

Verifiable Credentialing Infrastructure

User-Centric Architecture for Universal Credential & Data Sharing
Call for Action by ISVs

version 1.0
dated: 02-Sep-2024

Table of Contents

1. Introduction	3
2. Glossary	4
3. Intended Audience & Purpose	4
4. Potential Path Forward	5
4.1. Use Case Possibilities	6
5. Solution Approach to Credentialing DPI	6
5.1. Open loop VC issuance platforms	7
5.2. Inclusive approach to credential stores	8
5.3. Verifications SDK	8
5.4. Supporting Trust Infrastructure	9
6. Reference Country Context	9
6.1. Use Cases	9
6.2. Components	12
7. Reference Requirements Matrix	13
7.1. Functional (Technical/Program)	13
7.2. Non Functional (Technical)	16
Appendix - 1	17
Request for Quotation (RFQ)	17
1. Solution Overview	17
2. RFQ Form	17

1. Introduction

Credentials offer a mechanism for low-cost, high-trust, user-centric data sharing

Licences, documents, registries and certifications form the foundation of most human interactions in society; right from a birth registration certificate to vaccination records to school marksheets and driver's licences - every milestone is represented in the form of a record, and is usually paper-based.

However, not all records carry the same value or are able to unlock the same opportunities.

Records that are **paper-based** (while they are **powerful for inclusion**, particularly in developing economies) typically have **high-cost of creation** and **low-trust during acceptance**. The costs involve not just the costs of paper itself, but also of **time** (how much money is a daily wage worker losing by choosing to stand in a queue in order to receive a document by missing work?), **effort** (how many individuals are employed to manually issue documents at multiple locations), **and opportunity** (how many individuals are losing access to services because their documents cannot be verified). The low-trust during acceptance of documents stems from the **ease of fraud and fake** records - capabilities exponentially enhanced with the advent of artificial intelligence.

While converting paper-based documents into **digital records** has **eased the burden of cost**, the **concerns around trust remain**, and the capability of **inclusive access has been lost** due to the digital divide in societies.

Lack of trust often acts as **the bottleneck** for **equitably receiving services** in society. Think of the process of receiving a loan - simply sharing bank account statements is not enough to build trust with a lender. The lender also conducts an independent assessment process to ensure the legitimacy of the documents before being able to trust them, and provide a loan against them. There is a significant cost associated with this process of assessment. Therefore, lenders prefer undertaking this effort only when the value of the loan is large, and the borrower is capable of absorbing that cost into his interest rate value. This cost prohibits the lender from catering to large segments of the population seeking small and micro credit that may be lesser than the cost of verification itself. When individuals and MSMEs are denied access to formal credit, it has significant implications for the growth and formalisation of economies.

To complement digitisation efforts which lower the cost of obtaining records in society, a methodology is required which can **infuse trust into all the digital records** built.

While one approach slowly gaining traction is **system-to-system real time data sharing** through open application programming interfaces (APIs) - due to its **high cost and high capacity** needs of installation and operation, it can be exclusionary to small or local entities (such as hospitals, schools, any government departments with low technical capacity), as well as, not necessarily required for all use-cases where data remains constant (like birth certificates or vaccination records) and is not changing in real time, particularly in developing economies.

To complement, or even as a precursor to this whole-of-government data sharing approach, one minimalist layer that can be rapidly, independently deployed by countries is a credentialing infrastructure.

 *Regardless of the mode of data-sharing, the data must be credentialised*

All records - of attributes, qualifications, and transactions - must be credentialled. It is the only way to ensure tamper-proof, portable and machine-readable records that can be reused across sectors.

Once the data is credentialised, the choice of sharing that data - through system-to-system infrastructure or user-centric infrastructure - can be made depending on the use-case, requirements and capabilities of that sector for that type of data.

