stakeholders - Issuer, DPG Owner and the funder - sign off on the change request in consultation with impacted parties - DPI Owner, SP, DPG and ISV as applicable.

9.5 Assumptions

1. DPI Owner and Issuer will provide individuals with attested data who are entitled to receive Verifiable Credentials.

2. All the components of selected credentialing stack can be white labelled based on decisions by all the stakeholders - i.e DPI Owner, Issuer, etc.

10. PROJECT GOVERNANCE

Reporting framework to provide timely updates about the health of the project to all stakeholders. For example, Funders, DaaS Convenors, Country leadership may want a high level summary whereas DPG owners may want more granular reporting (around quality of software, documentation etc)

- Operational cadence - daily
- Internal steering committee reviews - country department stakeholders - once every 4 weeks
- Operation + program progress review (funders, DPG owners/Delegates, co-convenors of DaaS) - once every 6-8 weeks (duration is agreed among key actors)

APPENDIX - 1. Verifiable Credential and its Solution Approach to Credentialing

Credentialing both attributes and transactions is the necessary foundation for building digital, equitable economies

The digital public infrastructure (DPI) approach - which uses a combination of innovative technology, robust policy frameworks and incentives for community participation - offers an opportunity to convert paper-based or digital documents into verifiable credentials (VCs) for low-cost high-trust personal data sharing.

Credentialing refers to the process of digitally signing documents to make them portable, machine-readable and tamper-proof. Verifiable credentials are secure, cryptographically signed digital records issued by trusted entities (e.g., governments, universities, hospitals, employers) attesting to qualifications, attributes or transactions of individuals or entities.

Credentialing infrastructure has grown and recognized as one minimalist layer that can be rapidly, independently deployed by countries who want to build a foundational personal data sharing system that is low-cost, high-trust, and user-centric. Notable global examples include DiiA (Ukraine), MiArgentina (Argentina), SingPass (Singapore), DigiLocker (India) and many more.

VCs are a decentralised digital public infrastructure building block that can be built and reused across any sector. Popular records which have been credentialised include:

a. **Identity**: foundational id and functional id (tax, driver's licence, VISA, farmer id, medical id)
b. **Assets**: land records, jewellery records, car registration, fixed deposit slips
c. **Affiliations**: to a club, organisation, institution and relationships between teacher-student, employer-employee,
d. **Transactions**: money (receipt of salary, insurance premium payments, tax records), movement (mobility receipts of goods, individual travel logs)

Credentialing identity and assets is the first, foundational step required to unlock low-cost, high-trust records across sectors. The next layer involves the credentialing of affiliations and transactions. For example:

a. A green energy provider should be able to **prove his identity** and the **identity of his business** as being climate-positive to engage on a green energy platform.
b. He should also be able to **prove his relationship** with energy providers to build faith in his capability to meet the demand received through the platform.
c. Once he begins to engage on the platform, he should be able to **prove his transactions** to the government in order to receive tax subsidies or other similar benefits.

VCs represent a paradigm shift in the approach to sharing records and can have ripple effects across society:

1. Empower individuals: Unlike traditional stores of data which are owned by the entity which has collected it, VCs are owned by individuals themselves, thus giving them control to share their data in a manner that benefits their own interests. Moreover, due to their digital signatures, the VCs act as 'originals' and prevent the loss of physical documents.

2. Builds efficiency in processes: VCs streamline the process of verification to eliminate duplicate paperwork and mundane processes. This increase in efficiency can help reduce the costs of the services provided and thus make it viable for them to access diverse segments of the population that had previously been excluded due to the high trust and cost barriers.

Therefore leading to:

3. Inclusion and equitable growth: VCs provide optionality through multi-modal access. They can be carried through paper-based documents, PDFs or e-wallets depending on the preference of the individual. Regardless of the mode of display, the VCs can be verified with high trust and little to no cost, thus expanding the opportunities for equitable socio-economic development in countries.