2. Glossary

i.	DCS	Digital Credentials Stack
ii.	DaaS	DPI as a packaged Solution
iii.	DPG	Digital Public Good
iv.	DPI	Digital Public Infrastructure
v.	ISV	Independent Software Vendor
vi.	L1 Support	Level 1 support; setup, configuration, basic troubleshooting
vii.	L2 Support	Level 2 support; minor bug fixes to code, test, build and deploy
viii.	L3 Support	Level 3 support; new feature development, test, build and deploy
ix.	SaaS	Software as a Service
x.	SDK	Software Development Kit
xi.	VC	Verifiable Credential
xii.	VP	Verifiable Presentation

3. Intended Audience & Purpose

The intended audience of this document are

1. DPG: Contribute and review the scope; respond to ISV/SP queries
2. DPI Owner: Contribute and review the scope; respond to ISV/SP queries
3. Issuers: Contribute and review the scope; respond to ISV/SP queries
4. Accepting Entities: Contribute and review the scope; respond to ISV/SP queries
5. ISV: Respond to RFQ, meet ISV responsibilities of this scope doc


The purpose of this document is to provide required context for interested ISVs to participate in the larger credential market that is evolving across the globe.

1. Section 4: [Potential Path Forward](#) : Importance of credentialing infrastructure and use case at a country scale for ISV to imagine the possibilities
2. Section 5: [Solution Approach to Credentialing](#) : DPI based solution approach to roll out for a country that ISV **must adhere** to when responding with a solution proposal
3. Section 6: [Country Context](#) : Country specific context calling out key use cases, actors, and key component assumptions made by a typical country for a credentialing DPI rollout
4. Section 7: [Requirements Matrix](#) : Typical Functional & Non Functional requirements against which ISV's product offering will be evaluated.
5. Appendix 1: [Appendix - 1](#) : Request for Quotation Form for ISVs to respond.

4. Potential Path Forward

Credentialing both attributes and transactions are 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., universities, hospitals, employers, governments) attesting to qualifications, attributes or transactions of individuals or entities.

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.

1.

4.1. Use Case Possibilities

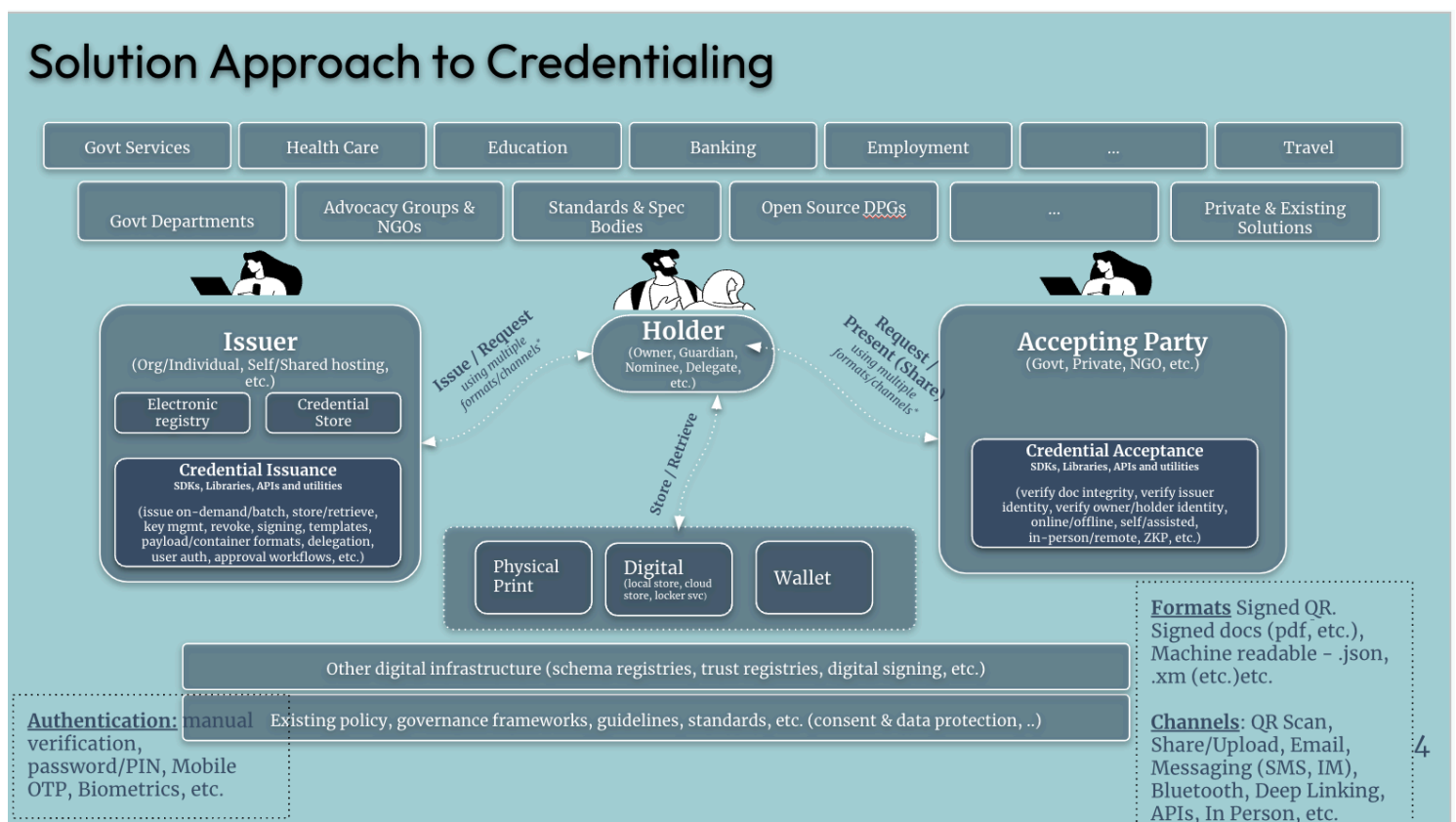
1. **Climate** - Issuing carbon credits as verifiable credentials for energy market trading, eligibility to subsidies etc.
2. **Education** - students having their education certificates / admission letters as verifiable credentials and sharing the same to prospective employers/loans/scholarships
3. **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

5. Solution Approach to Credentialing DPI

This section provides design & solutioning guidelines for DPG / ISV product 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 universal credentialing infrastructure offering. **Please note, these are not exhaustive lists but minimal criteria required to trigger an asynchronous adoption cycle.**



5.1. 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.

A detailed form for ISVs to respond for issuance/verification capabilities is available in [Appendix-1](#) of this scope document.

5.2. 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.

5.3. 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.,

A detailed form for ISVs to respond for issuance/verification capabilities is available in [Appendix-1](#) of this scope document.

5.4. 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 networks.

6. Reference Country Context

Below are a few reference use cases for ISVs to imagine the possibilities for building a user centric credential infrastructure that is highly decentralised, cater to multiple diverse use cases and can scale at the country population level.

6.1. Use Cases

Implementing a building block for the generation and verification of verifiable credentials is crucial for the government of Country X as it seeks to scale the provision of digital services across various sectors. This modular approach allows for the efficient deployment of services by

leveraging a single, reusable component, eliminating the need to reinvent the wheel for each new application.

Initially focused on education, with the University of Country X (UCX) as the first two use cases, this building block can be seamlessly extended to other areas such as healthcare, civil registries, licenses, and various official documents. By adopting this scalable solution, the government or private entity can ensure consistent, secure, and verifiable digital credentials across multiple domains, thereby enhancing the efficiency, accessibility, and trustworthiness of public services throughout the country.

Sample Use case 1 - Education - University Degree

Problem statement

UCX is the largest university in the country. There are 100,000 students enrolled and 25,000 people graduate every year. UCX issues all degrees on paper. As a result, graduates face complex, low-trust and time-consuming processes whenever document verification is required, whether for job applications, educational enrollments, or other official procedures.

For instance, when a job applicant is being considered for a position, a third-party agency typically verifies the authenticity of their degrees. This process often involves manually completing forms or making phone calls to the university, where a dedicated team checks the validity of the documentation. This manual approach not only delays the onboarding process between 2 and 4 weeks, but also increases the administrative burden on individuals, organizations, and institutions. In fact, UCX has a specific team dedicated to verifying this degrees. Moreover, it can compromise the integrity of the verification process, leading to inefficiencies and potential errors across various sectors.