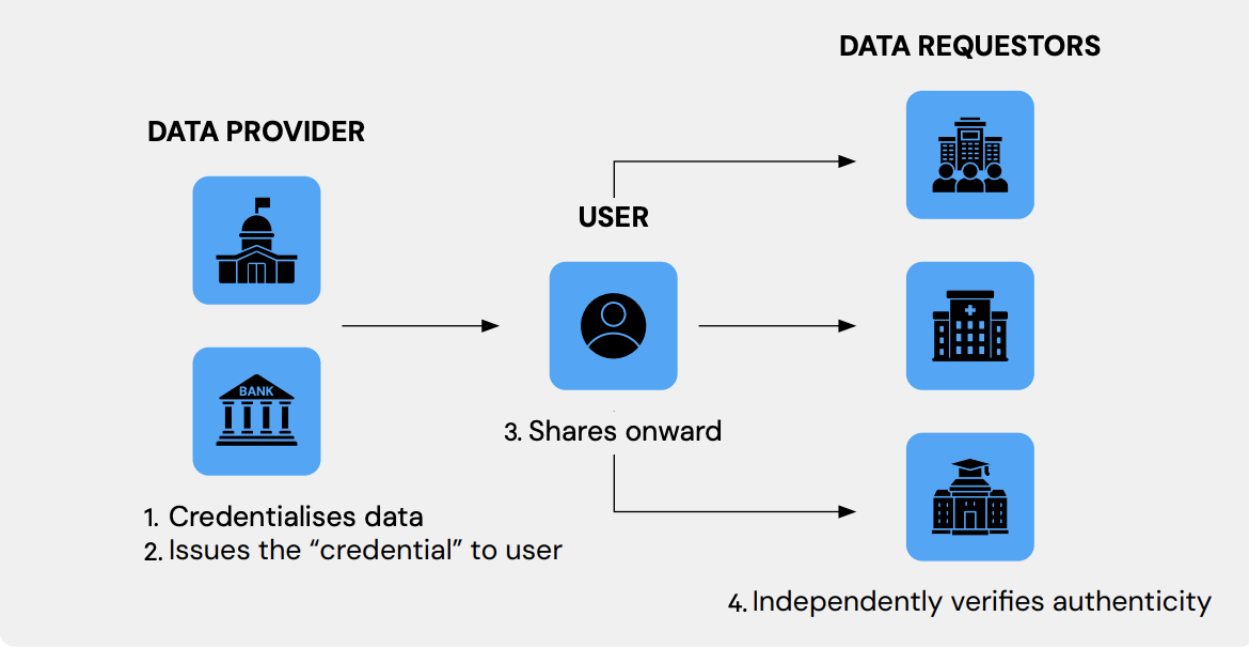
Use Case Possibilities

1. **Climate** - Issuing carbon credits as verifiable credentials for energy market trading, eligibility to subsidies etc.
2. **Education** - students having their education certificates / admission letters as verifiable credentials and sharing the same to prospective employers/loans/scholarships
3. **Healthcare** - Citizens holding their vaccination details as verifiable credential for eligibility for entering public spaces / Healthcare professionals with VCs of their professional licensing can present it enabling them to practise anywhere
4. **Govt/Business Entities** - Pay slips, work experience, technical courses, etc as credentials
5. **Banking** - Detailed bank statements, selective, summarised or aggregated statements like income / credit transactions, loan repayments transactions, average weekly/monthly balances, etc. as credentials
6. **Govt Services** - Passports as verifiable credentials to assist people in their easy commute in airport / Citizens having their civic certificates (Marriage licences, Voter ID, Social Security Information /Passport/Driving License) as verifiable credentials to be presented as required
7. **Business Owners** - holding Trade License / Bank records / Tax certificates as a verifiable credential for access to credit

Solution Approach to Credentialing DPI

This section provides design & solutioning guidelines for DPG / ISV product and Service Providers to enable credentialing capabilities across govt/private sectors at a country scale for asynchronous adoption. The solution is divided into four broad modules - issuance, store, acceptance and supporting trust infrastructure.