Rollout Objectives

This use case seeks to eliminate delays, reduce administrative burdens, and enhance the overall integrity of the job market by introducing verifiable digital credentials for UCX graduates. These credentials, including education certificates and admission letters, can be securely shared with prospective employers or used for applications for loans, scholarships, and other opportunities, streamlining the verification process and supporting a more efficient, trustworthy system.

Objectives:

- Technical: Successfully implement and operationalize the Inji Digital Credentialing Stack across the selected pilot use case with the ability to rapidly scale the infrastructure to other use cases as well.
- For graduates: Provide easy access and control over their academic credentials, allowing seamless sharing with potential employers or academic institutions, through enabling at least:
 - These formats: signed QRs, signed documents (pdf), and machine readable (json, xml);
 - These channels: in-person, web portal, mobile app, and wallet;
 - These storing mechanisms: physical and digital.
- For Employers: Facilitate instant efficient verification processes to save time and money, and ensure the authenticity of UCX certificates.
- For UCX: Reduce administrative workload and operational costs by streamlining the issuance, storage & verification process of digital credentials, enhancing the institution's reputation by enabling at least all the issuance and verification modes and channels listed above.

Use case 2 - Education - Skill Certification

Problem statement

UpSkillForOpportunities is an initiative by the Ministry of Human Resources aimed at providing access to training and mentorship in digital technology. These courses are delivered in collaboration with various third-party organizations, including Coursera, the Linux Foundation, EdX, Udemy, Cisco, and Intel.

Despite the valuable partnerships, the current structure requires the ministry to issue the certificates of completion. As a result, existing verification mechanisms for credentials cannot be utilized, which diminishes the credibility and recognition of these skill certificates in the job market.

Rollout Objectives

This use case seeks to increase the value of the courses by introducing verifiable digital credentials for graduates. These skills credentials can be securely shared with prospective employers or used for applications for loans, scholarships, and other opportunities, streamlining the verification process and supporting a more efficient, trustworthy system.

Objectives:

- **Technical:** Successfully implement and operationalize the Digital Credentialing solution across the selected pilot use case with the ability to rapidly scale the infrastructure to other use cases as well.
- **For graduates:** Provide easy access and control over their skills credentials, allowing seamless sharing with potential employers or academic institutions, through enabling at least:
 - These formats: signed QRs, signed documents (pdf), and machine readable (json, xml);
 - These channels: in-person, web portal, mobile app, and wallet;
 - These storing mechanisms: physical and digital.
- **For Employers:** Facilitate instant efficient verification processes to save time and money, and ensure the authenticity of the certificates.
- **For Beneficiaries:** Enhance the value of courses by streamlining the issuance, storage & verification process of skills credentials, enhancing the institution's reputation by enabling at least all the issuance and verification modes and channels listed above.

6.2. Components

IMPORTANT:

1. All the components should adhere to general design guidelines stated in section [Solution Approach to Credentialing DPI](#)
2. ISV solution for issuance and verification should integrate with the Credential Store stack.
3. ISV should demonstrate seamless working across issuance, verification and store modules.

#	Component / Functionality	Product Information
1	Credential Issuance <ul style="list-style-type: none"> - Issuer issues to the subject - Subject request with issuer 	Issuance: <ul style="list-style-type: none"> - ISV SDK/SaaS Offering Standard: <ul style="list-style-type: none"> - W3C-VC Schema: <ul style="list-style-type: none"> - Custom json schema (as agreed with Issuer) Formats: <ul style="list-style-type: none"> - Signed .pdf doc with signed QR

		<ul style="list-style-type: none"> - .json file
2	Credential Verification	<p>Verification:</p> <ul style="list-style-type: none"> - ISV SDK offering <p>Integrations with accepting entity for verification:</p> <ul style="list-style-type: none"> - 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 <p>Credential formats:</p> <ul style="list-style-type: none"> - 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	<p>eLocker: Inji Web</p> <p>Channels:</p> <ul style="list-style-type: none"> - In person collection - Download from the portal using demo auth (what you know) and/or OTP based authentication. <p>Wallet: Inji Mobile (and any other open standard compliant wallets)</p> <p>Support for additional stores to hold credentials:</p> <ul style="list-style-type: none"> - Holder personal computer/mobile device - Cloud storage - Physical print

7. Reference Requirements Matrix

Below are typical functional and non-functional requirements that align with above [Solution Approach to Credentialing DPI](#) section. [Request for Quotation \(RFQ\)](#) responses from ISVs will be evaluated against these core requirements.

7.1. Functional (Technical/Program)

Req ID	Requirements	Owner	Remarks
CI-01	Issuance solutions must be offered in at least one of the offerings: a) SDK b) SaaS offering c) Hosted solution	ISV	
CI-02	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	ISV	
CI-03	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.	ISV	
CI-04	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)	ISV	
CI-05	Issuance solutions must generate credentials in batch/on-demand through standard / popular APIs.	ISV	
CI-06	Issuance solutions must facilitate excel/csv file upload (of attested individuals' data) to generate credentials and return credential artefacts back to the issuer.	ISV	
CI-07	Issuance solutions must support issuance of credential in print format with signed QR e.g pdf, svg etc.,	ISV	

Req ID	Requirements	Owner	Remarks
CI-08	Issuance solutions must support issuance of the credentials to user controlled credential store either on cloud (eLocker) or mobile (wallet)	ISV	
CI-09	Issuance solutions must allow issuers to revoke credentials	ISV	
CI-10	Issuance solutions may optionally allow workflow based credential mgmt for issuance/revocation	ISV	
CI-11	Issuance solutions must support UI/UI customization, including templates, logo, language and colours, based on issuer requirements	ISV	
CI-12	Go-live by integrating all the above issuance capabilities with all the identified issuers and respective issuer systems.	ISV	
CI-13	L1, L2 and L3 Support of credential issuance solution	ISV	
CV-01	Verification solution must support offering credential verification in below channels: <ul style="list-style-type: none"> a. SDKs / Libraries / Utilities (mandatory) b. APIs c. Web portals / Mobile apps 	ISV	
CV-02	Verification solution must do the following checks: <ul style="list-style-type: none"> a) Verify doc integrity b) Verify issuer validity c) Verify subject/holder identity (based on txn risk) 	ISV	
CV-03	Verification solution must support online/offline validations	ISV	
CV-04	Verification solution must support in-person/remote acceptance of credentials	ISV	
CV-05	Verification solution must support self/assisted use cases	ISV	
CV-06	Verification solution optionally allow ZKP based selective disclosure based credential acceptance	ISV	
CV-07	Implementing credential verification flows: <ul style="list-style-type: none"> • SDK integration in accepting entity mobile app 	ISV	

Req ID	Requirements	Owner	Remarks
	<ul style="list-style-type: none"> Web app hosted by accepting entity (and/or issuer) 		
CV-08	Notification infrastructure through multiple channels - Mobile, Email, App based etc., to notify individuals during issuance, storing and verification as defined by respective module admins.	ISV	
CV-09	L1, L2 and L3 Support of credential issuance solution	ISV	
CS-01	<p>Credential store solution must allow below options with seamless integration with issuance and verification solutions across:</p> <ol style="list-style-type: none"> Digital - Personal Computer Local store Digital - Cloud Store Digital - eLockers Svc Mobile - Wallet 	ISV	
CS-02	<p>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.</p> <ol style="list-style-type: none"> Knowledge based auth OTP auth Biometric auth 	ISV	
CS-03	Credential store solutions must support holding of various types of credentials across issuers and in multiple standards.	ISV	

7.2. Non Functional (Technical)

Req ID	Requirements	Owner	Remarks
NFR-01	The ISV should do thorough integration testing and fix any critical/major bugs to ensure the smooth running of the system during the rollout	ISV	
NFR-02	The ISV should ensure the integrity of the data and the accuracy of credentials.	ISV	
NFR-03	The ISV should provide support for 6 months of the rollout.	ISV	
NFR-04	The ISV should monitor the availability and security of the systems.	ISV	
NFR-05	The ISV should ensure an uptime SLA of 99.9% for the system.	ISV	

Appendix - 1

Request for Quotation (RFQ)

Independent Software Vendors (ISVs) who have a product offering for credentialing (issuance & verification) that integrates with Inji Web/Wallet shall respond to below RFQ. Alternatively, ISVs may also demonstrate/propose alternative open interoperable wallets that adhere to the above solution guidelines called out in [Solution Approach to Credentialing DPI](#) section.