The following are the key design guidelines to follow for DaaS program offering. **Please note, these are not exhaustive lists but minimal criteria required to trigger an asynchronous adoption cycle.**



Open loop VC issuance platforms

1. Compliance to global VC standards and open schema specs
2. Support multiple delivery formats - e.g signed QRs, signed documents (pdf), machine readable (json, xml), etc.,
3. Generate credentials both at individual record and in bulk
4. Open loop issuance without forcing wallet and acceptance. Allow for asynchronous adoption with multiple options
5. Open pricing and choice to issuer's to sign up with an ecosystem of issuance providers to generate credentials as simple as "attested data file upload and credential download" through SaaS offering without any data getting stored in the SaaS instance

There are three models for DPGs/SPs/ISVs can consider offering VC issuance capability:

1. **SDK Offering** - Provide SDK/Libraries for issuers to generate credentials within the issuer's application/workflow context.
2. **SaaS Offering** - ISV hosted and operated SaaS offering on hyper scalers. Issuers to subscribe to credential generation services using File and API interfaces.

3. **Hosted Offering** - Issuers host the ISV product offering on the customer controlled public/private cloud or on-prem infra with the help of SPs and/or Issuer's engineering/operational personnel.

Inclusive approach to credential stores

1. Compliance to global VC standards to store and share
2. Issuance of credentials to subject/holder in multiple formats. E.g signed QRs, signed documents (pdf), machine readable (json, xml), etc.,
3. Choice to credential holder to receive credentials through multiple channels. E.g in-person, web portal, mobile app, wallet
4. Choice to credential holder to store the credentials in physical / digital worlds. E.g print outs, personal computers, mobile devices, cloud storage, wallets, etc.,
5. Compliant to open standards to authenticate (knowledge based, otp, biometric, etc.,) credential subjects/holders to fetch and store credentials in user controlled eLocker/wallet.

Verifications SDK

1. Compliance to global verifiable presentation (VP) standards to accept including Zero Knowledge Proofs (ZKPs)
2. Choice to credential holder to present credentials in multiple formats and channels
3. Verification module should do the following checks:
    a. Document integrity checks (not tampered)
    b. Issuer identity check (valid or recognized issuer as per VC accepting entity)
    c. Credential subject/holder identity check (Optional and as per transaction risk determined by VC accepting entity)
4. Verification SDK should support both offline & online acceptance
5. Enable easy integration with accepting entity applications, workflows for easy adoption to preserve machine readability for further downstream processing e.g auto fill forms, prove various domain context attributes like issue/expiry dates, status etc.,

Supporting Trust Infrastructure

1. Support for schema registries, issuer directory/registries, digital signing, etc to loosely bind above issuance, store and verifications components that can evolve independently and scale asynchronously.
2. Support for governance frameworks, guidelines and standards at a community, sector, regional and national level to enable inter and intra operable network

APPENDIX - 2. Qualification & Evaluation Criteria

Appendix 2.1 Qualification criteria

Category	Ref No	Criteria	Requirements	Compliance (Y/N)	Evidence to be submitted
Qualification	Q1	Registered company	1. Certificate of registration or incorporation 2. Valid proof of established office for last 3 years		Certified by Authorised Signatory 1. Copy of certificate of Incorporation / Registration
Qualification	Q2	Financial Stability	1. Should have had a positive net worth in the last 3 financial years (i.e, - FY 2022-23, FY 2021-22, FY 2020-21)		CA certified copy to be provided
Qualification	Q3	Turnover	1. Audited balance sheet for 3 years 2. Turnover should be from IT services similar to the DaaS project		CA certified copy should be provided mentioning business from total IT Services.
Qualification	Q4	Qualified Manpower	1. To have a minimum number 50 of resources in the IT Services 2. Minimum no of 5 open source resources 3. Minimum no of 10 project management resources		Details of resources with their specialization/certification
Qualification	Q5	In country capability and experience <else provide plan for enabling>	1. Local resource capability and local language capability, if required for program management and roll out 2. Local resources with past experience / past successful experience of deployment		Proof of local resources or Plan to enable local capacity with details of local organisations and arrangements with them.