1. Solution Overview

Issuance of VCs can be packaged as product offering by ISVs for rapid implementation by countries. Credentials issuance should be open loop i.e credential issued to a subject has a choice to store the credential anywhere of her preference and present in any channel relying (accepting) party would like.

There are three models ISVs should consider offering the issuance/verification 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.

2. RFQ Form

Instruction to fill the form:

1. If the capability is fully supported then ISVs should respond as Yes and provide brief info. Share additional information as links to product documentation pages to support the claim.
2. If the capability is not supported or partially supported, respond as No and provide additional information - partial capabilities available, future product plan.
3. If the capability is not applicable respond as NA.

4. For more information to fill the RFQ form, refer to the [Solution Approach to Credentialing](#) section of this document.
5. **IMPORTANT:** All information (including pricing) provided in this form **must** be available in the public domain. Please share the respective web page links. Only exception is for any special/subsidised pricing info that ISVs would like to share.

#	Description	Response* (Yes/No/NA and brief info with webpage links to publicly available information)	Additional Information
1	Product Overview	<link to product version and it's offerings>	
1.1	Credential schema configuration		
1.2	Supported credential standards		List all supported standards W3C VC, SD-JWT, mDL (1803-5)/mDOCs, ICAO MRTD, eMRTD, ISO/IEC 7501 MRP, country specific, etc.
1.3	Supported credential formats		e.g Signed QR, Signed Docs (pdf, etc), Machine Readable (json, xml, etc), etc.
1.3	Issuer signing/verification key mgmt		Capability to securely manage multiple keys to sign & verification key pairs
1.4	Credential revocation mgmt		
2	SDK/Library support		.
2.1	SDK/Library support for		

	issuance		
2.2	SDK/Library support for verification	a. Document integrity: b. Issuer validity: c. Subject/Holder identity: d. Support online/offline modes:	Capability for accepting party to easily integrate through multiple options - web flow, mobile app flow on holder or authorised agent device, etc.,
2.3	Languages supported with reference examples		
2.4	SLAs	e. Typical setup/configuration time: f. Typical response/throughput: g. L1 support turnaround: h. L2 support turnaround: i. L3 support turnaround:	
2.5	Licensing terms		
2.6	Pricing info		Skip if SDK/Library is available as part of SaaS or On-Prem models and price is included in these offerings.
2.7	Technical documentation for integration		
3	SaaS offering		
3.1	Supported hyper-scalers		List all supported cloud platforms
3.2	Supported Interfaces to issue credentials		File upload/download (CSV, Excel, etc), APIs, etc.,
3.3	Trial account info		

3.4	SLAs	a. Typical setup/configuration time: b. Typical response/throughput: c. Typical uptime: d. L1 support turnaround: e. L2 support turnaround: f. L3 support turnaround:	
3.5	Licence terms		
3.6	Pricing info		
3.7	Entry/Exit terms		Onboarding tools/support to import data, config, etc., Exist tools/support to export data, config, etc.,
3.8	Technical documentation for integration		
4	Hosted offering		
4.1	Supported orchestrating environments (cloud, container, virtual machine, etc.,)		
4.2	SLAs	a. Typical setup/configuration time: b. Typical response/throughput: c. L1 support turnaround: d. L2 support turnaround: e. L3 support turnaround:	
4.3	Licence terms		
4.4	Pricing info		
4.5	Technical documents for hosting, integration and maintenance		

5	Product Maturity/Support		
5.1	No of credentials issued by ISV		Share additional context/references, if any
5.2	List of trained Service Providers / ecosystem		List of SPs trained and can support
6	Company Overview		
6.1	Company established Mon/Year		
6.2	Employee count		
6.3	Company Registered HQ & Office Presence		