Qualification	Q6	Agreement with engineering partner organisation for VC solutions	1. provide the back to back agreement details with one of the engineering partner organisation for L2 and L3 support.		Copy of agreement to be provided
Qualification	Q7	Credentialing Solution understanding	1. Understanding scope of current work and architecture (as detailed in the functional requirements) 2. Demonstration of DPG stack deployment 3. Demonstration of the end-to-end credentialing workflow and its key components		Demo to be given
Qualification	Q8	Adherence to: DaaS participation terms DLA2.0_Services and Im... DLA2.0_Engagement A...	1. SP has signed on to the standard DaaS participation terms		Signed legal agreement (or email confirmation)
Qualification	Q9	Completion of training	1. DPG owner has certified that the SP has completed the DPG training		Email confirmation from DPG owner

Appendix 2.2. Evaluation Criteria

Category	Ref No	Criteria	Requirements	Marking	Evidence to be submitted
Functional requirements	F1	Compliance to Requirements	1. Solution Overview (7 marks) Detailed solution overview aligned to the solution guidelines Solution Approach to Credentialing DPI that aligns to use cases, actors, components, functional and non-functional requirements called out as per this scope document.	15	Submission of Detailed Scope Document as per template in the appendix 2

			2. Functional & Technical Requirements (8 marks) Responses to the functional (technical/program) and non-functional requirements called out in the Requirements Matrix.		
Functional requirements	F2	Stakeholder management	1. Ability to liaison with all stakeholders - Government, Social Sector, ISV's. - Stakeholder Management Plan, (5 marks) - Conflict resolution plan / Escalation plan (2 marks) - Stakeholder Communication Plan (2 marks) - Stakeholder Feedback and Satisfaction Reports (1 marks)	10	Engagement strategy and communication plan should be shared as per section 8.3 and section 9 in the scope document.
Functional requirements	F3	Program management at large scale (Conceptualization to Roll out)	1. Develop a comprehensive plan aligning with goals. (15 marks) - Efficient allocation and utilization of resources. - Identify, assess, and manage risks effectively. - Performance Monitoring and Reporting 2. Plan for Quality Assurance (5 marks) 3. Detailed walkthrough and clarity and delivery of the content (5 Marks)	25	Project plan and schedules of large projects that have been executed with a detailed walk through on the thinking.
Tech Requirements	T1	Large scale projects build, implement and deploy capabilities	1. The project(s) of minimum value USD 200,000. Per annum would be considered. (1 Marks for each project, with a maximum 10 marks)	10	Detail of the project with proof of involvement.

Tech Requirements	T2	Experience in cloud based implementations	1. Experience in deploying cloud-based solutions (preferably with leading cloud providers like AWS, GC, OCI or Azure or Openstack) Self-Declaration by bidder and Demo to be given at the time of presentation 2. Should have experience of setting-up cloud solutions for the last three years at a larger scale. The project(s) of minimum value USD 200,000. Per annum would be considered. (1 Marks for each project, with a maximum 5 marks)"	5	Detail of the project with proof of involvement. or Copy of Work Order & completion
Tech Requirements	T3	Open Source software capability	1. Active contribution to open-source projects - Contributed to more than 3 well-known projects (5 marks)	5	Any of the below: 1. Documentation of contributions to open-source projects (code commits, bug fixes, features added). OR 2. Any major open-source projects the company has developed or maintains. provide links to repositories or examples of contributions
IT Project Management capability	T4	IT Project Management capability	1 Approach and methodology, Detailed presentation on how you will - Deploy - Migrate - Project plan and timelines - Risk mitigation - Optimization strategy	10	Presentation and Demo

			2. Operations and Maintenance Plan		
IT Project Management capability	IT1	Financial Proposal	1. Cost of resources against roles (10 Marks) 2. Most optimal way executing this project with roles defined for the DaaS project (10 Marks)	20	Details of roles and plan for how the role will work on the project as per the Appendix 2 financial proposal (section 3 & 4 in appendix 2)

APPENDIX - 3. Technical Proposal Response - Template

1. **Solution Overview**

   Detailed solution overview aligned to Solution Approach to Credentialing DPI guideline that aligns to use cases, actors, components, functional and non-functional requirements called out as per this scope document.

2. **Compliance to Requirements**

   Responses to the functional (technical/program) and non-functional requirements called out in the Requirements Matrix.

3. **Financial Proposal**

   We recommend you to use this reference pricing template for populating your financials. Financials should factor the cloud cost of hosting the solution for the duration of the contract.

   In addition to the details, please also include a summary of the financials. The proposal must be inclusive of taxes.

4. **Team Composition Proposal (Technical/Program)**

   Resource details including name, email/phone, training/experience, etc., aligned to the role.



Centre for Digital
Public Infrastructure

www.cdpi.dev